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
Outline of the new SVP / CVP algorithm

Time bound of SVP/CVP algorithm for low density lattices

Factoring integers via "easy" CVP solutions

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 \( \mathbf{B} = [\mathbf{b}_1, \ldots, \mathbf{b}_n] \in \mathbb{Z}^{m \times n} \)

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 \( \lambda_1(\mathcal{L}) = \min\{\|\mathbf{b}\| \mid \mathbf{b} \in \mathcal{L}\setminus\{0\}\} \)

**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 \( r_{i,i} > 0 \), \( (r_{i,i} = \|\mathbf{b}^*_i\|) \)
- \( \mathbf{Q} \in \mathbb{R}^{m \times n} \) 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. \( |r_{i,j}| \leq \frac{1}{2} r_{i,i} \) for all \( j > i \) (**size-reduced**) \( (r_{i,j}/r_{i,i} = \mu_{j,i}) \)
2. \( \delta r_{i,i}^2 \leq r_{i,i+1}^2 + r_{i+1,i+1}^2 \) for \( i = 1, \ldots, n - 1 \).
3. \( \alpha^{-i+1} \leq \|\mathbf{b}_i\|^2 \lambda_i^{-2} \leq \alpha^{n-1} \) for \( i = 1, \ldots, n \),
4. \( \|\mathbf{b}_1\|^2 \leq \alpha^{\frac{n-1}{2}} (\det \mathcal{L})^{2/n} \), where \( \alpha = 1/(\delta - \frac{1}{4}) \).
Let $\mathcal{L}_t = \mathcal{L}(b_1, \ldots, b_{t-1})$ and $\pi_t : \text{span}(\mathcal{L}) \to \text{span}(\mathcal{L}_t)^\perp$ for \( t = 1, \ldots, n \) denote the orthogonal projection.

**Stage \((u_t, \ldots, u_n)\) of ENUM.**

$b := \sum_{i=t}^n u_i b_i \in \mathcal{L}$ and $u_t, \ldots, u_n \in \mathbb{Z}$ are given. The stage searches exhaustively for all $\sum_{i=1}^{t-1} u_i b_i \in \mathcal{L}$ such that $\| \sum_{i=1}^n u_i b_i \|^2 \leq A$ holds for some $A \geq \lambda_1^2$. Obviously

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

goal: $\leq A$ to be minimized spent

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

Stage $(u_t, \ldots, u_n)$ exhausts $B_{t-1}(\zeta_t, \rho_t) \cap \mathcal{L}_t$ where $B_{t-1}(\zeta_t, \rho_t) \subset \text{span} \mathcal{L}_t$ is the sphere of dimension $t - 1$ with center $\zeta_t$ and radius $\rho_t := (A - \| \pi_t(b) \|^2)^{1/2}$. 
The success rate $\beta_t$ of stages

The \textsc{gaussian} volume heuristics estimates $|B_{t-1}(\zeta_t, \rho_t) \cap \mathcal{L}_t|$ to

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

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

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

We call $\beta_t$ the \textbf{success rate} of stage $(u_t, \ldots, u_n)$.

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

$$\mathcal{P}_t := \{\sum_{i=1}^{t-1} r_i b_i | 0 \leq r_1, \ldots, r_{t-1} < 1\}$$

then

$$\mathbb{E}_{\zeta_t}[|B_{t-1}(\zeta_t, \rho_t) \cap \mathcal{L}_t|] = \beta_t$$

for $\zeta_t \in \mathbb{R} \mathcal{P}_t$, because $1/\det \mathcal{L}_t$ is the number of points of $\mathcal{L}_t$ per volume.

The center $\zeta_t = b - \pi_t(b) \in \text{span } \mathcal{L}_t$ changes rapidly within \textsc{new enum}. It is natural to assume that $\zeta_t \in \text{span}(\mathcal{L}_t)$ distributes nearly randomly, and thus the estimate $|B_{t-1}(\zeta_t, \rho_t) \cap \mathcal{L}_t| \approx \text{vol } B_{t-1}(\zeta_t, \rho_t)/\det \mathcal{L}_t$ of the vol. heur. holds on the average.
**I: Outline of New Enum for SVP**

**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. $s := 1, \quad L := \emptyset$, (we call $s$ the level)

2. **Perform algorithm ENUM [SE94] pruned to stages with $\beta_t \geq n^{-s}$:**
   Upon entry of stage $(u_t, \ldots, u_n)$ compute $\beta_t$. If $\beta_t < n^{-s}$ delay this stage and store $(\beta_t, u_t, \ldots, u_n)$ in the list $L$ of delayed stages. Otherwise perform stage $(u_t, \ldots, u_n)$ 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 $A := \|b\|^2 - 1$. Recompute the stored $\beta_t$.

3. Perform and delete the stages $(u_t, \ldots, u_n)$ of $L$ with $\beta_t \geq n^{-s-1}$ in increasing order of $t$ and for fixed $t$ in order of decreasing $\beta_t$. Collect the called substages $(u_t', \ldots, u_t, \ldots, u_n)$ with $\beta_t' < n^{-s-1}$ in $L$. **IF** $L = \emptyset$ **THEN** *terminate by exhaustion*.

4. $s := s + 1, \quad$ GO TO 3
We efficiently approximate $\beta_t$ 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 $\|b\| = \lambda_1$ 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 $b$ has length $\lambda_1$. 
II: Time Bound for the 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 $\mathcal{L}'$ of $\dim \mathcal{L}' = n$ and $\det \mathcal{L} = \det \mathcal{L}'$.

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

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 $\|b_1\| \leq \sqrt{e\pi} n^b \lambda_1, b \geq 0$, 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 $B = QR = Q[r_{i,j}]$ satisfy (for $r_{i,i} = \|b_i^*\|$):
\[
r_{i,i}^2 / r_{i-1,i-1}^2 = q \text{ for } i = 2, \ldots, n \text{ and some } q > 0.
\]

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

The condition $\|b_1\| \leq \sqrt{e\pi} n^b \lambda_1$ can "easily" be met for CVP.
Finding an unproved shortest vector $b'$ is easier than proving $\|b'\| = \lambda_1$. We study the time to find an SVP-solution $b'$ without proving $\lambda_1 = \|b'\|$ under the assumption:

$$\text{SA} \quad \|\pi_t(b')\|^2 \approx \frac{n-t+1}{n} \lambda_1^2$$

holds for all $t$ and NEW ENUM’s SVP-solution $b'$, where $\pi_t(b') \in \text{span}(b_1, \ldots, b_{t-1})^\perp$.

**Proposition 1.** Let a lattice basis be given that satisfies GSA, $\|b_1\| \leq \sqrt{e\pi/2} n^b \lambda_1$ and $rd(\mathcal{L}) \leq n^{-1+2b}$. If NEW ENUM finds a shortest lattice vector $b'$ satisfying SA it finds $b'$, without proving $\|b'\| = \lambda_1$, 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 $\|b'\| = \lambda_1$ is under the vol. heuristics $\Theta(n^{1/2} rd(\mathcal{L}))^{n/4}$. 
**II: Polynomial CVP time under the vol. heuristics 10**

**Corollary 1.** Given \( t \in \mathbb{R}^n \) and \( B \) of \( \mathcal{L}(B) \) satisfying GSA, if \( \| b_1 \| = \lambda_1 \) and \( rd(\mathcal{L}) \leq n^{-1/2} \) then NEW ENUM solves the CVP \( \| t - b \| = \| t - \mathcal{L} \| \) under the volume heuristics in poly-time.

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

We adjust the assumption SA from SVP to CVP:

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

**Corollary 2.** Let \( B = [b_1, ..., b_n] \) in \( \mathbb{Z}^{m \times n} \) satisfy GSA, \( \| b_1 \| = O(\lambda_1) \) and let \( b \) satisfy CA for \( B, t \). If \( rd(\mathcal{L}) = o(n^{-1/4}) \) and \( \| t - \mathcal{L} \| = O(\lambda_1) \) then NEW ENUM finds the CVP-solution \( \tilde{b} \in \mathcal{L} \) under the volume heuristics in polynomial time, but without proving \( \| t - \tilde{b} \| = \| t - \mathcal{L} \| \).
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 $\mathcal{L}(B)$, 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 $N' = N p_{n+j}$ for one of the next $n$ primes $p_{n+j} > p_n$, $j \leq n$.

**Lemma 5.3** [ MG02] \quad $\chi_1^2 \geq 2c \ln N$.

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

$$u = \prod_{e_j > 0} p_j^{e_j}, \quad v = \prod_{e_j < 0} p_j^{-e_j} \in \mathbb{N}.$$  

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

We compute vectors $\mathbf{b} = \sum_{i=1}^{n} e_i \mathbf{b}_i \in \mathcal{L}(\mathbf{B})$ close to $\mathbf{N}$ such that $|u - v\mathbf{N}'| < p_n$. The prime factorizations $|u - v\mathbf{N}'| = \prod_{i=1}^{n} p_i^{e'_i}$ and $u = \prod_{e_j > 0} p_j^{e_j}$ yield for "suitable" $\alpha, c$ a non-trivial relation

$$\prod_{e_i > 0} p_i^{e_i} = \pm \prod_{i=1}^{n} p_i^{e'_i} \mod N. \quad (7.1)$$

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

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

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

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

**Theorem 4 [S93/91]** 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 \( M_{\alpha,c,N} \neq \emptyset \) 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 \( \|b_1\| = O(\lambda_1) \) and \( M_{\alpha,c,N} \neq \emptyset \) for \( c = (\ln N)^\beta \), \( \alpha > 2\beta + 2 \) we can minimize \( \|\mathcal{L}(B) - N\| \) 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
\[
\|\mathcal{L} - N\|^2 \leq (2c - 1) \ln N' + 1 = (2c - 1 + o(1)) \ln N.
\]
Lemma 5.3 of [MG02] proves that \( \lambda_1^2 \geq 2c \ln N - \Theta(1) \)
\[
[ \lambda_1^2 = 2c \ln N + O(1) \text{ holds if } 0 < \frac{\alpha}{\alpha - 2\beta - 2} < c \leq (\ln N)^\beta. \]

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

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

Hence \( rd(\mathcal{L}) = o(n^{-1/4}) \). \qed
III: Providing a nearly shortest vector for $\mathcal{L}(\mathbf{B})$

For solving $\|\mathbf{t} - \mathbf{b}\| = \|\mathbf{t} - \mathcal{L}\|$ 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 $\mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_{n+1})$.

**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 \textit{GSA} and 
\[ \| b_1 \| \leq \sqrt{e\pi} n^b \lambda_1, \; b \geq 0, \] 
\textit{NEW ENUM} solves \textit{SVP} in time 
\[ 2^{O(n)}(n^{1/2+b} rd(\mathcal{L}))^{n/4}. \]

\textit{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 \textit{NEW ENUM}.

Let \( \beta'_t \) be the success rate of stage \((u'_t, ..., u'_n)\). 
\textit{NEW ENUM} performs stage \((u'_t, ..., u'_n)\) prior to all stages 
\((u_t, ..., u_n)\) of success rate \( \beta_t \leq \frac{1}{n} \beta'_t \)

\textit{Simplifying assumption.} We assume that \textit{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 \( n \).
Consider the number $M_t$ of stages $(u_t, ..., u_n)$ with
\[ \| \pi_t(\sum_{i=t}^n u_i b_i) \| \leq \lambda_1: \quad M_t := \#(B_{n-t+1}(0, \lambda_1) \cap \pi_t(L)). \]
Modulo the heuristic simplifications $M_t$ covers the stages that precede $(u_t', ..., u_n')$ and those that finally prove $\| b' \| = \lambda_1$.

**Lemma 1**

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

**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 $r_{i,i}^2 = \| b_1 \|^2 q^{i-1}$, $\lambda_1^2/(\gamma_n rd(L)^2) = (\det L)^2 = \| b_1 \|^2 q^{\frac{n-1}{2}}$
hold by GSA and thus $\gamma_n \geq \frac{n}{2 e\pi}$ directly imply for $i = t, ..., n$

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

By Lemma 1

\[ M_t \leq \prod_{i=t}^n \frac{e^{\sqrt{\pi} rd(L)^{-1} \lambda_1 q^{(2i-n-1)/4} + \sqrt{8e\pi} \lambda_1}}{\sqrt{n-t+1} r_{i,i}} \] (4.0)
For the remainder of the proof let $t := \frac{n}{2} + 1 - c$ and 
$m(q, c) := \begin{cases} q^{\frac{1-c^2}{4}} & \text{if } c > 0 \\ 1 & \text{else} \end{cases}$. Then

$$M_t \leq m(q, c) \left( \frac{2+\sqrt{e}}{\sqrt{n-t+1}} \frac{\sqrt{2} e\pi \lambda_1}{\sqrt{2e\pi \lambda_1}} \right)^{n-t+1} / \det \pi_t(\mathcal{L}), \quad (4.1)$$

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 $\det \pi_t(\mathcal{L}) = \|b_1\|^n t + 1 q \sum_{i=t}^{n-1} i/2$ that

$$M_t \leq m(q, c) \left( \frac{2+\sqrt{e}}{\sqrt{n-t+1}} \frac{\sqrt{2e\pi \lambda_1}}{\sqrt{2e\pi \lambda_1}} \right)^{n-t+1} / q \sum_{i=t}^{n-1} i/2 \quad (4.2)$$

The [KL78] bound

$$\gamma_n \leq \frac{1.744 (n+o(n))}{2e\pi} \leq \frac{n}{e\pi} \quad \text{for } n \geq n_0$$

and

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

and

$$q^{\frac{n-1}{2}} = \lambda_1^2 / (\|b\|^2 \gamma_n \sqrt{\det(\mathcal{L})}^2)$$

show

$$M_t \leq m(q, c) \left( \frac{2+\sqrt{e}}{\sqrt{n-t+1}} \frac{\sqrt{2e\pi \lambda_1}}{\sqrt{2e\pi \lambda_1}} \right)^{n-t+1} \left( \frac{\sqrt{n} \det(\mathcal{L}) \|b_1\|}{\sqrt{e\pi \lambda_1}} \right)^{n-t+1}.$$
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 \( \text{de}\left(\frac{n}{2} + 1 - c\right) = \frac{n^2/4 - c^2}{n-1} \). Hence for \( \|b_1\| \leq \sqrt{e\pi \ n^b \ \lambda_1} \) and all \( t \leq n \):

\[
\mathcal{M}_t \leq m(q, c) \left( (\sqrt{8} + \sqrt{2e}) \sqrt{\frac{n}{n-t+1}} \right)^{n-t+1} \left( n^1 + b \text{rd}(\mathcal{L}) \right)^{\frac{n^2/4 - c^2}{n-1}}
\]

For \( c > 0 \), \( t \leq \frac{n}{2} \) we have

\[
m(q, c) = q^{1-c^2/4} = \left( \frac{\|b_1\| \sqrt{\gamma_n \text{rd}(\mathcal{L})}}{\lambda_1} \right)^{\frac{c^2-1}{n-1}} \leq \left( n^1 + b \text{rd}(\mathcal{L}) \right)^{\frac{c^2-1}{n-1}}, \text{ and}
\]

thus:

\[
\mathcal{M}_t \leq \left(4 + 2\sqrt{e}\right)^{n-t+1} \left( n^1 + b \text{rd}(\mathcal{L}) \right)^{\frac{n+1}{4}}, \text{ where } \frac{n^2/4 - 1}{n-1} \leq \frac{n+1}{4}.
\]

For \( c \leq 0 \), \( t > \frac{n}{2} \) we have

\[
\mathcal{M}_t \leq \left( (\sqrt{8} + \sqrt{2e}) \sqrt{\frac{n}{n-t+1}} \right)^{n-t+1} \left( n^1 + b \text{rd}(\mathcal{L}) \right)^{\frac{n^2/4}{n-1}}
\]

\[
= 2^{O(n)} \left( n^1 + b \text{rd}(\mathcal{L}) \right)^{\frac{n+2}{4}}, \text{ where } \frac{n^2/4}{n-1} \leq \frac{n+2}{4}.
\]

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

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

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

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

The center $\zeta = 0$ of the sphere is bad for the vol. heur.

It can nearly maximize $|B_n(\zeta, \rho) \cap \mathcal{L}|$.

NEW ENUM for SVP tries to keep the center $\zeta_t = b - \pi_t(b)$

$\in \text{span } \mathcal{L}_t$ close to $0 \in \mathbb{R}^{t-1}$. Can this in practice generate substantial errors of the volume heuristics?.

NEW ENUM for CVP keeps for center $\zeta_t = b - t - \pi_t(b - t)$

close to $\pi_t(t)$. For random $t$ 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 \( n \ln^{O(1)} n \).


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

**BL05**  

**Ca98**  

**CEP83**  

**CS93**  

**FP85**  
GN08  

HHHW09  

HPS98  

H07  
<table>
<thead>
<tr>
<th>Reference</th>
<th>Authors</th>
<th>Title</th>
<th>Conference/Source</th>
</tr>
</thead>
</table>


