

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

Communicated by [], a withdrawn JMC submission, revised 29. 10. 2009

Abstract. We propose and analyze novel algorithms for finding shortest and closest lattice vectors. The algorithm NEW ENUM performs the stages of exhaustive enumeration of short / close lattice vectors in order of decreasing success rate. We analyze this algorithm under GSA which in practice holds on the average for well reduced bases. A shortest lattice vector is found in polynomial time if the density of the lattice is not close to maximum. We prove under GSA a worst case time bound $n^{\frac{n}{32}+o(n)}$ for lattices of dimension n . This gives NEW ENUM enormous power in attacking lattice based cryptographic schemes, in particular the AJTAI-DWORK scheme uses lattices of low density. The RSA scheme may also be affected. We show under GSA and standard assumptions on the distribution of smooth integers that integers N can be factored by solving $(\ln N)^{4+\epsilon}$ CVP's for the prime number lattice. But so far these CVP's are not easy and useful for factoring at the same time.

Keywords. Shortest vector problem (SVP), closest vector problem (CVP), LLL-reduction, NTRU cryptosystem, Ajtai-Dwork cryptosystem, factoring integers, discrete logarithms.

AMS classification. 11H55, 11Y16, 11Y05, 11E10, 68Q17.

1 Introduction and surviiew

Previous SVP and CVP algorithms of KANNAN [Ka87] and FINCKE, POHST [FP85] perform the stages of exhaustive enumeration of short/close lattice vectors in a straight forward order disregarding the success rate of stages. The algorithm ENUM of [SE94, SH95] locally performs stages in order of decreasing success rate and often finds short vectors much faster. Our algorithm NEW ENUM for SVP / CVP, presented in section 3 / 6, performs all stages in order of decreasing success rate, stages with high success rate are done first. This greatly reduces the number of stages that precede the finding of a shortest / closest lattice vector.

Section 4 analyzes the new SVP algorithm assuming that all quotients $r_{i,i}/r_{i+1,i+1}$ of the lengths $r_{i,i} = \|\mathbf{b}_i^*\|$ of the orthogonalized lattice basis coincide. This geometric series assumption (GSA) of [S03] approximately holds in practice for well reduced bases. We show under GSA how to find a shortest lattice vector in polynomial time if the *relative density* $rd(\mathcal{L})$ of \mathcal{L} , defined in section 2, satisfies $rd(\mathcal{L}) = o(n^{-\frac{1}{2}})$ in a strong sense. Our worst case SVP time $n^{\frac{n}{32}+o(n)}$ for lattices of dimension n is much better than the time bound $n^{\frac{n}{2e}+o(n)}$ of KANNAN's SVP algorithm proved in [HS07]. We use from [HS07] proven bounds for the number of lattice points in spheres.

Section 5 studies the relative density $rd(\mathcal{L})$ of various cryptographic lattices. The NTRU-lattices of [HHHW09] satisfy $rd(\mathcal{L}) > n^{-1/2}$, withstanding the new SVP algo-

rithm, but $rd(\mathcal{L}) \leq n^{-3+3/n}$ holds for the lattices used by Ajtai, Dwork [AD97]. Under GSA AJTAI's worst case / average case equivalence of n^c -unique SVP and SVP [Aj96] merely covers easy instances of n^c -unique SVP's making this equivalence void.

Section 6 extends NEW ENUM and its analysis to CVP. Cor. 6.1 shows that the CVP for the target vector $\mathbf{t} \in \text{span}(\mathcal{L})$ is solvable in polynomial time if $rd(\mathcal{L}) = n^{-\frac{1}{2}-\varepsilon}$ with $\varepsilon > 0$ and $\|\mathcal{L} - \mathbf{t}\| = O(\lambda_1)$.

Section 7 shows how to factor integers N by generating relations modulo N between smooth integers from CVP solutions for the prime number lattice. These CVP's would be solvable in polynomial time under GSA and standard assumptions on the distribution of smooth integers if $rd(\mathcal{L}) < n^{-1/2}$ holds for the prime number lattice \mathcal{L} . Hence factoring integers would be polynomial time under GSA if we can use prime number lattices with $rd(\mathcal{L}) < n^{-1/2}$ for factoring. However this latter condition is open.

Section 8 shows how to compute the discrete logarithm for the group of units in \mathbb{Z}_N by solving CVP's for the prime number lattice.

2 Lattices

Let $B = [\mathbf{b}_1, \dots, \mathbf{b}_n] \in \mathbb{R}^{m \times n}$ be a basis matrix consisting of n linearly independent column vectors $\mathbf{b}_1, \dots, \mathbf{b}_n \in \mathbb{R}^m$. They generate the lattice $\mathcal{L}(B) = \{B\mathbf{x} \mid \mathbf{x} \in \mathbb{Z}^n\}$ consisting of all integer linear combinations of $\mathbf{b}_1, \dots, \mathbf{b}_n$, the *dimension* of \mathcal{L} is n . The *determinant* of \mathcal{L} is $\det \mathcal{L} = (\det B^t B)^{1/2}$ for any basis matrix B and the transpose B^t of matrix B . The *length* of $\mathbf{b} \in \mathbb{R}^m$ is $\|\mathbf{b}\| = (\mathbf{b}^t \mathbf{b})^{1/2}$.

Let $\lambda_1, \dots, \lambda_n$ denote the successive minima of \mathcal{L} , λ_i is the minimal real number such that there are i linearly independent lattice vectors of length at most λ_i , and $\lambda_1 = \lambda_1(\mathcal{L})$ is the length of the shortest non-zero vector of \mathcal{L} . The HERMITE constant γ_n is the maximum of $\lambda_1^2 / \det(\mathcal{L})^{2/n}$ over all lattices of dimension n .

Let $B = QR \in \mathbb{R}^{m \times n}$, $R = [r_{i,j}]_{1 \leq i,j \leq n} \in \mathbb{R}^{n \times n}$ be the unique QR -factorization: $Q \in \mathbb{R}^{m \times n}$ is isometric and $R \in \mathbb{R}^{n \times n}$ is upper-triangular with positive diagonal entries. While the QR -factorization is standard in algebra and numerical analysis the recent literature on lattice basis reduction uses the Gram-Schmidt coefficients $\mu_{j,i} = r_{i,j} / r_{i,i}$ which are rational for integer matrices B . The orthogonal projection \mathbf{b}_i^* of \mathbf{b}_i in $\text{span}(\mathbf{b}_1, \dots, \mathbf{b}_{i-1})^\perp$ has length $r_{i,i} = \|\mathbf{b}_i^*\|$.

LLL-bases. A basis $B = QR$ is *LLL-reduced* or an *LLL-basis* for $\delta \in (\frac{1}{4}, 1]$ if

1. $|r_{i,j}| / r_{i,i} \leq \frac{1}{2}$ for all $j > i$,
2. $\delta r_{i,i}^2 \leq r_{i,i+1}^2 + r_{i+1,i+1}^2$ for $i = 1, \dots, n-1$.

Obviously, LLL-bases satisfy $r_{i,i}^2 \leq \alpha r_{i+1,i+1}^2$ for $\alpha := 1/(\delta - \frac{1}{4})$. [LLL82] introduced LLL-bases focusing on $\delta = 3/4$ and $\alpha = 2$. A famous result of [LLL82] shows that LLL-bases for $\delta < 1$ can be computed in polynomial time and that they nicely approximate the successive minima :

3. $\alpha^{-i+1} \leq \|\mathbf{b}_i\|^2 \lambda_i^{-2} \leq \alpha^{n-1}$ for $i = 1, \dots, n$,
4. $\|\mathbf{b}_1\|^2 \leq \alpha^{\frac{n-1}{2}} (\det \mathcal{L})^{2/n}$.

A basis $B = QR \in \mathbb{R}^{m \times n}$ is an *HKZ-basis* (HERMITE, KORKINE, ZOLOTAREFF) if $|r_{i,j}| / r_{i,i} \leq \frac{1}{2}$ for all $j > i$, and if each diagonal entry $r_{i,i}$ of $R = [r_{i,j}] \in \mathbb{R}^{n \times n}$ is

minimal under all transforms of B to BT , $T \in \text{GL}_n(\mathbb{Z})$ that preserve $\mathbf{b}_1, \dots, \mathbf{b}_{i-1}$.

A famous problem is the shortest vector problem (SVP): Given of a basis of \mathcal{L} find a shortest non-zero vector of \mathcal{L} , i.e., a vector of length λ_1 .

Closest vector problem (CVP): Given a basis of \mathcal{L} and a target $\mathbf{t} \in \text{span}(\mathcal{L})$ find a closest vector $\mathbf{b}' \in \mathcal{L}$ such that $\|\mathbf{t} - \mathbf{b}'\| = \|\mathbf{t} - \mathcal{L}\| =_{\text{def}} \min\{\|\mathbf{t} - \mathbf{b}\| \mid \mathbf{b} \in \mathcal{L}\}$.

Previous SVP-algorithms solve SVP by a full exhaustive search, disregard the success rate of stages, and prove to have found a shortest non-zero lattice vector.

Our novel SVP-algorithm most likely finds a shortest lattice vector rather fast by performing the stages in order of decreasing success rate. The efficiency of our new SVP-algorithm depends on the lattice invariant $rd(\mathcal{L}) := \lambda_1 \gamma_n^{-1/2} (\det \mathcal{L})^{-1/n}$ which we call the *relative density* of \mathcal{L} . Note that $rd(\mathcal{L}) = \lambda_1(\mathcal{L}) / \max \lambda_1(\mathcal{L}')$ holds for the maximum of $\lambda_1(\mathcal{L}')$ over the lattices \mathcal{L}' such that $\dim \mathcal{L} = \dim \mathcal{L}'$ and $\det \mathcal{L} = \det \mathcal{L}'$.

Clearly $0 < rd(\mathcal{L}) \leq 1$ holds for all \mathcal{L} , and $rd(\mathcal{L}) = 1$ if and only if \mathcal{L} has maximal density. Lattices of maximal density and γ_n are known for $n = 1, \dots, 8$ and $n = 24$. The new SVP-algorithm runs in polynomial time under GSA if $rd(\mathcal{L}) = n^{-\frac{1}{2}-\varepsilon}$ for $\varepsilon > 0$ and if the first basis vector is nearly shortest.

3 A novel enumeration of short lattice vectors

We first describe the design principle and give an outline of the novel SVP-algorithm. The new algorithm improves the algorithm ENUM of [SE94, SH95]. For its formal description we recall ENUM and then present NEW ENUM as a modification that essentially performs all stages of ENUM in decreasing order of success rates.

Let $B = [\mathbf{b}_1, \dots, \mathbf{b}_n] = QR \in \mathbb{Z}^{m \times n}$, $R = [r_{i,j}]_{1 \leq i,j \leq n} \in \mathbb{R}^{n \times n}$ be the given basis of $\mathcal{L} = \mathcal{L}(B)$. Let $\pi_t : \text{span}(\mathbf{b}_1, \dots, \mathbf{b}_n) \rightarrow \text{span}(\mathbf{b}_1, \dots, \mathbf{b}_{t-1})^\perp$ for $t = 1, \dots, n$ denote the orthogonal projections and let $\mathcal{L}_t = \mathcal{L}(\mathbf{b}_1, \dots, \mathbf{b}_{t-1})$.

The success rate of stages. At stage (u_t, \dots, u_n) of ENUM [SH95], $\mathbf{b} := \sum_{i=t}^n u_i \mathbf{b}_i \in \mathcal{L}$ and $u_t, \dots, u_n \in \mathbb{Z}$ 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 $\zeta_t := \mathbf{b} - \pi_t(\mathbf{b}) = Q\mathbf{v}_t \in \text{span} \mathcal{L}_t$ is the orthogonal projection in $\text{span} \mathcal{L}_t$ of the given $\mathbf{b} = \sum_{i=t}^n u_i \mathbf{b}_i$ and $\mathbf{v}_t = (v_1, \dots, v_{t-1}, 0^{n-t+1})^t$ for $v_i = \sum_{j=t}^n r_{i,j} u_j$. Stage (u_t, \dots, 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 $\mathcal{B}_{t-1}(\zeta_t, \rho_t) \subset \text{span} \mathcal{L}_t$ of dimension $t-1$ with radius $\rho_t := (A - \|\pi_t(\mathbf{b})\|^2)^{1/2}$ and center ζ_t .

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

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

Here $\text{vol} \mathcal{B}_{t-1}(\zeta_t, \rho_t) = V_{t-1} \rho_t^{t-1}$, $V_{t-1} = \pi^{\frac{t-1}{2}} / (\frac{t-1}{2})! \approx (\frac{2e\pi}{t-1})^{\frac{t-1}{2}} / \sqrt{\pi(t-1)}$ is

the volume of the unit sphere of dimension $t - 1$, and $\det \mathcal{L}_t = r_{1,1} \cdots r_{t-1,t-1}$. If $\zeta_t \bmod \mathcal{L}_t$ is uniformly distributed over $\{\sum_{i=1}^{t-1} r_i \mathbf{b}_i \mid 0 \leq r_1, \dots, r_{t-1} < 1\}$ the expected size of this intersection satisfies $\mathbb{E}_{\zeta_t} [|\mathcal{B}_{t-1}(\zeta_t, \rho_t) \cap \mathcal{L}_t|] = \beta_t$, where \mathbb{E}_{ζ_t} refers to a random $\zeta_t \bmod \mathcal{L}_t$. This holds because $1/\det \mathcal{L}_t$ is the number of lattice points of \mathcal{L}_t per volume in span \mathcal{L}_t . The formal analysis of NEW ENUM by Theorem 4.1 uses a proven version of the volume heuristics and does not assume that $\zeta_t \bmod \mathcal{L}_t$ is random.

The success rate β_t has been used in [SH95] to speed up ENUM by cutting stages of very small success rate. NEW ENUM proceeds differently, it first performs all stages with $\beta_t \geq 2^{-s}$ and collects during this process the stages with $\beta_t < 2^{-s}$ in the list L_s . Thereafter NEW ENUM performs the stages of L_s with $\beta_t \geq 2^{-s-1}$ in order of increasing t and for fixed t in order of decreasing β_t .

We will use that $A := \frac{n}{4} (\det B^t B)^{2/n} > \lambda_1^2$ holds for $n \geq 10$ as $\gamma_n < \frac{n}{4}$ for $n \geq 10$.

Outline of New Enum

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

1. $s := 1$, $L_s := \emptyset$, (we call s the level)
2. Perform algorithm ENUM of [SE94, SH95] pruned to stages with $\beta_t \geq 2^{-s}$:
 Upon entry of stage (u_t, \dots, u_n) compute β_t . If $\beta_t < 2^{-s}$ delay this stage and store $(\beta_t, u_t, \dots, u_n)$ in the list L_s of delayed stages. If $\beta_t \geq 2^{-s}$ perform stage (u_t, \dots, 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 $A := \|\mathbf{b}\|^2 - 1$.
3. $L_{s+1} := \emptyset$, perform the stages (u_t, \dots, 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 β_t . Collect the appearing substages $(u_{t'}, \dots, u_t, \dots, u_n)$ 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.

Comments on NEW ENUM. As soon as a vector $\mathbf{b} \in \mathcal{L}$ of length $c_1 = \|\mathbf{b}\|^2 \leq A$ has been found \mathbf{b} is given out and A is decreased to $\|\mathbf{b}\|^2 - 1$. The last vector \mathbf{b} that occurs as output is a shortest lattice vector, but this is only known after the subsequent exhaustive search terminates without finding a shorter vector. Such an unsuccessful exhaustive search takes more time than finding a shortest lattice vector.

Optimal value of A . If λ_1 is known it is best to set the input A to $A = \lambda_1^2$.

Reason of efficiency. For very short lattice vectors $\mathbf{b} = \sum_{i=1}^n u_i \mathbf{b}_i$ the stages (u_t, \dots, u_n) have large values β_t . If \mathbf{b} is short then so are the $\pi_t(\mathbf{b})$ for all t , on average $\|\pi_t(\mathbf{b})\|^2 \approx \frac{n-t+1}{n} \|\mathbf{b}\|^2$. Then the value $\rho_t^2 = A - \|\pi_t(\mathbf{b})\|^2$ is large and so is the corresponding β_t . New Enum tends to output at stages (u_1, \dots, u_n) very short lattice vectors $\sum_{i=1}^n u_i \mathbf{b}_i$ first. It tends to output a shortest lattice vector after only a few outputs.

For simplicity consider the case $A = \lambda_1^2$. Unlike ENUM, NEW ENUM delays most of the substages $(u_{t'}, \dots, u_t, \dots, u_n)$ of a passed stage (u_t, \dots, u_n) as their success rate $\beta_{t'}$ is to small. Prior to finding a shortest lattice vector $\mathbf{b}' = \sum_{i=1}^n u'_i \mathbf{b}_i$ NEW ENUM

essentially performs substages $(u_{t'}, \dots, u_n)$ of success rate $\beta_{t'} = V_{t'-1} \rho_{t'}^{t'-1} / \det \mathcal{L}_{t'}$ for $\rho_{t'}^2 = \lambda_1^2 - \|\pi_{t'}(\sum_{i=t'}^n u'_i \mathbf{b}_i)\|^2$. On average $\rho_{t'}^2 \approx \frac{t'-1}{n} \lambda_1^2$ holds for $\|\pi_{t'}(\mathbf{b}')\|^2 \approx \frac{n-t'+1}{n} \lambda_1^2$. While ENUM tries about $V_{t'-1} \lambda_1^{t'-1} / \det \mathcal{L}_{t'}$ substages $(u_{t'}, \dots, u_n)$ NEW ENUM tries only about a $(\frac{t'-1}{n})^{\frac{t'-1}{2}}$ fraction of them and delays the rest.

NEW ENUM is particularly fast for small λ_1 , the size of its search space is proportional to λ_1^n . Theorem 4.1 shows that NEW ENUM's search space is polynomial for moderately small λ_1 . Having found \mathbf{b}' the delaying of stages of small success rate fades away and NEW ENUM proves $\|\mathbf{b}'\| = \lambda_1$ by a complete exhaustive enumeration.

Running in linear space. Instead of storing the list L_s one can in step 3 restart NEW ENUM on the increased level $s + 1$. This lets NEW ENUM run in linear space and increases the running time by at most a factor $n \ln n$ as the various stages are repeated on average $\frac{n}{8} \ln n + o(n)$ times. We will show that NEW ENUM runs in time $n^{\frac{n}{8} + o(n)}$, and thus performs only stages with $\beta_t \geq n^{-\frac{n}{8} + o(n)}$. Hence $s \leq \frac{n}{8} \ln n + o(n \ln n)$.

Notation. We use the following function $c_t : \mathbb{Z}^{n-t+1} \rightarrow \mathbb{R}$:

$$c_t(u_t, \dots, u_n) = \|\pi_t(\sum_{i=t}^n u_i \mathbf{b}_i)\|^2 = \sum_{i=t}^n (\sum_{j=i}^n u_j r_{i,j})^2.$$

Clearly $c_t(u_t, \dots, u_n) = (\sum_{j=t}^n u_j r_{t,j})^2 + c_{t+1}(u_{t+1}, \dots, u_n)$.

Algorithm Enum [SH95]

INPUT BKZ-basis $B = QR \in \mathbb{Z}^{m \times n}$, $R = [r_{i,j}] \in \mathbb{R}^{n \times n}$ for block length 20,
OUTPUT $\mathbf{b} \in \mathcal{L}(B)$ such that $\mathbf{b} \neq \mathbf{0}$ has minimal length.

1. FOR $i = 1, \dots, n$ DO $c_i := u_i := y_i := 0$
 $u_1 := 1, t := t_{max} := 1, \bar{c}_1 := c_1 := \|\mathbf{b}_1\|^2$
 $(c_t = c_t(u_t, \dots, u_n) \text{ holds for the current } t, \bar{c}_1 \text{ is the current minimum of } c_1)$
2. WHILE $t \leq n$ #perform stage (u_t, \dots, u_n) :
 $c_t := c_{t+1} + (u_t + y_t)^2 r_{t,t}^2$
IF $c_t < \bar{c}_1$
THEN IF $t = 1$ THEN $\bar{c}_1 := c_1, \mathbf{b} := \sum_{i=1}^n u_i \mathbf{b}_i$
ELSE $t := t - 1, y_t := \sum_{i=t+1}^{t_{max}} u_i r_{t,i} / r_{t,t}, u_t := \lceil -y_t \rceil$
ELSE [$t := t + 1, t_{max} := \max(t, t_{max})$
IF $t = t_{max}$ THEN $u_t := u_t + 1$ ELSE $u_t := \text{next}(u_t, -y_t)$].
3. output \mathbf{b}

Given u_{t+1}, \dots, u_n ENUM tries the $u_t \in \mathbb{Z}$ close to $-y_t := -\sum_{i=t+1}^n u_i r_{t,i} / r_{t,t}$ in order of increasing distance, recursively as $u_t := \lceil -y_t \rceil, u_t := \text{next}(u_t, -y_t)$:

$$\lceil -y_t \rceil, \lceil -y_t \rceil - \sigma_t, \lceil -y_t \rceil + \sigma_t, \lceil -y_t \rceil - 2\sigma_t, \lceil -y_t \rceil + 2\sigma_t, \dots$$

for $\sigma_t := \text{sign}(\lceil -y_t \rceil + y_t) \in \{\pm 1\}$, $\text{sign}(0) := 1$, where $\lceil r \rceil =_{def} \lceil r - 0.5 \rceil$ denotes the nearest integer to $r \in \mathbb{R}$. The iteration $u_t := \text{next}(u_t, -y_t)$ increases or preserves $|u_t + y_t|$ and $c_t(u_t, \dots, u_n)$, decreases or preserves ρ_t and β_t so that ENUM performs the stages (u_t, \dots, u_n) for fixed u_{t+1}, \dots, u_n in order of increasing $c_t(u_t, \dots, u_n)$ and

decreasing success rate β_t . Note that $\text{next}(u_t, -y_t) = \text{next}_{\sigma_t, \nu_t}(u_t, -y_t)$ is a simple function of the number ν_t of iterations of next and the initial sign σ_t .

The algorithm ENUM of [SH95] performs a full exhaustive search of short lattice vectors and then outputs a proved shortest vector $\mathbf{b} \in \mathcal{L}$, $\|\mathbf{b}\| = \lambda_1$. ENUM works with the upper bound $A = \|\mathbf{b}_1\|^2$ of λ_1^2 , and does not decrease A during execution. ENUM does not specify the values σ_t, ν_t . The BKZ-basis for input is a recommendation of [SH95]. Various experiments [AEVZ02, NV07] demonstrate the strength of ENUM. Working with a simple LLL-basis ENUM is often much faster than KANNAN's SVP-algorithm that first HKZ-reduces the projected basis $\pi_2(\mathbf{b}_2, \dots, \mathbf{b}_n)$ in an expensive preprocessing. NEW ENUM improves ENUM along its successful design principle.

New Enum for SVP

INPUT LLL-basis $B = QR \in \mathbb{Z}^{m \times n}$, $R = [r_{i,j}] \in \mathbb{R}^{n \times n}$, $A := \frac{n}{4} (\det B^t B)^{2/n}$,

OUTPUT a sequence of $\mathbf{b} \in \mathcal{L}(B)$ of decreasing length $\|\mathbf{b}\|^2 \leq A$

terminating with $\|\mathbf{b}\| = \lambda_1$.

1. $u_1 := t := t_{max} := s := 1$, $u_2 := \dots := u_n := 0$, $c_1 := r_{1,1}^2$, $c_2 := \dots := c_{n+1} := 0$,
 $L_s := \emptyset$, $y_1 := 1$, $(c_t = c_t(u_t, \dots, u_n) \text{ always holds for the current } t)$
2. WHILE $t \leq n$ #perform stage (u_t, \dots, u_n) :
 $c_t := c_{t+1} + (u_t + y_t)^2 r_{t,t}^2$,
IF $c_t > A$ THEN GO TO 20,
 $\rho_t := (A - c_t)^{1/2}$, $\beta_t := V_{t-1} \rho_t^{t-1} / (r_{1,1} \dots r_{t-1,t-1})$,
IF $t = 1$ THEN [output $\mathbf{b} := \sum_{i=1}^n u_i \mathbf{b}_i$, $A := \|\mathbf{b}\|^2 - 1$, return],
IF $\beta_t \geq 2^{-s}$ THEN [$t := t - 1$, $y_t := \sum_{i=t+1}^{t_{max}} u_i r_{t,i} / r_{t,t}$,
 $u_t := \lceil -y_t \rceil$, $\sigma_t := \text{sign}(u_t + y_t)$, $\nu_t := 1$, return]
ELSE store $(y_t, \sigma_t, \nu_t, c_t, u_t, \dots, u_n)$ in L_s ,
- 2.1. $t := t + 1$, $t_{max} := \max(t, t_{max})$,
IF $t = t_{max}$ THEN $u_t := u_t + 1$, $\nu_t := 1$, $y_t := 0$
ELSE $u_t := \text{next}_{\sigma_t, \nu_t}(u_t, -y_t)$, $\nu_t := \nu_t + 1$.
3. $L_{s+1} := \emptyset$, perform all stages (u_t, \dots, u_n) of L_s on level $s + 1$ in increasing order of t , for fixed t in decreasing order of β_t , collect the delayed stages with $\beta_t < 2^{-s-1}$ in L_{s+1} .
IF $L_{s+1} \neq \emptyset$ THEN $s := s + 1$, GO TO 3 ELSE terminate by exhaustion.

4 Analysis of New Enum for SVP under GSA

We show under GSA that NEW ENUM runs in exponential time $n^{\frac{n}{32} + o(n)}$ and in polynomial time for moderately small $rd(\mathcal{L})$. All our time bounds must be multiplied by the work load per stage, a modest polynomial factor covering the steps performed at stage (u_1, \dots, u_n) before going to a subsequent stage.

GSA Let $B = QR = Q[r_{i,j}]$ satisfy $r_{i,i}^2 / r_{i-1,i-1}^2 = q$ for $i = 2, \dots, n$ for some $q > 0$.

W.l.o.g. let $q < 1$, otherwise the basis B satisfies $\|\mathbf{b}_i\| \leq \frac{1}{2} \sqrt{i+3} \lambda_i$ for all i .

The *geometrical series assumption* GSA of [S03] has been well used in practice [S03, S07], the security analysis of NTRU in [H07, [HHHW09] assumes GSA. Our worst case time bounds under GSA should approximately hold in practice as all quotients $r_{i,i}/r_{i+1,i+1}$ of well reduced bases nearly coincide on the average. GSA idealizes the practical requirement that the $r_{i,i}/r_{i-1,i-1}$ are all nearly equal. It is easier to work with the idealized assumption, [BL05] studies a practical definition of "nearly equal".

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

NEW ENUM runs in polynomial time if $rd(\mathcal{L}) \leq n^{-\frac{1}{2}-\varepsilon}$ and $\varepsilon > b$. Note that $rd(\mathcal{L}) \leq n^{-\frac{1}{2}-\varepsilon}$ holds if $\lambda_2 \geq n^{\frac{1}{2}+\varepsilon} \lambda_1$. This follows from HERMITE's second theorem: $\prod_{i=1}^n \lambda_i^2 \leq \gamma_n^n (\det \mathcal{L})^2$. In practice one can simply extend the basis B and the lattice by the required nearly shortest vector \mathbf{b}_1 without solving SVP with approximation factor $\sqrt{2e\pi} n^b$. For example we extend the prime number lattice in section 7.

LYUBASHEVSKY AND MICCIANCIO [LM09, Thms 4.1, 7.1] prove that GAPSVP_γ for $\gamma > 2\sqrt{n/\log n}$ is COOK-reducible to unique SVP with $\lambda_2 \geq \lambda_1 \gamma / (2\sqrt{n \log n})$. Combined with Theorem 4.1 this shows that λ_1 can be approximated under GSA in polynomial time with any approximation factor $n^{1+\varepsilon}$, $\varepsilon > 0$.

The LLL-algorithm finds a shortest vector in polynomial time if $\lambda_1 \leq 2^{-n/2} \lambda_2$. The latter condition implies $rd(\mathcal{L}) \leq 2^{-\frac{n-1}{2}}$

Proof of Theorem 4.1. 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 found by NEW ENUM. Let β'_t denote the success rate of stage (u'_t, \dots, u'_n) . NEW ENUM performs stage (u'_t, \dots, u'_n) prior to all stages (u_t, \dots, u_n) of success rate $\beta_t \leq \frac{1}{2} \beta'_t$.

Simplifying assumption. We assume that NEW ENUM performs (u'_t, \dots, u'_n) prior to all stages of success rate $\beta_t < \beta'_t$, i.e., with $\rho_t < \rho'_t$. By definition $\rho'_t{}^2 = A - \|\pi_t(\mathbf{b}')\|^2$. An elaborate analysis shows that, without this assumption, the time bound of Theorem 4.1 increases at most by the factor 2.

Consider the number \mathcal{M}_t of stages (u_t, \dots, u_n) with $\|\pi_t(\sum_{i=t}^n u_i \mathbf{b}_i)\| \leq \lambda_1$

$$\mathcal{M}_t := \#(\mathcal{B}_{n-t+1}(\mathbf{0}, \lambda_1) \cap \pi_t(\mathcal{L})).$$

Under the simplifying assumption \mathcal{M}_t covers the stages that precede (u'_t, \dots, u'_n) and those that finally prove $\|\mathbf{b}'\| = \lambda_1$. Lemma 4.2 gives a proven version of the volume heuristics, it polishes inequality (2) of [HS07].

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

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

$$\mathcal{E}_t = \{(x_t, \dots, x_n)^t \in \mathbb{R}^{n_t} \mid \|\pi_t(\sum_{i=t}^n x_i \mathbf{b}_i)\|^2 \leq \lambda_1^2\},$$

where $\|\pi_t(\sum_{i=t}^n x_i \mathbf{b}_i)\|^2 = \sum_{i=t}^n \sum_{j=i}^n (r_{i,j} x_j)^2 = \sum_{i=t}^n \sum_{j=i}^n (\mu_{j,i} x_j)^2 \|\mathbf{b}_i^*\|^2$.

By definition $\mathcal{M}_t \leq \#(\mathcal{E}_t \cap \mathbb{Z}^{n_t})$. We set

$$\begin{aligned}\sum_i \mathbf{x} &:= \sum_{j>i} \frac{r_{i,j}}{r_{i,i}} x_j \text{ and } x'_i := x_i + \lceil \sum_i \mathbf{x} \rceil, \\ \{\sum_i \mathbf{x}\} &:= \sum_i \mathbf{x} - \lceil \sum_i \mathbf{x} \rceil, \\ \mathcal{F}_t &:= \{(x'_t, \dots, x'_n)^t \in \mathbb{R}^{n_t} \mid \sum_{i=t}^n (x'_i + \{\sum_i \mathbf{x}\})^2 r_{i,i}^2 \leq \lambda_1^2\}.\end{aligned}$$

Claim $\#(\mathcal{E}_t \cap \mathbb{Z}^{n_t}) \leq \#(\mathcal{F}_t \cap \mathbb{Z}^{n_t})$.

Proof of the claim. The transformation $(x_t, \dots, x_n) \mapsto (x'_t, \dots, x'_n)$ is injective. In fact, if $i \geq t$ is the least index such that (y_i, \dots, y_n) and (z_i, \dots, z_n) differ then $y'_i \neq z'_i$. Moreover $(x'_i + \{\sum_i \mathbf{x}\}) r_{i,i} = \sum_{j=i}^n r_{i,j} x_j$. This proves the claim. \square

Next we cover \mathcal{F}_t by the simpler ellipsoid $\mathcal{E}'_t = \{\mathbf{x}' \in \mathbb{R}^{n_t} \mid \sum_{i=t}^n x_i'^2 r_{i,i}^2 \leq 4\lambda_1^2\}$.

Since $|\{\sum_i \mathbf{x}\}| \leq \frac{1}{2}$, $x_i \in \mathbb{Z}$ and $|x_i + \varepsilon|^2 \geq x_i^2/4$ holds for $|\varepsilon| \leq \frac{1}{2}$ we see that $\mathcal{F}_t \cap \mathbb{Z}^{n_t} \subset \mathcal{E}'_t \cap \mathbb{Z}^{n_t}$. So far we have proved $\mathcal{M}_t \leq \#(\mathcal{E}'_t \cap \mathbb{Z}^{n_t})$.

We bound $\#(\mathcal{E}'_t \cap \mathbb{Z}^{n_t})$ using the method of MAZO, ODLYZKO [MO90, Lemma 1].

Denoting $N_r := \#\{(k_t, \dots, k_n)^t \in \mathbb{Z}^{n_t} \mid \sum_{i=t}^n r_{i,i}^2 k_i^2 = r\}$ we have for any $s > 0$

$$\begin{aligned}\#(\mathcal{E}'_t \cap \mathbb{Z}^{n_t}) &= \sum_{0 \leq r \leq 4\lambda_1^2} N_r e^{s(4\lambda_1^2 - r)n_t} \leq e^{s4\lambda_1^2 n_t} \sum_{r \geq 0} N_r e^{-srn_t} \\ &= e^{s4\lambda_1^2 n_t} \prod_{i=t}^n \sum_{k_i \in \mathbb{Z}} e^{-sr_{i,i}^2 k_i^2} \leq e^{s4\lambda_1^2 n_t} \prod_{i=t}^n \left(1 + \frac{\sqrt{\pi}}{\sqrt{sr_{i,i}}} \right)\end{aligned}$$

since $\sum_{k \in \mathbb{Z}} e^{-Tk^2} = 1 + 2 \sum_{k=1}^{\infty} e^{-Tk^2} \leq 1 + 2 \int_0^{\infty} e^{-Tx^2} dx = 1 + \sqrt{\pi/T}$. We get

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

The additive constant 1 in Lemma 4.2 can be decreased close to $\frac{1}{2}$, in fact we see from $\sqrt{\pi/T} \leq \sum_{k \in \mathbb{Z}} e^{-Tk^2}$ that $\sum_{k \in \mathbb{Z}} e^{-Tk^2}$ is closer to $\frac{1}{2} + \sqrt{\pi/T}$.

We can improve the worst case upper bound of Lemma 4.2 on the average: replace in the above proof the lower bound $|x_i + \varepsilon|^2 \geq x_i^2/4$ by the expected value $\mathbb{E}_{\varepsilon}[|x_i + \varepsilon|^2] = x_i^2 + \frac{1}{12}$ for $\varepsilon \in \mathbb{R}[-\frac{1}{2}, \frac{1}{2}]$. Here we assume that $\{\sum_i \mathbf{x}\} \in [-\frac{1}{2}, \frac{1}{2}]$ is uniformly distributed. This replaces in Lemma 4.2 $\sqrt{8\pi}$ by $\sqrt{2\pi}$ and shows that

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

holds on the average for random $r_{i,i+1}/r_{i,i} \in \mathbb{R}[-\frac{1}{2}, \frac{1}{2}]$.

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

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

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

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

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

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 can nearly half $\bar{\eta}$ for an average time bound. Compared to the volume heuristics the bound (4.1) loses the factor $\bar{\eta}^{n-t+1}$. It remains to be seen how this theoretic loss is confirmed in practice.)

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

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

The equation $\lambda_1^2 / (\gamma_n rd(\mathcal{L})^2) = \|\mathbf{b}_1\|^2 q^{\frac{n-1}{2}}$ and $\gamma_n \leq \frac{1.744(n+o(n))}{2e\pi}$ [KL78] imply

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

(4.2), (4.3), $\frac{1}{n-1} \sum_{i=t-1}^{n-1} i = \frac{n}{2} - \frac{(t-1)(t-2)}{2(n-1)}$ and $q^{\frac{n-1}{2}} = \lambda_1^2 / (\|\mathbf{b}_1\|^2 \gamma_n rd(\mathcal{L})^2)$ yield

$$\mathcal{M}_t \leq m(q, c) \left(\frac{\bar{\eta} \sqrt{2e\pi} \lambda_1}{\sqrt{n-t+1} rd(\mathcal{L}) \|\mathbf{b}_1\|} \right)^{n-t+1} \left(\frac{\sqrt{n} rd(\mathcal{L}) \|\mathbf{b}_1\|}{\sqrt{e\pi} \lambda_1} \right)^{n - \frac{(t-1)(t-2)}{n-1}}. \quad (4.4)$$

Note that $\left(\frac{\bar{\eta} \sqrt{2e\pi} \lambda_1}{\sqrt{n-t+1} rd(\mathcal{L}) \|\mathbf{b}_1\|} \right)^{-1} = \Theta\left(\frac{\sqrt{n} rd(\mathcal{L}) \|\mathbf{b}_1\|}{\sqrt{e\pi} \lambda_1} \right)$ for $t \leq n(1 - \varepsilon)$. The difference of the exponents $\mathbf{de}(t) = n - \frac{(t-1)(t-2)}{n-1} - n + t - 1 = (t-1)\left(1 - \frac{t-2}{n-1}\right)$ is positive for $t \leq n$ and maximal for $t_{max} = \frac{n}{2} + 1$, $\mathbf{de}\left(\frac{n}{2} + 1 - c\right) = \frac{n+1}{4} + \frac{1/4 - c^2}{n-1}$. We get for $\|\mathbf{b}_1\| \leq \sqrt{2e\pi} n^b \lambda_1$, $t = \frac{n}{2} + 1 - c$ with $\frac{n}{2}(-1 + \varepsilon) \leq c \leq \frac{n}{2}$:

$$\mathcal{M}_t \leq m(q, c) \left(O(n^{\frac{1}{2} + b} rd(\mathcal{L})) \right)^{\frac{n+1}{4} + \frac{1/4 - c^2}{n-1}}.$$

As $m(q, c) = q^{\frac{1-c^2}{4}} = \left(\frac{\|\mathbf{b}_1\|^2 \gamma_n rd(\mathcal{L})^2}{\lambda_1^2} \right)^{\frac{c^2-1}{2(n-1)}} = \left(O(n^{\frac{1}{2} + b} rd(\mathcal{L})) \right)^{\frac{c^2-1}{n-1}}$ for $c > 0$ it follows that $\mathcal{M}_t = \left(O(n^{\frac{1}{2} + b} rd(\mathcal{L})) \right)^{\frac{n+1}{4}}$ with an $O(1)$ factor bounded by $(\bar{\eta} \sqrt{2e\pi})^{1/2}$. \square

A worst case time bound $n^{\frac{n}{32} + o(n)}$ under GSA. We elaborate the bounds (4.1), (4.4) for the case $rd(\mathcal{L}) = n^{-\frac{1}{2} + \varepsilon}$, $0 \leq \varepsilon \leq \frac{1}{2}$. Then $\sqrt{n/2} r_{i,i} \lesssim \frac{\sqrt{2e\pi} \lambda_1}{rd(\mathcal{L})^{\nu(i)} \|\mathbf{b}_1\|} \lambda_1$, where the exponent $\nu(i)$ decreases for $i = n/2 + 1, \dots, n$ from 1 to $\varepsilon' := \frac{1-4\varepsilon}{1-2\varepsilon}$. As $\nu(i)$ is on average bounded by $(1 + \varepsilon')/2 = \frac{1-3\varepsilon}{1-2\varepsilon}$ this decreases the exponent 1 of $rd(\mathcal{L})$ in (4.1) from 1 to $(1 + \varepsilon')/2$. This replaces $\sqrt{n-t+1} rd(\mathcal{L})$ in (4.4) by $\sqrt{n-t+1} rd(\mathcal{L})^{(1+\varepsilon')/2} = n^{3\varepsilon/2} / \sqrt{2}$, and implies for $\|\mathbf{b}_1\| \leq \sqrt{2e\pi} n^b \lambda_1$ and $t = \frac{n}{2} + 1 - c$ that

$$\mathcal{M}_t \leq m(q, c) \left(O(n^b) \right)^{\frac{n+1}{4} + \frac{1/4 - c^2}{n-1}} n^{\varepsilon\left(\frac{\varepsilon}{2} + \frac{1/4 - c^2}{n-1}\right)}.$$

Consider the case $b = 0$. Then this bound is maximal for $c = -\frac{n+1}{4}$, hence

$$\mathcal{M}_t \leq \Theta(1)^{n/4} n^{\varepsilon n/16} \leq n^{n/32 + o(n)}.$$

This time bound is much better than the time bound $n^{\frac{n}{2\varepsilon} + o(n)}$ of KANNAN's SVP algorithm proved in [HS07] but it requires a nearly shortest vector \mathbf{b}_1 and GSA.

Easier than worst cases. If some shortest vector \mathbf{b}' is in $\mathcal{L}(\mathbf{b}_1, \dots, \mathbf{b}_{t-1}) = \mathcal{L}_t$ then NEW ENUM finds \mathbf{b}' while working on the sublattice \mathcal{L}_t . Then SVP is solved in polynomial time if $rd(\mathcal{L}_t)$ is sufficiently small, no matter whether $rd(\mathcal{L})$ is large or small.

Worst case time bound of Kannan's SVP-algorithm. HANROT, STEHLÉ [HS07] show

that Kannan's SVP-algorithm runs in time $n^{O(1)} \sum_{t=1}^n N_t = n^{\frac{n}{2e} + o(n)}$ when given a quasi-HKZ-basis such that for a substantial part of the short vectors in $\pi_t(\mathcal{L})$ size-reduction scarcely increases the length. (4.5) indicates that the worst case time bound of Kannan's SVP-algorithm is proportional to $rd(\mathcal{L})^n$.

Moreover, HANROT, STEHLÉ prove in [HS08, Cor.1] the existence of HKZ-bases that require $n^{\frac{n}{2e} + o(n)}$ time. For these latter worst-case bases the quotients $r_{i,i}^2/r_{i-1,i-1}^2$ decrease with i . Such bases are very rare in practice, they are not typical and do not represent the average case. They are excluded by GSA.

4.2 Preprocessing. The bound $\|\mathbf{b}_1\| \leq \sqrt{2e\pi} n^b \lambda_1$ required for Theorem 4.1 does not hold for LLL-bases. It can be achieved by HKZ-reduction using NEW ENUM in dimensions $< n$. KANNAN's algorithm for HKZ-reduction [Ka87] first transforms the basis $B = QR \in \mathbb{Z}^{m \times n}$ into a quasi-HKZ-basis such that $R = [r_{i,j}] \in \mathbb{R}^{m \times n}$ satisfies:

1. $r_{1,1} \leq 2r_{2,2}$
2. $|r_{1,i}| \leq \frac{1}{2} r_{1,1}$ for $i = 2, \dots, n$
3. the basis matrix $[r_{i,j}]_{2 \leq i, j \leq n}$ is HKZ-reduced.

In particular, the quasi-HKZ-basis satisfies $\|\mathbf{b}_1\| \leq 2\lambda_1$.

KANNAN's algorithm transforms the given basis $B = B_1$ into a quasi-HKZ-basis by performing $\lceil 3 + \log_2 n \rceil$ SVP-computations on projected bases $\pi_2(B_i) \in \mathbb{R}^{(m-1) \times (n-1)}$ for $i = 1, \dots, \lceil 3 + \log_2 n \rceil$. Here B_{i+1} is obtained from $B_i = [\mathbf{b}_1, \dots, \mathbf{b}_n]$ by HKZ-reduction of $\pi_2(B_i)$ into $\pi_2(B_i)U_i$, with $U_i \in \text{GL}_{n-1}(\mathbb{Z})$, transforming $[\mathbf{b}_2, \dots, \mathbf{b}_n]$ into $[\mathbf{b}_2, \dots, \mathbf{b}_n]U_i$ and LLL-reduction of the basis vectors \mathbf{b}_1 of B_i and \mathbf{b}_2 resulting from $[\mathbf{b}_2, \dots, \mathbf{b}_n]U_i$.

Let $T_{NE}(n)$ denote the time bound of NEW ENUM in dimension n , the preprocessing that achieves $\|\mathbf{b}_1\| \leq 2\lambda_1$ included. During the preprocessing NEW ENUM is recursively called up to $3 + \log_2 n$ times in dimension $n - 1$, see [Ka87, S87, HS07]. This yields

$$T_{NE}(n) = \lceil 3 + \log_2 n \rceil T_{NE}(n-1) + n^{\frac{n}{8} + o(n)},$$

and thus $T_{NE}(n) = n^{\frac{n}{8} + o(n)}$ follows by induction on n .

As an immediate consequence HKZ-reduction of a lattice basis of dimension n runs in time $n^{\frac{n}{8} + o(n)}$. Moreover, HKZ-reduction runs in polynomial time under GSA if all input lattices \mathcal{L}' for the recursive calls of NEW ENUM satisfy $rd(\mathcal{L}') = o((\dim \mathcal{L}')^{-1/2})$. In fact the latter bound holds by Prop. 4.3 for the sublattices \mathcal{L}_t . Prop. 4.3 shows that if solving SVP for \mathcal{L} requires to solve SVP for \mathcal{L}_t then $rd(\mathcal{L}_t) \lesssim rd(\mathcal{L})$. However this does not hold for $\pi_t(\mathcal{L})$, see Prop. 4.4. Most likely HKZ-reduction is not polynomial time even if $rd(\mathcal{L}) \leq n^{-c}$ is arbitrarily small.

4.3 Finding an unproved shortest vector \mathbf{b}' is easier than proving $\|\mathbf{b}'\| = \lambda_1$.

Define $\eta(\mathcal{L}, \zeta, \rho) \in \mathbb{R}$, for a lattice \mathcal{L} of $\dim \mathcal{L} = n$ by the equation

$$|\mathcal{B}_n(\zeta, \rho) \cap \mathcal{L}(\mathbf{b}_1, \dots, \mathbf{b}_n)| = \eta(\mathcal{L}, \zeta, \rho)^n V_n \rho^n / \det \mathcal{L}.$$

For random $\zeta \bmod \mathcal{L}$ the expected value of $\eta(\mathcal{L}, \zeta, \rho)$ is 1. Following C.F. GAUSS the classical volume heuristics estimates $|\mathcal{B}_n(\zeta, \rho) \cap \mathcal{L}|$ by setting $\eta(\mathcal{L}, \zeta, \rho)$ to 1.

We study the time to find $\mathbf{b}' = \sum_{i=1}^n u'_i \mathbf{b}_i$ of length λ_1 provided that **AA** holds:

AA On average $\|\pi_t(\mathbf{b}')\|^2 \approx \frac{n-t+1}{n} \lambda_1^2$ holds for all t .

The number of stages *preceding* (u'_t, \dots, u'_n) and their upper bound (4.1) reduces under the average time assumption **AA** to

$$\begin{aligned} \mathcal{M}'_t &:= (\eta(\pi_t(\mathcal{L}), \mathbf{0}, \|\pi_t(\mathbf{b}')\|))^{n-t+1} V_{n-t+1} / (r_{t,t} \cdots r_{n,n}) \\ &< \left(\frac{\eta(\pi_t(\mathcal{L}), \mathbf{0}, \lambda_1)^2 2e\pi \lambda_1^2}{n \|\mathbf{b}_1\|^2} \right)^{\frac{n-t+1}{2}} / (r_{t,t} \cdots r_{n,n}). \end{aligned}$$

Inequality (4.4) translates for $\|\mathbf{b}_1\| \leq \sqrt{2e\pi} n^b \lambda_1$ into

$$\begin{aligned} \mathcal{M}'_t &\leq \left(\frac{\eta(\pi_t(\mathcal{L}), \mathbf{0}, \lambda_1)^2 2e\pi \lambda_1^2}{n \|\mathbf{b}_1\|^2} \right)^{\frac{n-t+1}{2}} \left(\frac{n rd(\mathcal{L})^2 \|\mathbf{b}_1\|^2}{e\pi \lambda_1^2} \right)^{n-t+1} \\ &\leq n^{(\frac{1}{2}+b)(n-t+1)+\frac{1}{2}+o(1)} (2 rd(\mathcal{L})^2)^{n-t+1} \eta(\pi_t(\mathcal{L}), \mathbf{0}, \lambda_1)^{n-t+1}. \end{aligned}$$

The exponent $(b + \frac{1}{2})(n-t+1)$ of n is maximal for $\alpha'_{max} = 1 - \frac{\ln 2}{\ln n}$. Note that $\alpha'_{max} = \alpha_{max} - \frac{n}{4} \frac{\ln 2 + o(1)}{\ln n}$ holds for α_{max} of the proof of Theorem 4.1, where $1 - \alpha/2$ stands for the factor $\frac{1}{2}$ of n^α . Using $n^{-\frac{n}{4} \frac{\ln 2}{\ln n}} = 2^{-n/4}$ we get

$$\max_t \mathcal{M}'_t \leq 2^{-\frac{n}{4}(1+\frac{o(n)}{\ln n})} \max_t \mathcal{M}_t = O(n^{b+\frac{1}{2}+o(1)} rd(\mathcal{L})^3)^{\frac{n}{4}}.$$

Thus finding an unproved shortest vector \mathbf{b}' is by the factor $2^{-\frac{n}{4}(1+\frac{o(n)}{\ln n})}$ faster than proving $\|\mathbf{b}'\| = \lambda_1$.

4.4 The relative density of \mathcal{L} and some sublattices of \mathcal{L} .

For the lattices $\mathcal{L} = \mathcal{L}(\mathbf{b}_1, \dots, \mathbf{b}_n)$ and $\mathcal{L}_t = \mathcal{L}(\mathbf{b}_1, \dots, \mathbf{b}_{t-1})$ we have

Proposition 4.3. *Under GSA we have that $\frac{\lambda_1(\mathcal{L})}{\lambda_1(\mathcal{L}_t)} \frac{rd(\mathcal{L}_t)}{rd(\mathcal{L})} \approx \left(\frac{n}{t-1}\right)^{\frac{1}{4}} q^{\frac{n-t+1}{4}}$.*

In fact GSA implies

$$\begin{aligned} \lambda_1(\mathcal{L}) / (\gamma_n^{1/2} rd(\mathcal{L})) &= (\det \mathcal{L})^{\frac{1}{n}} = \|\mathbf{b}_1\| q^{\frac{n}{2n}} = \|\mathbf{b}_1\| q^{\frac{n-1}{4}}, \\ \lambda_1(\mathcal{L}_t) / (\gamma_{t-1}^{1/2} rd(\mathcal{L}_t)) &= (\det \mathcal{L}_t)^{\frac{1}{t-1}} = \|\mathbf{b}_1\| q^{\frac{t-2}{4}}. \end{aligned}$$

Dividing the first equation by the second and using $\gamma_n/\gamma_{t-1} \approx \sqrt{\frac{n}{t-1}}$ yields the claim.

Conclusion. If $\lambda_1(\mathcal{L}_t) = \lambda_1(\mathcal{L})$ then $rd(\mathcal{L}_t) \lesssim rd(\mathcal{L})$ since in general $q^{n-t+1} \lesssim \frac{t-1}{n}$ holds for $q \leq 1 - \varepsilon_0 < 1$. Then SVP for \mathcal{L}_t is not harder than SVP for \mathcal{L} . This is important because solving SVP for \mathcal{L} requires to solve SVP for \mathcal{L}_t . On the other hand if $\lambda_1(\mathcal{L}_t) > \lambda_1(\mathcal{L})$ then possibly $rd(\mathcal{L}_t) > rd(\mathcal{L})$ and SVP for \mathcal{L}_t may be harder than SVP for \mathcal{L} . However, in this case NEW ENUM solves SVP for \mathcal{L} without solving SVP for \mathcal{L}_t .

As in the proof of Proposition 4.3 we get for the lattice $\pi_t(\mathcal{L}) \subset \text{span}(\mathbf{b}_1, \dots, \mathbf{b}_{t-1})^\perp$:

Proposition 4.4. *Under GSA and AA we have on average $\frac{rd(\pi_t(\mathcal{L}))}{rd(\mathcal{L})} \lesssim \left(\frac{n-t+1}{n}\right)^{\frac{1}{4}} q^{\frac{1-t}{4}}$.*

4.5 Failings of the volume heuristics. While $\eta(\mathcal{L}, \zeta, \rho)$ can deviate from 1 the deviation is negligible for $\rho \rightarrow \infty$. [MO90] studies $\max_{\zeta} \eta(\mathcal{L}, \zeta, \rho)$ as a function of ζ and ρ for the lattice \mathbb{Z}^n . Prop. 4.5 shows that $\eta(\mathcal{L}, \mathbf{0}, \lambda_1)$ is unbounded for very small $rd(\mathcal{L})$.

Proposition 4.5. $\eta(\mathcal{L}, \mathbf{0}, \lambda_1) > (\sqrt{2} rd(\mathcal{L}))^{-1}$ holds for $n \geq n_0$.

Proof. Consider $\#\lambda_1(\mathcal{L}) =_{def} \#\{\mathbf{b} \in \mathcal{L} \mid 0 \neq \|\mathbf{b}\| \leq \lambda_1\}$. We have

$$\#\lambda_1(\mathcal{L}) \leq V_n \eta(\mathcal{L}, \mathbf{0}, \lambda_1)^n \lambda_1^n / \det \mathcal{L}.$$

We see from $\lambda_1(\mathcal{L})^2 = \gamma_n rd(\mathcal{L})^2 (\det \mathcal{L})^{\frac{2}{n}}$ and $V_n \approx (\pi n)^{-\frac{1}{2}} \left(\frac{2e\pi}{n}\right)^{\frac{n}{2}}$ that

$$\#\lambda_1(\mathcal{L}) \leq \left(\frac{2e\pi}{n} \gamma_n\right)^{\frac{n}{2}} \eta(\mathcal{L}, \mathbf{0}, \lambda_1)^n rd(\mathcal{L})^n.$$

As $2e\pi \gamma_n/n \leq 2$ holds for $n \geq n_0$ and $\#\lambda_1(\mathcal{L}) \geq 2$ this proves the claim. \square

4.6 The number of nearly shortest vectors of \mathcal{L} is bounded proportional to $rd(\mathcal{L})^n$.

This is important as the time bound for SVP increases with the number of nearly shortest vectors in \mathcal{L} . The proof of Prop. 4.3 bounds $\#\lambda_1(\mathcal{L})$ as follows:

$$\#\{\mathbf{b} \in \mathcal{L} \mid 0 \neq \|\mathbf{b}\| \leq \lambda_1\} \leq \left(\frac{2e\pi}{n} \gamma_n\right)^{\frac{n}{2}} \eta(\mathcal{L}, \mathbf{0}, \lambda_1)^n rd(\mathcal{L})^n.$$

In the same way we see that the number of very short vectors is bounded proportional to $rd(\mathcal{L})^n$. Note that the time bound of Theorem 4.1 is proportional to $rd(\mathcal{L})^{n/2}$. Of course there exist lattices \mathcal{L} of arbitrarily small $rd(\mathcal{L})$ that have exponentially many nearly shortest vectors due to small values $\eta(\mathcal{L}, \mathbf{0}, \lambda_1)$. However these are very special cases, they are irrelevant on the average.

Obviously $\#\lambda_1(\mathbb{Z}^n) = 2n$ and $rd(\mathbb{Z}^n) = 1/\sqrt{\gamma_n} = \Theta(1/\sqrt{n})$. Every basis of \mathbb{Z}^n that consists of unit vectors satisfies GSA with $q = 1$. Interestingly $rd(\mathbb{Z}^n)$ is under GSA nearly minimal for lattices \mathcal{L} such that $\#\lambda_1(\mathcal{L}) > 2$:

Proposition 4.6. *Let \mathcal{L} have a basis satisfying GSA and $\|\mathbf{b}_1\| = \lambda_1$. If $rd(\mathcal{L}) < 1/\sqrt{\gamma_n}$ then $\#\lambda_1(\mathcal{L}) = 2$.*

Proof. Under GSA and $\|\mathbf{b}_1\| = \lambda_1$ we have

$$\|\mathbf{b}_1\|^2 = \gamma_n rd(\mathcal{L})^2 (\det \mathcal{L})^{\frac{2}{n}} = \gamma_n rd(\mathcal{L})^2 \|\mathbf{b}_1\|^2 q^{\frac{n-1}{2}}$$

hence $q = (\gamma_n rd(\mathcal{L})^2)^{\frac{-2}{n-1}} > 1$ holds for $rd(\mathcal{L}) < 1/\sqrt{\gamma_n}$, and thus $\#\lambda_1(\mathcal{L}) = 2$. \square

4.7 A relaxation of GSA that does not preserve Theorem 4.1. Every lattice $\mathcal{L} = \mathcal{L}(\mathbf{b}_1, \dots, \mathbf{b}_n)$ can easily be extended to \mathcal{L}' such that $\mathcal{L} \subset \mathcal{L}'$, $\lambda_1(\mathcal{L}) = \lambda_1(\mathcal{L}')$ and $rd(\mathcal{L}') \ll 1$. However, such an extension $\mathcal{L} \mapsto \mathcal{L}'$ is easy to invert if $rd(\mathcal{L}) \approx 1$. Moreover the reduced bases of \mathcal{L}' strongly violate GSA since at least one quotient $r_{i,i}/r_{i-1,i-1}$ deviates exponentially from the others. In fact Theorem 4.1 no more holds if all $r_{i,i}/r_{i-1,i-1}$ nearly coincide with one exception. Consider an extension

$$\mathcal{L}' = \mathcal{L} + \mathbf{b}_0 \mathbb{Z} \text{ for } \mathbf{b}_0 \perp \text{span } \mathcal{L} \text{ and } \|\mathbf{b}_0\| \gg \lambda_1(\mathcal{L}).$$

5 The relative density of some cryptographic lattices.

5.1 NTRU. The NTRUencrypt lattices proposed in [H07], [HHHW09] strictly satisfy $rd(\mathcal{L}) > n^{1/2}$. Let $\mathcal{R} = \mathbb{Z}[x]/(x^N - 1, q)$ denote the ring of polynomials modulo $x^N - 1$ with coefficients in $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$ and the convolution product $g = f * h$ defined by $g_\ell = \sum_{i+j \in \{\ell, \ell+N\}} f_i h_j$. We identify $f = \sum_{i=0}^{N-1} f_i x^i$ in \mathcal{R} with its coefficient vector $(f_0, \dots, f_{N-1}) \in \mathbb{Z}_q^N$. N is prime, $p = 3$, $\gcd(p, q) = 1$; p, q, N are public.

The *private key* $(f, g) \in \mathcal{R} \times \mathcal{R}$ and the *public key* $h \in \mathcal{R}$ satisfy $g = f * h$. The polynomials f, g are of the form $f = 1 + pF$, $g = 1 + G$ where $F, G \in \mathcal{R}$ are random having d_f, d_g coefficients 1 and d_f, d_g coefficients -1 , all other coefficients are 0. Then $f(1) = \sum_{i=0}^{N-1} f_i = 1 = g(1) = \sum_{i=0}^{N-1} g_i = h(1)$.

For example we consider the parameters proposed in [HWWW09] that require a work load 2^{112} for the combined lattice and meet-in-the-middle attack. Here $N = 401$, $q = 2048$, $p = 3$, $d_f = 113$, $d_g = \lfloor N/3 \rfloor$. This NTRU-lattice has dimension

$n = 2 \cdot 401 = 802$. The public column basis is $B = \begin{bmatrix} I_N & 0 \\ H & q \cdot I_N \end{bmatrix}$, $H \in \mathbb{Z}^{N \times N}$ is

the circular matrix associated with $h \in \mathcal{R}$ and I_N is the $N \times N$ identity matrix.

Moreover $(\det \mathcal{L})^{1/n} = (2048^{401})^{1/802} = 2^{5.5}$ and $\lambda_1^2 = 2p^2 d_f + 2d_g + 2 = 2302$. By the MINKOWSKI lower bound $\gamma_n \geq \frac{n + \ln n}{2\epsilon\pi} \approx 47.3$. Hence

$$rd(\mathcal{L}) \leq 2^{-5.5} (2302/47.3)^{1/2} \approx 0.154 \gg 0.035 \approx n^{-\frac{1}{2}}.$$

These lattices are not be affected by our new attack even if $rd(\mathcal{L})$ further decreases when γ_{802} surpasses the MINLOWSKI lower bound.

5.2 Unique-SVP lattices. These lattices satisfy the unique shortest vector property: every lattice vector that is linearly independent to a shortest nonzero lattice vector has at least length $n^c \lambda_1$ for a constant $c > 1$, i.e., $\lambda_2 \geq \lambda_1 n^c$. Unique-SVP lattices have been introduced by AJTAI [Aj96] in its proof of the worst case / average case equivalence. The original $c = 7$ [AD97] has been reduced to $3 + \delta + \epsilon$ [Ca98, Thm 6.1].

Hence Ajtai, Dwork lattices of [AD97] satisfy $\lambda_2 \geq n^3 \lambda_1$. MINKOWSKI's second theorem implies that $\lambda_1^n \leq n^{-3n+3} \gamma_n^{n/2} \det \mathcal{L}$, and thus $\lambda_1 \leq n^{-3+3/n} \gamma_n^{1/2} (\det \mathcal{L})^{1/n}$. This shows that $rd(\mathcal{L}) \leq n^{-(3+\epsilon)(1-1/n)}$ and that SVP is easy.

5.3 Ajtai's worst case / average case equivalence. AJTAI [Aj96, Thm 1] reduces SVP for a specific random lattice to SVP of an arbitrary lattice satisfying $\lambda_1 \leq \lambda_2/n^c$ for some $c > 3$ [Ca98, Thm 6.1]. Under GSA the latter SVP can be solved in polynomial time. Hence this does not imply hardness of SVP for the specific random lattice.

5.4 Lattices of high density. MINKOWSKI gave in (1905) a nonconstructive proof that lattices satisfying $\frac{1}{n} \log_2(\Delta) \geq -1$ exist but no constructions for such lattices are known. Constructions of lattices satisfying $\frac{1}{n} \log_2(\Delta) \geq -2.3$ by the methods of [CS93, ch. 8] are cited in [CS93]. The most efficient constructions of lattices of

high density use probabilistic algorithms. Deterministic constructions are either less efficient or provide smaller density.

The difficulty of constructing lattices of high density is a central point in the NP-hardness proof of SVP under probabilistic reductions. The core of the proof in [MG02] is a sphere packing construction. This construction uses a probabilistic reduction, so far no deterministic polynomial time reduction is known, see [MG02, chapt. 4-6].

6 New Enum for CVP

Given a target vector $\mathbf{t} = \sum_{i=1}^n \tau_i \mathbf{b}_i \in \mathbb{R}^m$ we minimize $\|\mathbf{t} - \mathbf{b}\|$ for $\mathbf{b} \in \mathcal{L}(B)$. [Ba86] solves $\|\mathbf{t} - \mathbf{b}\|^2 \leq \frac{1}{4} \sum_{i=1}^n r_{i,i}^2$ in polynomial time for $B = QR$, $R = [r_{i,j}]$.

Adaptation of NEW ENUM to CVP. We adapt NEW ENUM to solve $\|\mathbf{t} - \mathbf{b}\|^2 < \check{A}$. Initially we set $\check{A} := \frac{1}{4} \sum_{i=1}^n r_{i,i}^2$ so that $\|\mathbf{t} - \mathcal{L}\|^2 \leq \check{A}$. Having found some $\mathbf{b} \in \mathcal{L}$ such that $\|\mathbf{t} - \mathbf{b}\|^2 < \check{A}$ NEW ENUM gives out \mathbf{b} and decreases \check{A} to $\|\mathbf{t} - \mathbf{b}\|^2$.

New Enum for CVP

INPUT LLL-basis $B = QR \in \mathbb{Z}^{m \times n}$, $R = [r_{i,j}] \in \mathbb{R}^{n \times n}$, $(\tau_1, \dots, \tau_n)^t \in \mathbb{R}^n$,

OUTPUT A sequence of $\mathbf{b} \in \mathcal{L}(B)$ such that $\|\mathbf{t} - \mathbf{b}\|$ decreases and terminates with $\|\mathbf{t} - \mathcal{L}\|$.

1. $\check{A} := \frac{1}{4} \sum_{i=1}^n r_{i,i}^2$, $t := n$, $s := 1$, $L_s := \emptyset$,
 $y_n := \tau_n$, $u_n := \lceil -y_n \rceil$, $c_{n+1} := 0$,
 $(c_t = c_t(\tau_t - u_t, \dots, \tau_n - u_n))$ always holds for the current t
2. WHILE $t \leq n$ #perform stage (u_t, \dots, u_n) :
 $c_t := c_{t+1} + (u_t + y_t)^2 r_{t,t}^2$,
IF $c_t > \check{A}$ THEN GO TO 20,
 $\check{\rho}_t := (\check{A} - c_t)^{1/2}$, $\check{\beta}_t := V_{t-1} \check{\rho}_t^{t-1} / (r_{1,1} \cdots r_{t-1,t-1})$,
IF $t = 1$ THEN [output $\mathbf{b} := \sum_{i=1}^n u_i \mathbf{b}_i$, set $\check{A} := \|\mathbf{t} - \mathbf{b}\|^2$, return]
IF $\check{\beta}_t \geq 2^{-s}$ THEN [$t := t - 1$, $y_t := \tau_t + \sum_{i=t+1}^n (\tau_i - u_i) r_{t,i} / r_{t,t}$,
 $u_t := \lceil -y_t \rceil$, $\sigma_t := \text{sign}(u_t + y_t)$, $\nu_t := 1$, return]
ELSE store $(y_t, \sigma_t, \nu_t, c_t, u_t, \dots, u_n)$ in L_s ,
2.1. $t := t + 1$, $u_t := \text{next}_{\sigma_t, \nu_t}(u_t, -y_t)$, $\nu_t := \nu_t + 1$.
3. $L_{s+1} := \emptyset$, perform all stages (u_t, \dots, u_n) of L_s on level $s + 1$ in increasing order of t , for fixed t , for decreasing order of $\check{\beta}_t$, collect the delayed stages with $\check{\beta}_t < 2^{-s-1}$ in L_{s+1} .
4. IF $L_{s+1} \neq \emptyset$ THEN $s := s + 1$, GO TO 3 ELSE terminate by exhaustion.

At stage (u_t, \dots, u_n) NEW ENUM searches to extend the current $\mathbf{b} = \sum_{i=1}^n u_i \mathbf{b}_i \in \mathcal{L}$ to some $\mathbf{b}' = \sum_{i=1}^n u_i \mathbf{b}_i \in \mathcal{L}$ such that $\|\mathbf{t} - \mathbf{b}'\|^2 < \check{A}$. The adapted success rate $\check{\beta}_t$ of stage (u_t, \dots, u_n) is

$$\check{\beta}_t = V_{t-1} \check{\rho}_t^{t-1} / \det \mathcal{L}(\mathbf{b}_1, \dots, \mathbf{b}_{t-1}) \text{ for } \check{\rho}_t = (\check{A} - \|\pi_t(\mathbf{t} - \mathbf{b})\|^2)^{1/2}.$$

Previously, stage (u_{t+1}, \dots, u_n) determines u_t to yield the next integer minimum of

$$c_t(\tau_t - u_t, \dots, \tau_n - u_n) := \|\pi_t(\mathbf{t} - \mathbf{b})\|^2$$

$$= (\sum_{i=t}^n (\tau_i - u_i) r_{t,i})^2 + c_{t+1} (\tau_{t+1} - u_{t+1}, \dots, \tau_n - u_n).$$

Clearly, $\|\pi_t(\mathbf{t} - \mathbf{b})\|^2$ is minimal for $u_t = \lceil -\tau_t - \sum_{i=t+1}^n (\tau_i - u_i) r_{t,i} / r_{t,t} \rceil$.

Optimal value of \check{A} . If the distance $\|\mathbf{t} - \mathcal{L}\|$ to the closest vector $\mathbf{b} \in \mathcal{L}$ is known then we set initially $\check{A} := \|\mathbf{t} - \mathcal{L}\|^2$. This delays many unnecessary stages.

If NEW ENUM runs in polynomial time it should solve $\|\mathbf{t} - \mathcal{L}\| = \|\mathbf{t} - \mathbf{b}\|$ faster than LLL-reduction because the work load per stage is modest.

NEW ENUM solves CVP for \mathcal{L} and \mathbf{t} by first solving CVP for $\pi_t(\mathcal{L})$ and $\pi_t(\mathbf{t})$. The time for the latter is under GSA maximal for $t = 1$, $\pi_1(\mathcal{L}) = \mathcal{L}$.

Corollary 6.1 (GSA). *Given $\mathbf{b}_1 \in \mathcal{L}$ such that $0 \neq \|\mathbf{b}_1\| = O(\lambda_1)$, NEW ENUM finds $\mathbf{b} \in \mathcal{L}$ such that $\|\mathbf{t} - \mathbf{b}\| = \|\mathbf{t} - \mathcal{L}\|$ 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 $\|\mathcal{L} - \mathbf{t}\| = O(\lambda_1)$ and $rd(\mathcal{L}) \leq n^{-\frac{1}{2}-\varepsilon}$ for $\varepsilon > 0$.

Proof. We follow and adapt the proof of Theorem 4.1. Replacing λ_1 in (4.1) by $\|\mathcal{L} - \mathbf{t}\|$ we estimate the number \mathcal{M}'_t of stages (u_t, \dots, u_n) that satisfy $\|\pi_t(\sum_{i=t}^n u_i \mathbf{b}_i - \mathcal{L})\| \leq \|\mathcal{L} - \mathbf{t}\|$ under GSA to

$$\begin{aligned} \mathcal{M}'_t &:= \#(\mathcal{B}_{n-t+1}(\pi_t(\mathbf{t}), \|\mathcal{L} - \mathbf{t}\|) \cap \pi_t(\mathcal{L})) \\ &\leq m(q, c) \left(\frac{\bar{\eta} \sqrt{2\varepsilon\pi}}{\sqrt{n-t+1}} \frac{\|\mathcal{L} - \mathbf{t}\|}{\|\mathbf{b}_1\| rd(\mathcal{L})} \right)^{n-t+1} / q^{\sum_{i=t}^{n-1} i/2}. \end{aligned}$$

In particular we extend Lemma 4.2 from the sphere center $\zeta = \mathbf{0}$ to $\zeta = \pi_t(\mathbf{t})$. Here we define $\sum_i \mathbf{x} = \sum_{j>i} \frac{t_{i,j}}{r_{i,i}} - \tau_i$. (By Theorem 2 of [MO90] \mathcal{M}'_t is, up to a factor $n^{O(\sqrt{n})}$, maximal for $\zeta = \mathbf{0}$.) This transforms (4.4) into

$$\begin{aligned} \mathcal{M}'_t &\leq m(q, c) \left(\frac{\bar{\eta} \sqrt{2\varepsilon\pi} \|\mathcal{L} - \mathbf{t}\|}{\sqrt{n-t+1} rd(\mathcal{L}) \|\mathbf{b}_1\|} \right)^{n-t+1} \left(\frac{\sqrt{n} rd(\mathcal{L}) \|\mathbf{b}_1\|}{\sqrt{\varepsilon\pi} \lambda_1} \right)^{n - \frac{(t-1)(t-2)}{n-1}} \\ &= m(q, c) (O(\sqrt{n} rd(\mathcal{L}) \|\mathcal{L} - \mathbf{t}\|^2 \lambda_1^{-2}))^{\frac{n+1}{4} + \frac{1/4-c^2}{n-1}}. \end{aligned}$$

This proves the claim, in particular \mathcal{M}'_t and the time bound of NEW ENUM are polynomial if $\sqrt{n} \|\mathcal{L} - \mathbf{t}\|^2 rd(\mathcal{L}) = o(\lambda_1^2)$. \square

A worst case time bound. In case $rd(\mathcal{L}) = n^{-\frac{1}{2}+\varepsilon}$, $0 \leq \varepsilon \leq \frac{1}{2}$, the term $\sqrt{n-t+1} rd(\mathcal{L})$ in the above bound on \mathcal{M}'_t transforms, as in the proof of the worst case time bound subsequent to Theorem 4.1, into $\sqrt{n-t+1} rd(\mathcal{L})^{(1+\varepsilon')/2} = n^{3\varepsilon'/2} / \sqrt{2}$ for $\varepsilon' = \frac{1-4\varepsilon}{1-2\varepsilon}$. This proves for $t = \frac{n}{2} + 1 + c$

$$\mathcal{M}'_t \leq m(q, c) (O(\sqrt{n} rd(\mathcal{L}) \|\mathcal{L} - \mathbf{t}\|^2 \lambda_1^{-2}))^{\frac{n+1}{4} + \frac{1/4-c^2}{n-1}} n^{-\frac{1}{2}\varepsilon(\frac{n}{2}-c)},$$

where $m(q, c) = q^{\frac{1-c^2}{4}} = \Theta(1)^{n/4}$ as $\|\mathbf{b}_1\| = O(\lambda_1)$, and $(\frac{\sqrt{n-t+1} rd(\mathcal{L})}{n^{\frac{3}{2}\varepsilon/\sqrt{2}}})^{n-t+1} = n^{-\frac{1}{2}\varepsilon(\frac{n}{2}-c)}$. The exponent $\varepsilon(\frac{n+1}{4} + \frac{1/4-c^2}{n-1} - \frac{1}{2}(\frac{n}{2}-c))$ of n is maximal for $c = \frac{n-1}{4}$.

This yields for $t = \frac{n}{2} + 1 + \frac{n-1}{4}$, $\varepsilon \leq \frac{1}{2}$ the worst case time bound

$$\begin{aligned} \mathcal{M}'_t &= O(n^\varepsilon \|\mathcal{L} - \mathbf{t}\|^2 \lambda_1^{-2})^{\frac{n+1}{4} + \frac{n-1}{16}} n^{-\varepsilon n/4 + \varepsilon n/8} \\ &= n^{\varepsilon(\frac{1}{4} + \frac{3}{16}(n-1))} \Theta(1)^{\frac{n+1}{4} + \frac{n-1}{16}} = \Theta(n)^{\frac{3}{32}n}. \end{aligned}$$

This time bound is much faster than the fully proven time bound $n^{n/2+o(n)}$ of [HS07] for KANNAN's CVP-algorithm [Ka87].

7 Factoring integers by CVP solutions for the Prime Number Lattice

Let N be a positive integer that is not a prime power. We show how to factor N in polynomial time assuming GSA for the prime number lattice. Let $p_1 < \dots < p_n$ enumerate all primes less than $(\ln N)^\alpha$. Then $n = (\ln N)^\alpha / (\alpha \ln \ln N)(1 + o(1))$. Let the prime factors p of N satisfy $p > p_n$. We let the asymptotic $o(1)$ be for $N \rightarrow \infty$.

A classical method factors N by producing about n independent modular equations of the form $\prod_{i=1}^n p_i^{e_i} = \pm \prod_{i=1}^n p_i^{e'_i} \pmod{N}$. Theorem 7.2 shows how to construct such modular equations from CVP-solutions of small distance for the prime number lattice $\mathcal{L}(B)$. Theorems 7.4, 7.5, show how to guarantee a sufficiently small distance, and Theorem 7.6 shows that the CVP's are solvable in polynomial time.

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

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

$$\det \mathcal{L}(B)^2 = \prod_{i=1}^n (\ln p_i) (1 + N^{2c} \sum_{i=1}^n \ln p_i),$$

$$\det \mathcal{L}(B)^{2/n} = (\alpha - o(1)) \ln \ln N \cdot N^{2c/n}.$$

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

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

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

Lemma 7.1. *If $|u - vN'| = o(N^c)$ and $v = \Theta(N^{c-1})$ and $e_1, \dots, e_n \in \{0, \pm 1\}$ 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 $|\ln \frac{u}{vN'}| = |\ln(1 + \frac{u-vN'}{vN'})| = \frac{|u-vN'|}{vN'} (1 + o(1)) = \Theta(\frac{|u-vN'|}{N^{c-1}N'})$.

Combining these equations proves the claim. \square

Theorem 7.2. *If $\mathbf{b} \in \mathcal{L}(B)$ satisfies $\|\mathbf{b} - \mathbf{N}\|^2 \leq (2c - 1) \ln N + 2\delta \ln p_n$ then*

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

Proof. The bound on $\|\mathbf{b} - \mathbf{N}\|^2$ for $\mathbf{b} = \sum_{i=1}^n e_i \mathbf{b}_i$ implies

$$\sum_{i=1}^n |e_i \ln p_i| \leq \sum_{i=1}^n e_i^2 (\sqrt{\ln p_i})^2 \leq \|\mathbf{b} - \mathbf{N}\|^2 \leq (2c - 1) \ln N + 2\delta \ln p_n.$$

Using the bound on $\|\mathbf{b} - \mathbf{N}\|$ for the last coordinate z of $\mathbf{b} - \mathbf{N}$ we get

$$\begin{aligned} |z|N^{-c} &= \left| \sum_{i=1}^n e_i \ln p_i - \ln N' \right| = \left| \ln \frac{u}{vN'} \right| \\ &\leq N^{-c} ((2c - 1) \ln N + 2\delta \ln p_n)^{1/2} \leq N^{-c} p_n^{\frac{1}{\alpha} + o(1)} \end{aligned}$$

since $(\ln N)^\alpha \approx p_n$. This shows for $\beta = 1/\alpha$ the two inequalities required in Theorem 7.3. The claim follows from Theorem 7.3 adjusting vN to vN' . \square

Theorem 7.3. [S93, Thm 4.1] *The inequality $|u - vN| \leq p_n^{\beta + \delta + o(1)}$ holds for $\beta, \delta \geq 0$ if $|\sum_{i=1}^n e_i \ln p_i - \ln N| \leq N^{-c} p_n^{\beta + o(1)}$ and $\sum_{i=1}^n |e_i \ln p_i| \leq (2c - 1) \ln N + 2\delta \ln p_n$.*

Outline of the factoring method. We compute vectors $\mathbf{b} = \sum_{i=1}^n e_i \mathbf{b}_i \in \mathcal{L}(B)$ close to \mathbf{N} such that $|u - vN'| \leq p_n$ holds for a small integer multiple N' of N , and thus the prime factorizations of $u > N$ and $|u - vN'| = \prod_{i=1}^n p_i^{e'_i}$ yield a non-trivial relation

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

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 $\prod_{i=0}^n p_i^{e_{i,j} - e'_{i,j}} = 1 \pmod{N}$ for $j = 1, \dots, n + 1$.

Then any non trivial solution $z_1, \dots, z_{n+1} \in \{0, 1\}$ of the equations

$$\sum_{j=1}^{n+1} z_j (e_{i,j} - e'_{i,j}) = 0 \pmod{2} \text{ for } i = 0, \dots, n \quad (7.2)$$

solves $X^2 = Y^2 \pmod{N}$ with

$$X = \prod_{i=0}^n p_i^{\frac{1}{2} \sum_{j=1}^{n+1} z_j e_{i,j}} \pmod{N}, \quad Y = \prod_{i=0}^n p_i^{\frac{1}{2} \sum_{j=1}^{n+1} z_j e'_{i,j}} \pmod{N}.$$

In case that $X \neq \pm Y \pmod{N}$ this yields a factor $\gcd(X \pm Y, N)$ of N .

The linear system of equations (7.2) can be solved within $O(n^3)$ bit operations. This takes much less time than LLL-reduction of B that is done by arithmetic steps using large integers. We neglect this minor part of the work load of factoring N .

Theorem 7.2 shows that lattice vectors that are sufficiently close to \mathbf{N} provide a relation (7.1). Theorems 7.4 and 7.5 show that such close vectors exist, and Theorem 7.6 shows that the corresponding CVP's are polynomial time. We get independent relations (7.1) by constructing them for independent integer multiples N' of N .

The existence of lattice vectors $\mathbf{b} = \sum_{i=1}^n e_i \mathbf{b}_i \in \mathcal{L}(B)$ such that $|u - vN| = 1$.

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

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

Theorem 7.4 extends Theorem 5 of [S93] to the additional requirement that u, v are squarefree. The latter is equivalent to the condition $e_1, \dots, e_n \in \{0, \pm 1\}$ of Lemma 7.1.

Theorem 7.4. *Assuming that 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 $\alpha > 2\beta + 2$.*

Proof. Let $\Psi(x, y)$ denote the number of integers in $[1, x]$ that are y -smooth. Then

$$\Psi(x, x^{1/z}) \geq x z^{-z+o(z)} \text{ for } x \geq 1 \text{ and } z \geq 3$$

is shown in [CEP83, Thm 3.1]. We adapt this result to the condition that u, v are squarefree. Let $\Psi^*(z, y)$ denote the number of squarefree integers in $[1, z]$ that are y -smooth. POMERANCE as cited in [Ad95] observed for $z = \ln x / (\alpha \ln \ln x)$, $\ln^\alpha x = (\ln x)^\alpha$ that

$$\Psi^*(x, \ln^\alpha x) \geq x z^{-z+o(z)}.$$

Here is a short proof. Note that $(\ln x)^\alpha = x^{1/z}$. We obviously have for $z' := \lfloor z \rfloor$

$$\begin{aligned} \Psi^*(x, \ln^\alpha x) &\geq \binom{\pi(\ln^\alpha x)}{z'} \approx \pi(\ln^\alpha x)^{z'} / z'! \\ &\approx x \left(\frac{e}{z' \alpha \ln \ln x} \right)^{z'} / \sqrt{2\pi z'} = x z'^{-z'+o(z')} = x z z^{+o(z)}, \end{aligned}$$

where we count the number of distinct selections of z' out of $\pi(\ln^\alpha x)$. We use that $\pi(n) = n / \ln n + O(n(\ln n)^{-2})$ holds by the prime number theorem for the number $\pi(n)$ of primes in $[2, n]$ and $z'! \approx (z'/e)^{z'} \sqrt{2\pi z'}$ by STIRLING's approximation.

Let $r = \ln N / \alpha \ln \ln N$, and thus $(\ln N)^\alpha = N^{1/r}$. By the assumption of the theorem and the lower bound on $\Psi^*(N^c, \ln^\alpha N)$ we get

$$\#M_{\alpha,c,N} \geq N^{c-1} (rc - r)^{-rc+r} (rc)^{-rc+o(r)},$$

$$\ln \#M_{\alpha,c,N} \geq (c-1) \ln N - \frac{\ln N(1+o(1))}{\alpha \ln \ln N} ((c-1) \ln(rc-r) + c \ln rc).$$

Here N^{c-1} counts the number of $u \leq N^c$ such that $|u - vN| = 1$ holds for $v = \lceil u/N \rceil$, and $(rc - r)^{-rc+r+o(r)}$, $(rc)^{-rc+o(r)}$ lower bound the portions of those v and u that are $(\ln N)^\alpha$ -smooth and squarefree. Hence for $\frac{\alpha}{\alpha-2\beta-2} < c \leq \ln N$ and $\alpha > 2\beta + 2$:

$$\begin{aligned} \ln \#M_{\alpha,c,N} &\geq c \ln N - \ln N - \frac{2c \ln N \ln rc}{\alpha \ln \ln N} (1 + o(1)) \\ &= c \ln N - \ln N - \frac{2c \ln N (\beta+1) \ln \ln N}{\alpha \ln \ln N} (1 + o(1)) \\ &\geq -\ln N + c \ln N (1 - \frac{2\beta+2}{\alpha}) (1 + o(1)) \geq \Theta(\ln N). \quad \square \end{aligned}$$

Finding relations (7.1) by CVP-solutions. By Lemma 7.1 the $(u, v) \in M_{\alpha,c,N}$ are associated with some $\mathbf{b} = \sum_{i=1}^n e_i \mathbf{b}_i \in \mathcal{L}(B)$ such that $\|\mathbf{b} - \mathbf{N}\|^2 \leq (2c-1) \ln N + O(|u - vN|^2)$ holds provided that $e_1, \dots, e_n \in \{0, \pm 1\}$.

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

Proof. Let $\mathbf{b}' = \sum_{i=1}^n e'_i \mathbf{b}_i \in \mathcal{L}(B)$ be the vector corresponding to some $(u', v') \in M_{\alpha,c,N}$, $u' = \prod_{e'_i > 0} p_i^{e'_i}$, $v' = \prod_{e'_i < 0} p_i^{-e'_i}$ such that $|u' - v'N| = 1$.

We have $N^{c-1}/2 < v' < N^{c-1}$ and thus $v' = \eta N^{c-1}$ with $\frac{1}{2} < \eta < 1$. The proof of Lemma 7.1 shows

$$\|\mathbf{b}' - \mathbf{N}\|^2 \leq (2c-1) \ln N + \eta^{-2} + O(1).$$

Then the lattice vector $\mathbf{b} \in \mathcal{L}(B)$ that is closest to \mathbf{N} also satisfies

$$\|\mathbf{b} - \mathbf{N}\|^2 \leq (2c - 1) \ln N + \eta^{-2} + O(1).$$

Consider the $(u, v) \in \mathbb{N}^2$ corresponding to \mathbf{b} . Theorem 7.2 shows $|u - vN| \leq p_n^{\frac{1}{\alpha} + o(1)}$. Hence $\mathbf{b} = \sum_{i=1}^n e_i \mathbf{b}_i \in \mathcal{L}(B)$ provides a relation (7.1). \square

Factoring N reduces by Theorem 7.5 to solving about n CVP's for $\mathcal{L}(B)$ for which $M_{\alpha, c, N} \neq \emptyset$. These CVP's minimize $\|\mathcal{L}(B) - \mathbf{N}\|$ for various $N' = N, Np_{n+j}$.

Theorem 7.6 (GSA). *If $M_{\alpha, c, N} \neq \emptyset$ and $\|\mathbf{b}_1\|^2 = O(2c \ln N)$ holds for $c = n = \dim \mathcal{L}$ then we can minimize $\|\mathcal{L}(B) - \mathbf{N}\|$ in polynomial time.*

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

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

Lemma 5.3 of [MG02] proves that $\lambda_1^2 \geq 2c \ln N - \Theta(1)$ (with $\Theta(1) = 0$ if the prime 2 is excluded from the prime basis). Hence $\|\mathcal{L} - \mathbf{N}\| = \lambda_1(1 + o(1))$.

Claim: $\lambda_1^2 = 2c \ln N + O(1)$ holds if $\frac{\alpha}{\alpha - 2\beta - 2} < c \leq (\ln N)^\beta$ and $\alpha > 2\beta + 2$.

[The proof of $M_{\alpha, c, N} \neq \emptyset$ by Theorem 7.4 also shows that there exist $u = \prod_{i \leq n} p_i^{e_i}$ and $v = \prod_{i \leq n} p_i^{e'_i}$ with $e_i, e'_i \in \{0, 1\}$ such that $u = \Theta(N^c)$, $|u - v| = O(1)$, $\gcd(u, v) = 1$. As in the proof of Lemma 7.1 we have

$$\begin{aligned} \|\sum_{i \leq n} (e_i - e'_i) \mathbf{b}_i\|^2 &= 2c \ln N + O(1) + N^{2c} \ln(u/v)^2 \\ &= 2c \ln N + O(|u - v|)^2, \end{aligned}$$

where $\ln(u/v) = \ln(1 + \frac{u-v}{v}) = \Theta(|u - v|N^{-c})$.]

Next we bound $rd(\mathcal{L})$. We set $c := n = (\ln N)^\alpha / (\alpha \ln \ln N)(1 + o(1))$ and get

$$\gamma_n(\det \mathcal{L})^{\frac{2}{n}} \geq \frac{(\ln N)^\alpha}{2e\pi} \frac{(\alpha - o(1)) \ln \ln N}{\alpha \ln \ln N} \cdot N^{2c/n} \approx N^2 \frac{(\ln N)^\alpha}{2e\pi} (1 + o(1)).$$

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

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

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

A gap towards polynomial time factoring. Theorem 7.6 holds for $c = n \approx (\ln N)^\alpha$ but $M_{\alpha, c, N} \neq \emptyset$ holds by Theorem 7.4 merely for smaller $c = (\ln N)^\beta$, $\beta < \alpha/2 - 1$.

The extended basis \bar{B} providing a nearly shortest vector. We extend the prime base by a prime \bar{p}_{n+1} of order N^c such that $|u - \bar{p}_{n+1}| = O(1)$ holds for a squarefree $(\ln N)^\alpha$ -smooth integer $u = \prod_i p_i^{e_i}$. Then $\|\sum_i e_i \mathbf{b}_i - \mathbf{b}_{n+1}\|^2 = 2c \ln N + O(1)$ holds for the additional basis vector \mathbf{b}_{n+1} corresponding to \bar{p}_{n+1} . Hence $\sum_i e_i \mathbf{b}_i - \mathbf{b}_{n+1}$ is a nearly shortest vector of $\mathcal{L}(\bar{B})$, $\bar{B} = [\mathbf{b}_1, \dots, \mathbf{b}_{n+1}]$. This construction is efficient, we 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{B} and a nearly shortest vector \mathbf{b} of $\mathcal{L}(\bar{B})$ can be found in

probabilistic polynomial time. A single (\bar{B}, \mathbf{b}) can be used to solve all CVP's for the factorization of all integers of the order of N . Other extensions \bar{B} can be computed in deterministic polynomial time. So we can factor integers without using random bits.

An integer prime number lattice. The real basis vectors $\mathbf{b}_1, \dots, \mathbf{b}_n, \mathbf{N}$ must in practice be replaced by short finite vectors such that Lemma 7.1 and Theorem 7.2 still hold under the replacement. Simply replace $N^c \ln p_i, N^c \ln N$ by their nearest integers $\lfloor N^c \ln p_i \rfloor, \lfloor N^c \ln N \rfloor$. Moreover, replace the diagonal entries $\sqrt{\ln p_i}$ of B by $\lceil 2^{\bar{c}} \sqrt{\ln p_i} \rceil$ for a suitable constant \bar{c} , e.g., $\bar{c} = 100$. Then the whole CVP computation is done for an integer basis matrix B' with entries of bit length $\lceil \log_2(N^c (\ln N)^\alpha) \rceil$ in the last column and $\lceil \bar{c} + \frac{\alpha}{2} \log_2(\ln N) \rceil$ in the diagonal. See also [S93], [Ad95].

History of the prime number lattice $\mathcal{L}(B)$. [S93] uses a different lattice $\mathcal{L}(B')$, where the diagonal elements $\sqrt{\ln p_i}$ of the basis matrix B are replaced by $\ln p_i$. ADLEMAN [Ad95] proposed the diagonal elements $\sqrt{\ln p_i}$ of B to translate the method of [S93] from the $\|\cdot\|_1$ -norm used in [S93] to the square norm.

8 Computing discrete logarithms for \mathbb{Z}_N^* , N prime, via CVP solutions

We reduce the problem of computing discrete logarithms for \mathbb{Z}_N^* with N prime to solving $(\ln N)^\alpha$, $\alpha > 4$, CVP's for the prime number lattice of section 7. We follow the discrete logarithm algorithm of [S93, section 5].

Let $g \in \mathbb{Z}_N^*$ be a generator of the cyclic group of units $\mathbb{Z}_N^* = \langle g \rangle$. As $|\mathbb{Z}_N^*| = N - 1$ the logarithm $\log_g y$ of $y \in \mathbb{Z}_N^*$ to base g is the integer $x \in \mathbb{Z}_{N-1}$ such that $y = g^x$.

We adapt the target vector \mathbf{N} for factoring N to the DL-problem of computing $x = \log_g y$. Consider the extended basis $\bar{B} = [\mathbf{b}_1, \dots, \mathbf{b}_{n+1}] \in \mathbb{R}^{(n+2) \times n+1}$ of section 7 and the target vector $\bar{\mathbf{N}} = (0, \dots, N^c \ln(\bar{N}))^t$ with $\bar{N} = N p_{n+j} / (g y)$. Again p_{n+j} runs over the next n primes $> (\ln N)^\alpha$ and g, y are represented by integers less than N .

As in section 7 we identify vectors $\mathbf{b} = \sum_{i=1}^{n+1} e_i \mathbf{b}_i \in \mathcal{L}(\bar{B})$ with $u = \prod_{e_i > 0} p_i^{e_i}$ and $v = \prod_{e_i < 0} p_i^{-e_i} \in \mathbb{Z}$. Adapting Theorems 7.2, 7.3 from B, \mathbf{N} to $\bar{B}, \bar{\mathbf{N}}$ shows the following

Lemma 8.1. *Let $c = \ln N + 2$ then $|u g y - v N p_{n+j}| \leq p_n^{\frac{1}{\alpha} + \delta + o(1)}$ holds if $\|\mathbf{b} - \bar{\mathbf{N}}\| = \|\mathcal{L} - \bar{\mathbf{N}}\|$ and if there exists $\mathbf{b}' = \sum_{i=1}^{n+1} e'_i \mathbf{b}_i \in \mathcal{L}(\bar{B})$ with $e'_i \in \{0, \pm 1\}$ such that the corresponding u', v' satisfy $|u' g y - v' N p_{n+j}| = 1$ and $\|\mathbf{b}' - \bar{\mathbf{N}}\|^2 = (2c - 1) \ln N + 2\delta \ln p_n - \ln(gy/p_{n+j}) + O(1)$.*

Following the proof of Theorem 7.4 we see that the vector \mathbf{b}' required in Lemma 8.1 exists for $c = 2 + \ln N$ and $\alpha > 4$ under the assumption of Theorem 7.4. The increment of c by 2, compared to Thm. 7.4, makes sure that u' is of order $N^{\ln N}$ and ranges over at least $N^{\ln N}$ integers. The CVP to minimize $\|\mathbf{b} - \bar{\mathbf{N}}\|$ for $\mathbf{b} \in \mathcal{L}(\bar{B})$ is polynomial time under GSA given a nearly shortest vector of $\mathcal{L}(\bar{B})$.

Computing the discrete logarithm from CVP-solutions. Let the CVP-solution $\mathbf{b} =$

$\sum_{i=1}^{n+1} e_i \mathbf{b}_i$ of $\|\mathbf{b} - \tilde{\mathbf{N}}\| = \|\mathcal{L}(\tilde{B}) - \tilde{\mathbf{N}}\|$ solve $|u g y - v N p_{n+j}| \leq p_n$. Taking \log_g -values on both sides of the prime factorization $u g y - v N p_{n+j} = \prod_{i=0}^{n+1} p_i^{e'_i}$, with $p_0 = -1$ and $\log_g -1 = (N-1)/2$, yields the linear equation

$$1 + \log_g y + \sum_{i=1}^{n+1} (e_i - e'_i) \log_g p_i = e'_0 \log_g(-1) \pmod{(N-1)} \quad (8.1)$$

in $n+2$ unknowns $\log_g p_i, \log_g y$. Note that $\log_g : \mathbb{Z}_N^* \rightarrow \mathbb{Z}_{N-1}$ is a group homomorphism, and the multiples of N like $v N p_{n+j}$ disappear under \log_g . Most likely we can determine $\log_g y$ from $n+2$ linearly independent equations (8.1).

Conclusion. The discrete logarithm $\log_g y$ of $y \in \mathbb{Z}_N^*$, N prime, can be computed under GSA in probabilistic polynomial time by solving $n+2$ polynomial time CVP's for $\mathcal{L}(\tilde{B})$ and various $\tilde{\mathbf{N}}$, $\tilde{N} = N p_{n+j}/(g y)$ for $n+1 = \dim \mathcal{L}(\tilde{B})$ and $\alpha > 4$.

Acknowledgment. I am indebted to Phong Nguyen for pointing out inconsistencies and mistakes in a prior version of this work. I like to thank G. Hanrot and D. Stehlé for adjusting and explaining the method of [HS07, section 4.1] and J. von zur Gathen, B. Lange, R. Lindner and M. Rückert for clarifying remarks.

References

- [Ad95] L.A. Adleman, Factoring and lattice reduction. Manuscript, 1995.
- [AEVZ02] E. Agrell, T. Eriksson, A. Vardy and K. Zeger, Closest point search in lattices. *IEEE Trans. on Inform. Theory*, **48** (8), pp. 2201–2214, 2002.
- [Aj96] M. Ajtai, Generating hard instances of lattice problems. In Proc. 28th Annual ACM Symposium on Theory of Computing, pp. 99–108, 1996.
- [AD97] M. Ajtai and C. Dwork, A public-key cryptosystem with worst-case / average-case equivalence. In Proc 29-th STOC, ACM, pp. 284–293, 1997.
- [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 Lovász 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. ECC, Report No. 5, 1998.
- [CEP83] E.R. Canfield, P. Erdős 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-Verlag 1998.
- [FP85] U. Fincke and M. Pohst, Improved methods for calculating vectors of short length in a lattice, including a complexity analysis. *Math. of Comput.*, **44**, pp. 463–471, 1985.
- [HHHW09] P. Hirschhorn, J. Hoffstein, N. Howgrave-Graham and W. Whyte, Choosing NTRU-Encrypt 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 attack 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://arxiv.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.
- [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. Odlyzko*, 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](http://www.mi.informatik.uni-frankfurt.de).
- [SE94] *C.P. Schnorr and M. Euchner*, Lattice basis reduction: Improved practical algorithms and solving subset sum problems. *Mathematical Programming* **66**, pp. 181–199, 1994. [//www.mi.informatik.uni-frankfurt.de](http://www.mi.informatik.uni-frankfurt.de).
- [SH95] *C.P. Schnorr and H.H. Hörner*, Attacking the Chor–Rivest cryptosystem by improved lattice reduction. In Proc. EUROCRYPT’95, LNCS 921, Springer-Verlag, pp. 1–12, 1995. [//www.mi.informatik.uni-frankfurt.de](http://www.mi.informatik.uni-frankfurt.de).
- [S03] *C.P. Schnorr*, Lattice reduction by sampling and birthday methods. Proc. STACS 2003: 20th Annual Symposium on Theoretical Aspects of Computer Science, LNCS 2007, Springer-Verlag, pp. 146–156, 2003. [//www.mi.informatik.uni-frankfurt.de](http://www.mi.informatik.uni-frankfurt.de)
- [S06] *C.P. Schnorr*, Fast LLL-type lattice reduction. *Information and Computation*, **204**, pp. 1–25, 2006. [//www.mi.informatik.uni-frankfurt.de](http://www.mi.informatik.uni-frankfurt.de)
- [S07] *C.P. Schnorr*, Progress on LLL and lattice reduction, Proceedings LLL+25, Caen, France, June 29–July 1, 2007, Final version to appear; [//www.mi.informatik.uni-frankfurt.de](http://www.mi.informatik.uni-frankfurt.de).

Received

Author information

✉

Email: schnorr@cs.uni-frankfurt.de