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

Claus Peter Schnorr

Fachbereich Informatik und Mathematik,
Goethe-Universität Frankfurt, PSF 111932,
D-60054 Frankfurt am Main, Germany.
schnorr@cs.uni-frankfurt.de

April 16, 2012, work in progress

Abstract. We analyze pruned enumeration algorithms for finding shortest and closest lattice vectors of low density lattices. The algorithm New Enum performs the stages of exhaustive enumeration of short / close lattice vectors in order of decreasing success rate. The lattice problems **SVP** and **CVP** can only have maximal complexity if the relative density $rd(\mathcal{L})$ of the lattice $\mathcal{L}$ is close to maximum 1. **SVP** and **CVP** are much easier if $rd(\mathcal{L})$ is moderately small. Integers N can be factored by solving $(\ln N)^{O(1)}$ **CVP**'s for a prime number lattice $\mathcal{L}$ of relative density $o(n^{-1/4})$, $n = \dim \mathcal{L}$. Under the questionable volume heuristics these **CVP**'s are solvable in polynomial time.

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

1 Introduction and surview

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. The New Enum algorithm for **SVP** / **CVP**, presented in section 3 / 5, 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 New Enum for **SVP** and a given basis $\mathbf{B} = [\mathbf{b}_1, ..., \mathbf{b}_n]$ for which all quotients $r_{i,i}/r_{i+1,i+1}$ of the lengths $r_{i,i} = \|\mathbf{b}_i^*\|$ of the orthogonalized vectors $\mathbf{b}_i^*$ coincide. This geometric series assumption GSA of [S03] approximately holds in practice for well reduced bases. Prop. 1 shows for bases satisfying GSA that New Enum finds a shortest lattice vector $\mathbf{b}$ under the volume heuristics in polynomial time (without proving that $\mathbf{b}$ is shortest) if the *relative density* $rd(\mathcal{L})$ of $\mathcal{L}$ satisfies $rd(\mathcal{L}) \le n^{-1/4}(\lambda_1\sqrt{e\pi}/\|\mathbf{b}_1\|)^{1/2}$ where λ_1 is the minimal length of nonzero lattice vectors and $rd(\mathcal{L})$ is defined by $\lambda_1 = rd(\mathcal{L})\,\gamma_n^{1/2}(\det \mathcal{L})^{1/n}$ and the Hermite constant γ_n. Theorem 1 analyses New Enum without the volume heuristics.

Section 5 extends New Enum and its analysis to **CVP**. Cor. 1, translates Theorem 1 from **SVP** to **CVP** and shows that the **CVP** for $\mathcal{L}$ and a the target vector $\mathbf{t} \in \mathrm{span}(\mathcal{L})$ is solved in time $2^{O(n)}$ and linear space if $rd(\mathcal{L}) = O(n^{-1/2})$, $\|\mathcal{L} - \mathbf{t}\| = O(\lambda_1)$ and $\mathbf{b}_1$ is a nearly shortest vector of $\mathcal{L}$. Cor. 3 shows under the volume heuristics that, given a random target vector $\mathbf{t}$, a closest lattice vector can be found, without proving optimal closeness, in polynomial time if $rd(\mathcal{L}) \le n^{-1/4}(\lambda_1\sqrt{e\pi}/\|\mathbf{b}_1\|)^{1/2}$, $\|\mathcal{L} - \mathbf{t}\| = O(\lambda_1)$ and if the found closest vector behaves randomly (CA).

Section 6 studies the relative density $rd(\mathcal{L})$ of various cryptographic lattices. The NTRU-lattices of [HHHW09] satisfy $rd(\mathcal{L}) < (2n)^{-1/4}$. Moreover $rd(\mathcal{L}) \le n^{-1}\ln^{-O(1)} n$ holds for the lattices of Ajtai, Dwork [AD97]. Ajtai's [Aj96] worst case / average case equivalence of arbitrary n^c-unique **SVP**'s and **SVP** only covers unique **SVP** instances that may be easy in view of Prop. 1.

Section 7 studies factoring integers N by generating relations modulo N between smooth integers from **CVP** solutions for the prime number lattice. These **CVP**'s are solvable in polynomial time assuming GSA, the volume heuristics and standard assumptions on the distribution of smooth integers. Here we use a prime number lattice of relative density $\mathcal{L}$ such that $rd(\mathcal{L}) = o(n^{-1/4})$.

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

2 Lattices

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

Let $\lambda_1, \ldots, \lambda_n$ 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 nonzero 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 $\mathbf{B} = \mathbf{QR} \in \mathbb{R}^{m \times n}$, $R = [r_{i,j}]_{1 \le i,j \le n} \in \mathbb{R}^{n \times n}$ be the unique **QR**-factorization: $\mathbf{Q} \in \mathbb{R}^{m \times n}$ is isometric (with pairwise orthogonal column vectors of length 1) and $\mathbf{R} \in \mathbb{R}^{n \times n}$ is upper-triangular with positive diagonal entries $r_{i,i}$. The **QR**-factorization also provides the Gram-Schmidt coefficients $\mu_{j,i} = r_{i,j}/r_{i,i}$ which are rational for integer matrices $\mathbf{B}$. The orthogonal projection $\mathbf{b}_i^*$ of $\mathbf{b}_i$ in $\text{span}(\mathbf{b}_1, ..., \mathbf{b}_{i-1})^\perp$ has length $r_{i,i} = \|\mathbf{b}_i^*\|$.

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

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

Obviously, LLL-bases satisfy $r_{i,i}^2 \le \alpha\, r_{i+1,i+1}^2$ 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. $\alpha^{-i+1} \le \|\mathbf{b}_i\|^2 \lambda_i^{-2} \le \alpha^{n-1}$ for $i = 1, ..., n$, **4.** $\|\mathbf{b}_1\|^2 \le \alpha^{\frac{n-1}{2}} (\det \mathcal{L})^{2/n}$.

A basis $\mathbf{B} = \mathbf{QR} \in \mathbb{R}^{m \times n}$ is an HKZ-*basis* (HERMITE, KORKINE, ZOLOTAREFF) if $|r_{i,j}|/r_{i,i} \le \frac{1}{2}$ for all $j > i$, and if each diagonal entry $r_{i,i}$ of $\mathbf{R} = [r_{i,j}] \in \mathbb{R}^{n \times n}$ is minimal under all transforms of $\mathbf{B}$ to $\mathbf{BT}$, $\mathbf{T} \in \text{GL}_n(\mathbb{Z})$ that preserve $\mathbf{b}_1, ..., \mathbf{b}_{i-1}$.

A basis $\mathbf{B} = \mathbf{QR} \in \mathbb{R}^{m \times n}$. $\mathbf{B} = [r_{i,j}]$ is BKZ-*basis* for block length k [SE94] if the matrices $[r_{i,j}]_{h \le i,j < h+k} \in \mathbb{R}^{k \times k}$ form HKZ-bases for $h = 1, ..., n-k+1$.

A famous problem is the shortest vector problem (**SVP**): Given a basis of $\mathcal{L}$ find a shortest nonzero 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 $\|\mathbf{t} - \mathbf{b}'\| = \|\mathbf{t} - \mathcal{L}\| =_{def} \min\{\, \|\mathbf{t} - \mathbf{b}\| \mid \mathbf{b} \in \mathcal{L}\,\}$.

Previous **SVP**-algorithms solve **SVP** by a full exhaustive search, disregard the success rate of stages, and prove to have found a shortest nonzero lattice vector. Our novel **SVP**-algorithm NEW ENUM finds a shortest lattice vector $\mathbf{b}$ rather fast, without proving $\|\mathbf{b}\| = \lambda_1$, by performing the stages in order of decreasing success rate. Its efficiency 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 all lattices $\mathcal{L}'$ of $\dim \mathcal{L} = \dim \mathcal{L}'$ and $\det \mathcal{L} = \det \mathcal{L}'$.

Clearly $0 < rd(\mathcal{L}) \le 1$ 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 $n = 1, ..., 8$ and $n = 24$.

3 A novel enumeration of short lattice vectors

We first outline the novel **SVP**-algorithm based on the success rate of stages. NEW ENUM improves the algorithm ENUM of [SE94, SH95]. We recall ENUM and present NEW ENUM as a modification that essentially performs all stages of ENUM in decreasing order of success rates.

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

The success rate of stages. The vector $\mathbf{b} = \sum_{i=t}^n u_i \mathbf{b}_i \in \mathcal{L}$ and $A \ge \lambda_1^2$ are given at stage $(u_t, ..., u_n)$ of ENUM [SH95]. That stage calls the substages $(u_{t-1}, ..., u_n)$ such that $\|\pi_{t-1}(\sum_{i=t-1}^n u_i \mathbf{b}_i)\|^2 \le A$. Note that $\|\sum_{i=1}^n u_i \mathbf{b}_i\|^2 = \|\zeta_t + \sum_{i=1}^{t-1} u_i \mathbf{b}_i\|^2 + \|\pi_t(\mathbf{b})\|^2$. where $\zeta_t := \mathbf{b} - \pi_t(\mathbf{b}) \in$

span $\mathcal{L}_t$ is $\mathbf{b}$'s orthogonal projection in span $\mathcal{L}_t$. Stage $(u_t, ..., u_n)$ and its substages exhaustively enumerate the intersection $\mathcal{B}_{t-1}(\zeta_t, \rho_t) \cap \mathcal{L}_t$ for the sphere $\mathcal{B}_{t-1}(\zeta_t, \rho_t) \subset \operatorname{span} \mathcal{L}_t$ 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

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

Here $\operatorname{vol} \mathcal{B}_{t-1}(\zeta_t, \rho_t) = V_{t-1} \rho_t^{t-1}$, $V_{t-1} = \pi^{\frac{t-1}{2}} / (\frac{t-1}{2})! \approx (\frac{2e\pi}{t-1})^{\frac{t-1}{2}} / \sqrt{\pi(t-1)}$ 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 $\zeta_t \mod \mathcal{L}_t$ is uniformly distributed the expected size of this intersection satisfies $\mathrm{E}_{\zeta_t}[\, \#\big(|\mathcal{B}_{t-1}(\zeta_t, \rho_t) \cap \mathcal{L}_t\big) \,] = \beta_t$. 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 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 $\beta_t \geq 2^{-s} t$ and collects during this process the stages with $\beta_t < 2^{-s} t$ in the list L. Thereafter NEW ENUM performs the stages of L with $\beta_t \geq 2^{-s-1} t$. The test $\beta_t \geq 2^{-s} t$ gives priority to stages of small t, stages of large t require a higher success rate. The analysis in section 4 is independent of the factor t in $\beta_t < 2^{-s} t$.

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

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

Outline of New Enum

`INPUT` BKZ-basis $\mathbf{B} = \mathbf{QR} \in \mathbb{Z}^{m \times n}$, $R = [r_{i,j}] \in \mathbb{R}^{n \times n}$ for block length 20,
`OUTPUT` a sequence of $\mathbf{b} \in \mathcal{L}(\mathbf{B})$ of decreasing length terminating with $\|\mathbf{b}\| = \lambda_1$.

1. $s := 2^{20}$, $L := \emptyset$, $A := \frac{n}{4} (\det \mathbf{B}^t \mathbf{B})^{1/n}$ (we call s the *level*)
2. *Perform algorithm* ENUM *of [SE94, SH95], delaying stages with* $\beta_t < 2^{-s} t$: Upon entry of stage $(u_t, ..., u_n)$ compute β_t. If $\beta_t < 2^{-s} t$ store information about $(u_t, ..., u_n)$ in the list L of *delayed stages*. Otherwise perform stage $(u_t, ..., u_n)$ on level s, and as soon as some $\mathbf{b} \in \mathcal{L} - \mathbf{0}$ of length $\|\mathbf{b}\|^2 \leq A$ has been found, give out $\mathbf{b}$ and set $A := \|\mathbf{b}\|^2 - 1$.
3. $s := s + 1$, perform the stages $(u_t, ..., u_n)$ of L with $\beta_t \geq 2^{-s} t$. Delay the occuring substages $(u_{t'}, ..., u_t, ..., u_n)$ with $\beta_{t'} < 2^{-s} t'$ and store them in L.
4. `IF` $L \neq \emptyset$ `THEN GO TO 3 ELSE` *terminate* .

Running in linear space. If instead of storing the list L we restart NEW ENUM in step 3 on the level $s+1$ then NEW ENUM runs in linear space and its running time increases at most by a factor n.

Practical optimization. NEW ENUM computes $\mathbf{R}$, $\beta_t, V_t, \rho_t, c_t$ in floating point and $\mathbf{b}$, $\|\mathbf{b}\|^2$ in exact arithmetic. The final output $\mathbf{b}$ has length $\|\mathbf{b}\| = \lambda_1$, but this is only known when the more expensive final search does not find a vector shorter than $\mathbf{b}$.

Reason of efficiency. For short vectors $\mathbf{b} = \sum_{i=1}^n u_i \mathbf{b}_i \in \mathcal{L}$ the stages $(u_t, ..., u_n)$ have large success rate β_t. If $\mathbf{b}$ is short then so are the projections $\pi_t(\mathbf{b})$, on average $\|\pi_t(\mathbf{b})\|^2 \approx \frac{n-t+1}{n} \|\mathbf{b}\|^2$. Then $\rho_t^2 = A - \|\pi_t(\mathbf{b})\|^2$ and β_t are large. New Enum tends to output very short lattice vectors $\mathbf{b}$ first.

Consider the case $A = \lambda_1^2$. Prior to finding the shortest lattice vector $\mathbf{b}' = \sum_{i=1}^n u_i' \mathbf{b}_i$ NEW ENUM essentially performs only stages $(u_t, ..., u_n)$ of success rate $\beta_t = V_{t-1} \rho_t^{t-1} / \det \mathcal{L}_t$ where on average $\rho_t^2 = \lambda_1^2 - \|\pi_t(\mathbf{b}_t')\|^2 \approx \frac{t-1}{n} \lambda_1^2$ since on average $\|\pi_t(\mathbf{b}')\|^2 \approx \frac{n-t+1}{n} \lambda_1^2$. While ENUM calls nearly all stages $(u_t, ..., u_n)$ of $\beta_t > 0$ NEW ENUM only calls about a $(\frac{n-t+1}{n})^{\frac{n-t+1}{2}}$ fraction of them prior to finding $\mathbf{b}'$ and delays the rest to be performed later than $(u_t', ..., u_n')$.

NEW ENUM is particularly fast for small λ_1. The size of its search space is proportional to λ_1^n, and is by Prop. 1 heuristically polynomial if $rd(\mathcal{L}) = o(n^{-1/4})$. Having found $\mathbf{b}'$ NEW ENUM proves $\|\mathbf{b}'\| = \lambda_1$ in exponential time by a complete exhaustive enumeration.

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

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

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

Given $u_{t+1}, ..., u_n$ 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 $|u_t + y_t|$, recursively as $u_t := \lceil -y_t \rfloor$, $u_t := \operatorname{next}(u_t, -y_t)$:

$$\lceil -y_t \rfloor,\ \lceil -y_t \rfloor - \sigma_t,\ \lceil -y_t \rfloor + \sigma_t,\ \lceil -y_t \rfloor - 2\sigma_t,\ \lceil -y_t \rfloor + 2\sigma_t, \cdots$$

for $\sigma_t := sign(\lceil -y_t \rfloor + y_t) \in \{\pm 1\}$, $sign(0) := 1$, where $\lceil r \rfloor =_{def} \lceil r - 0.5 \rceil$ denotes the nearest integer

to $r \in \mathbb{R}$. The iteration $u_t := next(u_t, -y_t)$ increases or preserves $|u_t + y_t|$ and $c_t(u_t, ..., u_n)$, decreases or preserves ρ_t and β_t so that ENUM performs the stages $(u_t, ..., u_n)$ for fixed $u_{t+1}, ..., u_n$ in order of increasing $c_t(u_t, ..., u_n)$ 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 center $\zeta_t = \mathbf{b} - \pi_t(\mathbf{b}) = \sum_{i=t}^{n} u_i(\mathbf{b}_i - \pi_t(\mathbf{b}_i)) \in \text{span}(\mathcal{L}_t)$ changes continously within NEW ENUM. The volume heuristics holds on average if $\zeta_t \mod \mathcal{L}_t$ distributes nearly uniformly.

Algorithm Enum [SH95]

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

1. FOR $i = 1, ..., n$ DO $c_i := u_i := y_i := 0$
   $u_1 := 1,\ t := t_{max} := 1,\ \bar{c}_1 := c_1 := \|\mathbf{b}_1\|^2$. ($c_t = c_t(u_t, ..., u_n)$ *always holds for the current* t, $\bar{c}_1$ *is the current minimum of* c_1)
2. WHILE $t \leq n$ #*perform stage* $(u_t, ..., u_n)$:
   $c_t := c_{t+1} + (u_t + y_t)^2 r_{t,t}^2$
   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 $t := t - 1,\ y_t := \sum_{i=t+1}^{t_{max}} u_i r_{t,i}/r_{t,t},\ u_t := \lceil -y_t \rfloor$
   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 **b**

New Enum for SVP

INPUT BKZ-basis $\mathbf{B} = \mathbf{QR} \in \mathbb{Z}^{m \times n}$, $R = [r_{i,j}] \in \mathbb{R}^{n \times n}$ for block length 20,
OUTPUT a sequence of $\mathbf{b} \in \mathcal{L}(\mathbf{B})$ such that $\|\mathbf{b}\|$ decreases to λ_1.

1. $L := \emptyset,\ t := t_{max} := s := 2^{20},$ FOR $i = 1, ..., n$ DO $c_i := u_i := y_i := 0$, $u_1 := 1$,
   $c_1 := r_{1,1}^2$, $A := \frac{n}{4}(\det \mathbf{B}^t B)^{1/n}$ ($c_t = c_t(u_t, ..., u_n)$ *always holds for the current* t)
2. WHILE $t \leq n$ #*perform stage* $(u_t, ..., u_n)$:
   $c_t := c_{t+1} + (u_t + y_t)^2 r_{t,t}^2$,
   IF $c_t > A$ THEN GO TO 2.1,
   $\rho_t := (A - c_t)^{1/2},\ \beta_t := V_{t-1}\rho_t^{t-1}/(r_{1,1} \cdots r_{t-1,t-1})$,
   IF $t = 1$ THEN [$\mathbf{b} := \sum_{i=1}^{n} u_i \mathbf{b}_i$,
   IF $\|\mathbf{b}\|^2 < A$ THEN output **b**, $A := \|\mathbf{b}\|^2 - 1,$ GO TO 2],
   IF $\beta_t \geq 2^{-s} t$ THEN [$t := t - 1,\ y_t := \sum_{i=t+1}^{t_{max}} u_i r_{t,i}/r_{t,t}, u_t := \lceil -y_t \rfloor$,
   $\sigma_t := sign(u_t + y_t),\ \nu_t := 1,$ GO TO 2]
   ELSE store $(u_t, ...u_n, y_t, c_t, \sigma_t, \nu_t)$ in L.
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. $s := s + 1,$ perform all delayed stages $(u_t, ..., u_n, y_t, c_t, \sigma_t, \nu_t)$ of L on level s and delete them. Delay new stages with $\beta_{t'} < 2^{-s} t'$, $t' \leq t$ and store $(u_{t'}, ..., \nu_{t'})$ in L.
4. IF $L \neq \emptyset$ THEN GO TO 3 ELSE terminate.

Performing in step 3 a delayed stage $(u_t, ..., u_n, y_t, c_t, \sigma_t, \nu_t)$ means to restart the algorithm in step 2 with that information. The recursion initiated by this restart does not perform any stages $(u_{t"}, ..., u_n)$ with $t" > t$. These stages have already been performed. Therefore, within step 2.1 the running t-value t' must be restricted not to surpass by the t-value at the restart.

4 Analysis of pruned Enum for SVP and lattices of low density

We first study in Proposition 1 the time to find an **SVP**-solution $\mathbf{b}'$ without proving $\lambda_1 = \|\mathbf{b}'\|$. Finding an unproved shortest vector $\mathbf{b}'$ is easier than proving $\|\mathbf{b}'\| = \lambda_1$. NEW ENUM finds an

unproved shortest lattice vector $\mathbf{b}'$ in polynomial time under the following four assumptions:

- the given lattice basis $\mathbf{B} = [\mathbf{b}_1, ..., \mathbf{b}_n]$ and the relative density $rd(\mathcal{L})$ of $\mathcal{L}(\mathbf{B})$ satisfy $rd(\mathcal{L}) \le n^{-\frac{1}{4}}(\lambda_1\sqrt{e\pi}/\|\mathbf{b}_1\|)^{\frac{1}{2}}$, i.e., either $\mathbf{b}_1$ or $rd(\mathcal{L})$ is very small.

SA: NEW ENUM finds a shortest lattice vector $\mathbf{b}'$ of $\mathcal{L}$ such that $\|\pi_t(\mathbf{b}')\|^2 \lesssim \frac{n-t+1}{n}\lambda_1^2$ for all t.

- the volume heuristic estimation $\mathcal{M}_t^\rho := |\mathcal{B}_{n-t+1}(\mathbf{0}, \rho_t) \cap \pi_t(\mathcal{L})| \approx \frac{V_{n-t+1}\rho_t^{n-t+1}}{\det \pi_t(\mathcal{L})}$ for $\rho_t^2 = \frac{n-t+1}{n}\lambda_1^2$.

GSA: The basis $\mathbf{B} = \mathbf{QR} = \mathbf{Q}[r_{i,j}]$ satisfies $r_{i,i}^2/r_{i-1,i-1}^2 = q$ for $i = 2, ..., n$ for some $q > 0$

These are some sensitive points in these assumptions. No polynomial time algorithm is known that finds a nonzero vector $\mathbf{b}_1 \in \mathcal{L}$ such that $\|\mathbf{b}_1\|/\lambda_1 = n^{O(1)}$. Prop. 1 does not solve **SVP** in polynomial time unless $rd(\mathcal{L})$ is so small that already the LLL-algorithm solves **SVP** in polynomial time. This problem changes favorably for the translation of Prop. 1 from **SVP** to **CVP** in section 5. Many lattices $\mathcal{L}$, like the prime number lattice, can easily be extended by a vector of length $\lambda_1(\mathcal{L})$. This helps to solve **CVP**'s efficiently. Moreover, the volume heuristics underestimates the size of $\mathcal{B}_{n-t+1}(\mathbf{0}, \rho_t) \cap \pi_t(\mathcal{L})$ as the ball $\mathcal{B}_{n-t+1}(\mathbf{0}, \rho_t)$ is centered at the origin $\mathbf{0}$. The volume heuristics provably holds on the average for the **CVP** of minimizing $\|\mathbf{b} - \mathbf{t}\|$ for $\mathbf{b} \in \mathcal{L}(\mathbf{B})$ and a given random $\mathbf{t} \in \text{span}(\mathcal{L})$. But random $\mathbf{t}$ have large distance to the lattice which slows down the **CVP**-algorithm.

Remarks. **1.** If $q \ge 1$ holds in GSA the basis $\mathbf{B}$ satisfies $\|\mathbf{b}_i\| \le \frac{1}{2}\sqrt{i+3}\,\lambda_i$ for all i and $\|\mathbf{b}_1\| = \lambda_1$. Therefore, $q < 1$ unless $\|\mathbf{b}_1\| = \lambda_1$. GSA means that the reduction of the basis is "locally uniform". GSA should approximately hold in practice for lattices without particular structure as all quotients $r_{i,i}/r_{i+1,i+1}$ of well reduced bases nearly coincide on the average. It is easier to work with the idealized property that all $r_{i,i}/r_{i-1,i-1}$ are equal. [BL05] studies "nearly equality". GSA has been used in [S03, NS06, GN08, S07, N10] and in the security analysis of NTRU in [H07, HHHW09].

2. The assumption SA is supported by a fact proven in the full paper of [GNR10]:

$$\mathbf{Pr}[\,\|\pi_t(\mathbf{b}')\|^2 \le \tfrac{n-t+1}{n}\lambda_1^2 \text{ for } t = 1, ..., n\,] = \tfrac{1}{n} \qquad \text{holds for random } \mathbf{b}' \in \mathcal{B}_n(\mathbf{0}, \lambda_1).$$

The probability $1/n$ increases by iterating the search for a shortest lattice vector by statistical independent trials via permuted bases.

3. Failings of the volume heuristics. For the lattice $\mathbb{Z}^n$ we have for any $a = \Theta(1)$ and $n \ge n_0(a)$:

$$\#\{\mathbf{x} \in \mathbb{Z}^n \,|\, ||\mathbf{x}||^2 \le an\} \ge \left(2e\sqrt{n/a}\right)^{\sqrt{an}} = n^{\Theta(\sqrt{n})},$$

whereas the volume heuristics estimates this cardinality to $O(1)$ for $a \le \frac{1}{2e\pi}$, also see Figure 1 of [MO90]. [GN08] reports that extensive experiments on high density random lattices show only negligible errors of the volume heuristics. The situation for low density lattices as $\mathcal{L} = \mathbb{Z}^n$ and small radius $\rho_t \ll \sqrt{n}\,\lambda_1$ is less clear.

4. *A trade-off* between $\|\mathbf{b}_1\|/\lambda_1$ and $rd(\mathcal{L})$ under GSA. B. LANGE observed that

$$\|\mathbf{b}_1\|/\lambda_1 = \|\mathbf{b}_1\|/(rd(\mathcal{L})\gamma_n^{1/2}\det(\mathcal{L})^{\frac{1}{n}}) = q^{\frac{1-n}{4}}/(rd(\mathcal{L})\gamma_n^{1/2}).$$

Therefore $rd(\mathcal{L})\,\gamma_n^{1/2}\,\|\mathbf{b}_1\|/\lambda_1 \le 1$ implies under GSA that $q \ge 1$ and thus $\|\mathbf{b}_1\| = \lambda_1$. Hence the trade-off implies $rd(\mathcal{L})\gamma_n^{1/2}\,\|\mathbf{b}_1\|/\lambda_1 > 1$ unless $\|\mathbf{b}_1\| = \lambda_1$. Moreover, solving SVP with approximation factor $1/(rd(\mathcal{L})\,\gamma_n^{1/2})$ and a basis satisfying GSA already solves SVP exactly.

Also this trade-off implies $n^{\frac{1}{2}+b}rd(\mathcal{L}) > \|\mathbf{b}_1\|/(\det\mathcal{L})^{\frac{1}{n}} = q^{\frac{1-n}{4}} > 1$ for $q < 1$ and $n \ge n_0$ due to $\gamma_n < \frac{n}{e\pi}$ [KL78]. This shows that the time bound of Theorem 1 is at best exponential $2^{O(n)}$.

All our time bounds must be multiplied by the work load per stage, a modest polynomial factor covering the steps performed at stage $(u_1, ..., u_n)$ before going to a subsequent stage.

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

Proof. Let $\mathbf{b}' = \sum_{j=1}^n u_i'\mathbf{b}_i$ be the shortest vector found by NEW ENUM and let $\mathcal{M}_t^\rho$ be the number of stages $(u_t, ..., u_n)$ that precede $(u_t', ..., u_n')$ in NEW ENUM's enumeration. We use the following

Simplifying assumption.(see the proof of Theorem 1) We assume that NEW ENUM performs stage $(u'_t, ..., u'_n)$ prior to all stages of success rate $\beta_t < \beta'_t$, i.e., $\rho_t < \rho'_t := (A - \|\pi_t(\mathbf{b}')\|^2)^{1/2}$. Without this assumption the time bound increases, under reasonable heuristics, at most by a constant factor. The simplifying assumption, the volume heuristics and SA show for $\|\pi_t(\mathbf{b}')\|^2 \le \rho_t^2 = \frac{n-t+1}{n}\lambda_1^2$:

$$\begin{aligned}\mathcal{M}_t^\rho = \#\mathcal{B}_{n-t+1}(\mathbf{0}, \rho_t) \cap \pi_t(\mathcal{L}) &\le (\sqrt{\tfrac{n-t+1}{n}}\,\lambda_1)^{n-t+1} V_{n-t+1}/(r_{t,t}\cdots r_{n,n}) \\ &< \big(\tfrac{\sqrt{2e\pi}\lambda_1}{\sqrt{n}}\big)^{n-t+1}/(r_{t,t}\cdots r_{n,n}).\end{aligned}$$

We used Stirling's approximation for V_{n-t+1}. (attention: the volume heuristics underestimates $\#\mathcal{B}_{n-t+1}(\mathbf{0}, \rho_t) \cap \pi_t(\mathcal{L})$ for the center $\mathbf{0}$ and small radius ρ_t.)
Moreover GSA and $\|\mathbf{b}_i^*\| = \|\mathbf{b}_1\| q^{\frac{i-1}{2}}$ yield

$$(r_{t,t}\cdots r_{n,n}) = \det \pi_t(\mathcal{L}) = \|\mathbf{b}_1\|^{n-t+1} q^{\sum_{i=t-1}^{n-1} i/2}.$$

We get from $q^{\frac{n-1}{2}} = \frac{(\det \mathcal{L})^{\frac{2}{n}}}{\|\mathbf{b}_1\|^2} = \frac{\lambda_1^2}{\gamma_n rd(\mathcal{L})^2}\frac{1}{\|\mathbf{b}_1\|^2}$ and $\gamma_n \le \frac{n}{e\pi}$ for $n \ge n_0$ [KL78] that

$$\begin{aligned}\mathcal{M}_t^\rho &\le \big(\tfrac{\lambda_1}{\|\mathbf{b}_1\|}\sqrt{\tfrac{2e\pi}{n}}\big)^{n-t+1}\big(\sqrt{\tfrac{n}{e\pi}}\, rd(\mathcal{L})\,\tfrac{\|\mathbf{b}_1\|}{\lambda_1}\big)^{n-\frac{(t-1)(t-2)}{n-1}} \\ &= rd(\mathcal{L})^{n-\frac{(t-1)(t-2)}{n-1}}\, 2^{\frac{n-t+1}{2}}\big(\sqrt{\tfrac{n}{e\pi}}\tfrac{\|\mathbf{b}_1\|}{\lambda_1}\big)^{\frac{t-1}{n-1}(n-t+1)}\end{aligned}$$

(The factor $2^{\frac{2-t+1}{2}}$ disappears if γ_n is close to the Minkowski lower bound $\gamma_n \ge \frac{n+\ln n}{2e\pi}$.) Evaluating this upper bound at $rd(\mathcal{L}) = n^{-\frac{1}{4}}(\lambda_1\sqrt{e\pi}/\|\mathbf{b}_1\|)^{\frac{1}{2}}$ yields

$$\begin{aligned}\mathcal{M}_t^\rho &\le \big(\sqrt{\tfrac{e\pi}{n}}\tfrac{\|\mathbf{b}_1\|}{\lambda_1}\big)^{\frac{n}{2}-\frac{1}{2}\frac{(t-1)(t-2)}{n-1}}\, 2^{\frac{n-t+1}{2}}\big(\sqrt{\tfrac{n}{e\pi}}\tfrac{\|\mathbf{b}_1\|}{\lambda_1}\big)^{\frac{t-1}{n-1}(n-t+1)} \\ &= n^{-\frac{n}{4}+\frac{1}{4}\frac{(t-1)(t-2)}{n-1}+\frac{1}{2}\frac{t-1}{n-1}(n-t+1)} 2^{\frac{n-t+1}{2}}\big(\tfrac{\lambda_1\sqrt{e\pi}}{\|\mathbf{b}_1\|}\big)^{\frac{n}{2}-\frac{1}{2}\frac{(t-1)(t-2)}{n-1}-\frac{t-1}{n-1}(n-t+1)} \\ &= n^{-\frac{n}{4}+\frac{t-1}{4}\frac{2n-1}{n-1}} 2^{\frac{n-t+1}{2}}\big(\tfrac{\lambda_1\sqrt{e\pi}}{\|\mathbf{b}_1\|}\big)^{\frac{n}{2}-\frac{t-1}{2}\frac{2n-t}{n-1}} = \big(\tfrac{\lambda_1\sqrt{e\pi}}{\sqrt{n}\,\|\mathbf{b}_1\|}\big)^{\frac{n}{2}-\frac{t-1}{2}\frac{2n-t}{n-1}}.\end{aligned}$$

The upper bound on $\mathcal{M}_t^\rho$ takes its maximum $2^{1/2}$ at $t = n$. This proves the theorem. □

Note that errors of the volume heuristics are negligible if t is close to n because then the dimension of the lattice $\pi_t(\mathcal{L})$ is small. On the other hand, if t is small then $\rho_t = \sqrt{\frac{n-t+1}{n}}\lambda_1$ is large which also reduces the errors of the volume heuristics. Note that $\mathcal{M}_t$ is already polynomial in n for $t = \frac{n}{2}$ if $rd(\mathcal{L}) \le n^{\frac{-1}{6-\varepsilon}}(\lambda_1\sqrt{e\pi}/\|\mathbf{b}_1\|)^{\frac{1}{2}}$ for some $\varepsilon > 0$ which allows larger $rd(\mathcal{L})$ then Prop. 1.

Theorem 1. *Given a lattice basis* $\mathbf{B} \in \mathbb{Z}^{m\times n}$ *satisfying GSA and* $\|\mathbf{b}_1\| \le \sqrt{e\pi}\, n^b\, \lambda_1$ *for some* $b \ge 0$, ENUM *and* NEW ENUM *solve* **SVP** *and prove to have found a solution in time* $2^{O(n)}(n^{\frac{1}{2}+b}rd(\mathcal{L}))^{\frac{n+1}{4}}$.

The running time of Theorem 1 is maximal, under and without SA, for $t = 1$ while under the volume heuristics it is by the proof of Prop. 1 maximal for $t = n$. The time bound of Theorem 1 is at best $2^{O(n)}$, namely if $rd(\mathcal{L}) = O(\gamma_n^{-\frac{1}{2}}\lambda_1/\|\mathbf{b}_1\|)$ which is close to the point where $\|\mathbf{b}_1\| = \lambda_1$ holds under GSA. However, the translation of Theorem 1 from **SVP** to **CVP** in Cor. 1 of section 5 gives an **CVP**-algorithm that solves many important **CVP**-problems in time $2^{O(n)}$.

Proof. NEW ENUM essentially performs stages in decreasing order of the success rate β_t. We denote $\mathbf{b}' = \sum_{i=1}^n u'_i\mathbf{b}_i \in \mathcal{L}$ NEW ENUM's **SVP**-solution. Let β'_t denote the success rate of stage $(u'_t, ..., u'_n)$. NEW ENUM performs stage $(u'_t, ..., u'_n)$ prior to all stages $(u_t, ..., u_n)$ of success rate $\beta_t \le \frac{1}{2}\beta'_t$.

Simplifying assumption. We assume that NEW ENUM performs stage $(u'_t, ..., u'_n)$ prior to all stages of success rate $\beta_t < \beta'_t$, i.e., $\rho_t < \rho'_t := (A - \|\pi_t(\mathbf{b}')\|^2)^{1/2}$. Without this assumption the time bound of Theorem 1 increases, under reasonable heuristics, at most by a constant factor. For this we guess $A > \lambda_1^2$ such that $A \approx \lambda_1^2$. Then $\mathcal{M}_t$ defined below is under the volume heuristics maximal for $t \approx \frac{n}{2}$. If stage $(u_t, ..., u_n)$ with $t \approx \frac{n}{2}$ has success rate $\beta_t \approx \frac{1}{2}\beta'_t$ then most likely $\|\pi_t(\sum_{\mathbf{i=t}}^{\mathbf{n}} \mathbf{u_i}\mathbf{b_i})\|^2 \approx 2^{4/n}||\pi_t(\mathbf{b}')||^2 \approx 2^{4/n}\frac{1}{2}\lambda_1^2$, hence $\operatorname{vol}\mathcal{B}_{n-t+1}(\mathbf{0}, \|\pi_t(\mathbf{b}')\|)/\operatorname{vol}\mathcal{B}_{n-1+1}(\mathbf{0}, \|\pi_t(\mathbf{b})\|) = \Theta(1)$.

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

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

In fact NEW ENUM enumerates $\frac{1}{2}\mathcal{M}_t$ stages $(u_t,...,u_n)$ since $u_N>0$ holds for the last nonzero u_N. Under the simplifying assumption $\mathcal{M}_t$ covers the stages that precede $(u'_t,...,u'_n)$; it also covers the stages of the final exhaustive enumeration that proves $\|\mathbf{b}'\|=\lambda_1$. Lemma 1 gives a proven version of the volume heuristics, it replaces in inequality (2) of [HS07] the factor $(4e(1+\sqrt{\pi}))^n$ by $e^{\frac{n-t+1}{2}}$ and corrects misprints in the proof.

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

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

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

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

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

$$\sigma_i(\mathbf{x}):=\textstyle\sum_{j>i}\frac{r_{i,j}}{r_{i,i}}x_j\quad\text{and}\quad x'_i:=x_i+\lceil\sigma_i(\mathbf{x})\rfloor,$$
$$\{\sigma_i(\mathbf{x})\}:=\sigma_i(\mathbf{x})-\lceil\sigma_i(\mathbf{x})\rfloor,$$
$$\mathcal{F}_t:=\{(x'_t,...,x'_n)^t\in\mathbb{R}^{n_t}\mid\textstyle\sum_{i=t}^n(x'_i+\{\sigma_i(\mathbf{x})\})^2r_{i,i}^2\le\lambda_1^2\,\}.$$

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

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

We cover $\mathcal{F}_t$ by the simpler ellipsoid $\mathcal{E}'_t=\{\mathbf{x}'\in\mathbb{R}^{n_t}\mid\sum_{i=t}^n {x'_i}^2r_{i,i}^2\le 4\lambda_1^2\}$. As $|\,\{\sigma_i(\mathbf{x})\}\,|\le\frac{1}{2}$ we have $(x'_i+\{\sigma_i(\mathbf{x})\})^2\ge(x'_i)^2$, hence $\mathcal{F}_t\cap\mathbb{Z}^{n_t}\subset\mathcal{E}'_t\cap\mathbb{Z}^{n_t}$. This proves $\mathcal{M}_t\le\#(\mathcal{E}'_t\cap\mathbb{Z}^{n_t})$.

We bound $\#(\mathcal{E}'_t\cap\mathbb{Z}^{n_t})$ using the method of MAZO, ODLYZKO [MO90, Lemma 1]. Denoting $N_r:=\#\{(k_t,...,k_n)^t\in\mathbb{Z}^{n_t}\mid\sum_{i=t}^n r_{i,i}^2k_i^2=r\}$ there are countably many $r\in\mathbb{R}$ with $N_r\ne0$ and thus for all $s>0$ (These upper bounds by infinite sums are far from being tight.) :

$$\#(\mathcal{E}'_t\cap\mathbb{Z}^{n_t})\le\sum_{0\le r\le 4\lambda_1^2}N_r\,e^{s(4\lambda_1^2-r)n_t}<e^{s4\lambda_1^2n_t}\sum_{r\ge0}N_r\,e^{-srn_t}$$
$$=e^{s4\lambda_1^2n_t}\prod_{i=t}^n\sum_{k_i\in\mathbb{Z}}e^{-sr_{i,i}^2k_i^2n_t}<e^{s4\lambda_1^2n_t}\prod_{i=t}^n(1+\tfrac{\sqrt{\pi}}{\sqrt{sn_t}\,r_{i,i}}),$$

since $\sum_{k\in\mathbb{Z}}e^{-Tk^2}=1+2\sum_{k=1}^\infty e^{-Tk^2}\le1+2\int_0^\infty e^{-Tx^2}dx=1+\sqrt{\pi/T}$ holds for $T=sr_{i,i}^2n_t$.

We get for $s:=1/(8\lambda_1^2)$: $\#(\mathcal{E}'_t\cap\mathbb{Z}^{n_t})\le e^{n_t/2}\prod_{i=t}^n(1+\frac{\sqrt{8\pi}\,\lambda_1}{\sqrt{n_t}\,r_{i,i}})$. □

We can improve the worst case upper bound of Lemma 1 on the average: replace in the above proof the lower bound $|x_i+\varepsilon|^2\ge x_i^2/4$ by the expected value $\mathrm{E}_\varepsilon[\,|x_i+\varepsilon|^2\,]=x_i^2+\frac{1}{12}$ for $\varepsilon\in_R[-\frac{1}{2},+\frac{1}{2}]$. Here we assume that $\{\sigma_i(\mathbf{x})\}\in[-\frac{1}{2},+\frac{1}{2}]$ is uniformly distributed. This replaces in Lemma 1 $\sqrt{8\pi}$ by $\sqrt{2\pi}$ and shows that $\mathcal{M}_t\le e^{\frac{n-t+1}{2}}\prod_{i=t}^n(1+\frac{\sqrt{2\pi}\,\lambda_1}{\sqrt{n-t+1}\,r_{i,i}})$

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

Proof of Theorem 1 continued. The equations $r_{i,i}^2=\|\mathbf{b}_1\|^2q^{i-1}$, $\lambda_1^2/(\gamma_n rd(\mathcal{L})^2)=(\det\mathcal{L})^{\frac{2}{n}}=\|\mathbf{b}_1\|^2q^{\frac{n-1}{2}}$ from GSA and the Minkowski lower bound $\gamma_n\ge\frac{n}{2\,e\pi}$ directly imply for $i=t,...,n$

$$\sqrt{n-t+1}\,r_{i,i}=\sqrt{n-t+1}\,\|\mathbf{b}_1\|q^{\frac{i-1}{2}}\le\sqrt{2\,e\pi}\,rd(\mathcal{L})^{-1}\lambda_1q^{\frac{2i-n-1}{4}}.$$

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

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

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

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

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

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

The [KL78] bound $\gamma_n \le \frac{1.744\,(n+o(n))}{2e\pi} \le \frac{n}{e\pi}$ for $n \ge n_0$

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

$$\mathcal{M}_t \le m(q,c)\big(\tfrac{(2+\sqrt{e})\,\sqrt{2e\pi}\,\lambda_1}{\sqrt{n-t+1}\, rd(\mathcal{L})\,\|\mathbf{b}_1\|}\big)^{n-t+1}\big(\tfrac{\sqrt{n}}{\sqrt{e\pi}}\, rd(\mathcal{L})\,\tfrac{\|\mathbf{b}_1\|}{\lambda_1}\big)^{n-\frac{(t-1)(t-2)}{n-1}}. \tag{4.3}$$

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

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

This upper bound on $\mathcal{M}_t$ is maximal at $t=1$, $c=\frac{n}{2}$, As $m(q,c) = q^{\frac{1-c^2}{4}} = \big(\frac{\|\mathbf{b}_1\|\sqrt{\gamma_n}\, rd(\mathcal{L})}{\lambda_1}\big)^{\frac{c^2-1}{n-1}} \le (n^{\frac{1}{2}+b} rd(\mathcal{L}))^{\frac{c^2-1}{n-1}}$ holds for $c>0$ this proves

$$\max_t \mathcal{M}_t \le (\sqrt{8}+\sqrt{2e})^n\,\big(n^{\frac{1}{2}+b} rd(\mathcal{L})\big)^{\frac{n^2/4-1}{n-1}} < 5.16001^n\big(n^{\frac{1}{2}+b} rd(\mathcal{L})\big)^{\frac{n+1}{4}},$$

where $\frac{n^2/4-1}{n-1} < \frac{n+1}{4}$. □

5 Pruned New Enum for CVP

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

Adaption of New Enum *to* **CVP**. We adapt New Enum to solve $\|\mathbf{t}-\mathbf{b}\|^2 < \ddot{A}$. Initially we set $\ddot{A} := 0.01 + \frac{1}{4}\sum_{i=1}^n r_{i,i}^2$ so that $\|\mathbf{t}-\mathcal{L}\|^2 < \ddot{A}$. Having found some $\mathbf{b} \in \mathcal{L}$ such that $\|\mathbf{t}-\mathbf{b}\|^2 < \ddot{A}$ New Enum gives out $\mathbf{b}$ and decreases $\ddot{A}$ to $\|\mathbf{t}-\mathbf{b}\|^2$.

New Enum for CVP
INPUT LLL-basis $\mathbf{B} = \mathbf{QR} \in \mathbb{Z}^{m\times n}$, $\mathbf{R} = [r_{i,j}] \in \mathbb{R}^{n\times n}$, $\mathbf{t} = \sum_{i=1}^n \tau_i \mathbf{b}_i \in \mathrm{span}(\mathcal{L})$
OUTPUT A sequence of $\mathbf{b} \in \mathcal{L}(\mathbf{B})$ such that $\|\mathbf{t}-\mathbf{b}\|$ decreases to $\|\mathbf{t}-\mathcal{L}\|$.

1. $\ddot{A} := 0.01 + \frac{1}{4}\sum_{i=1}^n r_{i,i}^2$, $t := n$, $s := 1$, $L := \emptyset$, (We call s the level)
   $y_n := \tau_n$, $u_n := \lceil -y_n \rfloor$, $\ddot{c}_{n+1} := 0$,
   ($\ddot{c}_t = \ddot{c}_t(\tau_t - u_t, ..., \tau_n - u_n)$ *always holds for the current* $t, u_t, ..., u_n$)
2. WHILE $t \le n$ *#perform stage* $(u_t, ..., u_n)$:
   $\ddot{c}_t := \ddot{c}_{t+1} + (u_t - y_t)^2 r_{t,t}^2$,
   IF $\ddot{c}_t \ge \ddot{A}$ THEN GO TO 2.1,
   $\ddot{\rho}_t := (\ddot{A} - \ddot{c}_t)^{1/2}$, $\ddot{\beta}_t := V_{t-1}\ddot{\rho}_t^{t-1}/(r_{1,1}\cdots r_{t-1,t-1})$,
   IF $t = 1$ THEN [output $\mathbf{b} := \sum_{i=1}^n u_i \mathbf{b}_i$, $\ddot{A} := \|\mathbf{t}-\mathbf{b}\|^2$, GO TO 2]
   IF $\ddot{\beta}_t \ge 2^{-s} t$ THEN [$t := t-1$, $y_t := \tau_t + \sum_{i=t+1}^n (\tau_i - u_i) r_{t,i}/r_{t,t}$,
   $u_t := \lceil y_t \rfloor$, $\sigma_t := sign(u_t + y_t)$, $\nu_t := 1$, GO TO 2]
   ELSE store $(u_t, ..., u_n, y_t, \ddot{c}_t, \sigma_t, \nu_t)$ in L,
2.1. $t := t+1$, $u_t := \mathrm{next}_{\sigma_t,\nu_t}(u_t, y_t)$, $\nu_t := \nu_t + 1$.
3. $s := s+1$, perform all delayed stages $(u_t, ..., u_n, y_t, \ddot{c}_t, \sigma_t, \nu_t)$ of L on level s and delete them. Delay all new stages with $\ddot{\beta}_{t'} < 2^{-s} t'$, $t' \le t$ and store $(u_{t'}, ..., \nu_{t'})$ in L.
4. IF $L \ne \emptyset$ THEN GO TO 3 ELSE *terminate*.

At stage $(u_t, ..., u_n)$ New Enum searches to extend the current $\mathbf{b} = \sum_{i=t}^n u_i \mathbf{b}_i \in \mathcal{L}$ to some $\mathbf{b}' = \sum_{i=1}^n u_i \mathbf{b}_i \in \mathcal{L}$ such that $\|\mathbf{t}-\mathbf{b}'\|^2 < \ddot{A}$. The expected number of such $\mathbf{b}'$ is for random $\mathbf{t}$:

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

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

$$c_t(\tau_t - u_t, ..., \tau_n - u_n) := \|\pi_t(\mathbf{t} - \mathbf{b})\|^2$$
$$= (\sum_{i=t}^{n}(\tau_i - u_i)r_{t,i})^2 + c_{t+1}(\tau_{t+1} - u_{t+1}, ..., \tau_n - u_n).$$

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

NEW ENUM solves **CVP** for $\mathcal{L}$, $\mathbf{t}$ by first solving **CVP** for $\pi_t(\mathcal{L})$ and $\pi_t(\mathbf{t})$ $t = n, ..., 1$.

Optimal value of $\ddot{A}$. If the distance $\|\mathbf{t} - \mathcal{L}\|$ or a close upper bound of it is known then we initially choose $\ddot{A}$ to be that close upper bound. This prunes away many irrelevant stages.

[HS07] prove the time bound $n^{n/2+o(n)}$ for solving **CVP** by KANNAN's **CVP**-algorithm [Ka87]. Minimizing $\|\mathbf{b}\|$ for $\mathbf{b} \in \mathcal{L} - \{\mathbf{0}\}$ and minimizing $\|\mathbf{t} - \mathbf{b}\|$ for $\mathbf{b} \in \mathcal{L}$ require nearly the same work if $\|\mathbf{t} - \mathcal{L}\| \approx \lambda_1$. In fact, replacing in (4.3) λ_1 by $\|\mathcal{L} - \mathbf{t}\|$ the proof of Theorem 1 yields:

Corollary 1. *Given a basis* $\mathbf{B} = [\mathbf{b}_1, ..., \mathbf{b}_n]$ *satisfying* GSA, $\|\mathbf{b}_1\| \leq \sqrt{e\pi}\, n^b \lambda_1$ *with* $b \geq 0$ *and* $\mathbf{t} \in \text{span}(\mathcal{L})$ *with* $\|\mathcal{L} - \mathbf{t}\| \leq \lambda_1$, NEW ENUM *solves this* **CVP** *in time* $2^{O(n)}(n^{\frac{1}{2}+b} rd(\mathcal{L}))^{\frac{n}{4}}$.

Corollary 1 yields for moderately small $rd(\mathcal{L})$ a CVP time bound $2^{O(n)}$ which merely requires linear space (by iterating NEW ENUM for $s = 1, ..., O(n)$ without storing delayed stages). Note however that a subexponential time bound is excluded since $n^{1/2} rd(\mathcal{L}) \geq 1/\sqrt{e\pi}$ holds by the trade-off between $\|\mathbf{b}_1\|/\lambda_1$ and $rd(\mathcal{L})$ under GSA, see remark 4 of section 4.

Next we translate the assumption SA from **SVP** to **CVP**:

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

CA holds with probability $1/n$ for random $\ddot{\mathbf{b}}$ [GNR10]. This probability increases by iterating the search for a closest lattice vector by statistically independent trials via permuted bases.

Let $R_{\mathcal{L}} = \max_{\mathbf{u} \in \text{span}(\mathcal{L})} \|\mathbf{u} - \mathcal{L}\|$ be the covering radius of $\mathcal{L}$, where $\text{span}\,\mathcal{L}(\mathbf{B}) = \{\mathbf{Bx} \,|\, \mathbf{x} \in \mathbb{R}^n\}$.

Corollary 2. *Let a basis* $\mathbf{B} = [\mathbf{b}_1, ..., \mathbf{b}_n] \in \mathbb{Z}^{m \times n}$ *of* $\mathcal{L}$ *be given that satisfies* GSA, $\|\mathbf{b}_1\| = O(\lambda_1)$ *and* $rd(\mathcal{L}) \leq n^{-\frac{1}{4}}(\lambda_1\sqrt{e\pi}/\|\mathbf{b}_1\|)^{\frac{1}{2}}$. *Let the target vector* $\mathbf{t}$ *and its closest lattice vector* $\ddot{\mathbf{b}}$ *found by* NEW ENUM *satisfy* CA *then* NEW ENUM *finds* $\ddot{\mathbf{b}}$ *for random* $\mathbf{t}$ *in average time* $n^{O(1)}(R_{\mathcal{L}}/\lambda_1)^n$.

Proof. We follow the proof of Proposition 1. NEW ENUM's time bound $n^{O(1)}$ for **SVP** under GSA and SA extends to **CVP** under GSA and CA. For random $\mathbf{t} \in_R \text{span}(\mathcal{L})$ we have

$$\text{E}_{\mathbf{t}}\, |\mathcal{B}_{n-t+1}(\pi_t(\mathbf{t}), \rho_t) \cap \pi_t(\mathcal{L})| = \tfrac{V_{n-t+1}}{\det \pi_t(\mathcal{L})} \rho_t^{n-t+1}$$

and thus the volume heuristics estimation provably holds on the average. NEW ENUM for **CVP** enumerates lattice vectors of a ball of the covering radius $R_{\mathcal{L}}$ while NEW ENUM for **SVP** does this for a ball of radius λ_1, hence the additional time factor $(R_{\mathcal{L}}/\lambda_1)^n$. Note that the time factor $(R_{\mathcal{L}}/\lambda_1)^n$ overestimates the running time if $\|\mathbf{t} - \mathcal{L}\| \ll R_{\mathcal{L}}$. □

Cor. 1 and Cor. 2 do not use the questionable volume heuristics. Cor. 2 eliminates the volume heuristics by randomizing the target vector $\mathbf{t}$. This randomization increases $\|\mathbf{t} - \mathcal{L}\|$ nearly to $R_{\mathcal{L}}$ and cannot be used for Cor. 3 which proves a polynomial time bound under the volume heuristics if in addition $\|\mathbf{t} - \mathcal{L}\| \lesssim \lambda_1$ holds. It remains to analyze the error of the polynomial time bound of Cor. 3 that results from the volume heuristics. Prop. 1 translates into

Corollary 3. *Let a basis* $\mathbf{B} = [\mathbf{b}_1, ..., \mathbf{b}_n] \in \mathbb{Z}^{m \times n}$ *of* $\mathcal{L}$ *be given satisfying* GSA, $\|\mathbf{b}_1\| = O(\lambda_1)$ *and* $rd(\mathcal{L}) \leq n^{-\frac{1}{4}}(\lambda_1\sqrt{e\pi}/\|\mathbf{b}_1\|)^{\frac{1}{2}}$. *If the target vector* $\mathbf{t}$ *and its closest lattice vector* $\ddot{\mathbf{b}}$ *found by* NEW ENUM *satisfies* CA *and* $\|\mathbf{t} - \mathcal{L}\| \lesssim \lambda_1$ *then* NEW ENUM *finds* $\ddot{\mathbf{b}}$ *under the volume heuristics in polynomial time.*

6 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 $(f_0, ..., f_{N-1}) \in \mathbb{Z}_q^N$. 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 $f(1) = \sum_{i=0}^{N-1} f_i = 1 = g(1) = \sum_{i=0}^{N-1} g_i = h(1)$.

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 $\mathbf{B} = \begin{bmatrix} I_N & 0 \\ H & q\, I_N \end{bmatrix}$, $H \in \mathbb{Z}^{N\times N}$ is the circulant 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 $\gamma_n \geq \frac{n+\ln n}{2e\pi} \approx 47.3$. The polynomial **SVP**-time bound under GSA the volume heuristics and $n^{\frac{1}{2}+b} rd(\mathcal{L}) \leq 1$ does not break NTRU since

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

However $rd(\mathcal{L}) \approx 0.154 < 0.158 \approx (2n)^{-1/4}$. Therefore **SVP** for $\mathcal{L}$ is heuristically easy by Prop. 1 if we are given a sufficiently short lattice vector. Such a short vector can possibly be constructed by either lattice extension or lattice reduction.

5.2 n^c-unique-SVP lattices. These lattices satisfy the unique shortest vector property: 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., $\lambda_2 \geq \lambda_1 n^c$.Then Minkowski's second theorem $\prod_{i=1}^n \lambda_i \leq \gamma_n^{n/2} \det \mathcal{L}$ implies that $rd(\mathcal{L}) \leq n^{-c+c/n}$.

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. The original $c = O(1)$ of [Aj96] has been subsequently reduced to $3 + \varepsilon$ [Ca98, M04], and most recently [MR07] reduce n^c to $n \ln^{O(1)} n$.

5.4 Lattices of high density. The density $\triangle = V_n(\lambda_1/2)^n / \det \mathcal{L}$ of lattice $\mathcal{L}$ is the volume portion of $\text{span}(\mathcal{L})$ that is covered by the spheres of radius $\lambda_1/2$ centered at points in $\mathcal{L}$.

Minkowski gave in (1905) a nonconstructive proof that lattices exist satisfying $\log_2(\triangle) \geq n-1$, but no construction of such lattices is known. The infinite class field towers found by Golod, Shfarevich, Martinet and others produce infinite sequences of lattices of particular dimensions satisfying, in the most favorable case known, $\frac{1}{n}\log_2(\triangle) \geq -2.218$ for $n \to \infty$. The prime number lattice of section 7 satisfies for $c = n/(2 \ln N)$ that $\frac{1}{n}\log_2(\triangle) \geq -\frac{1}{2}\log_2 \ln n + 0.924 - o(1)$. This density holds for arbitrary dimension $n \in \mathbb{N}$.

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

7 Factoring via CVP solutions for the Prime Number Lattice

Let N be a positive integer that is not a prime power. We show under various heuristics how to factor N in polynomial time by solving $(\ln N)^{2+\varepsilon}$ easy **CVP**'s for the prime number lattice. We use the volume heuristics and GSA for the prime number lattice and CA for the **CVP**'s to be solved.

Let $p_1 < \cdots < p_n$ enumerate all primes less than $(\ln N)^\alpha$, $\alpha > 2$. Then $n = (\ln N)^\alpha/(\alpha \ln\ln N)(1+o(1))$. Let the prime factors p of N satisfy $p > p_n$. We use the asymptotic $o(1)$ for $N \to \infty$.

A classical method factors N via $n + o(n)$ modular equations $\prod_{i=1}^n p_i^{e_i} = \pm \prod_{i=1}^n p_i^{e_i'} \mod N$. Theorem 2 constructs such modular equations from **CVP**-solutions of small distance for the prime

number lattice $\mathcal{L}(\mathbf{B}_{\alpha,c})$. Theorems 4, 5 presents α, c that guarantee the distance required by Theorem 2. Theorem 6 shows these **CVP**'s to be solvable in polynomial time due to $rd(\mathcal{L}) = o(n^{-1/4})$.

Consider the lattice basis $\mathbf{B}_{\alpha,c} = [\mathbf{b}_1, \ldots, \mathbf{b}_n] \in \mathbb{R}^{(n+1)\times n}$ and the target vectors $\mathbf{N} \in \mathbb{R}^{n+1}$:

$$\mathbf{B}_{\alpha,c} = \begin{bmatrix} \sqrt{\ln p_1} & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \sqrt{\ln p_n} \\ N^c \ln p_1 & \cdots & N^c \ln p_n \end{bmatrix}, \qquad \mathbf{N} = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ N^c \ln N \end{bmatrix}, \qquad c = (\ln N)^\beta \geq 1, \tag{7.0}$$

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

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

We identify the vector $\mathbf{b} = \sum_{i=1}^n e_i \mathbf{b}_i \in \mathcal{L}(\mathbf{B}_{\alpha,c})$ with the pair (u, v) of integers

$$u = \textstyle\prod_{e_j>0} p_j^{e_j}, \ \ v = \prod_{e_j<0} p_j^{-e_j} \in \mathbb{N}. \tag{7.1}$$

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

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

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

$$\ln u + \ln v = (2c-1)\ln N + O(\pm 1).$$

Moreover $\quad |\ln \frac{u}{vN}| = |\ln\big(1 + \frac{u-vN}{vN}\big)| = \frac{|u-vN|}{vN}(1 + o(1)) = \Theta(\frac{|u-vN|}{N^{c-1}N})$.
Combining these equations proves the claim. □

Theorem 2. *If* $\|\mathbf{b} - \mathbf{N}\|^2 \leq (2c-1)\ln N + 2\delta \ln p_n$ *and* $c = (\ln N)^\beta$ *then*

$$|u - vN| \leq p_n^{\frac{1+\alpha\beta}{2\alpha} + \delta + o(1)}.$$

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 of $\mathbf{b} - \mathbf{N}$ we get

$$|z| N^{-c} = |\textstyle\sum_{i=1}^n e_i \ln p_i - \ln N| = |\ln \frac{u}{vN}|$$

$$\leq N^{-c}((2c-1)\ln N + 2\delta \ln p_n)^{1/2} \leq N^{-c} p_n^{\frac{1+\beta}{2\alpha} + o(1)}$$

since $(\ln N)^\alpha \approx p_n$. This shows for $\gamma = \frac{1+\beta}{2\alpha}$ the two inequalities required in Theorem 3. The claim follows from Theorem 3. □

Theorem 3. [S93, Theorem 1] *The* u, v *of* (7.1) *satisfy* $|u - vN| \leq p_n^{\gamma+\delta+o(1)}$ *for* $\gamma, \delta \geq 0$ *if*
1. $|\sum_{i=1}^n e_i \ln p_i - \ln N| \leq N^{-c} p_n^{\gamma + o(1)}$ **2.** $\sum_{i=1}^n |e_i \ln p_i| \leq (2c-1)\ln N + 2\delta \ln p_n$.

Proof. We see from inequality **1.** that

$$\big|\ln\big(1 + \tfrac{u-vN}{vN}\big)\big| = \big|\ln \tfrac{u}{vN}\big| = |\textstyle\sum_{i=1}^n e_i \ln p_i - \ln N| \leq N^{-c} p_n^{\gamma+o(1)}$$

Using that $\ln(1+x) = x + O(x^2)$ holds for $|x| \leq 1/2$ this yields

$$|u - vN| \leq vN^{1-c} p_n^{\gamma+o(1)}$$

It remains to prove that $vN^{1-c} \leq p_n^{\delta+o(1)}$. We see from **1.** that

$$\ln v \leq \ln u - \ln N + N^{-c} p_n^{\gamma+o(1)}$$

$$\leq -\ln v + (2c - 1 - 1)\ln N + 2\delta \ln p_n + N^{-c} p_n^{\gamma+o(1)} \ \text{ due to } \mathbf{2}.$$

Hence $\quad 2\ln v \leq 2(c-1)\ln N + 2\delta \ln p_n + N^{-c} p_n^{\gamma+o(1)}$ and thus $vN^{1-c} \leq p_n^{\delta}(1 + o(1))$. □

Outline of the factoring method. We compute vectors $\mathbf{b} = \sum_{i=1}^{n} e_i \mathbf{b}_i \in \mathcal{L}(\mathbf{B}_{\alpha,c})$ close to $\mathbf{N}$ such that $|u - vN| \le p_n$ holds for 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

$$\prod_{e_i>0} p_i^{e_i} = \pm \prod_{i=1}^{n} p_i^{e'_i} \mod N. \tag{7.2}$$

Given $n+1$ independent relations (7.2) we write these relations with $p_0 = -1$ and $e_{i,j}, e'_{i,j} \in \mathbb{N}$ as

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

Any solution $z_1, ..., z_{n+1} \in \{0, 1\}$ of the equations

$$\sum_{j=1}^{n+1} z_j (e_{i,j} - e'_{i,j}) = 0 \mod 2 \quad \text{for } i = 0, ..., n \tag{7.3}$$

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

In case that $X \neq \pm 1 \mod N$ this yields two factors $\gcd(X \pm 1, N) \notin \{1, N\}$ of N.

The linear system of equations (7.3) can be solved within $O(n^3)$ bit operations. This takes much less time than LLL-reduction of $\mathbf{B}_{\alpha,c}$ that is done by arithmetic steps using large integers. We neglect this minor part of the work load of factoring N.

By Theorem 2 lattice vectors very close to $\mathbf{N}$ provide a relation (7.2). Theorems 4 and 5 show that such close vectors exist. Theorem 6 shows a heuristic time bound of the corresponding **CVP**'s. We get independent relations (7.2) by constructing them for independent integer multiples N of N.

The existence of lattice vectors $\mathbf{b} = \sum_{\mathbf{i=1}}^{\mathbf{n}} \mathbf{e_i b_i} \in \mathcal{L}(\mathbf{B}_{\alpha,c})$ such that $|u - vN| = \mathbf{1}$.
An integer z is called *y-smooth*, if all prime factors p of z satisfy $p \le y$. We denote for $c \ge 1$

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

Theorem 4 extends Theorem 5 of [S93] to the additional requirement that u, v are squarefree. The latter is equivalent to the condition $e_1, ..., e_n \in \{0, \pm 1\}$ of Lemma 2. Theorems 4 and 5 show that there are $N^{\varepsilon + o(\varepsilon)}$ lattice vectors close to $\mathbf{N}$ that provide $N^{\varepsilon + o(\varepsilon)}$ relations (7.2).

Theorem 4. *Assuming that the equation $|u - \lceil u/N \rfloor N| = 1$ is for random $u = \Theta(N^c)$ nearly statistically independent from the event that $u, \lceil u/N \rfloor$ are squarefree and $(\ln N)^{\alpha}$-smooth then $\#M_{\alpha,c,N} \ge N^{\varepsilon + o(\varepsilon)}$ holds if $\alpha > 2\beta + 2 > 2$ and $\frac{\alpha + \alpha\varepsilon - 1 - \beta}{\alpha - 2\beta - 2} < c = (\ln N)^{\beta}$ for some $\varepsilon > 0$.*

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

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

is shown in [CEP83, Thm 3.1]. Let $\Psi^*(z, y)$ denote the number of squarefree, y–smooth integers in $[1, z]$. Pomerance, as cited in [Ad95], observed that (we abbreviate $\ln^{\alpha} x = (\ln x)^{\alpha}$)

$$\Psi^*(x, \ln^{\alpha} x) \ge x\, z^{-z + o(z)} \quad \text{for } z = \ln x / (\alpha \ln\ln x), \text{ i.e., } (\ln x)^{\alpha} = x^{1/z}.$$

Here is a short proof. We obviously have for $z' := \lfloor z \rfloor$ that

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

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 $(\ln N)^{\alpha} = N^{1/r}$. The assumption of the theorem and the lower bound on $\Psi^*(N^c, \ln^{\alpha} N)$ yields :

$$\begin{aligned} \#M_{\alpha,c} &\ge N^{c-1} (rc - r)^{-rc + r} (rc)^{-rc + o(r)}, \\ \ln \#M_{\alpha,c} &\ge (c-1) \ln N - \tfrac{\ln N (1 + o(1))}{\alpha \ln\ln N} \big((c-1) \ln(rc - r) + c \ln rc \big). \end{aligned}$$

Here N^{c-1} counts twice the number of v, $\frac{1}{2} N^{c-1} \le v \le N^{c-1}$. For every such v there are two $u = vN \pm 1$, 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 we get for $\frac{\alpha + \alpha\varepsilon - 1 - \beta}{\alpha - 2\beta - 2} < c = (\ln N)^{\beta}$ and $\alpha > 2\beta + 2$ that

$$\ln \#M_{\alpha,c} > c\ln N - \ln N - \tfrac{(2c-1)\ln N \ln(rc)}{\alpha \ln\ln N}(1+o(1))$$
$$> c\ln N - \ln N - \tfrac{(2c-1)\ln N(1+\beta)\ln\ln N}{\alpha\ln\ln N}(1+o(1)) \quad (\text{as } \ln r < \ln\ln N \text{ and } \ln c = \beta \ln\ln N)$$
$$= \ln N(-1 + \tfrac{\alpha\, c-(2c-1)(1+\beta)(1+o(1))}{\alpha}) = \ln N(-1 + \tfrac{c(\alpha-2\beta-2)+1+\beta}{\alpha(1+o(1))}) \geq (\varepsilon - o(\varepsilon)\ln N$$

since $-1 + \frac{c(\alpha-2\beta-2)+1+\beta}{\alpha} > \varepsilon$ holds under our assumptions. Hence $\#M_{\alpha,c} \geq N^{\varepsilon+o(\varepsilon)}$. □

Finding relations (7.2) by **CVP***-solutions.* By Lemma 2 the $(u,v) \in M_{\alpha,c}$ are associated with some $\mathbf{b} = \sum_{i=1}^n e_i\mathbf{b}_i \in \mathcal{L}(\mathbf{B}_{\alpha,c})$ such that $\|\mathbf{b}-\mathbf{N}\|^2 \leq (2c-1)\ln N + O(|u-vN|^2)$ holds provided that $e_1,...,e_n \in \{0,\pm 1\}$.

Theorem 5. *The vector* $\mathbf{b} = \sum_{i=1}^n e_i\mathbf{b}_i \in \mathcal{L}(\mathbf{B}_{\alpha,c})$ *that is closest to* $\mathbf{N}$ *provides a non-trivial relation* (7.2) *provided that* $M_{\alpha,c} \neq \emptyset$ *and* $1+\beta < 2\alpha$.

Proof. Let $\mathbf{b}' = \sum_{i=1}^n e_i'\mathbf{b}_i \in \mathcal{L}(\mathbf{B}_{\alpha,c})$ be the vector corresponding to some $(u',v') \in M_{\alpha,c}$, $u' = \prod_{e_i'>0} p_i^{e_i'}$, $v' = \prod_{e_i'<0} p_i^{-e_i'}$ 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 2 shows $\|\mathbf{b}'-\mathbf{N}\|^2 \leq (2c-1)\ln N + \eta^{-2} + O(1)$.

Then the lattice vector $\mathbf{b} \in \mathcal{L}(\mathbf{B}_{\alpha,c})$ 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 2 shows $|u-vN| \leq p_n^{\frac{1+\beta}{2\alpha}+o(1)}$. Hence $\mathbf{b} = \sum_{i=1}^n e_i\mathbf{b}_i \in \mathcal{L}(\mathbf{B}_{\alpha,c})$ provides a relation (7.2). □

Factoring N reduces by Theorem 5 to finding about n vectors $\sum_{i=1}^n e_i\mathbf{b}_i \in \mathcal{L}(\mathbf{B}_{\alpha,c})$ that are so close to $\mathbf{N}$ that the corresponding (u,v) of (7.1) are in $\mathcal{M}_{\alpha,c}$.

Theorem 6. *Let a reduced version of the basis* $\mathbf{B}_{\alpha,c}$ *of* $\mathcal{L}$ *be given that satisfies* GSA, $\|\mathbf{b}_1\|^2 = 2c\ln N + O(1)$, $M_{\alpha,c} \neq \emptyset$ *and* $\alpha > 2\beta+2$. *Then* $\|\mathbf{b}_1\|^2 = \lambda_1^2 + O(1)$, $\|\mathcal{L}-\mathbf{N}\| < \lambda_1$ *and* $rd(\mathcal{L}) = o(n^{-1/4})$. *If* New Enum *finds a vector* $\ddot{\mathbf{b}} \in \mathcal{L}$ *closest to* $\mathbf{N}$ *that satisfies CA it finds* $\ddot{\mathbf{b}}$ *for random* $\mathbf{N} \in_R \operatorname{span}\mathcal{L}$ *in average time* $n^{O(1)}(R_{\mathcal{L}}/\lambda_1)^n$. *Under the volume heuristics* New Enum *finds* $\ddot{\mathbf{b}}$ *in polynomial time.*

Proof. We first prove that $\lambda_1^2 = 2c\ln N + O(1)$. $M_{\alpha,c} \neq \emptyset$ holds by Theorem 4, moreover we see from that proof argument 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 $u = \Theta(N^c)$, $|u-v| \leq 2$, $\gcd(u,v) = 1$. In particular, let

$$\widetilde{M}_{\alpha,c} = \Big\{(u,v) \in \mathbb{N}^2 \;\Big|\; \begin{array}{l} |u-v| = 1,\ N^c/2 \leq v \leq N^c \\ u,v \text{ are squarefree and } (\ln N)^\alpha\text{-smooth} \end{array}\Big\}.$$

Then $\#\widetilde{M}_{\alpha,c} \geq N^c(rc)^{-2rc+o(r)}$ holds for $r = \ln N/(\alpha\ln\ln N)$, and thus

$$\ln \#\widetilde{M}_{\alpha,c} \geq \ln N(\tfrac{\alpha-2-2\beta-o(1)}{\alpha}\, c) = \Theta(c\ln N).$$

Similar to the proof of Lemma 2 we have

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

where $\ln(u/v) = \ln(1+\frac{u-v}{v}) = \Theta(|u-v|N^{-c})$. Hence $\lambda_1^2 \leq 2c\ln N + O(1)$. On the other hand Lemma 5.3 of [MG02] proves that $\lambda_1^2 > 2c\ln N$ if the prime $p_1 = 2$ is neglected. Hence the claim.

Lemma 2 shows that $M_{\alpha,c} \neq \emptyset$ implies $\|\mathcal{L}-\mathbf{N}\|^2 \leq (2c-1)\ln N + O(1)$, and thus $\|\mathcal{L}-\mathbf{N}\|^2/\lambda_1^2 \approx 1 - 1/2c$. Forl $c \approx 1$ we minimizte $\|\mathbf{b}-\mathbf{N}\|$ for $\mathbf{b} \in \mathcal{L}$ by solving SVP for the lattice with basis $[\mathbf{N}, \mathbf{B}_{\alpha,c}]$. In particular, $\|\mathcal{L}(\mathbf{B}_{\alpha,1}) - \mathbf{N}\|^2 \approx \frac{1}{2}\lambda_1^2$ and thus $rd(\mathcal{L}(\mathbf{N}, \mathbf{B}_{\alpha,1}))^2 \approx \frac{1}{2}\, rd(\mathcal{L}(\mathbf{B}_{\alpha,1}))^2$.

Next we bound $rd(\mathcal{L})$ for $\mathcal{L} = \mathcal{L}(\mathbf{B}_{\alpha,c})$. For $n = (\ln N)^\alpha/(\alpha\ln\ln N)(1+o(1))$ we have

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

Hence $$rd(\mathcal{L}) = \lambda_1/(\sqrt{\gamma_n}(\det\mathcal{L})^{\frac{1}{n}}) = \big(\tfrac{2e\pi\, 2c\ln N}{(\ln N)^\alpha}\big)^{\frac{1}{2}}/N^{c/n}(1+o(1)).$$

We have for $\beta < \alpha/2 - 1$ that $c = (\ln N)^\beta < (\ln N)^{\alpha/2-1}$ and $\frac{c\ln N}{(\ln N)^\alpha} \leq \frac{1}{(\ln N)^{\alpha/2}} = o(n^{-1/2})$.

We see from $c/n \le (\ln N)^{\beta-\alpha}\alpha \ln\ln N\,(1+o(1))$ and $\beta-\alpha+1<-\alpha/2$ that

$$N^{c/n} = N^{\frac{1}{\ln N}(\ln N)^{\beta-\alpha+1}\alpha\ln\ln N\,(1+o(1))}$$
$$\le e^{(\ln N)^{-\alpha/2}\,\alpha\ln\ln N\,(1+o(1))} = e^{o(1)} = 1+o(1).$$

Hence $rd(\mathcal{L}) = O\big((\frac{c\ln N}{(\ln N)^{\alpha}})^{1/2}\big) = o(n^{-1/4})$ since $2+2\beta<\alpha$.

By Corollary 2 NEW ENUM minimizes $\|\mathbf{b}-\mathbf{N}\|$ for $\mathbf{b}\in\mathcal{L}$ under GSA and CA in average time $n^{O(1)}(R_{\mathcal{L}}/\lambda_1)^n$ for random $\mathbf{N}\in_R \operatorname{span}\mathcal{L}$. This proves the first time bound of Theorem 6. Recall that the factor $(R_{\mathcal{L}}/\lambda_1)^n$ overestimates NEW ENUM's running time because $\|\mathcal{L}-\mathbf{N}\|<\lambda_1$ NEW ENUM enumerates lattice points in a ball of radius $\|\mathcal{L}-\mathbf{N}\|<\lambda_1 \ll R_{\mathcal{L}} = \max_{\mathbf{u}\in\operatorname{span}(\mathcal{L})}\|\mathbf{u}-\mathcal{L}\|$.

A polynomial time bound: Following the proof of Prop. 1 and Cor. 3 NEW ENUM finds for the $\alpha, c=(\ln N)^{\beta}$ of Theorem 4 some $\mathbf{b}\in\mathcal{L}(\mathbf{B}_{\alpha,c})$ that minimizes $\|\mathbf{b}-\mathbf{N}\|$ under the volume heuristics in polynomial time, without proving correctness of the minimization. Any $\mathbf{b}\in\mathcal{L}$ sufficiently close to $\mathbf{N}$ provides a relation (7.2) by Theorems 4 and 5. While only a large $c=(\ln N)^{\beta}$ guarantees $rd(\mathcal{L})=o(n^{-1/4})$ and factors integers in polynomial time our experiments are much faster for $c\approx 1$. Also the volume heuristics can underestimate by far the number of $\mathbf{b}\in\mathcal{L}$ such that $\|\mathbf{b}-\mathbf{N}\|\le\lambda_1$ since $\mathbf{N}$ is very close to the lattice. □

Constructing a nearly shortest vector of $\mathcal{L}(\bar{\mathbf{B}}_{\alpha,c})$ for an extended basis $\bar{\mathbf{B}}_{\alpha,c}$. In order to factor N heuristically in polynomial time via Theorem 6 we must find a very short vector of the prime number lattice. For this we extend the basis $\mathbf{B}_{\alpha,c}=[\mathbf{b}_1,...,\mathbf{b}_n]\in\mathbb{R}^{(n+1)\times n}$ by a suitable prime $\bar{p}_{n+1}$ and the corresponding vector $\bar{\mathbf{b}}_{n+1}=[0,....0,\sqrt{\ln(\bar{p}_{n+1})},N^c\ln(\bar{p}_{n+1})]^t\in\mathbb{R}^{n+2}$ to $\bar{\mathbf{B}}_{\alpha,c}=[\bar{\mathbf{b}}_1,...,\bar{\mathbf{b}}_n,\bar{\mathbf{b}}_{n+1}]\in\mathbb{R}^{(n+2)\times(n+1)}$ and construct such a short vector of the extended lattice. We construct the prime $\bar{p}_{n+1}$ such that $\bar{p}_{n+1}=\Theta(N^c)$ and $|u-\bar{p}_{n+1}|=O(1)$ holds for a squarefree $(\ln N)^{\alpha}$-smooth integer $u=\prod_{i=1}^{n}p_i^{e_i}$. From the initial part of the proof of Theorem 6 and that of Lemma 2 we see that $\|\bar{\mathbf{b}}\|^2=2c\ln N+O(1)=\lambda_1^2(\mathcal{L}(\bar{\mathbf{B}}_{\alpha,c})+O(1)$ holds for $\bar{\mathbf{b}}:=\sum_{i=1}^{n}e_i\bar{\mathbf{b}}_i-\bar{\mathbf{b}}_{n+1}$. This construction is efficient, we generate $u=\prod_i p_i=\Theta(N^c)$ at random and test the $\bar{p}$ near to u for primality. If the density of primes near the u is not exceptionally small we find a prime $\bar{p}_{n+1}=u+O(1)$ within $O(c\ln N)$ primality tests on such $\bar{p}$. Therefore $\bar{\mathbf{B}}_{\alpha,c}$ and a nearly shortest vector $\bar{\mathbf{b}}$ of $\mathcal{L}(\bar{\mathbf{B}}_{\alpha,c})$ can be found in probabilistic polynomial time. A single $(\bar{\mathbf{B}}_{\alpha,c},\bar{\mathbf{b}})$ can be used to solve all **CVP**'s for the factorization of all integers of the order of N.

Corollary 4. *Integers N can be factored under the vol. heuristics,* GSA and CA *in polynomial time by solving $(\ln N)^{\alpha}$* **CVP***'s for the prime number lattice of dimension $n<(\ln N)^{\alpha}$ and $c=(\ln N)^{\beta}$ such that $0<\frac{\alpha-\beta-1}{\alpha-2\beta-2}<c$ and $\|\mathbf{b}_1\|^2=O(2c\ln N)$. This lattice satisfies $rd(\mathcal{L})=o(n^{-1/4})$.*

Proof. We apply Theorems 4, 5 and 6 to $c=(\ln N)^{\beta}$. Then the condition $0<\frac{\alpha-1-\beta}{\alpha-2\beta-2}<c$ required for Theorem 4 holds for arbitrary $0<\beta<\alpha/2-1$ and sufficiently large N. The proof of Theorem 6 shows that $rd(\mathcal{L})=o(n^{-1/4})$ is clearly smaller than required for Prop. 1 and Cor. 3. Therefore the errors of the volume heuristics should not be extreme. □

Parameters for poly-time factoring N. Theorem 4 and Cor. 4 require that $\frac{\alpha-\beta-1}{\alpha-2\beta-2}<c=(\ln N)^{\beta}$.

For $N\ge 2^{50}$ and $\alpha=3.25$, $\beta=0.35$ we have that $\frac{\alpha-\beta-1}{\alpha-2\beta-2}\approx 2.923<3.58\approx(\ln 2^{50})^{0.35}$.

For $N\ge 2^{200}$ and $\alpha=3$ and $\beta=0.3$ we have that $\frac{\alpha-\beta-1}{\alpha-2\beta-2}=4.25<4.33\approx(\ln 2^{200})^{0.3}$.

For $N\ge 2^{500}$ and $\alpha=2.9$ and $\beta=0.3$ we have that $\frac{\alpha-\beta-1}{\alpha-2\beta-2}\approx 5.33<5.78\approx(\ln 2^{500})^{0.3}$.

These prime number lattices for factoring N vhave fairly large dimension $n\approx(\ln N)^{\alpha}/(\alpha\ln\ln N)$, namely $n\approx 1.3\cdot 10^6$ for $N\approx 2^{500}$ and $n\approx 8765$ for $N\approx 2^{50}$. However, experimental data show that the inequality $0<\frac{\alpha-\beta-1}{\alpha-2\beta-2}<c=(\ln N)^{\beta}$ is excessively demanding. For $N\approx 2^{14}$, $\alpha\approx 1.865$, $c=1$, $\beta=0$, $n=100$ we easily found 27 relations (7.2) using only the first 100 primes. This may indicate that we can find relations (7.2) for factoring $N\approx 2^{750}$ using only the first $10000=10^4$ primes.

Experiments by B. Lange, see the appendix. Let $\mathbf{B}_{\alpha,c}$ be a prime base of the $n=125$ smallest primes, $p_{125}=691$, and $N\approx 10^{14}\approx 2^{46.5}$ thus $\alpha\approx 1.94$. The target vector $\mathbf{N}$ has been added in front of $\mathbf{B}_{\alpha,c}$. We multiply the real entries of $\mathbf{B}_{\alpha,c}$ and $\mathbf{N}$ by 10^4 and round the products to the nearest integer. Instead of solving **CVP** for $\mathbf{B}_{\alpha,c},\mathbf{N}$ we solve **SVP** for $\mathcal{L}(\mathbf{N},\mathbf{B}_{\alpha,c})$ and $c\approx 1$ then $\|\mathbf{N}-\mathbf{B}_{\alpha,1}\|^2\approx\frac{1}{2}\lambda_1^2(\mathcal{L}(\mathbf{B}_{\alpha,1})$ and $rd(\mathcal{L}(\mathbf{N},\mathbf{B}_{\alpha,1}))\approx rd(\mathcal{L}(\mathbf{B}_{\alpha,1}))/\sqrt{2}$

Prime number lattices of maximal density. Consider a prime number lattice, where the prime 2 is excluded. Then Lemma 5.3 of [MG02] proves $\lambda_1^2 \geq 2c \ln N$. Using that $n = (\ln N)^\alpha/(\alpha \ln\ln N)(1+o(1))$ and $\gamma_n \leq \frac{1.744\, n}{2e\pi}$ we see that

$$rd(\mathcal{L}) = \frac{\lambda_1}{\sqrt{\gamma_n}(\det \mathcal{L})^{1/n}} \geq \big(\tfrac{2e\pi\, 2c \ln N}{1.744\, n\, \alpha \ln\ln N}\big)^{1/2} N^{-c/n}.$$

A detailed calculation shows that the right hand side is maximal at $c = \frac{n}{2 \ln N}$. Using $\ln\ln N \approx \ln(n^{1/\alpha}) = \frac{1}{\alpha}\ln n$ we get for this c

$$rd(\mathcal{L}) \geq (1.898 + o(1))/\sqrt{\ln n}.$$

The density $\triangle$ of $\mathcal{L}$ satisfies $\triangle = rd(\mathcal{L})^n 2^{-n} V_n \gamma_n^{n/2} \gtrsim rd(\mathcal{L})^n 2^{-n}/\sqrt{\pi\, n}$, since $\gamma_n \gtrsim \frac{n}{2e\pi}$. Hence

$$\tfrac{1}{n}\log_2 \triangle \geq -\tfrac{1}{2}\log_2 \ln n + \log_2(1.898/2) + o(1).$$

If the MINKOWSKI lower bound $\gamma_n \geq \frac{n+\ln n}{2e\pi}$ is close for large n (which is quite realistic) we even get that $rd(\mathcal{L}) \geq (1.506\sqrt{1.744} + o(1))/\sqrt{\ln n}$ and thus $\frac{1}{n}\log_2 \triangle \geq -\frac{1}{2}\log_2 \ln n + \log_2(2.506/2) + o(1)$. The prime number lattice achieves this fairly high density $\triangle$ for all dimensions n. Explicit constructions of lattice sphere packings of higher density are only known for particular dimensions n.

History of the prime number lattice $\mathcal{L}(\mathbf{B}_{\alpha,c})$.[S93] uses a lattice $\mathcal{L}(\mathbf{B'}_{\alpha,c})$ with diagonal elements $\ln p_i$.ADLEMAN [Ad95] proposed the diagonal elements $\sqrt{\ln p_i}$ of $\mathbf{B}_{\alpha,c}$ translating the method of [S93] from the $\|\ \|_1$-norm used in [S93] to the square norm.

.

8 Computing discrete logarithms for $\mathbb{Z}_N^\star$ via CVP solutions

We reduce the problem of computing discrete logarithms for $\mathbb{Z}_N^\star$ with N prime to solving $n \approx (\ln N)^\alpha/(\alpha \ln\ln N)$ heuristically easy **CVP**'s for the extended prime number lattice $\mathcal{L}(\bar{\mathbf{B}}_{\alpha,c})$ with $\alpha > 2\beta + 2$ and $c = (\ln n)^\beta$. We follow the discrete logarithm algorithm of [S93, section 5].

Let the cyclic group $\mathbb{Z}_N^\star = \langle g\rangle$ have generator g. As $|\mathbb{Z}_N^\star| = N-1$ the logarithm $\log_g y$ of $y \in \mathbb{Z}_N^\star$ to base g is the integer $x \in [1, N-1]$ such that $y = g^x$. We use the extended basis $\bar{\mathbf{B}}_{\alpha,c} = [\mathbf{b}_1, ..., \mathbf{b}_{n+1}] \in \mathbb{R}^{(n+2)\times(n+1)}$ of section 7, where $\mathbf{b}_{n+1}$, related to a large prime $\bar{p}_{n+1} \approx N^c$, yields a nearly shortest vector $\sum_{i=1}^n e_i\mathbf{b}_i - \mathbf{b}_{n+1} \in \mathcal{L}(\bar{\mathbf{B}})$. We compute $\log_g y$ from **CVP**-solutions for the target vectors $\bar{\mathbf{N}} = (0, \cdots, 0, N^c \ln(\bar{N}))^t \in \mathbb{R}^{n+2}$, where $\bar{N} = N/g_y$ and $g_y = g^j y^k \mod N \in [1, N-1]$ for various $j, k \in \mathbb{N}$.

Again we identify vectors $\mathbf{b} = \sum_{i=1}^{n+1} e_i\mathbf{b}_i \in \mathcal{L}(\bar{\mathbf{B}}_{\alpha,c})$ 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 2, 3 from $\mathbf{B}, \mathbf{N}$ to $\bar{\mathbf{B}}_{\alpha,c}, \bar{\mathbf{N}}$ shows the following

Lemma 3. *For a* **CVP***-solution* $\|\mathbf{b} - \bar{\mathbf{N}}\| = \|\mathcal{L} - \bar{\mathbf{N}}\|$ *we have that* $|u\, g_y - vN| \leq p_n^{1/\alpha+\delta+o(1)}$ *if there exists* $\mathbf{b}' = \sum_{i=1}^{n+1} e_i'\mathbf{b}_i \in \mathcal{L}(\bar{\mathbf{B}}_{\alpha,c})$ *with* $e_i' \in \{0, \pm 1\}$ *such that the corresponding* u', v' *satisfy* $|u'\, g_y - v'N| = 1$ *and* $\|\mathbf{b}' - \bar{\mathbf{N}}\|^2 = (2c-1)\ln N + 2\delta \ln p_n$.

Following the proof of Theorem 4 the vector $\mathbf{b}'$ required in Lemma 3 exists for $c = (\ln N)^\beta$ if $\alpha > 2\beta + 2 > 2$ under the assumption that the equation $|u' g_y - \lceil u' g_y/N \rfloor N| = 1$ is for random $u' = O(N^c)$ nearly statistically independent from the event that $u', \lceil u' g_y/N \rfloor$ are squarefree and $(\ln N)^\alpha$–smooth. We assume that a well reduced basis of $\mathcal{L}(\bar{\mathbf{B}}_{\alpha,c})$ starts with the known nearly shortest lattice vector, satisfies GSA and that $\bar{\mathbf{N}}$ satisfies CA for this basis. Then the **CVP** to minimize $\|\mathbf{b} - \bar{\mathbf{N}}\|$ for $\mathbf{b} \in \mathcal{L}(\bar{\mathbf{B}}_{\alpha,c})$ is polynomial time under the volume heuristics because $rd(\mathcal{L}(\bar{B})) = o(n^{-1/4})$, see Theorem 6.

Computing the discrete logarithm from **CVP***-solutions.* By Lemma 3 with $1/\alpha + \delta < 1$ the **CVP**-solution $\mathbf{b} = \sum_{i=1}^{n+1} e_i\mathbf{b}_i$ of $\|\mathbf{b} - \bar{\mathbf{N}}\| = \|\mathcal{L}(\bar{\mathbf{B}}_{\alpha,c}) - \bar{\mathbf{N}}\|$ solves $|u\, g_y - vN| \leq p_n$. Taking $\log_g$-values on $g_y \prod_{i=1}^{n+1} p_i^{e_i} - vN = u\, g_y - vN = \prod_{i=0}^{n+1} p_i^{e_i'}$, with $p_0 = -1$ and $\log_g(-1) = (N-1)/2$, yields

$$\log_g g_y + \textstyle\sum_{i=1}^{n+1}(e_i - e_i')\log_g p_i = e_0' \frac{N-1}{2} \mod (N-1) \tag{8.1}$$

These linear equation in $n+2$ unknowns $\log_g p_i$, $\log_g y$ where $\log_g g_y = j + k\log_g y$. Under the homomorphism $\log_g : \mathbb{Z}_N^\star \to \mathbb{Z}_{N-1}$ the multiples vN of N disappear. So we can determine $\log_g y$ from

$n+2$ linearly independent equations (8.1) where $g_y = g^j y^k \mod N$ ranges over various $j, k \in \mathbb{N}$.

Conclusion. The discrete logarithm $\log_g y$ of $y \in \mathbb{Z}_N^\star$, N prime, can be computed in heuristic polynomial time by solving about $n+2 < (\ln N)^\alpha$ easy **CVP**'s for $\mathcal{L}(\bar{\mathbf{B}}_{\alpha,c})$ and target vectors $\bar{\mathbf{N}}$, $\alpha > 2\beta + 2$. These **CVP**'s are polynomial time under the volume heuristics and standard heuristics if $0 < \frac{\alpha}{\alpha - 2\beta - 2} < c = (\ln N)^\beta$, a well-reduced version of $\bar{\mathbf{B}}_{\alpha,c}$ satisfies GSA and **CVP**-solution for the target vectors $\bar{\mathbf{N}} = (0, \cdots, 0, N^c \ln(\bar{N}))^t \in \mathbb{R}^{n+2}$ with $\bar{N} = N/g^j y^k$ satisfy CA.

Acknowledgment. I am indebted to Phong Nguyen for pointing out inconsistencies and mistakes in several 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, J. Hastad, B. Lange, R. Lindner and M. Rückert for clarifying remarks. I thank B. Lange (U. Frankfurt) for implementing New Enum and for pointing out inconsistent assumptions on GSA, $rd(\mathcal{L})$ and $\|\mathbf{b}_1\|/\lambda_1$. I also thank some anonymous referees for their comments.

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. ECCC, Report No. 5, 1998.

[CEP83] E.R. Canfield, P. Erdös and C. Pomerance, On a problem of Oppenheim concerning "Factorisatio Numerorum". *J. of Number Theory*, **17**, pp. 1–28, 1983.

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

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

[GNR10] *N. Gama, P.Q. Nguyen and O. Regev*, Lattice enumeration using extreme pruning, Proc. EUROCRYPT 2010, LNCS 6110, Springer-Verlag, pp. 257–278, 2010; final version to be published.

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

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

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

[HS07] *G. Hanrot and D. Stehlé*, Improved analysis of KannaNs shortest lattice vector algorithm. In Proc. CRYPTO 2007, LNCS 4622, Springer-Verlag, pp. 170–186, 2007.

[HS08] *G. Hanrot and D. Stehlé*, Worst-case Hermite-Korkine-Zolotarev reduced lattice bases. CoRR, abs/0801.3331, http://arxix.org/abs/0801.3331.

[Ka87] *R. Kannan*, Minkowski's convex body theorem and integer programming. *Math. Oper. Res.*, **12**, pp. 415–440, 1987.

[KL78] *G.A. Kabatiansky and V.I. Levenshtein*, Bounds for packing on a sphere and in space. *Problems of Information Transmission*, **14**, pp. 1–17, 1978.
[LLL82] *H.W. Lenstra Jr., A.K. Lenstra and L. Lovász*, Factoring polynomials with rational coefficients, Mathematische Annalen 261, pp. 515–534, 1982.
[L86] *L. Lovász*, An Algorithmic Theory of Numbers, Graphs and Convexity, SIAM, 1986.
[LM09] *V. Lubashevsky and D. Micciancio*, On bounded distance decoding, unique shortest vectors and the minimum distance problem. In Proc. CRYPTO 2009, LNCS 5677, Springer-Verlag, pp. 577–594, 2009.
[MO90] *J. Mazo and A. Odlydzko*, Lattice points in high-dimensional spheres. Monatsh. Math. 110, pp. 47–61, 1990.
[M04] *D. Micciancio*, Almost perfect lattices, the covering radius problem, and applications to Ajtai's connection factor. SIAM J. on Computing, **37**(1), pp. 118–169, 2004.
[MG02] *D. Micciancio and S. Goldwasser*, Complexity of Lattice Problems: A Cryptographic Perspective. Kluwer Academic Publishers, Boston, London, 2002.
[MR07] *D. Micciancio and O. Regev*, Worst-case to average-case reduction based on gaussian measures. SIAM J. on Computing, **37**(1), pp. 267–302, 2007.
[MV09] *D. Micciancio and P. Voulgaris* Faster exponential time algorithms for the shortest vector problem. ECCC Report No. 65, 2009
[NS06] *P.Q. Nguyen and D. Stehlé*, LLL on the average. In Proc. of ANTS-VII, LNCS 4076, Springer-Verlag, 2006.
[N10] *P.Q. Nguyen*, Hermite's Constant and Lattice Algorithms. in The LLL Algorithm, Eds. P.Q. Nguyen, B. Vallée, Springer-Verlag, Jan. 2010.
[S87] *C.P. Schnorr*, A hierarchy of polynomial time lattice basis reduction algorithms. *Theoret. Comput. Sci.*, **53**, pp. 201–224, 1987.
[S93] *C.P. Schnorr*, Factoring integers and computing discrete logarithms via Diophantine approximation. In *Advances in Computational Complexity*, AMS, *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, **13**, pp. 171–182, 1993. Preliminary version in Proc. EUROCRYPT'91, LNCS 547, Springer-Verlag, pp. 281–293, 1991. //www.mi.informatik.uni-frankfurt.de.
[SE94] *C.P. Schnorr and M. Euchner*, Lattce basis reduction: Improved practical algorithms and solving subset sum problems. Mathematical Programming **66**, pp. 181–199, 1994. //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. In
[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
[S06] *C.P. Schnorr*, Fast LLL-type lattice reduction. Information and Computation, **204**, pp. 1–25, 2006. //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, The LLL Algorithm, Eds. P.Q. Phong, B. Vallée, Springer Verlag, Jan 2010. //www.mi.informatik.uni-frankfurt.de

9 Appendix. Example Relations

Let $N = 100000980001501 \approx 10^{14}$. We give example relations (7.2) of the form $|u - vN| \leq p_{125}^2$ such that $u, v, |u - vN|$ are p_{125}-smooth for $p_{125} = 691$. The examples show that there are much more relations (7.2) than one would expect from the bounds of Theorems 4 and 5. New Enum generates each of these relations (7.2) in just a few seconds on a current PC.

New Enum for **SVP** is applied to variants of BKZ-bases of $\mathcal{L}(\mathbf{N}, \mathbf{B}_{\alpha,c})$ with blocksize 20 / 32. New Enum restricted to success probability $\beta_t \geq 2^{-18}$ and pruned if $\beta_t < 2^{-18}$ performs in general about10^6 stages, taking a couple of seconds per found relation (7.2). In order to find many relations (7.2) we iterate New Enum over the $N^c = N2^\ell$ for $\ell = -4, ..., 10$, and we let New Enum search distinct parts of the enumeration tree. In these experiments $c \approx 1$, $\beta = \ln c / \ln \ln N \approx 0$ and $\alpha \approx 1.94$ are clearly smaller than required for Theorems 4, 6. Moreover $rd(\mathcal{L}(\mathbf{N}, \mathbf{B}_{\alpha,1})) \approx 0.56 > n^{-1/4} \approx 0.3$ is larger than required for Cor. 3 and Theorem 6.

	u	v	$\lvert u - vN\rvert$
1.	$3 \cdot 5^2 \cdot 7 \cdot 17 \cdot 29 \cdot 101 \cdot 103 \cdot 109 \cdot 127 \cdot 151 \cdot 181$	$61 \cdot 167$	$2^2 \cdot 503$
2.	$2 \cdot 19 \cdot 23 \cdot 29 \cdot 41 \cdot 83 \cdot 103 \cdot 107 \cdot 137 \cdot 181 \cdot 193$	$7 \cdot 67 \cdot 97$	$5 \cdot 13 \cdot 101$
3.	$2^2 \cdot 3 \cdot 23 \cdot 41 \cdot 79 \cdot 97 \cdot 131 \cdot 151 \cdot 211 \cdot 239$	$5 \cdot 173$	$17 \cdot 31$
4.	$31 \cdot 41 \cdot 61 \cdot 67 \cdot 89 \cdot 109 \cdot 181 \cdot 223 \cdot 601$	$2 \cdot 3 \cdot 17 \cdot 127$	$7^2 \cdot 641$
5.	$3^2 \cdot 5 \cdot 29 \cdot 31 \cdot 37 \cdot 61 \cdot 73 \cdot 79 \cdot 97 \cdot 181 \cdot 191 \cdot 461$	$7 \cdot 41 \cdot 113 \cdot 251$	$2 \cdot 167$
6.	$5 \cdot 11 \cdot 19 \cdot 47 \cdot 50 \cdot 73 \cdot 127 \cdot 149 \cdot 151 \cdot 331 \cdot 467$	$2 \cdot 29 \cdot 89 \cdot 181$	$113 \cdot 691$
7.	$2 \cdot 3 \cdot 5 \cdot 31 \cdot 37 \cdot 59 \cdot 97 \cdot 103 \cdot 173 \cdot 199 \cdot 233 \cdot 239$	$11 \cdot 23 \cdot 29 \cdot 53$	$107 \cdot 307$
8.	$7 \cdot 17 \cdot 19 \cdot 37 \cdot 59 \cdot 61 \cdot 67 \cdot 71 \cdot 89 \cdot 223 \cdot 467$	$2 \cdot 3 \cdot 5 \cdot 41 \cdot 107$	601
9.	$2 \cdot 3 \cdot 7 \cdot 11 \cdot 71 \cdot 103 \cdot 127 \cdot 137 \cdot 293 \cdot 389$	67	$13 \cdot 167$
10.	$2 \cdot 7 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 71 \cdot 89 \cdot 149 \cdot 239 \cdot 503$	3^2	$5 \cdot 61$
11.	$11^2 \cdot 13 \cdot 23 \cdot 29 \cdot 37 \cdot 41 \cdot 67 \cdot 89 \cdot 113 \cdot 131 \cdot 191$	$53 \cdot 61 \cdot 89$	$2 \cdot 19 \cdot 653$
12.	$3 \cdot 13 \cdot 31 \cdot 53 \cdot 67 \cdot 127 \cdot 137 \cdot 661$	$2^3 \cdot 17$	$7^2 \cdot 53$
13.	$2^2 \cdot 5 \cdot 19 \cdot 23 \cdot 29 \cdot 37 \cdot 67 \cdot 149 \cdot 173 \cdot 251 \cdot 263$	$11 \cdot 71 \cdot 389$	$3^2 \cdot 367$
14.	$5 \cdot 7 \cdot 11 \cdot 43 \cdot 79 \cdot 139 \cdot 181 \cdot 199 \cdot 269 \cdot 277 \cdot 593$	$3 \cdot 37 \cdot 113 \cdot 233$	$2^3 \cdot 613$
15.	$2^2 \cdot 11 \cdot 37 \cdot 59 \cdot 61 \cdot 83 \cdot 89 \cdot 137 \cdot 181 \cdot 223 \cdot 229 \cdot 359$	$7 \cdot 19 \cdot 53 \cdot 103 \cdot 271$	$113 \cdot 401$
16.	$19 \cdot 29 \cdot 59 \cdot 79 \cdot 83 \cdot 181 \cdot 211 \cdot 229 \cdot 431 \cdot 479$	$2 \cdot 7 \cdot 17 \cdot 103 \cdot 157$	$5 \cdot 269$
17.	$11^2 \cdot 13 \cdot 43 \cdot 53 \cdot 59 \cdot 73 \cdot 79 \cdot 157 \cdot 163 \cdot 197$	$7^2 \cdot 17 \cdot 103 \cdot 173 \cdot 313$	$2 \cdot 97$
18.	$5 \cdot 7 \cdot 29 \cdot 53 \cdot 67 \cdot 107 \cdot 139 \cdot 151 \cdot 167 \cdot 191 \cdot 233 \cdot 251$	$11 \cdot 13 \cdot 17 \cdot 179 \cdot 347$	$2 \cdot 3^2 \cdot 131$
19.	$2 \cdot 3 \cdot 31 \cdot 59 \cdot 73 \cdot 157 \cdot 197 \cdot 199 \cdot 227 \cdot 233 \cdot 263 \cdot 281$	$11 \cdot 37 \cdot 97 \cdot 167 \cdot 293 \cdot 349$	$5^2 \cdot 379$
20.	$2 \cdot 11 \cdot 23 \cdot 73 \cdot 83 \cdot 281 \cdot 313 \cdot 347 \cdot 353 \cdot 383$	$13 \cdot 37 \cdot 263$	683
21.	$3 \cdot 5 \cdot 23 \cdot 37 \cdot 67 \cdot 79 \cdot 103 \cdot 107 \cdot 127 \cdot 191 \cdot 229$	$7 \cdot 19 \cdot 311$	$2 \cdot 233 \cdot 383$
22.	$3^2 \cdot 7 \cdot 11 \cdot 13 \cdot 47 \cdot 101 \cdot 107 \cdot 151 \cdot 157 \cdot 283$	307	$2 \cdot 53 \cdot 89$
23.	$3 \cdot 41 \cdot 61 \cdot 103 \cdot 107 \cdot 163 \cdot 197 \cdot 239 \cdot 367$	$17 \cdot 137$	$2^3 \cdot 5 \cdot 13 \cdot 59$
24.	$13 \cdot 29 \cdot 47 \cdot 53 \cdot 61 \cdot 83 \cdot 103 \cdot 163 \cdot 233$	$3^3 \cdot 37 \cdot 97$	$2 \cdot 673$
25.	$5 \cdot 7 \cdot 31 \cdot 41 \cdot 67 \cdot 167 \cdot 191 \cdot 211 \cdot 229 \cdot 421$	$83 \cdot 233$	$2 \cdot 3^2 \cdot 13 \cdot 181$
26.	$7 \cdot 23 \cdot 37 \cdot 59 \cdot 97 \cdot 107 \cdot 127 \cdot 149 \cdot 263 \cdot 347$	$5 \cdot 43 \cdot 293$	$2^2 \cdot 3 \cdot 53 \cdot 101$
27.	$5 \cdot 23^2 \cdot 29 \cdot 83 \cdot 101 \cdot 163 \cdot 197 \cdot 199 \cdot 337$	$61 \cdot 227$	$2^2 \cdot 3 \cdot 13 \cdot 67$
28.	$7 \cdot 23 \cdot 41 \cdot 43 \cdot 89 \cdot 103 \cdot 179 \cdot 193 \cdot 241 \cdot 389$	$11 \cdot 17 \cdot 163$	$2^4 \cdot 59 \cdot 263$
29.	$7 \cdot 17 \cdot 23 \cdot 73 \cdot 107 \cdot 167 \cdot 179 \cdot 197 \cdot 271 \cdot 503$	$13 \cdot 43 \cdot 307$	$2 \cdot 163 \cdot 577$
30.	$7 \cdot 11 \cdot 17 \cdot 53 \cdot 73 \cdot 103 \cdot 107 \cdot 139 \cdot 181 \cdot 223 \cdot 367$	$31 \cdot 131 \cdot 283$	$2^4 \cdot 59 \cdot 461$
31.	$11^2 \cdot 13 \cdot 23 \cdot 29 \cdot 37 \cdot 41 \cdot 67 \cdot 89 \cdot 113 \cdot 131 \cdot 191$	$53 \cdot 61 \cdot 83$	$2 \cdot 19 \cdot 653$
32.	$5 \cdot 11 \cdot 13 \cdot 23 \cdot 29 \cdot 61 \cdot 67 \cdot 89 \cdot 97 \cdot 107 \cdot 139 \cdot 149 \cdot 349$	$7 \cdot 17 \cdot 79 \cdot 109 \cdot 127$	$2^4 \cdot 3 \cdot 47 \cdot 113$
33.	$5 \cdot 13 \cdot 19 \cdot 23 \cdot 29 \cdot 37 \cdot 47 \cdot 109 \cdot 127 \cdot 179 \cdot 307 \cdot 571$	$11 \cdot 31 \cdot 71 \cdot 257$	$2^2 \cdot 3 \cdot 17 \cdot 283$
34.	$2 \cdot 3 \cdot 5 \cdot 13 \cdot 29 \cdot 43 \cdot 73 \cdot 139 \cdot 157 \cdot 167 \cdot 233 \cdot 241$	$7 \cdot 97 \cdot 107$	$17^2 \cdot 47$

	u	v	$\lvert u - vN\rvert$
35.	$5 \cdot 11 \cdot 31 \cdot 41 \cdot 43 \cdot 53 \cdot 257 \cdot 271 \cdot 313 \cdot 373$	$2 \cdot 3 \cdot 17 \cdot 127$	$19 \cdot 449$
36.	$11 \cdot 13 \cdot 17 \cdot 67 \cdot 79 \cdot 157 \cdot 173 \cdot 197 \cdot 223 \cdot 233$	$83 \cdot 431$	$2^3 \cdot 19 \cdot 29 \cdot 31$
37.	$2 \cdot 3 \cdot 7^2 \cdot 53 \cdot 61 \cdot 97 \cdot 109 \cdot 139 \cdot 227 \cdot 277 \cdot 313 \cdot 577$	$43 \cdot 71 \cdot 223 \cdot 233$	$13 \cdot 73 \cdot 251$
38.	$2 \cdot 3 \cdot 59 \cdot 79 \cdot 103 \cdot 191 \cdot 193 \cdot 197 \cdot 251 \cdot 263$	$73 \cdot 173$	$7 \cdot 17 \cdot 269$
39.	$3 \cdot 23 \cdot 41 \cdot 43 \cdot 107 \cdot 113 \cdot 179 \cdot 211 \cdot 269 \cdot 277$	$11 \cdot 53 \cdot 71$	$2^{10} \cdot 251$
40.	$97 \cdot 163 \cdot 191 \cdot 211 \cdot 229 \cdot 257 \cdot 277 \cdot 317$	$13 \cdot 17 \cdot 149$	$2 \cdot 7 \cdot 103 \cdot 179$
41.	$3 \cdot 11 \cdot 37 \cdot 43 \cdot 53 \cdot 113 \cdot 131 \cdot 139 \cdot 167 \cdot 233 \cdot 251$	$23 \cdot 41 \cdot 593$	$2^2 \cdot 7 \cdot 647$
42.	$3 \cdot 7 \cdot 19 \cdot 53 \cdot 61 \cdot 67 \cdot 139 \cdot 149 \cdot 293 \cdot 337 \cdot 389$	$23 \cdot 167 \cdot 179$	$2^2 \cdot 109 \cdot 113$
43.	$7 \cdot 11 \cdot 23 \cdot 47 \cdot 59 \cdot 113 \cdot 163 \cdot 199 \cdot 269 \cdot 349$	$3 \cdot 43 \cdot 131$	$2^2 \cdot 19 \cdot 439$
44.	$17 \cdot 23 \cdot 41 \cdot 71 \cdot 79 \cdot 149 \cdot 239 \cdot 251 \cdot 263 \cdot 311$	$37 \cdot 109 \cdot 163$	$2^3 \cdot 47 \cdot 463$
45.	$3^2 \cdot 23 \cdot 29 \cdot 37 \cdot 97 \cdot 131 \cdot 229 \cdot 263 \cdot 523$	$7 \cdot 127$	$2^3 \cdot 59$

Comments We spedify the lattice reduction and the lattice bases that provide these relations.
1. - 18. These relations result from BKZ-reduction with blocksize 20 /32 of the basis $(\mathbf{N}, \mathbf{B}_{\alpha,c})$ of dimension $n = 126$, followed by NEW ENUM pruned to stages of success rate $\beta_t \geq 2^{-18}$ and letting N^c range over $N/2^5 \leq N^c \leq N2^{10}$. Relations **6. 7. 8.** all result from BKZ-20 reduction of the same input $N^c = N \cdot 10$ and continued NEW ENUM iteration. Relations **1. 10. 11** resp. **12. 17. 19.** result directly from BKZ-20, resp. BKZ-32 without invoking NEW ENUM. NEW ENUM's time increases with N^c, e.g., 48 seconds for $N^c = N2^{10}, N2^{11}$ for relations **14. 15.**, 76 seconds for $N^c = N2^{11}$, relation **16** and 155 seconds for $N^c = N2^{16}$, relation **18.**.

In order to work with small numbers even for large c we iteratively increase N to $2N$: multiply the $n+1$-coordinates of all basis vectors of the reduced basis by 2 and then resume the reduction.

19. Here $N^c = N\,2^{18}$ yields large u, v.
20. We have increased the diagonal entries $\sqrt{\ln p_i}$ of $\mathbf{B}_{\alpha,c}$ to $\sqrt{2 \ln p_i}$ for the first 50 primes $2, ..., 229$. The resulting relation (7.2) has 6 prime factors of u, v that are larger than 229.
21. - 24. The prime 2 has been eliminated from the prime base of $\mathbf{B}_{\alpha,c}$.
25. - 33. The primes 2 and 3 have both been eliminated from the prime base.
34. - 37. The primes 2, 3 have been eliminated but the non prime 6 has been added to the base.
38. The diagonal entries $\sqrt{\ln p_i}$ of the basis matrix have been steadily increased for $i < n$.
39 - 45. The primes 2 and 5 have been eliminated from the prime basis.
40 - 42. The diagonal entries $\sqrt{\ln p_i}$ of the basis matrix have been steadily increased for $i < n$.
Comparison with [S93]. [S93] reports on experiments for $N = 2131438662079 \approx 2.1 \cdot 10^{12}$, $N^c = 10^{25}$, $c \approx 2.00278$ and the prime lattice basis with diagonal entries $\ln p_i$ for $i = 1, ..., n$. The larger diagonal entries $\ln p_i$ require a larger c and this increases the time for the construction of relations (7.2). The latter took 10 hours per found relation on a PC of 1993 per found relation.

Conclusions. Many more relations (7.2) should be obtained by eliminating from a previous input basis that resulted in a relation (7.2) of the form $|u - vN| \leq p_{125}^2$ some prime factor of uv.

Interestingly 32 of the 45 relations above are relations for the first 100 primes 2,...,541. This may indicate that we can factor integers of order 10^{14} by using merely the first 100 primes. Then $\alpha = 1.865$ would be sufficient for $N \approx 19^{14}$.

The v value of the constructed relations is clearly larger than the N^{c-1} value of the given lattice basis. For instance v of relation **19.** satisfies $v \approx 2.57 \cdot 10^6 \cdot 2^{18} = 2.57 \cdot 10^6 \cdot N^{c-1}$.
In fact this increases N^c by a factor $2.57 \cdot 10^6$. Therefore the c value of Theorems 4 and 6 must be clearly larger than the c value of the given prime basis. This partly explains why the inequality $0 < \frac{\alpha-\beta-1}{\alpha-2\beta-2} < c = (\ln N)^\beta$ required for Theorems 4 and 6 is to demanding.

Extrapolation for factoring larger integers N**.** If $\alpha = 1.865$ is sufficient for factoring $N \approx 2^{750}$ then we can factor integers $N \approx 2^{750}$ by using the $10000 = 10^4$ smallest primes. For $n = 10^4$ our construction of relations (7.2) should still be feasable