Factoring Integers by CVP and SVP Algorithms

Claus Peter Schnorr

Fachbereich Informatik und Mathematik,
Goethe-Universität Frankfurt, PSF 111932,
D-60054 Frankfurt am Main, Germany.
schnorr@cs.uni-frankfurt.de
work in progress 23.02.2017

Abstract. We factor an integer N by enumeration algorithms that find vectors of the prime number lattice $\mathcal{L}(\mathbf{B}_{n,c})$ close to a specific target vector $\mathbf{N}_c$ representing N. The algorithm New Enum performs the stages of exhaustive enumeration of close, respectively short lattice vectors in order of decreasing success rate, stages with high success rate are done first. These algorithms generate for the n-th prime p_n triples of p_n-smooth integers $u, v, |u - vN|$ that factorize the integer N. An integer N can be factored by about $n + 1$ p_n-smooth triples $u, v, |u - vN|$. Our **CVP**-algorithm generates for $n = 90$, $n + 1$ such relations and factors $N \approx 10^{14}$ in 6.2 seconds.

Keywords. Factoring integers, enumeration of close lattice vectors, the prime number lattice.

1 Introduction and surview

The enumeration algorithm Enum of [SE94, SH95] for **SVP** / **CVP** for short / close lattice vectors performs stages in order of decreasing success rate, stages with high success rate are done first. New Enum finds short / close vectors much faster than previous **SVP** and **CVP** algorithms of Kannan [Ka87] and Fincke, Pohst [FP85] that disregard the success rate of stages. This greatly reduces the number of stages that precede the finding of a shortest / closest lattice vector.

Section 4 summarizes results on time bounds of Enum under **linear pruning** for **SVP** / **CVP** for a lattice basis $\mathbf{B} = [\mathbf{b}_1, ..., \mathbf{b}_n] \in \mathbb{Z}^{n\times n}$ that satisfies **GSA** (i.e., the local reduction strength of the reduced basis is "uniform" for all 2-dimensional basis blocks). Prop. 1 shows that Enum finds under linear pruning a shortest lattice vector $\mathbf{b}$ that behaves randomly (**SA**) under the volume heuristics in polynomial time if $rd(\mathcal{L}) = o(n^{-1/4})$ holds for the relative density $rd(\mathcal{L})$ of $\mathcal{L}$, defined in section 2. It follows that the maximal **SVP**-time of Enum under linear pruning for lattices of dim. n is $2^{\frac{8}{n}+o(n)}$. Cor. 3 translates Prop. 1 from **SVP** to **CVP** proving pol. time under similar conditions as Prop. 1 if $\|\mathcal{L} - \mathbf{t}\| \lesssim \lambda_1$ holds for the target vector $\mathbf{t}$.

Sections 5 and 6 study factoring integers N by approximate **CVP** solutions for the prime number lattice $\mathcal{L}(\mathbf{B}_{n,c})$ and a target vector $\mathbf{N}_c$ that represents N. These **CVP** solutions provide p_n-smooth triples of integers $u, v, |u - vN|$. Given $n + 1$ such triples we can easily factor N. For given N, n, c we determine $\delta \in \mathbb{R}_+$ that maximizes the number of p_n-smooth triples $u, v, |u - vN|$ in the range $\frac{1}{2}N^\delta \le v \le N^\delta$, $|u - vN| \le p_n^3$. We can efficiently enumerate these p_n-smooth triples by the **CVP**-algorithm for the prime number lattice $\mathcal{L}(\mathbf{B}_{n,c})$, target vector $\mathbf{N}_c$ and $c = \delta + 1 - \frac{3 \ln p_n}{\ln N}$. Under heuristic assumptions this **CVP**-algorithm is polynomial time due to Prop.1, 2 and 3 and Cor. 3 of section 4. These time bounds, i.e., their bounds on the number of performed stages also hold for New Enum because stages that are cut under linear pruning have extremely small success rate and are not performed by New Enum. We explain the example factorization of some $N \approx 10^{14}$ using the $n = 90$ smallest primes by New Enum and study its extension to $N \approx 2^{800}$.

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 $\mathcal{L}$ 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 minimal γ such that $\lambda_1^2 \leq \gamma(\det \mathcal{L})^{2/n}$ holds for all lattices of dimension n.

Let $\mathbf{B} = \mathbf{QR} \in \mathbb{R}^{m\times n}$, $\mathbf{R} = [r_{i,j}]_{1\leq i,j\leq n} \in \mathbb{R}^{n\times n}$ the unique $\mathbf{QR}$-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 $\mathbf{QR}$-factorization 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 $\mathrm{span}(\mathbf{b}_1, ..., \mathbf{b}_{i-1})^\perp$ has length $r_{i,i} = \|\mathbf{b}_i^*\|$, $r_{1,1} = \|\mathbf{b}_1\|$, .

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

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

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

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

A basis $\mathbf{B} = \mathbf{QR} \in \mathbb{R}^{m\times n}$ is an HKZ-*basis* (HERMITE, KORKINE, ZOLOTAREFF) if $|r_{i,j}|/r_{i,i} \leq \frac{1}{2}$ 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 $\mathbf{BT}$, $\mathbf{T} \in \mathrm{GL}_n(\mathbb{Z})$ that preserve $\mathbf{b}_1, ..., \mathbf{b}_{i-1}$.

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

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 $\mathbf{t} \in \mathrm{span}(\mathcal{L})$ find a closest vector $\mathbf{b}' \in \mathcal{L}$ such that $\|\mathbf{t} - \mathbf{b}'\| = \|\mathbf{t} - \mathcal{L}\| =_{def} \min\{\, \|\mathbf{t} - \mathbf{b}\| \mid \mathbf{b} \in \mathcal{L}\,\}$.

The efficiency of our algorithms 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 $0 < rd(\mathcal{L}) \leq 1$ holds for all $\mathcal{L}$, and $rd(\mathcal{L}) = 1$ if and only if $\mathcal{L}$ has maximal density. Lattices of maximal density and γ_n are known for $n = 1, ..., 8$ 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. 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 by performing the stages in order of decreasing success rate.

Let $\mathbf{B} = [\mathbf{b}_1, ..., \mathbf{b}_n] = \mathbf{QR} \in \mathbb{Z}^{m\times n}$, $\mathbf{R} = [r_{i,j}]_{1\leq i,j\leq n} \in \mathbb{R}^{n\times n}$ be the given basis of $\mathcal{L} = \mathcal{L}(\mathbf{B})$. Let $\pi_t : \mathrm{span}(\mathbf{b}_1, ..., \mathbf{b}_n) \to \mathrm{span}(\mathbf{b}_1, ..., \mathbf{b}_{t-1})^\perp = \mathrm{span}(\mathbf{b}_t^*, ..., \mathbf{b}_n^*)$ 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 $A \geq \lambda_1^2$ are given at stage $(u_t, ..., u_n)$ of ENUM [SH95]. That stage calls the substages $(u_{t-1}, ..., u_n)$ such that $\|\pi_{t-1}(\sum_{i=t-1}^n u_i \mathbf{b}_i)\|^2 \leq A$. 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 $\zeta_t := \mathbf{b} - \pi_t(\mathbf{b}) \in \mathrm{span}\,\mathcal{L}_t$ is $\mathbf{b}$'s orthogonal projection in $\mathrm{span}\,\mathcal{L}_t$. Stage $(u_t, ..., u_n)$ and its substages exhaustively enumerate the intersection $\mathcal{B}_{t-1}(\zeta_t, \varrho_t) \cap \mathcal{L}_t$ for the sphere $\mathcal{B}_{t-1}(\zeta_t, \varrho_t) \subset \mathrm{span}\,\mathcal{L}_t$ with radius $\varrho_t := (A - \|\pi_t(\mathbf{b})\|^2)^{1/2}$ and center ζ_t.

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

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

Here $\mathrm{vol}\,\mathcal{B}_{t-1}(\zeta_t, \varrho_t) = V_{t-1}\varrho_t^{t-1}$, $V_{t-1} = \pi^{\frac{t-1}{2}}/(\frac{t-1}{2})! \approx (\frac{2e\pi}{t-1})^{\frac{t-1}{2}}/\sqrt{\pi(t-1)}$ 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 $\mathrm{E}_{\zeta_t}[\ \#\big(|\mathcal{B}_{t-1}(\zeta_t,\varrho_t)\cap\mathcal{L}_t\big)\ ]=\beta_t$. 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 first performs all stages with sufficiently large β_t giving priority to small t and collects during this process the unperformed stages in the list L. For instance it first performs all stages with $\lg\beta_t \geq -s+\lceil \lg\lg t\rceil$, i.e. $\beta_t\geq 2^{-s+\lceil\lg\lg t\rceil}$, where $\lg := \log_2$. Thereafter New Enum inceases s to $s+1$. So far our experiments perform all stages with $\beta_t\geq 2^{-s}$.

We will use that $A := \frac{n}{4}\,(\det \mathbf{B}^t\mathbf{B})^{1/n} > \lambda_1^2$ holds for $n\geq 10$ where $\gamma_n<\frac{n}{4}$.
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 $\mathbf{B}=\mathbf{QR}\in\mathbb{Z}^{m\times n}$, $\mathbf{R}=[r_{i,j}]\in\mathbb{R}^{n\times n}$ for block size 32,
`OUTPUT` a sequence of $\mathbf{b}\in\mathcal{L}(\mathbf{B})$ of decreasing length terminating with $\|\mathbf{b}\|=\lambda_1$.

1. Start at *level* $s:=\lceil\lg\lg n\rceil$, $L:=\emptyset$, $A:=\frac{n}{4}(\det\mathbf{B}^t\mathbf{B})^{1/n}$ or $A:=\lambda_1^2$
2. *Perform via algorithm* Enum *of [SE94, SH95], all stages with* $\beta_t\geq 2^{-s+\lceil\lg\lg t\rceil}$: Upon entry of stage $(u_t,...,u_n)$ compute β_t. If $\beta_t<2^{-s+\lceil\lg\lg t\rceil}$ then store $(u_t,...,u_n)$ 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. $s:=s+1$, `IF` $L\neq\emptyset$ `THEN GO TO 2` (*to perform all stages* $(u_t,...,u_n)$ *of* L *with* $\beta_t\geq 2^{-s+\lceil\lg\lg t\rceil}$.) `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 $\mathbf{R}$, $\beta_t, V_t, \varrho_t, c_t$ 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 the final $\mathbf{b}$.

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 $\|\pi_t(\mathbf{b})\|^2\approx\frac{n-t+1}{n}\|\mathbf{b}\|^2$ holds for a random $\mathbf{b}\in_R\mathcal{B}_n(\mathbf{0},\lambda)$ of length λ.) Therefore $\varrho_t^2=A-\|\pi_t(\mathbf{b})\|^2$ 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 $\beta_t=V_{t-1}\varrho_t^{t-1}/\det\mathcal{L}_t$ where on average $\varrho_t^2=\lambda_1^2-\|\pi_t(\mathbf{b}_t')\|^2\approx\frac{t-1}{n}\lambda_1^2$ 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 $c_t:\mathbb{Z}^{n-t+1}\to\mathbb{R}$:

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

Hence
$$c_t(u_t,...,u_n)=(\textstyle\sum_{i=t}^n u_ir_{t,i})^2+c_{t+1}(u_{t+1},...,u_n).$$

Given $u_{t+1},...,u_n$ Enum tests for u_t the integers closest to $-y_t:=-\sum_{i=t+1}^n u_ir_{t,i}/r_{t,t}$ in order of increasing distance to $-y_t$ adding to the initial $u_t:=-\lceil y_t\rfloor$ iteratively $\lfloor\nu_t/2\rfloor(-1)^{\nu_t}\varsigma_t$ where $\varsigma_t:=sign(u_t+y_t)\in\{\pm1\}$ and ν_t numbers the iterations starting with $\nu_t=0,1,2,..$:

$$-\lceil y_t\rfloor,\ -\lceil y_t\rfloor-\varsigma_t,\ -\lceil y_t\rfloor+\varsigma_t,\ -\lceil y_t\rfloor-2\varsigma_t,\ -\lceil y_t\rfloor+2\varsigma_t,\cdots,-\lceil y_t\rfloor+\lfloor\nu_t/2\rfloor(-1)^{\nu_t}\varsigma_t,\cdots$$

Let $sign(0):=1$ and let $\lceil r\rfloor$ denote a nearest integer to $r\in\mathbb{R}$. The iteration does not decrease $|u_t+y_t|$ and $c_t(u_t,...,u_n)$, it does not increase ϱ_t and β_t. 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. The center $\zeta_t=\mathbf{b}-\pi_t(\mathbf{b})=\sum_{i=t}^n u_i(\mathbf{b}_i-\pi_t(\mathbf{b}_i))\in\operatorname{span}(\mathcal{L}_t)$ changes continously within New Enum.

Algorithm Enum adapted from [SH95]

`INPUT` BKZ-basis $\mathbf{B} = \mathbf{QR} \in \mathbb{Z}^{m\times n}$, $\mathbf{R} = [r_{i,j}] \in \mathbb{R}^{n\times n}$ for block size 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` $c_t < \bar{c}_1$ and $t > 1$ `THEN` [$t := t - 1, \nu_t := 1, y_t := \sum_{i=t+1}^{t_{max}} u_i r_{t,i}/r_{t,t}$
   $u_t := -\lceil y_t \rfloor,\ \varsigma_t := sign(u_t - y_t)$]
   `ELSE` [`IF` $c_t < \bar{c}_1$ and $t = 1$ `THEN` $\bar{c}_1 := c_1,\ \mathbf{b} := \sum_{i=1}^{n} u_i \mathbf{b}_i,\ t := t + 1$
   $t_{max} := \max(t, t_{max})$, `IF` $t = t_{max}$ `THEN` $u_t := u_t + 1, \nu_t := 1$
   `ELSE` $u_t := -\lceil y_t \rfloor + \lfloor \nu_t/2 \rfloor (-1)^{\nu_t} \varsigma_t,\ \nu_t := \nu_t + 1.$].
3. `output` $\mathbf{b}$

New Enum for SVP

`INPUT` BKZ-basis $\mathbf{B} = \mathbf{QR} \in \mathbb{Z}^{m\times n}$, $\mathbf{R} = [r_{i,j}] \in \mathbb{R}^{n\times n}$ of block size 32, $s = \lceil \lg\lg n \rceil$,
`OUTPUT` a sequence of $\mathbf{b} \in \mathcal{L}(\mathbf{B})$ such that $\|\mathbf{b}\|$ decreases to λ_1.

1. $L := \emptyset$, $t := t_{max} := 1$,, `FOR` $i = 1, ..., n$ `DO` $c_i := u_i := y_i := 0$, $\nu_t := u_1 := 1$,
   $c_1 := r_{1,1}^2$, $A := \frac{n}{4}(\det \mathbf{B}^t B)^{1/n}$ ($c_t = c_t(u_t, ..., u_n)$ *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` $c_t \geq A$ `THEN GO TO` 2.1,
   $\varrho_t := (A - c_t)^{1/2},\ \beta_t := V_{t-1}\varrho_t^{t-1}/(r_{1,1}\cdots r_{t-1,t-1})$,
   `IF` $t = 1$ `THEN` [$\mathbf{b} := \sum_{i=1}^{n} u_i \mathbf{b}_i$,
   `IF` $\|\mathbf{b}\|^2 < A$ `THEN output` $\mathbf{b}$, $A := \|\mathbf{b}\|^2 - 1$, `GO TO 2.1`],
   `IF` $\beta_t \geq 2^{-s+\lceil \lg\lg t \rceil}$ `THEN` [$t := t - 1,\ y_t := \sum_{i=t+1}^{t_{max}} u_i r_{t,i}/r_{t,t}, u_t := -\lceil y_t \rfloor$,
   $\varsigma_t := sign(u_t - y_t),\ \nu_t := 1,$ `GO TO 2`]
   `ELSE` store $(u_t, ...u_n, y_t, c_t, \nu_t, \beta_t, A)$ 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` $u_t := -\lceil y_t \rfloor + \lfloor \nu_t/2 \rfloor (-1)^{\nu_t} \varsigma_t,\ \nu_t := \nu_t + 1.$]]

3. $s := s + 1$, perform step 2 for all delayed stages $(u_t, ..., u_n, y_t, c_t, \nu_t, \beta_t, A)$ of L.
   Delay new stages with $\beta_{t'} < 2^{-s+\lceil \lg\lg t' \rceil}$ and store in L.
4. `IF` $L \neq \emptyset$ `THEN GO TO 3 ELSE` terminate.

The performance of step 2 for a delayed stage $(u_t, ..., u_n, y_t, c_t, \nu_t, \beta_t, A)$ does not perform any stages $(u_{t"}, ..., u_n)$ with $t" > t$. The t-value t' cannot surpass within step 2 the t-value at the restart.

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

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 $\|\mathbf{t} - \mathbf{b}\|^2$.

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.

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 $\mathbf{t}$:

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

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

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

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 solving **CVP** for $(\pi_t(\mathcal{L}), \pi_t(\mathbf{t}))$ for $t = n, ..., 1$.

New Enum for CVP

`INPUT` BKZ-basis $\mathbf{B} = \mathbf{QR} \in \mathbb{Z}^{m\times n}$ of block size 32, $\mathbf{R} = [r_{i,j}] \in \mathbb{R}^{n\times n}$, $s = \lceil \lg\lg t \rceil$, $\mathbf{t} = \sum_{i=1}^n \tau_i \mathbf{b}_i \in \text{span}(\mathcal{L})$, $\tau_1, ..., \tau_n \in \mathbb{Q}$, $\ddot{A} \in \mathbb{Q}$ such that $\|\mathbf{t} - \mathcal{L}(\mathbf{B})\|^2 < \ddot{A}$.

`OUTPUT` A sequence of $\mathbf{b} = \sum_{i=1}^n u_i \mathbf{b}_i \in \mathcal{L}(\mathbf{B})$ such that $\|\mathbf{t}-\mathbf{b}\|$ decreases to $\|\mathbf{t}-\mathcal{L}\|$.

1. $t := n$, $L := \emptyset$, $y_n := \tau_n$, $u_n := \lceil y_n \rfloor$, $\ddot{c}_{n+1} := 0$,
   ($\ddot{c}_t = c_t(\tau_t - u_t, ..., \tau_n - u_n)$ *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`,
   $\ddot{\varrho}_t := (\ddot{A} - \ddot{c}_t)^{1/2}$, $\ddot{\beta}_t := V_{t-1} \ddot{\varrho}_t^{t-1} / (r_{1,1} \cdots r_{t-1,t-1})$,
   `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 2.1`]
   `IF` $\ddot{\beta}_t \ge 2^{-s+\lceil \lg\lg t \rceil}$ `THEN` [$t := t-1$, $y_t := \tau_t + \sum_{i=t+1}^n (\tau_i - u_i) r_{t,i}/r_{t,t}$,
   $u_t := \lceil y_t \rfloor$, $\varsigma_t := sign(u_t - y_t)$, $\nu_t := 1$, `GO TO 2`]
   `ELSE` store $(u_t, ..., u_n, y_t, \ddot{c}_t, \nu_t, \ddot{\beta}_t, \ddot{A})$ in L,

2.1. $t := t+1$, $u_t := \lceil y_t \rfloor + \lfloor \nu_t/2 \rfloor \varsigma_t$, $\nu_t := \nu_t + 1$, $\varsigma_t := -\varsigma_t$]]

3. $s := s+1$, perform all delayed stages $(u_t, ..., u_n, y_t, \ddot{c}_t, \nu_t, \ddot{\beta}_t, \ddot{A})$ of L on level s.
   Delay new stages with $\ddot{\beta}_{t'} < 2^{-s+\lceil \lg\lg t' \rceil}$ and store them in L.
4. `IF` $L \ne \emptyset$ `THEN GO TO 3 ELSE` *terminate.*

4 Performance of pruned New Enum for SVP and CVP

Proposition 1 bounds under linear pruning the time to find $\mathbf{b}' \in \mathcal{L}(\mathbf{B})$ with $||\mathbf{b}'|| = \lambda_1$. Finding an unproved shortest vector $\mathbf{b}'$ is easier than proving $\|\mathbf{b}'\| = \boldsymbol{\lambda_1}$. New Enum finds an unproved shortest lattice vector $\mathbf{b}'$ in polynomial time under the following conditions and 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
  $rd(\mathcal{L}) \le \left(\sqrt{\frac{e\,\pi}{2\,n}} \frac{\lambda_1}{\|\mathbf{b}_1\|}\right)^{\frac{1}{2}}$, i.e., both $\mathbf{b}_1$ and $rd(\mathcal{L})$ are sufficiently small.

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

SA: There is a vector $\mathbf{b}' \in \mathcal{L}(\mathbf{B})$ such that $\|\mathbf{b}'\| = \lambda_1$ and $\|\pi_t(\mathbf{b}')\|^2 \lesssim \frac{n-t+1}{n} \lambda_1^2$ for $t = 1, \ldots, n$.

(Later we will use a similar assumption **CA** for **CVP**).

- the vol. heur. is close: $\mathcal{M}_t^{\varrho} := \#\mathcal{B}_{n-t+1}(\mathbf{0}, \varrho_t) \cap \pi_t(\mathcal{L}) \approx \frac{V_{n-t+1} \varrho_t^{n-t+1}}{\det \pi_t(\mathcal{L})}$ for $\varrho_t^2 = \frac{n-t+1}{n} \lambda_1^2$.

Remarks. **1.** If **GSA** holds with $q \ge 1$ 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", i.e., the $r_{i,i}^2$ form a geometric series. It is easier to work with the idealized property that all $r_{i,i}/r_{i-1,i-1}$ are equal. In practice $r_{i,i}/r_{i-1,i-1}$ slightly increases on the average with i. [BL05] studies "nearly equality". B. Lange [La13] shows that **GSA** can be replaced by the weaker property that the reduction potential of $\mathbf{B}$ is sufficiently small. **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]:

$$\mathbf{Pr}[\,\|\pi_t(\mathbf{b}')\|^2 \le \tfrac{n-t+1}{n}\lambda_1^2 \text{ for } t = 1, ..., n\,] = \tfrac{1}{n}$$

for random $\mathbf{b}' \in_R \text{span}(\mathcal{L})$ with $||\mathbf{b}'|| = \lambda_1$. Lange [La13, Kor. 4.3.2] proves that the prob. $1/n$ increases to $1 - e^{-d^2}$ by increasing $\frac{n-t+1}{n}$ of linear pruning to $\frac{n-t+1}{n} + d/\sqrt{n}$. **Linear pruning** means to cut off all stages $(u_t, ..., u_n)$ that satisfy $||\pi_t(\sum_{i=t}^n u_i \mathbf{b}_i)||^2 > \frac{n-t+1}{n}\lambda_1^2$. Linear pruning is impractical because it does not provide any information on **SVP, CVP** in case of failure. We use linear pruning only as a theoretical model for easy analysis. We have implemented **SVP, CVP** via New Enum and we will show in section 5 that stages $(u_t, ..., u_n)$ that are cut by linear pruning have extremely low success probability so they will not be performed by New Enum.

3. Errors of the volume heuristics. The minimal and maximal values of $\#_n := \#(\mathcal{B}_n(\zeta_n, \varrho_n) \cap \mathcal{L})$, and similar for $\#_t := \#(\mathcal{B}_t(\zeta_t, \varrho_t) \cap \pi_{n-t+1}(\mathcal{L}))$, are for fixed n, ϱ_n very close for large radius ϱ_n, but can differ considerably for small ϱ_n since $\#_n$ can change a lot with the actual center ζ_n of the sphere. For small ϱ_n the minimum of $\#_n$ can be very small and then the average value for random center ζ_n is closer to the maximum of $\#_n$. For more details see the theorems and Table 1 of [MO90]. As New Enum works with average values for $\#_n, \#_t$ its success rate β_t frequently overestimates the success rate for the actual ζ_t. A cut of the smallest (resp. closest) lattice vector by New Enum in case that it underestimates $\#_t$ can nearly be excluded if stages are only cut for very small β_t.

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

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

Therefore $rd(\mathcal{L})\sqrt{\gamma_n}\,\|\mathbf{b}_1\|/\lambda_1 \le 1$ implies under **GSA** that $\det\mathcal{L} \ge 1$ and $q \ge 1$ and thus $\|\mathbf{b}_1\| = \lambda_1$. Hence $rd(\mathcal{L}) > \frac{\lambda_1}{\|\mathbf{b}_1\|}/\sqrt{\gamma_n}$ holds under **GSA** if $\|\mathbf{b}_1\| > \lambda_1$.

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

Proposition 1. *Let* $\mathbf{B} = \mathbf{QR}$, $\mathbf{R} \in \mathbb{R}^{n\times n}$ *satisfy* $rd(\mathcal{L}) \le \big(\frac{\lambda_1}{\|\mathbf{b}_1\|}\sqrt{\frac{e\,\pi}{2\,n}}\big)^{\frac{1}{2}}$ *and* **GSA** *and have a shortest lattice vector* $\mathbf{b}'$ *that satisfies* **SA**. *Then* Enum *with linear pruning finds such* $\mathbf{b}'$ *under the volume heuristics in polynomial time.*

Proof. For simplicity we assume that λ_1 is known. Pruning all stages $(u_t, ..., u_n)$ that satisfy $||\pi_t(\sum_{i=t}^n u_i \mathbf{b}_i)||^2 > \frac{n-t+1}{n}\lambda_1^2 =: \varrho_t^2$ does not cut off any shortest lattice vector $\mathbf{b}'$ that satisfies **SA**. The volume heuristics approximates the number $\mathcal{M}_t^{\varrho}$ of performed stages $(u_t, ..., u_n)$ to

$$\begin{aligned}\mathcal{M}_t^{\varrho} := \#\mathcal{B}_{n-t+1}(\mathbf{0}, \varrho_t) \cap \pi_t(\mathcal{L}) &\approx (\sqrt{\tfrac{n-t+1}{n}}\,\lambda_1)^{n-t+1} V_{n-t+1}/(r_{t,t}\cdots r_{n,n}) \\ &\approx (\sqrt{\tfrac{n-t+1}{n}}\,\lambda_1)^{n-t+1}\big(\tfrac{2e\pi}{n-t+1}\big)^{\frac{n-t+1}{2}}/(r_{t,t}\cdots r_{n,n}\,\sqrt{\pi(n-t+1)}\,) \\ &< \big(\lambda_1\sqrt{\tfrac{2e\pi}{n}}\big)^{n-t+1}/(r_{t,t}\cdots r_{n,n}). \end{aligned} \tag{4.1}$$

Here $\approx$ uses Stirling's approximation $V_n = \pi^{n/2}/(n/2)! \approx (\frac{2e\pi}{n})^{n/2}/\sqrt{\pi n}$. Obviously $\|\mathbf{b}_i^*\| = r_{1,1}q^{\frac{i-1}{2}}$ holds by **GSA** and thus

$$(r_{t,t}\cdots r_{n,n})/r_{1,1}^{n-t+1} = q^{\sum_{i=t-1}^{n-1} i/2} = q^{\frac{n(n-1)-(t-1)(t-2)}{4}}.$$

For $t = 1$ this yields $q^{\frac{n-1}{4}} = (\det\mathcal{L})^{1/n}/r_{1,1} = \lambda_1/(r_{1,1}\sqrt{\gamma_n}rd(\mathcal{L}))$. Combining (4.1) with this equation and $\gamma_n < \frac{n}{e\pi}$ which holds for $n > n_0$, we get

$$\mathcal{M}_t^{\varrho} \lesssim \big(\tfrac{\lambda_1}{r_{1,1}}\sqrt{\tfrac{2e\pi}{n}}\big)^{n-t+1}\big(\sqrt{\tfrac{n}{e\pi}}\,rd(\mathcal{L})\,\tfrac{r_{1,1}}{\lambda_1}\big)^{n-\frac{(t-1)(t-2)}{n-1}} \tag{4.2}$$

Evaluating this upper bound for $rd(\mathcal{L}) \le \big(\frac{\lambda_1}{r_{1,1}}\sqrt{\frac{e\,\pi}{2\,n}}\big)^{\frac{1}{2}}$ yields

$$\mathcal{M}_t^{\varrho} \lesssim \big(\sqrt{\tfrac{n}{2\,e\,\pi}}\tfrac{r_{1,1}}{\lambda_1}\big)^{-n+t-1}\big(\sqrt{\tfrac{n}{2\,e\,\pi}}\tfrac{r_{1,1}}{\lambda_1}\big)^{+\frac{n}{2}-\frac{1}{2}\frac{(t-1)(t-2)}{n-1}}.$$

This approximate upper bound has for $t \le n$ its maximum 1 at $t = n$. This proves Prop. 1. □

Extension of Prop. 1 to $\mathbf{GSA_{m,q}}$-bases, i.e lattice bases that satisfy for some m, $1 \le m \le n$:

$$r_{i,i}^2/r_{i-1.i-1}^2 = \begin{cases} \text{q} & \text{for } i \le m \\ 1 & \text{for } i > m \end{cases}, \qquad r_{i,i}^2/r_{1,1}^2 = \begin{cases} q^{i-1} & \text{for } i \le m \\ q^{m-1} & \text{for } i > m \end{cases}$$

This increases $r_{i,i}/r_{i-1,i-1}$ of **GSA** for $i \ge m$; many LLL-bases have such an increase for large i.

Proposition 2. *Let* $\mathbf{B} = \mathbf{QR}$, $\mathbf{R} \in \mathbb{R}^{n\times n}$ *be a* $\mathbf{GSA_{m,q}}$*-basis,* $rd(\mathcal{L}(\mathbf{B})) \le \frac{1}{\sqrt{2}}\big(\frac{\lambda_1}{\|\mathbf{b}_1\|}\sqrt{\frac{2\,e\,\pi}{n}}\big)^{\frac{m}{2n}}$ *and* $\mathcal{L}$ *have a shortest lattice vector* $\mathbf{b}'$ *that satisfies* **SA**. *Then* Enum *with linear pruning finds such* $\mathbf{b}'$ *under the volume heuristics in polynomial time.*

Proof. We modify the proof of Prop. 1 and concentrate on $t \ge m$ since $\mathcal{M}_t^{\varrho}$ has its maximum for $t \ge m$. Then we have for $t \ge m$

$$(r_{t,t}\cdots r_{n,n})/r_{1,1}^{n-t+1} = q^{(n-t+1)\frac{m-1}{2}}$$

$$(\det \mathcal{L})^{1/n}/r_{1,1} = q^{\sum_{i=1}^{m} \frac{i-1}{2}/n + \frac{m-1}{2}\frac{n-m}{n}} = \frac{\lambda_1}{r_{1,1}\sqrt{\gamma_n}\, rd(\mathcal{L})}$$

where $\quad \sum_{i=1}^{m} \frac{i-1}{2}/n + \frac{m-1}{2}\frac{n-m}{n} = \frac{(m+1)m}{4n} - \frac{m}{2n} + \frac{m-1}{2}(1-\frac{m}{n}) = \frac{m-1}{2}(1-\frac{m}{2n})$. Hence

$$\mathcal{M}_t^{\varrho} \approx \big(\tfrac{\lambda_1}{r_{1,1}}\sqrt{\tfrac{2e\pi}{n}}\big)^{n-t+1}/q^{(n-t+1)\frac{m-1}{2}} = \big(\tfrac{\lambda_1}{r_{1,1}}\sqrt{\tfrac{2e\pi}{n}}\big)^{n-t+1}\big(\tfrac{r_{1,1}}{\lambda_1}\sqrt{\gamma_n}\, rd(\mathcal{L})\big)^{\frac{n-t+1}{1-m/2n}}$$

Evaluating $\frac{r_{1,1}}{\lambda_1}\sqrt{\gamma_n}\, rd(\mathcal{L})$ for $rd(\mathcal{L}) \le \frac{1}{\sqrt{2}}\big(\frac{\lambda_1}{\|\mathbf{b}_1\|}\sqrt{\frac{2\,e\,\pi}{n}}\big)^{\frac{m}{2n}}$ and $\gamma_n \le \frac{n}{e\pi}$ we get

$$\tfrac{r_{1,1}}{\lambda_1}\sqrt{\gamma_n}\, rd(\mathcal{L}) \le \tfrac{r_{1,1}}{\lambda_1}\sqrt{\tfrac{n}{2e\pi}}\sqrt{2}\ \tfrac{1}{\sqrt{2}}\big(\tfrac{\lambda_1}{\|\mathbf{b}_1\|}\sqrt{\tfrac{2\,e\,\pi}{n}}\big)^{\frac{m}{2n}} = \big(\tfrac{\lambda_1}{r_{1,1}}\sqrt{\tfrac{2e\pi}{n}}\big)^{\frac{m}{2n}-1}$$

and thus $\quad \mathcal{M}_t^{\varrho} \lesssim \big(\frac{\lambda_1}{r_{1,1}}\sqrt{\frac{2e\pi}{n}}\big)^{(1-(1-\frac{m}{2n})/(1-\frac{m}{2n}))(n-t+1)} = \big(\frac{\lambda_1}{r_{1,1}}\sqrt{\frac{2e\pi}{n}}\big)^{0} = 1.$

In particular $\mathcal{M}_t^{\varrho} \approx 1$ holds for all $t \ge m$ if $rd(\mathcal{L}) = \frac{1}{\sqrt{2}}\big(\frac{\lambda_1}{r_{1,1}}\sqrt{\frac{2\,e\,\pi}{n}}\big)^{\frac{m}{2n}}$ and $\gamma_n = \frac{n}{e\pi}$. $\square$

Prop. 2 handles the case that $r_{i,i}$ decreases uniformly for $i \le m$ with an abrupt stop at $i = m$. Prop. 3 assumes a lattice basis of dimension n that satisfies for some $0 < q < 1$ that

$$r_{i+1,i+1}/r_{i.i} = q^{1-i/n} for\ i = 1, \cdots, n-1 \tag{4.3}$$

Hence $r_{j,j}/r_{1,1} = q^{j-1-\sum_{i=1}^{j-1} i/n}$ and $r_{i,i}$ decreases slower and slower from $i = 1$ to $i = n$ and the decrease vanishes for $i \approx n$. In fact for LLL-bases the decrease of $r_{i,i}$ can vanish slowly towards the end of the basis because the LLL-algorithm works uniformly on the initial part but merely performs size-reduction towards the end of an high-dimensional basis.

Proposition 3. *Let* $\mathbf{B} = \mathbf{QR}, \mathbf{R} \in \mathbb{R}^{n\times n}$ *be a basis of lattice* $\mathcal{L}$ *satisfying (4.3),* $n > 2e\pi$ *and* $rd(\mathcal{L}) \le \big(\frac{\lambda_1}{\|\mathbf{b}_1\|}\sqrt{\frac{e\pi}{n}}\big)^{\frac{1}{2}}$ *and let* $\mathcal{L}$ *have a shortest lattice vector* $\mathbf{b}'$ *that satisfies* **SA**. *Then* ENUM *with linear pruning finds such* $\mathbf{b}'$ *under the volume heuristics in polynomial time.*

Proof. Modifying the proofs of Prop.1, 2 we have $\ r_{t,t}\cdots r_{n,n}/r_{1,1}^{n-t+1} = q^{\sum_{j=t}^{n}\sum_{i=1}^{j-1} 1-i/n}$, where

$$\sum_{j=t}^{n}\sum_{i=1}^{j-1} 1 - i/n = \sum_{j=t}^{n}[j-1-\tfrac{(j-1)j}{2n}] = \tfrac{n(n-1)}{2} - \tfrac{t(t-1)}{2} - \tfrac{n((n+1)(2n+1)}{12\ n}$$
$$+\tfrac{(t-1)t(2t-1)}{12\ n} + \tfrac{n(n+1)}{4\ n} - \tfrac{(t-1)t}{4\ n} = n^2/3 + \tfrac{t^2(t-3n)}{6\ n} + O(n)$$

Hence $\quad \big(\frac{\lambda_1}{r_{1,1}\sqrt{\gamma_n}rd(\mathcal{L})}\big)^n = \det\mathcal{L}/r_{1,1}^n = q^{n^2/3+O(n)}.\quad$ We get that

$$\mathcal{M}_t^{\varrho} \lesssim \big(\lambda_1\sqrt{\tfrac{2e\pi}{n}}\big)^{n-t+1}/r_{t,t}\cdots r_{n,n}$$
$$= \big(\tfrac{\lambda_1}{r_{1,1}}\sqrt{\tfrac{2e\pi}{n}}\big)^{n-t+1} q^{-n^2/3-\frac{t^2(t-3n)}{6n}-O(n)}$$
$$= \big(\tfrac{\lambda_1}{r_{1,1}}\sqrt{\tfrac{2e\pi}{n}}\big)^{n-t+1}\big[(\det(\mathcal{L})^{1/n}/r_{1,1}\big]^{\frac{-n^2/3-t^2(t-3n)/6n-O(n)}{n/3+O(1)}}$$
$$= \big(\tfrac{\lambda_1}{r_{1,1}}\sqrt{\tfrac{2e\pi}{n}}\big)^{n-t+1}\big(\tfrac{r_{1,1}\sqrt{\gamma_n}rd(\mathcal{L})}{\lambda_1}\big)^{n+\frac{t^2(t-3n)}{2n^2}+O(1)}. \tag{4.2'}$$

We get for $rd(\mathcal{L}) \le \big(\frac{\lambda_1}{r_{1,1}}\sqrt{\frac{e\pi}{n}}\big)^{\frac{1}{2}}$ and $\gamma_n < \frac{n}{e\pi}$ that $\quad r_{1,1}\sqrt{\gamma_n}rd(\mathcal{L})/\lambda_1 \le \big(\frac{r_{1,1}}{\lambda 1}\sqrt{\frac{n}{e\pi}}\big)^{1/2}$ and thus :

$$\mathcal{M}_t^{\varrho} \lesssim \big(\tfrac{\lambda_1}{r_{1,1}}\sqrt{\tfrac{2e\pi}{n}}\big)^{n-t+1-n/2-(t^2(t-3n)-O(1))/4n^2} 2^{\frac{n-t+1}{2}} =: \mathcal{H}_t$$

For $n > 2e\pi$ this upper bound $\mathcal{H}_t$ of $\mathcal{M}_t^{\varrho}$ is monotonous decreasing in $t \le n$. This holds because the exponent of $\frac{\lambda_1}{r_{1,1}}\sqrt{\frac{2e\pi}{n}}$ is monotonous increasing in t and $\frac{\lambda_1}{r_{1,1}}\sqrt{\frac{2e\pi}{n}} < 1$. Hence for $n > 4e\pi$:

$$\mathcal{M}_t^{\varrho} \lesssim \mathcal{M}_1^{\varrho} \lesssim \big(\tfrac{\lambda_1}{r_{1,1}}\sqrt{\tfrac{e\pi}{n}}\big)^{n/2+O(1/n)} 2^{n/2} = o(1).$$

$\square$

In practice all relevant bases satisfy some slightly modified version of **GSA**. The main problem for the fast **SVP** algorithms for them is to find a sufficiently short $\mathbf{b}_1 \in \mathcal{L}$. For this we first iteratively BKZ-reduce the basis $\mathbf{B}$ with block sizes $2, 4, 8, 16, 32$ and then for larger block sizes we use NEW ENUM with pruning and arranged to enumerate smallest vectors first.

The γ**-unique SVP** is to solve **SVP** for a lattice $\mathcal{L}$ of dim. n where all vectors $\mathbf{b} \in \mathcal{L}$ of length $0 < ||\mathbf{b}|| \le \gamma\lambda_1$ are parallel to each other. Minkowski's second theorem shows for such $\mathcal{L}$ with successive minima $\lambda_1, ..., \lambda_n$ that $\quad \lambda_1^n\gamma^{n-1} < \lambda_1\cdots\lambda_n \le \gamma_n^{n/2}\det\mathcal{L}$ and thus

$$\lambda_1^2 < \gamma^{-2+2/n}\gamma_n(\det\mathcal{L})^{2/n} \text{ hence } \quad rd(\mathcal{L}) < \gamma^{-1+1/n}.$$

Prop. 3 shows that **SVP** for such $\mathcal{L}$ is solvable in polynomial time under **SA, GSA** and the volume heuristic if $\ \big(\frac{\lambda_1}{||\mathbf{b}_1||}\sqrt{\frac{e\pi}{n}}\big)^{1/2} \le \gamma^{-1+1/n}$. Thus every n^a-unique **SVP** of dim. n is by Prop. 3 solvable in heuristic pol. time if $n^{-a+a/n} \le \big(\frac{\lambda_1}{\|\mathbf{b}_1\|}\sqrt{\frac{e\pi}{n}}\big)^{1/2}$. It has been proved that every BKZ-basis of block size k satisfies $\|\mathbf{b}_1\|/\lambda_1 \le \gamma_k^{(n-1)/(k-1)}$. Hence the heuristic pol. time for n^a-unique **SVP** holds if $n^{-2a+2a/n+1/2} \le \gamma_k^{-(n-1)/(k-1)}\sqrt{e\pi}$, i.e. if $\gamma_k^{(n-1)/(k-1)} \le n^{2a-2a/n-1/2}\sqrt{e\pi}$. The latter holds for

1. $a = 1.5$, $k = 24$, $\gamma_{24} = 4$ for all $n \le 245$
2. $a = 1$, $k = 24$, $\gamma_{24} = 4$ for all $n \le 140$

We see that the security of cryptosystems based on n^a-unique **SVP** is quite weak for practical, not extremely large dimension n. For cryptosystems based on n^a-unique **SVP** see [Reg04], [MR05].

SVP-time bound for rd($\mathcal{L}$)$\le$ 1. Under the conditions of Prop. 1 but for $rd(\mathcal{L}) \le 1$ (4.2) proves

$$\mathcal{M}_t^{\varrho} \lesssim \big(\sqrt{\tfrac{n}{e\pi}}\,\tfrac{r_{1,1}}{\lambda_1}\big)^{n-\frac{(t-1)(t-2)}{n-1}-n+t-1}2^{\frac{n-t+1}{2}}.$$

The exponent $n - \frac{(t-1)(t-2)}{n-1} - n + t - 1$ is maximal for $t = n/2+1$ with maximal value $\frac{1}{4}\frac{n^2}{n-1}$. This proves for $r_{1,1}/\lambda_1 = n^{o(1)}\sqrt{e\pi}$ the heuristic **SVP** time bound

$$n^{O(1)}\big(\sqrt{\tfrac{n}{e\pi}}\,\tfrac{r_{1,1}}{\lambda_1}\big)^{\frac{1}{4}\frac{n^2}{n-1}}2^{n/4} = n^{n/8+o(n)}\ . \tag{4.4}$$

This beats under heuristics the proven **SVP** time bound $n^{\frac{n}{2e}+o(n)}$ of HANROT, STEHLE [HS07] which holds for a quasi-HKZ-basis $\mathbf{B}$ satisfying $\|\mathbf{b}_1\| \le 2\|\mathbf{b}_2^*\|$ and having a HKZ-basis $\pi_2(\mathbf{B})$. In fact $\frac{1}{2e} \approx 0.159 > 0.125 = \frac{1}{8}$. The **SVP**-algorithm of Prop.1 can use fast BKZ for preprocessing and works even for $\|\mathbf{b}_1\| \gg 2\lambda_1$ – see the attack on γ-unique **SVP** – whereas [HS07] requires HKZ-reduction for preprocessing. This HKZ-reduction already guarantees $\|\mathbf{b}_1\| \le 2\lambda_1$ and performs the main **SVP** work during preprocessing. Our **SVP** time bound $n^{n/8+o(n)}$ only assumes $\|\mathbf{b}_1\| \le n^{o(1)}\sqrt{e\pi}\lambda_1$.

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* $b \ge 0$, NEW ENUM *solves* **SVP** *and proves to have found a solution in time* $2^{O(n)}(n^{\frac{1}{2}+b}rd(\mathcal{L}))^{\frac{n+1+o(1)}{4}}$.

Theorem 1 is proven in [S10], it does not assume **SA** and the vol. heuristic. Recall from remark 4 that $n^{\frac{1}{2}+b}rd(\mathcal{L}) \ge 1$ holds under **GSA**. For $b = o(1)$ Thm. 1 shows the **SVP**-time bound $n^{\frac{n}{8}+o(n)}$ which beats $n^{\frac{n}{2e}+o(n)}$ from HANROT, STEHLE [HS07]. Cor. 1 translates Thm. 1 from **SVP** to **CVP**, it shows that the corresponding **CVP**-algorithm solves many important **CVP**-problems in simple exponential time $2^{O(n)}$ and linear space.

[HS07] proves 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 the proof of Theorem 1 yields:

Corollary 1. [S10] *Given a basis* $\mathbf{B} = [\mathbf{b}_1, ..., \mathbf{b}_n]$ *satisfying* **GSA**, $\|\mathbf{b}_1\| \le \sqrt{e\pi}\,n^b\lambda_1$ *with* $b \ge 0$ *and* $\mathbf{t} \in \mathrm{span}(\mathcal{L})$ *with* $\|\mathcal{L}-\mathbf{t}\| \le \lambda_1$, NEW ENUM *solves this* **CVP** *in time* $2^{O(n)}(n^{\frac{1}{2}+b}rd(\mathcal{L}))^{\frac{n}{4}}$.

Corollary 1 proves under **GSA**, $rd(\mathcal{L}) = O(n^{-\frac{1}{2}-b})$ and $\|\mathcal{L}-\mathbf{t}\| \le \lambda_1$ the **CVP** time bound $2^{O(n)}$ even using linear space (by iterating NEW ENUM for $s = 1, ..., O(n)$ without storing delayed stages). Moreover it proves under **GSA** and $\|\mathbf{b}_1\| = O(\lambda_1)$ and $\|\mathcal{L}-\mathbf{t}\| \le \lambda_1$ the time bound $2^{O(n)}$. However subexponential time remains unprovable due to remark 4 of section 4.

CA: $\|\pi_t(\mathbf{t}-\ddot{\mathbf{b}})\|^2 \lesssim \frac{n-t+1}{n}\|\mathbf{t}-\mathcal{L}\|^2$ holds for $t = 1, ..., n$ and some $\ddot{\mathbf{b}} \in \mathcal{L}$ closest to $\mathbf{t}$.

CA translates the assumption **SA** from **SVP** to **CVP**. **CA** holds with probability $1/n$ for random $\ddot{\mathbf{b}} \in \mathrm{span}(\mathcal{L})$ such that $\|\mathbf{t}-\ddot{\mathbf{b}}\| = \|\mathbf{t}-\mathcal{L}\|$ [GNR10]. Obviously linear pruning extends naturally from **SVP** to **CVP**. B. LANGE [La13] proves that the probability $1/n$ increases towards 1 for the increased bounds $\|\pi_t(\mathbf{t}-\ddot{\mathbf{b}})\|^2 \lesssim \frac{n-t+1}{n}\|\mathbf{t}-\mathcal{L}\|^2(1+1/\sqrt{n})$ for $t = 1, ..., n$.

Corollary 2. [S10] *Given a basis* $\mathbf{B} = [\mathbf{b}_1, ..., \mathbf{b}_n] \in \mathbb{Z}^{m\times n}$ *of* $\mathcal{L}$ *that satisfies* **GSA**, $\|\mathbf{b}_1\| = O(\lambda_1)$ *and* $rd(\mathcal{L}) \le \big(\frac{\lambda_1}{\|\mathbf{b}_1\|}\sqrt{\frac{e\,\pi}{2\,n}}\big)^{\frac{1}{2}}$. *Let some lattice vector* $\ddot{\mathbf{b}}$ *that is closest to the target vector* $\mathbf{t}$ *satisfy* **CA** *then* NEW ENUM *finds* $\ddot{\mathbf{b}}$ *for random* $\mathbf{t}$ *in average time* $n^{O(1)}\mathbf{E}_{\mathbf{t}}[(\|\mathbf{t}-\mathcal{L}\|/\lambda_1)^n]$.

Cor. 2 eliminates the volume heuristics for a random target vector $\mathbf{t}$. 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* $rd(\mathcal{L}) \le \big(\frac{\lambda_1}{\|\mathbf{b}_1\|}\sqrt{\frac{e\,\pi}{2\,n}}\big)^{\frac12}$. *Let some lattice vector* $\ddot{\mathbf{b}}$ *that is closest to the target vector* $\mathbf{t}$ *satisfy* **CA** *and let* $\|\mathbf{t}-\mathcal{L}\| \lesssim \lambda_1$ *then* New Enum *with linear pruning for* **CVP** *finds* $\ddot{\mathbf{b}}$ *under the volume heuristics in pol. time.*

B. Lange [La13] shows that **GSA** for **B** can be replaced by a less rigid condition, namely that the "reduction potential" $\prod_{\ell_i \ge 1} \ell_i$ for $\ell_i = \|\mathbf{b}_i^*\|/(\det \mathcal{L})^{1/n}$ of the basis **B** is sufficiently small.

5 Factoring by CVP solutions for the Prime Number Lattice

Let $N > 2$ be an odd integer that is not a prime power, with all prime factors larger than p_n the n-th smallest prime. An integer is called p_n*-smooth* if it has no prime factor larger than p_n. A classical method factors N via $n+1$ independent triples of integers $u_j, v_j, |u_j - v_jN|$ for $j = 1, ..., n+1$ where $u_j, |u_j - v_jN|$ are p_n-smooth, i.e.

$$u_j = \textstyle\prod_{i=1}^n p_i^{e_{i,j}},\ |u_j - v_jN| = \prod_{i=1}^n p_i^{e'_{i,j}} \quad \text{with } e_{i,j}, e'_{i,j} \in \mathbf{N}. \tag{5.1}$$

The classical factoring method. Setting $p_0 := -1$ we have $u_j - v_jN = \prod_{i=0}^n p_i^{e'_{i,j}}, e'_{i,j} \in \mathbb{N}$. Hence $\prod_{i=1}^n p_i^{e_{i,j}} = \prod_{i=1}^n p_i^{e'_{i,j}} = 1 \mod N$, $\prod_{i=0}^n p_i^{e_{i,j}-e'_{i,j}} = 1 \mod N$ for $j = 1, ..., n+1, e_{0,j} = 1$. Any solution $t_1, ..., t_{n+1} \in \{0, 1\}$ of the equations

$$\textstyle\sum_{j=1}^{n+1} t_j(e_{i,j} - e'_{i,j}) = 0 \mod 2 \qquad \text{for } i = 0, ..., n \tag{5.2}$$

solves $X^2 = 1 \mod N$ by $X = \prod_{i=0}^n p_i^{\frac12 \sum_{j=1}^{n+1} t_j(e_{i,j}-e'_{i,j})} \mod N$. In case that $X \ne \pm 1 \mod N$ this yields two non-trivial factors $\gcd(X \pm 1, N) \notin \{1, N\}$ of N.

The linear equations (5.2) can be solved within $O(n^3)$ bit operations. We neglect this minor part of the work load of factoring N. This reduces factoring N to finding about $n+1$ p_n-smooth integers $u, |u - vN|$. This factoring method goes back to Morrison & Brillhart [MB75] and let to the first factoring algorithm in subexponetial time by J. Dixon [D81].

We construct p_n-smooth triples $u, v, |u - vN|$ from **CVP** solutions for the prime number lattice $\mathcal{L}(\mathbf{B}_{n,c})$ with basis $\mathbf{B}_{n,c} = [\mathbf{b}_1, \ldots, \mathbf{b}_n] \in \mathbb{R}^{(n+1)\times n}$ and target vector $\mathbf{N}_c \in \mathbb{R}^{n+1}$ for some $c > 0$:

$$\mathbf{B}_{n,c} = \begin{bmatrix} \sqrt{\ln p_1} & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \sqrt{\ln p_n} \\ N^c \ln p_1 & \cdots & N^c \ln p_n \end{bmatrix}, \qquad \mathbf{N}_c = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ N^c \ln N \end{bmatrix}, \tag{5.3}$$

$$\big(\det \mathcal{L}(\mathbf{B}_{n,c})\big)^2 = \big(\textstyle\prod_{i=1}^n \ln p_i\big)\ (1 + N^{2c} \sum_{i=1}^n \ln p_i),$$
$$\big(\det \mathcal{L}(\mathbf{B}_{n,c})\big)^{2/n} = \ln p_n \cdot (1 \pm o(1)) \cdot N^{2c/n}$$

as the prime number theorem implies $\prod_{i=1}^n \ln p_i^{1/n} / \ln p_n = 1 - o(1)$ for $n \to \infty$. By definition let $o(1) \to 0$ for $n, N \to \infty$. We identify each vector $\mathbf{b} = \sum_{i=1}^n e_i \mathbf{b}_i \in \mathcal{L}(\mathbf{B}_{n,c})$ with the pair (u, v) of relative prime and p_n-smooth integers

$$u = \textstyle\prod_{e_i>0} p_i^{e_i},\ \ v = \prod_{e_i<0} p_i^{-e_i} \in \mathbb{N}, \text{ we denote } \mathbf{b} \sim (u, v).$$

Clearly uv is square-free if and only if $e_1, ..., e_n \in \{0, \pm1\}$. Let $\hat{z}_\mathbf{b} := N^c \ln \frac{u}{v}$, $\hat{z}_{\mathbf{b}-\mathbf{N}_c} := N^c \ln \frac{u}{vN}$ denote the last coordinates of $\mathbf{b}$ and $\mathbf{b} - \mathbf{N}_c$. As a factor $p_i^{e_i}$ of uv contributes $e_i \ln p_i$ to $\ln uv$ and $e_i^2 \ln p_i$ to $\|\mathbf{b}\|^2$ we have $\|\mathbf{b}\|^2 \ge \ln uv + \hat{z}_\mathbf{b}^2$ with equality if and only if uv is square-free. Similarly

Fact 1. $\|\mathbf{b} - \mathbf{N_c}\|^2 \ge \ln uv + \hat{z}^2_{\mathbf{b}-\mathbf{N}_c}$ holds for $(u, v) \sim \mathbf{b} \in \mathcal{L}(\mathbf{B}_{n,c})$ with equality iff uv is square-free.

In practice $\|\mathcal{L}(\mathbf{B}_{n,c}) - \mathbf{N}_c\|^2$ is close to the minimum of $\ln uv + \hat{z}^2_{\mathbf{b}-\mathbf{N}_c}$ for nearly square-free uv.

Lemma 1. *Let* $(u, v) \sim \mathbf{b} \in \mathcal{L}(\mathbf{B}_{n,c})$ *satisfy* $\frac12 N^\delta \le v \le N^\delta$, *and* $|u - vN| = o(vN)$. *Then*
1. $\|\mathbf{b} - \mathbf{N}_c\|^2 \ge (2\delta + 1 - o(1)) \ln N + \hat{z}^2_{\mathbf{b}-\mathbf{N}_c}$ **2.** $|\hat{z}_{\mathbf{b}-\mathbf{N}_c}| = N^c \frac{|u-vN|}{vN}(1 \pm o(1))$.

Proof. Clearly $0 \le \delta \ln N - \ln v \le \ln 2$ and thus for $n, N \to \infty$ we have $\ln v = \delta \ln N(1 - o(1))$, $\ln u = \ln(vN)(1 - o(1))$ and $\ln uv = (2\delta - o(1) + 1)\ln N$. Then **1** follows from Fact 1 and this upper bound is sharp if uv is nearly square-free. Moreover $\ln(1 + \frac{u-vN}{vN}) = \frac{u-vN}{vN}(1 \pm o(1))$ and thus $|\hat{z}_{\mathbf{b}-\mathbf{N}_c}| = N^c \frac{|u-vN|}{vN}(1 \pm o(1))$ which proves **2.** $\square$

Lemma 5.3 of [MG02] proves that $\lambda_1^2 > 2c \ln N$ holds if the prime 2 is excluded from the prime basis. Lemma 2 extends this proof to include the prime 2 and increases the lower bound by $1 - o(1)$.

Lemma 2. *$\lambda_1^2 > 2c\ln N + 1 - \frac{1}{2}N^{-c} \pm \Theta(N^{-2c})$ holds for the lattice $\mathcal{L}(\mathbf{B}_{n,c})$ for $N^c \ge 10^3$.*

Proof. Let $\mathbf{b} = \mathbf{B}_{n,c}\mathbf{u} \ne \mathbf{0}$ be a shortest vector of $\mathcal{L}(\mathbf{B}_{n,c})$, corresponding to (u, v). Let $u > v$, otherwise change $\mathbf{u}$ into $-\mathbf{u}$. Then $\ln \frac{u}{v}$ minimizes for some $u \ge v + 1$. Hence

$$\begin{aligned} \ln \tfrac{u}{v} &\ge \ln(1 + 1/v) > \ln(1 + 1/\sqrt{uv}) && \text{since } u \ge v+1 \text{ and} \sqrt{uv} > v \\ &> \tfrac{1}{\sqrt{uv}} - \tfrac{1}{2}\tfrac{1}{uv} = \tfrac{1}{\sqrt{uv}}(1 - \tfrac{1}{2}\tfrac{1}{\sqrt{uv}}) && \text{since } \ln(1+x) = \textstyle\sum_{i=1}^{\infty}(-1)^{i+1}x^i/i \text{ for } |x| < 1. \end{aligned}$$

Hence $\lambda_1^2 \ge \ln uv + N^{2c}\ln^2(\frac{u}{v}) > \ln uv + N^{2c}\frac{1}{uv}(1 - \frac{1}{2\sqrt{uv}})^2 =: f(\sqrt{uv})^2$ where $N^c \ln \frac{u}{v} = \hat{z}_{\mathbf{b}}$ is the last coordinate of $\mathbf{b}$. We abbreviate $h := \sqrt{uv}$. The derivative $\frac{\vartheta f(h)}{\vartheta h} = h^{-5}[2h^4 + N^{2c}[-2h^2 + 3h - 1]\,]$ is zero for some h with $N^c - 0.751 < h < N^c - 0.75$ and this h determines the minimal value $f(h)$ of f. Then the Lemma follows from

$$\begin{aligned} f(N^c - \varepsilon) &= \ln(N^c - \varepsilon)^2 + \tfrac{N^{2c}}{(N^c-\varepsilon)^2}(1 - \tfrac{1}{2(N^c-\varepsilon)}) \\ &= 2c\ln N + 2\ln(1 - \varepsilon/N^c) + 1 + \tfrac{2\varepsilon N^c - \varepsilon^2}{(N^c-\varepsilon)^2} - \tfrac{N^{2c}}{2(N^c-\varepsilon)^3} \\ &\ge 2c\ln N + 1 - \tfrac{1}{2}N^{-c} \pm \Theta(N^{-2c}) \text{ for } |\varepsilon - 0.7505| \le 10^{-3} \text{ by an easy proof.} \end{aligned}$$ $\square$

If p_n-smooth u, v exist such that $u = v+1$, uv is square-free, $u = O(N^c)$ then $\lambda_1^2 = 2c\ln N + O(1)$. Otherwise λ_1^2 increases by the minimum of $\hat{z}_{\mathbf{b}}^2 \ge N^{2c}\ln^2(\frac{u}{v})$ for p_n-smooth $v < u$ of order $u = O(N^c)$.

Let $\Psi(X, y)$ denote the number of integers in $[1, X]$ that are y-smooth. Dickman [1930] shows

$$\lim_{y\to\infty} \Psi(y^z, y)y^{-z} = \rho(z) \quad \text{for any fixed } z > 0. \tag{5.4}$$

$\rho(z)$ is the Dickman, De Bruijn ρ - function, see [G08] for a recent surview. It is known that

-

$$\rho(z) = 1 - \ln z \quad \text{for} \quad 1 \le z \le 2$$

$$\rho(z) = \left(\tfrac{e \pm o(1)}{z\ln z}\right)^z = 1/z^{z+o(z)} \text{ for } z \to \infty \tag{5.5}$$

Hildebrand [H84] extended (5.5) to a wide finite range of y and z. For any fixed $\varepsilon > 0$

$$\Psi(y^z, y)y^{-z} = \rho(z)\big(1 + O\big(\tfrac{\ln(z+1)}{\ln y}\big)\big) \tag{5.6}$$

holds uniformly for $1 \le z \le y^{1/2-\varepsilon}$, $y \ge 2$ if and only if the Riemann Hypothesis is true.

Let $\Phi(N, p_n, \sigma)$ denote the number of triples $(u, v, |u - vN|) \in \mathbb{N}^3$ that are p_n–smooth and bounded as $v, |u - vN| \le p_n^{\sigma}$. We conclude from (5.6) that

$$\Phi(N, p_n, \sigma) = \Theta(2p_n^{2\,\sigma}\,\rho\big(\tfrac{\ln(Np_n^{\sigma})}{\ln p_n}\big)\rho^2(\sigma)) \tag{5.7}$$

uniformly holds for $\frac{\ln N}{\ln p_n} + \sigma \le p_n^{1/2-\varepsilon}$ if the p_n-smoothness events of $u, v, |u - vN|$ are nearly statistically independent. We will use (5.7) in a range where $\frac{\ln N}{\ln p_n} + \sigma < p_n^{0.4}$ and we will neglect the $O(1)$-factor of (5.7).

Proof of (5.7). There are $2p_n^{2\sigma}$ pairs of integers u, v such that $0 < v, |u - vN| \le p_n^{\sigma}$. Clearly $u \le Np_n^{\sigma} + p_n^{\sigma} \le p_n^z$ holds for $z = \frac{\ln(N+1)}{\ln p_n} + \sigma$. Then (5.6) for $y^z = p_n^z = (N+1)p_n^{\sigma}$ shows that the fraction of u that are p_n-smooth is $\rho(z)\big(1 + O\big(\frac{\ln(z+1)}{\ln p_n}\big)\big)$ if $\frac{\ln N}{\ln p_n} + \sigma \le p_n^{0.4}$.

Moreover (5.6) for $y = p_n$, $z = \sigma$ shows that the fraction of $0 < v \le p_n^{\sigma}$ that are p_n-smooth is $\rho(\sigma)\big(1 + O\big(\frac{\ln(\sigma+1)}{\ln p_n}\big)\big)$ if $\sigma \le p_n^{1/2-\varepsilon}$. Therefore the statistical independence of the p_n-smoothness events of $u, v, |u - vN|$ implies (5.7) if $\ln(z + 1) = O(\ln p_n)$ holds in both cases. The latter holds due to $\frac{\ln N}{\ln p_n} + \sigma \le p_n^{0.4}$.

Example factoring. Let $N = 100000980001501 \approx 10^{14}$ and $n = 90$, $p_{90} = 463$, $c = 1/2$. (5.7) shows that there are $\Theta(6.4 \cdot 10^5)$ relations (5.1) such that $v, |u - vN| \le 463^3$ are p_n-smooth.

M. Charlet has constructed in 2013 several hundred such relations (5.1) for the above N by the following program pruned to stages with success rate $\ddot{\beta}_t \geq 2^{-14}$. This program found on average a relation every 6.5 seconds. This amounts to a factoring time of 10 minutes. (Increasing c from 1/2 to 5/7 did on average increase the v-values of the found relations (5.1) and of course the entries in the last row of $[\mathbf{B}_{n,c}, \mathbf{N}_c]$ that are multiples of N^c. However the average time for constructing a relation (5.1) decreased from 6.5 to 6.08 seconds.

A program for finding relations (5.1) efficiently. Initially the given basis $\mathbf{B}_{n,c}$ gets strongly BKZ-reduced with block size 32 and the target vector $\mathbf{N}_c$ is shifted modulo lattice vectors into the ground mesh of the reduced basis. The initial value $\ddot{A}$, the upper bound on $\|\mathbf{N}_c - \mathcal{L}(\mathbf{B}_{n,c})\|^2$ is set to $\frac{1}{5}\frac{1}{4}\sum_{i=1}^n r_{i,i}^2$ which is $\frac{1}{5}$ the standard upper bound.

LOOP. In each round the vectors of the reduced basis of $\mathcal{L}(\mathbf{B}_{n,c})$ and the shifted $\mathbf{N}_c$ are randomly scaled as follows. For $i = 1, ..., n$ with probabiliy 1/2 all i-th coordinates of the basis vectors and the shifted target vector are multiplied by 2. (The "scaled" primes p_i will appear less frequently as factors of uv in relations (5.1) resulting from **CVP**-solutions.) The scaled basis gets slightly reduced by BKZ-reduction of block size 20. Then New Enum for **CVP** is called to search for lattice vectors that are close to the shifted target vector $\mathbf{N}_c$. New Enum always decreases $\ddot{A}$ to the square distance to $\mathbf{N}_c$ of the closest found lattice vector. Whenever a relation (5.1) has been found New Enum stops further decreasing $\ddot{A}$ for this round and continues to enumerate all $\mathbf{b} \in \mathcal{L}(\mathbf{B}_{n,c})$ such that $||\mathbf{b} - \mathbf{N}_c||^2 \leq \ddot{A}$. Random scalings per round let each round produce relations (5.1) that most likely are distinct from the relations found by other rounds.

Here are the first 10 of these example relations for $c = 1/2$, they mostly satisfy $v, |u - vN| \leq p_{90}^3$.

round	u	v	$\|u - vN\|$
6	$19 \cdot 29^2 \cdot 31 \cdot 73 \cdot 109 \cdot 139 \cdot 211 \cdot 359$	415	$2^2 \cdot 11 \cdot 37 \cdot 439$
6	$29 \cdot 37 \cdot 83 \cdot 139 \cdot 191 \cdot 269 \cdot 307 \cdot 443$	865	$2 \cdot 11 \cdot 239 \cdot 383$
12	$2 \cdot 3 \cdot 17^2 \cdot 103 \cdot 263 \cdot 317 \cdot 379 \cdot 443$	25	$13 \cdot 173$
14	$2 \cdot 5 \cdot 47 \cdot 83 \cdot 157 \cdot 179 \cdot 307 \cdot 331 \cdot 421$	469	$19 \cdot 43 \cdot 373$
19	$7^2 \cdot 13 \cdot 41 \cdot 43 \cdot 107 \cdot 109 \cdot 113 \cdot 131 \cdot 409 \cdot 461$	365571	$2^4 \cdot 5 \cdot 11^2 \cdot 197 \cdot 433$
19	$2 \cdot 7 \cdot 13 \cdot 31 \cdot 107 \cdot 127 \cdot 149 \cdot 179 \cdot 383 \cdot 397 \cdot 439$	1364927	$3 \cdot 5 \cdot 11 \cdot 61 \cdot 337 \cdot 419$
21	$43 \cdot 131 \cdot 139 \cdot 193 \cdot 307 \cdot 353 \cdot 401 \cdot 439$	28829	$2 \cdot 3^2 \cdot 5^2 \cdot 13 \cdot 41 \cdot 107$
30	$19 \cdot 31 \cdot 53 \cdot 61 \cdot 67 \cdot 131 \cdot 163 \cdot 241 \cdot 313$	2055	$2^2 \cdot 59 \cdot 71 \cdot 89$
31	$13^2 \cdot 17 \cdot 101 \cdot 137 \cdot 199 \cdot 229 \cdot 277 \cdot 331$	1661	$2^6 \cdot 3 \cdot 19 \cdot 233$
33	$19 \cdot 101 \cdot 107 \cdot 127 \cdot 131 \cdot 179 \cdot 191 \cdot 211 \cdot 379$	93398	$3^3 \cdot 13 \cdot 29 \cdot 109 \cdot 167$

A. Schickedanz improved in 2015 Charlet's program and found for $N = 100000980001501 \approx 10^{14}$, $n = 90$, $p_{90} = 463$, $c = 1/2$ and pruned to stages with $\ddot{\beta}_t \geq 2^{-14}$ on average one relation (5.1) in 0.32 seconds. This factors $N \approx 10^{14}$ in 30 seconds. He scaled a strong BKZ-basis of $\mathcal{L}(\mathbf{B}_{n,c})$ by multiplying many of the first n rows only with probability 1/4 by 2 and almost skipped to adjust success rates of the stored stages when $\ddot{A}$ has been decreased. But for $N \approx 10^{20}$ this program took for $n = 150$, $c = 1/2$ about 34.5 seconds per relation (5.1) and factored N in 86 minutes.

Alternatively we can find more relations (5.1) in fewer scaling rounds by decreasing $\ddot{A}$ only to $||\mathbf{b} - \mathbf{N}_c||^2(1 + \epsilon)$ for the closest found $\mathbf{b} \in \mathcal{L}(\mathbf{B}_{n,c})$. This larger final $\ddot{A}$ increases all final success rates $\ddot{\beta}_t$ and extends the final enumeration of $\mathbf{b}$ with $||\mathbf{b} - \mathbf{N}_c||^2 \leq \ddot{A}$. We should experimentally choose ϵ to maximize the number of relations (5.1) that are finally found for the available space to store undone stages. The first round should work with an unscaled **BKZ**-basis and then one can iterate with randomly scaled bases. Next this should experimentally be done for $N \approx 10^{20}$.

Extending the search of relations (5.1) to large v. This is necessary for factoring $N \gg 10^{14}$ because $\Phi(N, n, \sigma)$ gets to small for $\sigma = 3$. Let $\#_{N,n,\delta}$ denote the number and $rel_{N,n,\delta}$ the set of relations (5.1) consisting of p_n-smooth $u, v, |u - vN|$ such that $|u - vN| \leq p_n^3$ and $\frac{1}{2}N^\delta \leq v \leq N^\delta$. Neglecting the $O(\frac{\ln z+1}{\ln y})$-term of (5.6), the number of p_n-smooth $v \in [\frac{1}{2}N^\delta, N^\delta]$ is

$$\Psi(N^\delta, p_n) - \Psi(N^\delta/2, p_n) \approx N^\delta\big(\rho(z_v) - \tfrac{1}{2}\rho(z'_v)\big) \text{ for } z_v = \tfrac{\delta \ln N}{\ln p_n}\ ,\ z'_v = z_v - \tfrac{\ln 2}{\ln p_n}.$$

Hence random $v \in_R [\frac{1}{2}N^\delta, N^\delta]$ are p_n-smooth with probability close to $2(\rho(z_v) - \frac{1}{2}\rho(z'_v))$. For the number of p_n-smooth $u \in [\frac{1}{2}N^{1+\delta}, N^{1+\delta}]$ we replace δ by $1+\delta$, $z_u = \frac{(1+\delta)\ln N}{\ln p_n}$, $z'_u = z_u - \frac{\ln 2}{\ln p_n}$. Then random $u \in_R [\frac{1}{2}N^{\delta+1}, N^{\delta+1}]$ are p_n-smooth with probability close to $2(\rho(z_u) - \frac{1}{2}\rho(z'_u))$. $\#_{N,n,\delta}$ is the product of the probabilities of p_n-smoothness for random $v, u, |u - vN|$ and $\frac{1}{2}N^\delta$, the number of $v \in [\frac{1}{2}N^\delta, N^\delta]$ and $2p_n^3$, the number of $u - vN \in [-p_n^3, p_n^3]$. This yields

$$\#_{N,n,\delta} \approx 4\, N^\delta p_n^3\, \rho(3)\big(\rho(z_u) - \tfrac{1}{2}\rho(z'_u)\big)\big(\rho(z_v) - \tfrac{1}{2}\rho(z'_v)\big) \tag{5.8}$$

assuming that for random u, v, $\frac{1}{2}N^\delta \le v \le N^\delta$ and $u \in [\frac{1}{2}N^{1+\delta}, N^{1+\delta}]$ such that $|u - vN| \le p_n^3$ the p_n-smoothness events for u, v and $|u - vN|$ are nearly statistically independent. We compute the $\rho(z)$ values for integers $z = 2, .., 200$ via [Sage] and we interpolate $\rho(\lfloor z \rfloor + \varepsilon) \approx \rho(\lfloor z \rfloor) \cdot (\rho(\lceil z \rceil)/\rho(\lceil z \rceil))^\varepsilon$. We choose n, δ for N so that $\#_{N,n,\delta} \gg n$ and $\#_{N,n,\delta}$ is nearly maximal for N, n.

$N \approx$	10^{14}	10^{20}	2^{100}	2^{200}	2^{400}	2^{800}
n	96	128	350	1600	8500	42000
p_n	503	719	2357	13499	87553	506131
δ	0.5	0.7	1.1	1.4	1.96	2.17
$\#_{N,n,\delta}$	$1.8 \cdot 10^5$	$5.9 \cdot 10^3$	$5 \cdot 10^4$	$2.4 \cdot 10^5$	$3.1 \cdot 10^5$	$3.1 \cdot 10^5$

Table 1 : parameters for factoring N

Our prime base is much smaller than the prime base for the quadratic sieve which uses for $N \approx 2^{400}$ that $p_n \approx e^{1/2\sqrt{\ln N \cdot \ln\ln N}} \approx 1.53 \cdot 10^{12} \approx p_{8500}^{2.39}$, see [CP01, section 6.1].

Table 2 presents rounded values for $c = \delta + 1 - \frac{\ln p_n^3}{\ln N}$ of Cor. 4 and upper bounds for $rd(\mathcal{L}')$, $\mathcal{L}' := \mathcal{L}([\mathbf{B}_{n,c}, \mathbf{N}_c])$ for the N, n, δ of Table 1. For **CVP** of $\mathcal{L} := \mathcal{L}(\mathbf{B}_{n,c})$ with target vector $\mathbf{N}_c$ we assume that some $\mathbf{b} \in \mathcal{L}$ nearly minimizes $||\mathbf{b} - \mathbf{N}_c||$ and $\mathbf{b} \sim (u, v)$ where uv is nearly square-free and $N^\delta/2 \le v \le N^\delta$. Then Lemma 2 shows that $\lambda_1^2 = 2c\ln N + 1 \pm o(1)$ and thus $rd(\mathcal{L}) = \lambda_1/(\sqrt{\gamma_n}(\det\mathcal{L})^{\frac{1}{n}}) \approx \big(\frac{2c\cdot\ln N}{\gamma_n \ln p_n}\big)^{\frac{1}{2}}/N^{c/n}(1 \pm o(1))$, where $(\det\mathcal{L})^{2/n} = (\ln p_n \pm o(1)) \cdot N^{2c/n}$. Note that $\det\mathcal{L}' = \det\mathcal{L} \cdot ||\pi_{n+1}(\mathbf{N}_c)||$ where $\pi_{n+1}(\mathbf{N}_c) \in \mathit{span}(\mathcal{L}')^\perp$ is the projection, orthogonal to $\mathbf{b}_1, ..., \mathbf{b}_n$ Moreover $\gamma_n(\det\mathcal{L})^{2/n}$ and $\gamma_{n+1}(\det\mathcal{L}')^{2/(n+1)}$ are for large n assymptotically similar $\gamma_n(\det\mathcal{L})^{2/n}/\gamma_{n+1}(\det\mathcal{L}')^{2/(n+1)} = 1 \pm o(1)$ and so we can exchange them. Cor. 4 shows for large n that $||\mathcal{L} - \mathbf{N}_c|| < \lambda_1(\mathcal{L})$ and thus $\lambda_1(\mathcal{L}') < \lambda_1(\mathcal{L})$ and $rd(\mathcal{L}') < rd(\mathcal{L})$ for large n. Then

$$||\mathbf{b} - \mathbf{N}_c||^2 \approx \ln uv(1 \pm o(1)) + \hat{z}^2_{\mathbf{b}-\mathbf{N}} = (2\delta + 1)\ln N(1 + o(1)) + \hat{z}^2_{\mathbf{b}-\mathbf{N}}$$

follows from Fact 1 and Lemma 1 if $\hat{z}^2_{\mathbf{b}-\mathbf{N}} = \ln uv \cdot o(1)$. Hence

$$\lambda_1^2(\mathcal{L}') < ||\mathbf{b} - \mathbf{N}_c||^2 < \ln uv(1 \pm o(1)) = (2\delta + 1)\ln N(1 \pm o(1))$$

due to $|u - vN| = o(vN)$. Therefore we have $\quad rd(\mathcal{L}') \lesssim \big(\frac{(2\delta+1)\ln N}{\gamma_{n+1}\ln p_n}\big)^{1/2}/N^{\frac{c}{n+1}}$.

$N \approx$	10^{14}	10^{20}	2^{100}	2^{200}	2^{400}	2^{800}
$c = \delta + 1 - \frac{\ln p_n^3}{\ln N}$	0.92	1.2715	1.7639	2.194	2.8269	3.0989
$rd(\mathcal{L}') \lesssim$	0.81	0.77	0.62	0.48	0.339	0.22
$n^{-1/4}$	0.32	0.29	0.24	0.16	0.11	0.07

Table 2 : parameters $c, rd(\mathcal{L}'), n^{-1/4}$

For $n = 96, 128$ we use $\gamma_n = 4 \cdot 2^{\delta_n 2/n} \approx 8.4526, 11.4865$ the maximal known value of $\lambda_1/(\det\mathcal{L})^{1/n}$ for lattices $\mathcal{L}$ of dim. n [CS98] and for larger n the Kabatianski, Levenshtein upper bound $\gamma_n \le \frac{1.744}{2e\pi}n \approx 0.102111 \cdot n$; γ_n can be as small as the Minkowski, Hlawka lower bound $\frac{n}{2e\pi}$.

Corollary 4. *Let $c \le \delta + 1 - \frac{\ln p_n^3}{\ln N}$, $p_n^3 = o(N)$ and let $(u, v) \sim \mathbf{b} \in \mathcal{L}(\mathbf{B}_{n,c})$ be nearly square-free, $||\mathbf{b} - \mathbf{N}_c||^2 \approx ||\mathcal{L}(\mathbf{B}_{n,c}) - \mathbf{N}_c||^2$ and $\frac{1}{2}N^\delta \le v \le N^\delta$ and $|u - vN| \le p_n^3$. Then $||\mathbf{b} - \mathbf{N}_c||^2 \lesssim \lambda_1^2 - \ln N$.*

Proof. We have $\lambda_1^2 > 2c\ln N + 1 - o(1) \ge (2\delta + 2)\ln N + 1 - o(1)$ by Lemma 2 and by Lemma 1 :

$$\begin{aligned} ||\mathbf{b} - \mathbf{N}_c||^2 &\lesssim (2\delta + 1)\ln N + o(1) + \hat{z}^2_{\mathbf{b}-\mathbf{N}_c} \\ &\le (2\delta + 1)\ln N + o(1) + N^{2(c-1-\delta)}|u - vN|^2(1 + o(1)) \\ &\le (2\delta + 1)\ln N + 1 + o(1) < \lambda_1^2 - \ln N + o(1), \end{aligned}$$

the latter since $|u - vN| \le p_n^3$, $N^{2(c-1-\delta)} \le p_n^{-6}$ and Lemma 2. $\square$

Consequences. Cor. 4 shows for $c := \delta + 1 - \ln p_n^3 / \ln N$ that we can enumerate the square-free (u, v) of $\mathbf{b} \in rel_{N,n,\delta}$ by the approximate **CVP**-solutions minimizing $||\mathcal{L}(\mathbf{B}_{n,c}) - \mathbf{N}_c||$ or by approximate **SVP**-solutions of $\mathcal{L}' := \mathcal{L}([\mathbf{B}_{n,c}, \mathbf{N}_c])$. We see from Lemma 1 that $|u - vN| \le vN^{1-c}(\frac{(2\delta+1)\ln N}{n})^{1/2} \le p_n^3 (\frac{(2\delta+1)\ln N}{n})^{1/2}$ if $\hat{z}^2_{\mathbf{b}-\mathbf{N}_c} \lesssim (2\delta+1)\ln N/n$. Also the **SVP** solution for $\mathcal{L}'$ most likely provides a relation (5.1), possibly with N replaced by N^a, $a \in \mathbb{N}$ and most likely $a = 1$. Note that Cor. 4 also holds with p_n^3 replaced by any p_n^σ, $\sigma > 0$. Cor. 4 also shows that Cor. 3 extends Prop. 1 to the **CVP** of $\mathcal{L} = \mathcal{L}(\mathbf{B}_{n,c})$ with target vector $\mathbf{N}_c$ because that $||\mathcal{L} - \mathbf{N}_c|| \le \lambda_1(\mathcal{L})$.

Time bound of New Enum for solving SVP of $\mathcal{L}'$. $\mathcal{L}'$. (4.4) shows that **SVP** of $\mathcal{L}'$ can be solved in heuristic time $n^{n/8+o(1)}$ and in this time the enumeration of nearly shortest lattice vectors also yields $n + 1$ relations (5.1) and factors N. (4.4) is based on linear pruning and we next show that New Enum does not perform stages that are cut off by linear pruning. However New Enum performs stages in the order of their success rate, stages of high success rate are done first. (4.4) is a worst case time bound valid for the construction of short lattice vectors via arbitrary stages that are not cut off by linear pruning. While New Enum should certainely find some short lattice vectors much faster than in worst case time under linear pruning but this has still to be analysed.

Stages $(\mathbf{u_t}, ..., \mathbf{u_n})$ that are cut by linear pruning have extremely small success rates. Such stages are also not performed by New Enum. This extends the polynomial time bounds for Enum under linear pruning to New Enum. We give details for $N \lesssim 2^{800}$.

In solving **SVP** or **CVP** for the lattice $\mathcal{L}(\mathbf{B}_{n,c})$ and target vector $\mathbf{N}_c$ New Enum works on a well reduced basis $\mathbf{B} = [\mathbf{b}_1, ..., \mathbf{b}_n] = \mathbf{QR}$ of $\mathcal{L}(\mathbf{B}_{n,c})$ for which we assume that some form of **GSA** of Prop.1-3, holds. We show that New Enum does not perform any stage $(u_t, ..., u_n)$ that is cut by linear pruning because the success rate of such stages is extremely small. A stage $(u_t, ..., u_n)$ is cut by linear pruning if $||\pi_t(\sum_{i=t}^n u_i \mathbf{b}_i)||^2 > \frac{n-t+1}{n}\lambda_1^2$. Here $||\pi_t(\sum_{i=t}^n u_i \mathbf{b}_i)||^2$ is the consumed square length by $(u_t, ..., u_n)$ and $\lambda_1^2 - ||\pi_t(\sum_{i=t}^n u_i \mathbf{b}_i)||^2 < \frac{t-1}{n}\lambda_1^2$ can still be consumed by $(u_1, ..., u_{t-1})$.

The volume heuristics evaluates the expected number of such stages $(u_1, ..., u_{t-1})$ to

$$V_{t-1}\left(\tfrac{t-1}{n}\right)^{\frac{t-1}{2}} = \frac{\pi^{\frac{t-1}{2}}}{\left(\frac{t-1}{2}\right)!}\left(\tfrac{t-1}{n}\right)^{\frac{t-1}{2}} \approx \left(\tfrac{2e\pi}{n}\right)^{\frac{t-1}{2}} / \sqrt{\pi(t-1)}$$

Hence stage $(u_t, ..., u_n)$ has the success rate $\quad \beta_t = \left(\frac{2e\pi}{n}\right)^{\frac{t-1}{2}} / (r_{1,1} \cdots r_{t-1,t-1}\sqrt{\pi(t-1)})$
where $r_{1,1} \cdots r_{t-1,t-1} = \det(\mathcal{L}([\mathbf{b}_1, ..., \mathbf{b}_{t-1}]))$ and we have due to **GSA** that

$$r_{1,1} \cdots r_{t-1,t-1} = r_{1,1}^{t-1} q^{\frac{(t-1)(t-2)}{4}} = (\det \mathcal{L})^{\frac{(t-1)(t-2)}{n(n-1)}}.$$

Hence $\quad \beta_t \approx \left(\frac{2e\pi}{n}\right)^{\frac{t-1}{2}} (\det \mathcal{L}(\mathbf{B}_{n,c}))^{-\frac{(t-1)(t-2)}{n(n-1)}} / \sqrt{\pi(t-1)}$

where $\quad \det(\mathcal{L}(\mathbf{B}_{n,c})) \approx N^c (\ln p_n)^{n/2} \sqrt{n \ln p_n}(1 + o(1))$

Note that β_t is decreasing in t. For $N \approx 2^{800}$, $n = 43000$, $c = 3.1$, $t = 5$ the volume heuristics yields

$$\beta_5 \approx \left(\tfrac{2e\pi}{n}\right)^2 2^{-\frac{800 \cdot 2 \cdot 3.1}{43000^2}} / \sqrt{4\pi} \approx 4 \cdot 10^{-8} / \sqrt{4\pi}$$

Hence stage $(u_5, ..., u_n)$ will be cut by New Enum because β_5 is extremely small. As the above β_t is decreasing in t the same holds for all stages $(u_t, ..., u_n)$ for $t \ge 5$: if they are cut by linear pruning they are also cut by New Enum. This holds for **SVP** of $\mathcal{L}$ and similarly for $\mathcal{L}'$.

Outline of the CVP-algorithm without scaling. Let $\mathbf{B} = \mathbf{QR} = \mathbf{B}_{n,c}\mathbf{T} = [\mathbf{b}_1, ..., \mathbf{b}_n] \in \mathbb{Z}^{(n+1)\times n}$ be a BKZ-basis of $\mathcal{L}(\mathbf{B}_{n,c})$, $|\det(\mathbf{T})| = 1$. For $\mathbf{u} = (u_1, ..., u_n)^t \in \mathbb{Z}^n$ we denote $\mathbf{u}' = (u_1', ..., u_n')^t = \mathbf{Tu}$ so that $\mathbf{b} := \mathbf{B}_{n,c}\mathbf{u}' = \mathbf{Bu} \sim (u, v)$, with p_n-smooth $u = \prod_{u_i' > 0} p_i^{u_i'}$, $v = \prod_{u_i' < 0} p_i^{-u_i'} \in \mathbb{N}$. We replace the input $\mathbf{N}_c$ by its projection $\tau(\mathbf{N}_c) = \sum_{i=1}^n \tau_i \mathbf{b}_i \in \mathrm{span}(\mathcal{L})$, where $\tau : \mathbb{R}^{n+1} \to \mathrm{span}(\mathcal{L})$ satisfies $\mathbf{N}_c - \tau(\mathbf{N}_c) \in \mathcal{L}^\perp$. Then $\tau(\mathbf{N}_c) = d\,\mathbf{B}_{n,c}\mathbf{1} = d\,\mathbf{B}\,\mathbf{T}^{-1}\mathbf{1}$ holds for $d := \ln N / (N^{-2c} + \sum_{i=1}^n \ln p_i)$, $\mathbf{1} := (1, ..., 1)^t \in \mathbb{Z}^n$.

Starting at $t = n$ the algorithm tries to satisfy (5.9) as t decreases to 1.

$$||\pi_t(\,\mathbf{b} - \tau(\mathbf{N}_c))\,||^2 \le \tfrac{n-t+1}{n}(2c-1)\ln N + \hat{z}^2_{\mathbf{b}-\tau(\mathbf{N}_c)} \quad \text{for } \mathbf{b} = \mathbf{Bu} \sim (u, v) \tag{5.9}$$

(5.9) clearly holds for $t = n + 1$. If (5.9) holds at $t = 1$ then $||\,\mathbf{b} - \tau(\mathbf{N}_c)||$ and $|u - vN|$ are so small that they can provide a relation (5.1). We denote $\ddot{c}_t = c_t(\tau_t - u_t, ..., \tau_n - u_n) = ||\pi_t(\tau(\mathbf{N}_c) - \mathbf{Bu})||^2$. Recall that $\ddot{\beta}_t := V_{t-1}\ddot{\varrho}_t^{t-1} / (r_{1,1} \cdots r_{t-1,t-1})$ for $\ddot{\varrho}_t := (\ddot{A} - \ddot{c}_t)^{1/2}$ where $\ddot{A} \ge ||\mathcal{L} - \tau(\mathbf{N}_c)||^2$. The success rate $\ddot{\beta}_t$ increases as $\ddot{c}_t$ decreases, The stored stages with small success rate $\ddot{\beta}_t$ will be done after all stages with higher success rate $\ddot{\beta}_t$. They can be cut off if $\ddot{\beta}_t$ is extremely small or if to many stages with higher success rate $\ddot{\beta}_t$ have been stored and the algorithm runs out of storage space.

New Enum for CVP of the prime number lattice creating relations (5.1)

INPUT $\mathbf{B}$, $\mathbf{R} = [r_{i,j}] \in \mathbb{R}^{n\times n}$, $\mathbf{B}_{n,c}$, c, $\mathbf{T}$, $\tau_1, ..., \tau_n$, $\ddot{A} \in \mathbb{Q}$ s.t. $||\mathcal{L} - \mathbf{N}_c||^2 < \ddot{A}$, $s = \lceil \lg\lg n \rceil$.

OUTPUT A sequence of $\mathbf{b} = \sum_{i=1}^n u_i \mathbf{b}_i \in \mathcal{L}$ where $\|\mathbf{b} - \mathbf{N}_c\|$ decreases to $||\mathcal{L} - \mathbf{N}_c||$.

1. $t := n$, $L := \emptyset$, $y_n := \tau_n$, $u_n := \lceil y_n \rfloor$, $\ddot{c}_{n+1} := 0$,
   \# $\ddot{c}_t = c_t(\tau_t - u_t, ..., \tau_n - u_n)$ *always holds for the current* $t, u_t, ..., u_n$
   $\mathbf{u} := (0, ..., 0, u_n)^t \in \mathbb{Z}^n$, $\mathbf{b} := \mathbf{B} \cdot \mathbf{u}$, $\mathbf{u}' := \mathbf{T} \cdot \mathbf{u}$.
2. WHILE $t \le n$ \#*perform stage* $(t, u_t, ..., u_n, ..., y_t)$:
   [[$\ddot{c}_t := \ddot{c}_{t+1} + (u_t - y_t)^2 r_{t,t}^2$,
   IF $\ddot{c}_t \ge \ddot{A}$ THEN GO TO 2.1 \# *this cuts the present stage*
   $\ddot{\varrho}_t := (\ddot{A} - \ddot{c}_t)^{1/2}$, $\ddot{\beta}_t := V_{t-1}\ddot{\varrho}_t^{t-1}/(r_{1,1} \cdots r_{t-1,t-1})$,
   IF $t = 1$ THEN [output $\mathbf{b}$, $\ddot{A} := \ddot{c}_1 = \|\mathbf{b} - \tau(\mathbf{N}_c)\|^2$,
   update all stored $\ddot{\varrho}_{t'}$, $\ddot{\beta}_{t'}$ to the new $\ddot{A}$ GO TO 2.1]
   IF $\ddot{\beta}_t < 2^{-s+\lceil \lg\lg t \rceil}$ THEN [store the stage and $\ddot{\varrho}_t$, $\ddot{\beta}_t$ in L GO TO 2.1]
   [$t := t - 1$, $y_t := \tau_t + \sum_{i=t+1}^n (\tau_i - u_i) r_{t,i}/r_{t,t}$, $\varsigma_t := sign(u_t - y_t)$
   $u_t := \lceil y_t \rfloor$, $\nu_t := 1$, $u_i' := u_i' + t_{i,t} u_i$ for $i = 1, ..., n$, GO TO 2.]

2.1. IF $t < n$ THEN $t := t + 1$, $u_t := \lceil y_t \rfloor + \lceil \nu_t/2 \rceil \varsigma_t, \nu_t := \nu_t + 1, \varsigma_t := -\varsigma_t$.]]

3. $s := s + 1$, perform all delayed stages $(u_t, ..., u_n, y_t, \ddot{c}_t, \nu_t, \ddot{\beta}_t, \ddot{A})$ of L on level s.
   Delay new stages with $\ddot{\beta}_{t'} < 2^{-s+\lceil \lg\lg t' \rceil}$ and store them in L.
4. IF $s < s_{max}$ THEN $s := s + 1$ GO TO 3 ELSE *terminate.*

For the corresponding **SVP**- algorithm for $\mathcal{L}'$ we initially replace $\mathbf{B}_{n,c}$ by $[\mathbf{N}_c, \mathbf{B}_{n,c}]$. Note that **BKZ** reduction and New Enum can easily be iterated by iteratively increasing c.

Improving New Enum by continued fractions (CF). A. Schickedanz has extended New Enum by continued fractions. Take $\mathbf{b} = \sum_{j=1}^n u_j \mathbf{b}_j \in \mathcal{L}(\mathbf{B}_{n,c})$ at stage $(1, u_1, ..., u_n)$ and $(u, v) \sim \mathbf{b}$, $u = \prod_{u_j > 0} p_j^{u_j}$ and compute the regular CF $\frac{h_i}{k_i}$ of $\delta := \frac{u}{N} - \lceil \frac{u}{N} \rfloor$ with denominators $k_i \lesssim p_n^3$.

This starts with $\alpha_0 = |\delta|, \alpha_1 = 1/|\delta|$ and iterates $\alpha_{i+1} := 1/(\alpha_i - \lfloor \alpha_i \rfloor)$ as long as $\alpha_i > \lfloor \alpha_i \rfloor$. Then $\frac{h_i}{k_i}$ is given by $h_i = \lfloor \alpha_i \rfloor h_{i-1} + h_{i-2}$ and $k_i = \lfloor \alpha_i \rfloor k_{i-1} + k_{i-2}$ where $(h_{-1}, k_{-1}, h_0, k_0) = (1, 0, 0, 1)$ and $h_1 = 1$, $k_1 = \lfloor \alpha_1 \rfloor$, hence $k_i \ge \prod_{j=1}^i \lfloor \alpha_j \rfloor$. Each $\frac{h_i}{k_i}$ is a best approximation under all rational approximations $\frac{h_i'}{k_i'}$ of $|\delta|$ with denominators $k_i' \le k_i$. Lagrange has proved that $||\delta| - \frac{h_i}{k_i}| \le \frac{1}{k_i k_{i+1}}$, where equality holds if and only if $|\delta| = \frac{h_{i+1}}{k_{i+1}}$. This implies

Lemma 3. *$|u_i - v_i N| \le N/k_{i+1}$ holds for $u_i := u k_i$ and $v_i := \lceil \frac{u}{N} \rfloor k_i + sign(\delta) h_i$, where $|u_i - v_i N|$ yields a relation (5.1) if k_i and $|u_i - v_i N|$ are p_n-smooth.*

Proof.
$$|u_i - v_i N| = |(u - \lceil \tfrac{u}{N} \rfloor N) k_i - \mathrm{sign}(\delta) h_i N|$$
$$= |(\tfrac{u}{N} - \lceil \tfrac{u}{N} \rfloor - \mathrm{sign}(\delta)\tfrac{h_i}{k_i}) N k_i| = |(\delta - \mathrm{sign}(\delta)\tfrac{h_i}{k_i}) N k_i| \le N/k_{i+1}$$
since $||\delta| - \frac{h_i}{k_i}| \le \frac{1}{k_i k_{i+1}}$ due to Lagrange's inequality. □

This way CF extends New Enum to extremely large v_i that need not be p_n-smooth. The number of such relations increases rapidly with the bit length of v_i. We can increase the number of p_n-smooth k_i by using $\alpha_{i+1} := 1/(\alpha_i - \alpha_i')$ for both $\alpha_i' = \lceil \alpha_i \rceil$ and $\alpha_i' = \lfloor \alpha_i \rfloor$.

For $N \approx 10^{14}$, $n = 90$ and $c = 1.4$ Schickedanz's program found 14.000 relations (5.1) in 966 seconds, i.e. it took 0.067 seconds per relation. This yields a factoring time for $N \approx 10^{14}$ of 6.8 seconds. These 14.000 relations have been found for one fixed scaling. We present the first 10 of the 14.000 relations. These example relations for $N \approx 10^{14}$ and $c = 1.4$ have extremely large $v \gtrsim N^2$.

The first 10 of the 14.000 relations found for $\mathbf{N \approx 10^{14}}$ via continued fractions for just one scaling

$u = 29 \cdot 89 \cdot 101 \cdot 103 \cdot 109 \cdot 127 \cdot 163 \cdot 167 \cdot 179 \cdot 227 \cdot 257 \cdot 337 \cdot 401 \cdot 409 \cdot 431 \cdot 449 \cdot 457 \cdot 461^2 \cdot 463$
$v = 508169841688914466584296878342775$ $\quad |u - vN| = 2^6 \cdot 13 \cdot 157$

$u = 3 \cdot 5^2 \cdot 31 \cdot 101 \cdot 109 \cdot 157^2 \cdot 167^2 \cdot 229^2 \cdot 257 \cdot 263 \cdot 347 \cdot 349 \cdot 383 \cdot 389 \cdot 409 \cdot 439 \cdot 449 \cdot 457 \cdot 461 \cdot 463$
$v = 88490004923637711487480829355666391349$ $\quad |u - vN| = 2 \cdot 19 \cdot 79 \cdot 113$

$u = 3 \cdot 5 \cdot 11 \cdot 23 \cdot 37^2 \cdot 43 \cdot 47 \cdot 73 \cdot 101 \cdot 157 \cdot 163 \cdot 211 \cdot 257 \cdot 263 \cdot 277 \cdot 293 \cdot 313 \cdot 347 \cdot 409 \cdot 431^2 \cdot 449 \cdot 463$
$v = 39337475528468020686337374289751504 \qquad |u - vN| = 41 \cdot 53 \cdot 383$

$u = 3 \cdot 43 \cdot 47^2 \cdot 73^2 \cdot 101 \cdot 131 \cdot 157 \cdot 163^2 \cdot 167 \cdot 257 \cdot 263 \cdot 269^2 \cdot 409 \cdot 431 \cdot 449 \cdot 457 \cdot 461 \cdot 463$
$v = 5285053154856578428430584864963772 \qquad |u - vN| = 13 \cdot 199$

$u = 3^2 \cdot 23 \cdot 37 \cdot 43 \cdot 59 \cdot 107 \cdot 157 \cdot 163 \cdot 167 \cdot 179 \cdot 197 \cdot 229 \cdot 257 \cdot 313 \cdot 331 \cdot 379 \cdot 389 \cdot 409 \cdot 431 \cdot 449 \cdot 463$
$v = 103217349317428292671717081216913 \qquad |u - vN| = 2 \cdot 227 \cdot 311 \cdot 461$

$u = 2^2 \cdot 5^2 \cdot 43 \cdot 47 \cdot 67 \cdot 109 \cdot 137 \cdot 163 \cdot 167 \cdot 229 \cdot 257 \cdot 331 \cdot 389^2 \cdot 409^2 \cdot 439 \cdot 449 \cdot 457 \cdot 463$
$v = 1131979263675500365247847048973 \qquad |u - vN| = 83 \cdot 157 \cdot 317$

$u = 2^5 \cdot 5 \cdot 19^2 \cdot 61 \cdot 101 \cdot 103 \cdot 107 \cdot 157^2 \cdot 163 \cdot 257 \cdot 281 \cdot 313 \cdot 331^2 \cdot 389 \cdot 409 \cdot 449 \cdot 457 \cdot 463$
$v = 5898454839361247518321213045467 \qquad |u - vN| = 7 \cdot 13^3 \cdot 53$

$u = 2 \cdot 5^3 \cdot 7 \cdot 19^2 \cdot 59 \cdot 79^2 \cdot 89 \cdot 113 \cdot 137 \cdot 197 \cdot 263 \cdot 313 \cdot 313 \cdot 389^2 \cdot 431 \cdot 439 \cdot 449 \cdot 457 \cdot 463$
$v = 46796679363237306927028762631303 \qquad |u - vN| = 11 \cdot 97 \cdot 359$

$u = 5^2 \cdot 13 \cdot 19^2 \cdot 59 \cdot 101^2 \cdot 197 \cdot 293 \cdot 313 \cdot 331 \cdot 347 \cdot 389 \cdot 409 \cdot 439 \cdot 449 \cdot 457 \cdot 461 \cdot 463$
$v = 4482276109673039704152771836 \qquad |u - vN| = 3^2 \cdot 7^3 \cdot 71 \cdot 307$

$u = 17 \cdot 19^2 \cdot 43 \cdot 47 \cdot 73 \cdot 103 \cdot 109 \cdot 113 \cdot 257 \cdot 263 \cdot 281 \cdot 313 \cdot 337 \cdot 347^2 \cdot 431 \cdot 449 \cdot 457 \cdot 463$
$v = 113457285559875139699227627406 \qquad |u - vN| = 3 \cdot 5^2 \cdot 13^2 \cdot 23 \cdot 89 \cdot 199$

Note that $|u-vN|$ no more increases with v, the CF stopped this former increase. Interestingly the New Enum only found 78 relations at $t = 1$ without CF. The performance of CF for $N \approx 10^{14}$ is due to $N < p_n^6$. So far CF does not work for $N > p_n^6$. For $p_n^6 < N$ it may help to generalize CF to include $\alpha_{i+1} := 1/(\alpha_i - \beta_i)$ for all $\beta_i \in \mathbb{N}$ that satisfy $|\beta_i - \alpha_i| = O(1)$.

A. Schickedanz uses the following hardware and software.
Hardware: Prozessor AMD Phenom II X4 965 (3.41 GHz), storage: : 16 GB
Software operating system Windows 7 (64 Bit Version), Compiler: GCC 5.2.0 (Mingw-w64 Toolchain)
NTL: 9.6.2 (-02 -m64) Compiler Flags: -std=c++11 -O3 -m64

Comparison with [S93]. Our new results show an enormous progress compared to the previous approach of [S93]. [S93] reports on experiments for $N = 2131438662079 \approx 2.1 \cdot 10^{12}$, $N^c = 10^{25}$, $c \approx 2.0278$ and the prime number basis of dimension $n = 125$ with diagonal entries $\ln p_i$ for $i = 1, ..., n$ instead of $\sqrt{\ln p_i}$. The larger diagonal entries $\ln p_i$ require a larger c and more time for the construction of relations (5.1). The latter took 10 hours per found relation on a PC of 1993.

6 Exponentially many factoring relations (5.1) for large v

Now let $p_n = (\ln N)^\alpha$ for a small $\alpha > 2$ and a large N. Then p_n and n are larger than for the factoring experiments reported in section 5. Theorem 2 shows for the larger n that there are exponentially many p_n-smooth u, v such that $|u - vN| = 1$, $\frac{1}{2}N^\delta \leq v \leq N^\delta$. Theorem 3 shows under the assumptions of Theorem 2 and Prop. 1 that vectors $\mathbf{b} \in \mathcal{L}(\mathbf{B}_{n,c})$ closest to $\mathbf{N}_c$ can be found in pol. time. The proof combines the results of Theorem 2, Prop. 1, Lemma 1, Lemma 2 and Cor. 3. We denote for $\delta > 0$

$$M_{N,n,\delta} = \left\{ (u,v) \in \mathbb{N}^2 \;\middle|\; \begin{array}{l} |u - vN| = 1, \; \frac{1}{2}N^\delta \leq v \leq N^\delta \\ u, v \text{ are } p_n\text{-smooth} \end{array} \right\}.$$

Clearly every $(u,v) \in M_{N,n,\delta}$ yields a relation (5.2) because $|u - vN| = 1$ and uv is p_n-smooth. Theorem 2 shows that $\#M_{N,n,\delta} \geq N^\varepsilon = 2^{\varepsilon k}$, it is exponential in the bit length k of N.

Theorem 2. *Let $\alpha \geq 1.01 \frac{2\delta+1}{\delta-\varepsilon}$ and $0 < \varepsilon < \delta < \alpha \ln \ln N$. Assume the events that u, resp. v is p_n-smooth are nearly statistically independent for random v, $\frac{1}{2}N^\delta \leq v \leq N^\delta$ under the equation $|u - vN| = 1$ then $\#M_{N,n,\delta} \geq N^\varepsilon$ holds for sufficiently large N.*

Proof. (5.7) shows for $y^z = N$, $y = (\ln N)^\alpha = p_n = N^{1/z}$, $z = \ln N / \alpha \ln \ln N$ that

$$\Psi(N,p_n)/N = \left(\tfrac{e+o(1)}{z\ln z}\right)^z = z^{-z-o(z)} \quad \text{holds for } z \to \infty.$$

Extending this equation from N to N^δ and $N^{1+\delta}$ our assumption shows for large N :

$$\#M_{N,n,\delta} \geq N^\delta (z\delta)^{-z\delta-o(1)}(z\delta+z)^{-z\delta-z-o(z)},$$
$$\ln \#M_{N,n,\delta} \geq \delta \ln N - z\delta\ln(z\delta) - (z\delta+z)\ln(z\delta+z)\,(1+o(1)).$$

Here N^δ counts twice the number of integers v, $\frac{1}{2}N^\delta \leq v \leq N^\delta$. For every such v there are two $u = vN \pm 1$; $(z\delta)^{-z\delta-o(z)}$ and $(z\delta+z)^{-z\delta-z-o(z)}$ lower bound the portions of these v and u that are p_n-smooth. We assume that the p_n-smoothness events for u and v are nearly statistical independent of the equation $|u - vN| = 1$. Hence we get for $z = \ln N/\alpha \ln\ln N$ that

$$\begin{aligned}
&\ln \#M_{N,n,\delta} > \delta \ln N - \tfrac{(2\delta+1)\ln N \ln(z\delta)}{\alpha \ln\ln N}(1+o(1)) \\
&(\text{ since } \ln(z\delta+z) = \ln(z\delta)(1+o(1)) \text{ for large } z \text{ and constant } \delta\ ) \\
&> \delta\ln N - \tfrac{(2\delta+1)\ln N\,(\ln\ln N - \ln(\alpha\ln\ln N)+\ln\delta)}{\alpha\ln\ln N}(1+o(1)) \qquad (\text{ since } \delta < \alpha\ln\ln N\ ) \\
&\geq \ln N\big(\delta - \tfrac{2\delta+1}{\alpha}1.01\big) \qquad (\text{ for large } N\ ) \\
&> \varepsilon \ln N \qquad \text{since } \alpha > 1.01\tfrac{2\delta+1}{\delta-\varepsilon}. \qquad \text{Hence } \#M_{N,n,\delta} \geq N^\varepsilon. \qquad \square
\end{aligned}$$

Theorem 3. *Let $1 < c < (\ln N)^{\alpha/2-1}$. Assume the events that u, resp. v is p_n-smooth are nearly statistically independent for random v, $\frac{1}{2}N^c \leq v \leq N^c$ under the equation $|u-v| = 1$. Then $\lambda_1^2 = 2c\ln N(1+o(1))$ and $rd(\mathcal{L}) = o(n^{-1/4})$. If a reduced version of the basis $\mathbf{B}_{n,c}$ is given that satisfies* **GSA** *and $\|\mathbf{b}_1\|^2 = O(2c\ln N)$ and if some vector $\ddot{\mathbf{b}} \in \mathcal{L}(\mathbf{B}_{n,c})$ closest to $\mathbf{N}_c$ of (5.3) satisfies* **CA** *then* New Enum *finds $\ddot{\mathbf{b}}$ under the volume heuristics in pol. time.*

Remarks. Theorem 3 shows that $rd(\mathcal{L}) = o(n^{-1/4})$ is as small as required for Prop. 1 and Cor. 3.

Without the volume heuristics the time bound of Theorem 3 increases to $n^{O(1)}(R_\mathcal{L}/\lambda_1)^n$ where $R_\mathcal{L} = \max_{\mathbf{u}\in\text{span}(\mathcal{L})}\|\mathcal{L} - \mathbf{u}\|$ is the covering radius of $\mathcal{L}$. The factor $(R_\mathcal{L}/\lambda_1)^n$ overestimates New Enum's running time since New Enum essentially enumerates only lattice points in a ball of radius $\|\mathcal{L} - \mathbf{N}_c\| < \lambda_1 < R_\mathcal{L}$.

Proof. We first prove that $\lambda_1^2 = 2c\ln N\ (1+o(1))$ for $\mathcal{L} := \mathcal{L}(\mathbf{B}_{n,c})$ and $N \to \infty$. We denote

$$\widetilde{M}_{N,n,c} =_{def} \left\{(u,v)\in\mathbb{N}^2 \;\middle|\; \begin{array}{l} |u-v| = 1,\ \frac{1}{2}N^c \leq v \leq N^c \\ uv\ p_n - \text{smooth} \end{array}\right\}.$$

Following the proof of Theorem 2 for $\delta = c$ we see that $\#\widetilde{M}_{N,n,c} \geq N^c(zc)^{-2zc-o(z)}$ holds for $z = \frac{\ln N}{\alpha\ln\ln N}$. Recall that $(u,v)\in\widetilde{M}_N, n, c$ defines a vector $\mathbf{b}\sim(u,v)$ in $\mathcal{L}$. Hence

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

since $\alpha > 2$ due to $1 < (\ln N)^{\alpha/2-1}$. Let $\mathcal{L}(\mathbf{B}_{n,c}) \ni \mathbf{b} \sim (u,v) \in \widetilde{M}_{N,n,c}$ and let uv be essentially square-free except for a few small primes. We see from $\frac{1}{2}N^c \leq v \leq N^c$ and $u = v\pm 1$ that

$$\|\mathbf{b}\|^2 = \ln uv\ (1+o(1)) + \hat{z}_\mathbf{b}^2 \leq 2c\ln N\ (1+o(1)) + \hat{z}_\mathbf{b}^2,$$

where $c\ln N - \ln 2 \leq \ln v \leq c\ln N$. Moreover $\hat{z}_\mathbf{b}^2 = N^{2c}\ln^2(u/v)$ where $|\ln(u/v)| = |\ln(1+\frac{u-v}{v})| \leq \frac{1}{v}(1+o(1)) \leq 2N^{-c}(1+o(1))$ holds for large N. Hence $\hat{z}_\mathbf{b}^2 \leq 4(1+o(1))$ and thus $\lambda_1^2 \leq 2c\ln N\ (1+o(1))$. On the other hand $\lambda_1^2 \geq 2c\ln N$ holds by Lemma 2 and thus $\|\mathbf{b}\|^2/\lambda_1^2 = 1+o(1)$.

Next we bound $rd(\mathcal{L})$ for $\mathcal{L} = \mathcal{L}(\mathbf{B}_{n,c})$. Using $\gamma_n \geq \frac{n}{2e\pi}$ we get

$$\gamma_n(\det\mathcal{L})^{\frac{2}{n}} \geq \tfrac{n}{2e\pi}(\ln p_n \pm o(1))\cdot N^{2c/n}, \text{ and thus}$$
$$rd(\mathcal{L}) = \lambda_1/(\sqrt{\gamma_n}(\det\mathcal{L})^{\frac{1}{n}}) = \big(\tfrac{2e\pi\,2c\ln N}{n\ln p_n}\big)^{\frac{1}{2}}/N^{c/n}(1\pm o(1)).$$

Moreover $c \leq (\ln N)^{\alpha/2-1} = \sqrt{p_n}/\ln N$ implies $N^{c/n} = e^{\sqrt{p_n}/n} = e^{o(1)}$ and $N^{c/n} = 1+o(1)$. Hence

$$\begin{aligned} rd(\mathcal{L}) &= (\tfrac{4e\pi c\ln N}{n\ln p_n})^{1/2}(1+o(1)) = O(\tfrac{\ln N}{p_n})^{1/2} \\ &= O(p_n^{\alpha/2-1})^{1/2} = O(p_n^{-1/4}) = o(n^{-1/4}). \end{aligned}$$

since $p_n = O(n\ln p_n)$ and $c < (\ln N)^{\alpha/2-1}$ and $\ln N = p_n^{1/\alpha}$ and $\alpha > 2$.

Following the proof of Prop. 1 and Cor. 3 New Enum for **CVP** finds for $p_n = (\ln N)^\alpha$ some $\mathbf{b} \in \mathcal{L}(\mathbf{B}_{n,c})$ that minimizes $\|\mathbf{b} - \mathbf{N}_c\|$ in polynomial time, without proving correctness of the minimization. This proves the polynomial time bound. □

References

[Ad95] *L.A. Adleman*, Factoring and lattice reduction. Manuscript, 1995.

[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.

[Ch13] *M.Charlet*, Faktorisierung ganzer Zahlen mit dem NEW ENUM-Gitteralgorithmus. Diplomarbeit, Frankfurt 2013.

[CP01] *R. Crandall and C. Pomerance*, Prime Numbers, A Computational Perspective. Springer-Verlag, New York, 2001.

[CS98] *J.H. Conway and N.J.A. Sloane*, Sphere Packings Lattices and Groups. Material for Third Edition. Springer-Verlag, 1998.

[D30] *K. Dickman*, On the frequency of numbers containing prime factors of a certain relative magnitude. *Ark. Math. Astr. Fys.* **22**, pp. 1–14, 1930.

[D81] *J.D. Dixon*, Asymptotically Fast Factorization of Integers. *Mathematics of Computation* **36**(153), pp. 255–260, 1981.

[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.

[G08] *A. Granville*, Smooth numbers: computational number theory and beyond. in Algorithmic Number Theory, MSRI Publications, **44**, pp. 267–323, 2008.

[H84] *A. Hildebrand*, Integers free of large prime factors and the Riemann hypothesis. *Mathematika* **31**, pp. 258–271, 1984.

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

[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.

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

[La13] *B. Lange*, Neue Schranken für SVP-Approximation und SVP-Algorithmen. Dissertation, Frankfurt 2013, //www.mi.informatik.uni-frankfurt.de/ Ph.D. Theses.

[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.

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

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

[MR05] *D. Micciancio and O. Regev*, Worst-case to Average-case Reductions 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

[MB75] *M.A. Morrison and J. Brillhart*: *A Method of Factoring and the Factorization of* F_7, Mathematics of Computation **29**(129), pp. 183 –205, 1975.

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

[Reg04] *O. Regev*, New lattice-based cryptographic constructions, J. ACM 51 (6), pp. 899-942, 2004.

[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/

[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/

[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/

[S10] *C.P. Schnorr*, Average Time Fast SVP and CVP Algorithms for Low Density Lattices and the Factorisation of Integers, //www.mi.informatik.uni-frankfurt.de/ publications 2010

[S13] *C.P. Schnorr*, Factoring integers by CVP Algorithms, Proceedings Number Theory and Cryptography, LNCS 8260, Springer-Verlag, Nov. 2013, pp. 73–93, this is an early version of the most recent version in //www.mi.informatik.uni-frankfurt.de/ Publications 2013

[Sage] http://doc.sagemath.org/html/en/reference/functions/sage/functions/transcendental.html