Factoring Integers by CVP 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 20.07.2016

Abstract. We use pruned enumeration algorithms to find lattice vectors close to a specific target vector for the prime number lattice $\mathcal{L}(\mathbf{B}_{n,c})$. These algorithms generate triples of p_n-smooth integers $u, v, |u - vN|$ that factorize the integer N. The algorithm New Enum performs the stages of exhaustive enumeration of close lattice vectors in order of decreasing success rate. For example an integer $N \approx 10^{14}$ can be factored by about 90 prime number relations modulo N for the 90 smallest primes. So far our randomized algorithm generates 91 such relations and factors N in 6.2 seconds. It is a challenge to optimize this method towards factorizing integers in average polynomial time.

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

1 Introduction and surview

The enumeration algorithm for short / close lattice vectors Enum of [SE94, SH95] locally performs stages in order of decreasing success rate and 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. The New Enum algorithm for **SVP** / **CVP** presented in section 3 performs all stages in order of decreasing success rate, stages with high success rate are done first. This greatly reduces the number of stages that precede the finding of a shortest / closest lattice vector.

Section 4 summarizes results on time bounds of New Enum for **SVP** / **CVP** for a basis $\mathbf{B} = [\mathbf{b}_1, ..., \mathbf{b}_n]$ that satisfies **GSA** (meaning that the local reduction strength of the reduced basis is "uniform" for all 2-dimensional basis blocks). Prop. 1 shows that New 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 $\mathcal{L}$. Theorem 1 shows that the maximal **SVP**-time of New Enum ranges between $2^{O(n)}$ and $n^{O(n)}$ depending on $rd(\mathcal{L})$. Cor. 3 translates Prop. 1 from **SVP** to **CVP** proving pol. time under similar conditions as Prop.1 if $\|\mathcal{L} - \mathbf{t}\| = O(\lambda_1)$ holds for the target vector $\mathbf{t}$. Cor.1 translates Theorem 1 from **SVP** to **CVP** and shows that **CVP** for $\mathcal{L}$ and the target vector $\mathbf{t} \in \text{span}(\mathcal{L})$ is solved in time $2^{O(n)}$ and linear space if $rd(\mathcal{L}) = O(n^{-1/2})$, $\|\mathcal{L} - \mathbf{t}\| = O(\lambda_1)$ and a sufficiently short vector $\mathbf{b}_1$ of $\mathcal{L}$ is given.

Sections 5 and 6 study factoring integers N from **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 such triples we can easily factor N. For given N, n, c we can easily 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 enumerate these p_n-smooth triples by the **CVP**-algorithm for the lattice $\mathcal{L}(\mathbf{B}_{n,c})$, target vector $\mathbf{N}_c$ and a particular $c = c(N, n, \delta)$. Under heuristic assumptions this **CVP**-algorithm is polynomial time. We explain as example the factorization of some $N \approx 10^{14}$ using the $n = 90$ smallest primes and clever pruning of New Enum in 6.2 seconds. This algorithm can be further optimized, in particular for large n, N.

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

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 $\mathbf{BT}$, $\mathbf{T} \in \text{GL}_n(\mathbb{Z})$ that preserve $\mathbf{b}_1, ..., \mathbf{b}_{i-1}$.

A basis $\mathbf{B} = \mathbf{QR} \in \mathbf{R}^{m \times n}$. $\mathbf{R} = [r_{i,j}]$ 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 $\mathbf{t} \in \text{span}(\mathcal{L})$ find a closest vector $\mathbf{b}' \in \mathcal{L}$ such that $\|\mathbf{t} - \mathbf{b}'\| = \|\mathbf{t} - \mathcal{L}\| =_{def} \min\{\, \|\mathbf{t} - \mathbf{b}\| \mid \mathbf{b} \in \mathcal{L} \,\}$.

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 $\pi_t : \text{span}(\mathbf{b}_1, ..., \mathbf{b}_n) \to \text{span}(\mathbf{b}_1, ..., \mathbf{b}_{t-1})^\perp = \text{span}(\mathbf{b}_t^*, ..., \mathbf{b}_n^*)$ for $t = 1, ..., n$ denote the orthogonal projections and let $\mathcal{L}_t = \mathcal{L}(\mathbf{b}_1, ..., \mathbf{b}_{t-1})$.

The success rate of stages. The vector $\mathbf{b} = \sum_{i=t}^n u_i \mathbf{b}_i \in \mathcal{L}$ and $A \geq \lambda_1^2$ 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 $\zeta_t := \mathbf{b} - \pi_t(\mathbf{b}) \in \text{span}\, \mathcal{L}_t$ is $\mathbf{b}$'s orthogonal projection in $\text{span}\, \mathcal{L}_t$. Stage $(u_t, ..., u_n)$ and its substages exhaustively enumerate the intersection $\mathcal{B}_{t-1}(\zeta_t, \rho_t) \cap \mathcal{L}_t$ for the sphere $\mathcal{B}_{t-1}(\zeta_t, \rho_t) \subset \text{span}\, \mathcal{L}_t$ with radius $\rho_t := (A - \|\pi_t(\mathbf{b})\|^2)^{1/2}$ and center ζ_t.

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

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

Here $\text{vol}\, \mathcal{B}_{t-1}(\zeta_t, \rho_t) = V_{t-1} \rho_t^{t-1}$, $V_{t-1} = \pi^{\frac{t-1}{2}} / (\frac{t-1}{2})! \approx (\frac{2e\pi}{t-1})^{\frac{t-1}{2}} / \sqrt{\pi(t-1)}$ is the volume of the unit sphere of dimension $t-1$ and $\det \mathcal{L}_t = r_{1,1} \cdots r_{t-1,t-1}$. If $\zeta_t \mod \mathcal{L}_t$ is uniformly distributed

the expected size of this intersection satisfies $\mathrm{E}_{\zeta_t}[\ \#\big(|\mathcal{B}_{t-1}(\zeta_t,\rho_t)\cap\mathcal{L}_t\big)\ ]=\beta_t$. This holds because $1/\det\mathcal{L}_t$ is the number of lattice points of $\mathcal{L}_t$ per volume in $\operatorname{span}\mathcal{L}_t$.

The success rate β_t has been used in [SH95] to speed up ENUM by cutting stages of very small success rate. NEW ENUM proceeds differently, it first performs all stages with $\beta_t \geq 2^{-s}t$ and collects during this process the stages with $\beta_t < 2^{-s}t$ in the list L. Thereafter NEW ENUM performs the stages of L with $\beta_t \geq 2^{-s-1}t$. The test $\beta_t \geq 2^{-s}t$ gives priority to stages of small t, stages of large t require a higher success rate. The initial value $s = 10$ guarantes for $n \leq 100$ that $2^{-s}/n > 0.097$ and can be increased for larger n. The analysis in section 4 is independent of the factor t in $\beta_t < 2^{-s}t$.

We will use that $A := \frac{n}{4}(\det \mathbf{B}^t\mathbf{B})^{1/n} > \lambda_1^2$ holds for $n \geq 10$ since $\gamma_n < \frac{n}{4}$ for $n \geq 10$.
Optimal value of A. If λ_1 is known it is best to set the input A to $A := \lambda_1^2$.

Outline of New Enum

`INPUT` BKZ-basis $\mathbf{B}=\mathbf{QR}\in\mathbb{Z}^{m\times n}$, $\mathbf{R}=[r_{i,j}]\in\mathbb{R}^{n\times n}$ 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. $s := 10,\ \ L := \emptyset,\ \ A := \frac{n}{4}(\det \mathbf{B}^t\mathbf{B})^{1/n}$ (we call s the *level*)
2. *Perform via algorithm* ENUM *of [SE94, SH95], all stages with* $\beta_t \geq 2^{-s}t$: Upon entry of stage $(u_t, ..., u_n)$ compute β_t. If $\beta_t < 2^{-s}t$ store information about $(u_t, ..., u_n)$ in the list L of *delayed stages*. Otherwise perform stage $(u_t, ..., u_n)$ on level s, and as soon as some $\mathbf{b} \in \mathcal{L} - \mathbf{0}$ of length $\|\mathbf{b}\|^2 \leq A$ has been found, give out $\mathbf{b}$ and set $A := \|\mathbf{b}\|^2 - 1$.
3. $s := s + 1$, `IF` $L \neq \emptyset$ `THEN GO TO 2` (*to perform all stages* $(u_t, ..., u_n)$ *of* L *with* $\beta_t \geq 2^{-s}t$.) `ELSE` *terminate.*

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

Practical optimization. NEW ENUM computes $\mathbf{R}$, $\beta_t, V_t, \rho_t, c_t$ in floating point and $\mathbf{b}$, $\|\mathbf{b}\|^2$ in exact arithmetic. The final output $\mathbf{b}$ has length $\|\mathbf{b}\| = \lambda_1$, but this is only known when the more expensive final search does not find a vector shorter than 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 $\rho_t^2 = A - \|\pi_t(\mathbf{b})\|^2$ and β_t are large. New Enum tends to output very short lattice vectors $\mathbf{b}$ first.

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

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

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

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

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

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

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

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 [$t := t-1, \nu_t := 1, y_t := \sum_{i=t+1}^{t_{max}} u_i r_{t,i}/r_{t,t}$
   $u_t := -\lceil y_t \rfloor\ \sigma_t := sign(u_t - y_t)$]
   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 $u_t := -\lceil y_t \rfloor + \lfloor \nu_t/2 \rfloor (-1)^{\nu_t} \sigma_t,\ \nu_t := \nu_t + 1.$].
3. output $\mathbf{b}$

New Enum for SVP

INPUT BKZ-basis $\mathbf{B} = \mathbf{QR} \in \mathbb{Z}^{m\times n}$, $\mathbf{R} = [r_{i,j}] \in \mathbb{R}^{n\times n}$ for block length 32,

OUTPUT a sequence of $\mathbf{b} \in \mathcal{L}(\mathbf{B})$ such that $\|\mathbf{b}\|$ decreases to λ_1.

1. $L := \emptyset, t := t_{max} := 1, s := 10,$ 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,
   $\rho_t := (A - c_t)^{1/2},\ \beta_t := V_{t-1} \rho_t^{t-1} / (r_{1,1} \cdots r_{t-1,t-1}),$
   IF $t = 1$ THEN [$\mathbf{b} := \sum_{i=1}^{n} u_i \mathbf{b}_i,$
   IF $\|\mathbf{b}\|^2 < A$ THEN output $\mathbf{b}$, $A := \|\mathbf{b}\|^2 - 1,$ GO TO 2.1],
   IF $\beta_t \geq 2^{-s} t$ THEN [$t := t-1,\ y_t := \sum_{i=t+1}^{t_{max}} u_i r_{t,i}/r_{t,t}, u_t := -\lceil y_t \rfloor,$
   $\sigma_t := sign(u_t - y_t),\ \nu_t := 1,$ GO TO 2]
   ELSE store $(u_t, ...u_n, y_t, c_t, \sigma_t, \nu_t)$ in L.
2.1. $t := t+1,\ t_{max} := \max(t, t_{max}),$
   IF $t = t_{max}$ THEN $u_t := u_t + 1,\ \nu_t := 1,\ y_t := 0$
   ELSE $u_t := -\lceil y_t \rfloor + \lfloor \nu_t/2 \rfloor (-1)^{\nu_t} \sigma_t,\ \nu_t := \nu_t + 1.$
3. $s := s+1,$ perform all delayed stages $(u_t, ..., u_n, y_t, c_t, \sigma_t, \nu_t)$ of L on level s and delete them. Delay new stages with $\beta_{t'} < 2^{-s} t'$, $t' \leq t$ and store $(u_{t'}, ..., \nu_{t'})$ in L.
4. IF $L \neq \emptyset$ THEN GO TO 3 ELSE terminate.

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

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 $\mathbf{t}$:

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

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

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

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

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

New Enum for CVP

`INPUT` BKZ-basis $\mathbf{B} = \mathbf{QR} \in \mathbb{Z}^{m\times n}$ for block size 32, $\mathbf{R} = [r_{i,j}] \in \mathbb{R}^{n\times n}$,
$\mathbf{t} = \sum_{i=1}^{n} \tau_i \mathbf{b}_i \in \text{span}(\mathcal{L})$, $\tau_1, ..., \tau_n \in \mathbb{Q}^n$, $\ddot{A} \in \mathbb{Q}$ 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. $s := 10,\ t := n,\ L := \emptyset,\ y_n := \tau_n,\ u_n := \lceil y_n \rfloor,\ \ddot{c}_{n+1} := 0$, (We call s the level)
   ($\ddot{c}_t = c_t(\tau_t - u_t, ..., \tau_n - u_n)$ *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,
   $\ddot{\rho}_t := (\ddot{A} - \ddot{c}_t)^{1/2},\ \ddot{\beta}_t := V_{t-1}\ddot{\rho}_t^{t-1}/(r_{1,1} \cdots r_{t-1,t-1})$,
   `IF` $t = 1$ `THEN` [output $\mathbf{b} := \sum_{i=1}^{n} u_i \mathbf{b}_i,\ \ddot{A} := \|\mathbf{t} - \mathbf{b}\|^2$, `GO TO 2.1`]
   `IF` $\ddot{\beta}_t \ge 2^{-s} t$ `THEN` [$t := t - 1,\ y_t := \tau_t + \sum_{i=t+1}^{n}(\tau_i - u_i)r_{t,i}/r_{t,t},$
   $u_t := \lceil y_t \rfloor,\ \sigma_t := sign(u_t - y_t),\ \nu_t := 1,$ `GO TO 2`]
   `ELSE` store $(u_t, ..., u_n, y_t, \ddot{c}_t, \sigma_t, \nu_t)$ in L,
2.1. $t := t + 1,\ u_t := \lceil y_t \rfloor + \lfloor \nu_t/2 \rfloor \sigma_t,\ \nu_t := \nu_t + 1, \sigma_t := -\sigma_t$]]
3. $s := s + 1$, perform all delayed stages $(u_t, ..., u_n, y_t, \ddot{c}_t, \sigma_t, \nu_t)$ of L on level s and delete them from L. Delay all new stages with $\ddot{\beta}_{t'} < 2^{-s}t'$, $t' \le t$ and store $(u_{t'}, ..., u_n, y_{t'}, \ddot{c}_{t'}, \sigma_{t'}, \nu_{t'})$ in L.
4. `IF` $L \neq \emptyset$ `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 solve $||\mathbf{b}'|| = \lambda_1$ with $\mathbf{b}' \in \mathcal{L}(\mathbf{B})$. Finding an unproved shortest vector $\mathbf{b}'$ is easier than proving $\|\mathbf{b}'\| = \lambda_1$. New Enum finds an unproved shortest lattice vector $\mathbf{b}'$ in polynomial time under the following 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 $rd(\mathcal{L}) \le \big(\sqrt{\frac{e\,\pi}{2\,n}}\frac{\lambda_1}{\|\mathbf{b}_1\|}\big)^{\frac{1}{2}}$, i.e., both $\mathbf{b}_1$ and $rd(\mathcal{L})$ are sufficiently small.

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

(**SA** assumes a vector $\mathbf{b}' \in \mathcal{L}(\mathbf{B})$ that satisfies the linear pruning upper bound for **SVP**. Later we will use a similar assumption **CA** for **CVP**. **GSA** means that the $r_{i,i}^2$ form a geometric series.)

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

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

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". 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 $||\mathbf{b}'|| = \lambda_1$. We call pruning to stages $(u_t, ..., u_n)$ satisfying

$||\pi_t(\sum_{i=t}^n \mathbf{b}_i)||^2 \leq \frac{n-t+1}{n}\lambda_1^2$ **linear pruning** for **SVP**. 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 $\frac{n-t+1}{n}+d/\sqrt{n}$.

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

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

whereas the volume heuristics estimates this cardinality to $O(1)$ for $a \leq \frac{1}{2e\pi}$, also see Figure 1 of [MO90]. [GN08] reports that extensive experiments on high density random lattices show only negligible errors of the volume heuristics.

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 $rd(\mathcal{L})\sqrt{\gamma_n}\,\|\mathbf{b}_1\|/\lambda_1 \leq 1$ implies under **GSA** that $q \geq 1$ and thus $\|\mathbf{b}_1\| = \lambda_1$. Hence $rd(\mathcal{L}) > \frac{\lambda_1}{||\mathbf{b}_1||}/\sqrt{\gamma_n}$ holds under **GSA** if $\|\mathbf{b}_1\| > \lambda_1$. If $\frac{\lambda_1}{\|\mathbf{b}_1\|}/\sqrt{\gamma_n} \leq rd(\mathcal{L}) \leq \left(\frac{\lambda_1}{\|\mathbf{b}_1\|}\sqrt{\frac{e\,\pi}{2\,n}}\right)^{\frac{1}{2}}$ then **SVP** is solvable in pol. time by Prop. 1. Moreover the time bound of Theorem 1 is at best $2^{O(n)}$.

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

Proposition 1. *Given a basis* $\mathbf{B}=\mathbf{QR}$, $\mathbf{R}\in\mathbb{R}^{n\times n}$ *satisfying* $rd(\mathcal{L}) \leq \left(\frac{\lambda_1}{\|\mathbf{b}_1\|}\sqrt{\frac{e\,\pi}{2\,n}}\right)^{\frac{1}{2}}$ *and* **GSA**. *If a shortest lattice vector* $\mathbf{b}'$ *satisfies* **SA** *then* ENUM *and* NEW ENUM *with linear pruning find 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 $||\pi_t(\sum_{i=t}^n u_i\mathbf{b}_i)||^2 > \frac{n-t+1}{n}\lambda_1^2$ does not cut off any shortest lattice vector $\mathbf{b}'$ satisfying **SA**. As ENUM only performs stages $(u_t,...,u_n)$ with the "spend" length square $||\pi_t(\sum_{i=t}^n u_i\mathbf{b}_i)||^2 \leq \frac{n-t+1}{n}\lambda_1^2 =: \rho_t^2$ the volume heuristics bounds the number $\mathcal{M}_t^\rho$ of performed stages $(u_t,...,u_n)$ to

$$\begin{aligned}\mathcal{M}_t^\rho &:= \#\mathcal{B}_{n-t+1}(\mathbf{0},\rho_t)\cap\pi_t(\mathcal{L}) \leq (\sqrt{\tfrac{n-t+1}{n}}\,\lambda_1)^{n-t+1}V_{n-t+1}/(r_{t,t}\cdots r_{n,n})\\ &\lesssim (\sqrt{\tfrac{n-t+1}{n}}\,\lambda_1)^{n-t+1}\left(\tfrac{2e\pi}{n-t+1}\right)^{\frac{n-t+1}{2}}/(r_{t,t}\cdots r_{n,n})\\ &\leq \left(\lambda_1\sqrt{\tfrac{2e\pi}{n}}\right)^{n-t+1}/(r_{t,t}\cdots r_{n,n}). \qquad (4.1)\end{aligned}$$

We used Stirling's approximation of $(\frac{n-t+1}{2})!$ in approximating V_{n-t+1}. The volume heuristics can underestimate $\#\mathcal{B}_{n-t+1}(\mathbf{0},\rho_t)\cap\pi_t(\mathcal{L})$, however NEW ENUM already finds $\mathbf{b}'$ after enumerating a very small fraction of $\mathcal{B}_{n-t+1}(\mathbf{0},\rho_t)\cap\pi_t(\mathcal{L})$. 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 these equations and $\gamma_n < \frac{n}{e\pi}$ for $n > n_0$ we get

$$\mathcal{M}_t^\rho \lesssim \left(\tfrac{\lambda_1}{r_{1,1}}\sqrt{\tfrac{2e\pi}{n}}\right)^{n-t+1}\left(\sqrt{\tfrac{n}{e\pi}}\,rd(\mathcal{L})\,\tfrac{r_{1,1}}{\lambda_1}\right)^{n-\frac{(t-1)(t-2)}{n-1}}.$$

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

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

This upper bound has for $t \leq n$ its maximum 1 at $t=n$. This proves Proposition 1. □

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

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

Proposition 2. *Let* $\mathbf{R}\in\mathbb{R}^{n\times n}$ *be a* $\mathbf{GSA_{m,q}}$*-basis satisfying* $rd(\mathcal{L}) \leq \left(\frac{\lambda_1}{r_{i,i}}\sqrt{\frac{e\,\pi}{2\,n}}\right)^{\frac{m}{2n}}$ *having a shortest lattice vector* $\mathbf{b}'$ *satisfying* **SA**. *Then* ENUM *and* NEW ENUM *with linear pruning find such* $\mathbf{b}'$ *under the volume heuristics in polynomial time.*

Proof. We concentrate on $t \geq m$ since $\mathcal{M}_t^\rho$ has its maximum for $t \geq m$. There we have that

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

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

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

This yields for $t \geq m$ and $\gamma_n \leq \frac{2n}{e\pi}$ that

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

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

Hence $\mathcal{M}_t^\rho \lesssim 1$ iff $rd(\mathcal{L}) \leq \big(\frac{\lambda_1}{r_{1,1}}\sqrt{\frac{e\pi}{2n}}\big)^{\frac{m}{2n}}$. □

Prop. 2 extends Prop. 1 to the case that $r_{i,i}/r_{i-1,i-1}$ decreases uniformly for $i \leq m$ but the decrease stops completely for $i > m$. In practice this occurs naturally as the LLL-algorithm nicely reduces the initial part of a high-dimensional basis but merely performs size-reduction on the rest of the basis. Prop. 2 indicates that Prop. 1 also holds if the decrease of $r_{i,i}/r_{i-1,i-1}$ slowly vanishes for $i = 2, ..., n$ as $r_{i,i}/r_{i-1,i-1}$ increases from q to 1. Prop. 2 shows that the polynomial time bound for **SVP** in practice even holds if $rd(\mathcal{L}) \leq \big(\frac{\lambda_1}{r_{1,1}}\sqrt{\frac{e\pi}{2n}}\big)^{\frac{1}{2}-\varepsilon}$ for a small ε.

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 $0 < ||\mathbf{b}|| \leq \gamma\lambda_1$ are parallel to each other. Minkowski's second theorem shows for such $\mathcal{L}$ with successive minima $\lambda_1, ..., \lambda_n$ that $\lambda_1^n \gamma^{n-1} < \lambda_1 \cdots \lambda_n \leq \gamma_n^{n/2} \det \mathcal{L}$ and thus

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

Prop. 1 indicates that **SVP** for such $\mathcal{L}$ is solvable in pol. time under **SA** and the vol. heur. if

$$\gamma^{-2+2/n} \leq \big(\tfrac{\lambda_1}{||\mathbf{b}_1||}\sqrt{\tfrac{e\pi}{2n}}\big)^{1/2},$$

Ajtai, Dwork [AD97] propose a cryptosystem with security based on n^8-unique **SVP**. Prop.1 indicates that such **SVP** is solvable in pol. time for $n \leq 4000$. In fact $n^8 \geq \big(\frac{||\mathbf{b}_1||}{\lambda_1}\sqrt{\frac{2n}{e\pi}}\big)^{\frac{1}{4-4/n}}$ holds if $||\mathbf{b}_1|| \leq n^{31}\lambda_1$ since this implies $\big(\frac{||\mathbf{b}_1||}{\lambda_1}\sqrt{n}\big)^{\frac{1}{4-4/n}} \leq n^8$. Also BKZ-reduction with block size 24 of a basis of $\dim \mathcal{L} = n \leq 4000$ yields in practice in pol. time $||\mathbf{b}_1||/\lambda_1 \leq 4^{\frac{4000}{23}} < 4000^{31}$. Regev [Reg04] has build a cryptosystem with security based on $n^{1.5}$-unique **SVP** for $\mathcal{L}$ of dim. n. Prop. 1 indicates that such $n^{1.5}$-unique **SVP** is in practice solvable in pol. time if $\big(\frac{||\mathbf{b}_1||}{\lambda_1}\sqrt{\frac{2n}{e\pi}}\big)^{\frac{1}{4-4/n}} \leq n^{1.5}$. The latter holds for $n \leq 570$ if $\frac{||\mathbf{b}||}{\lambda:1} \leq n^{5.44}$. In fact BKZ-reduction with block size 24 of a basis with $n \leq 570$ yields $||\mathbf{b}_1||/\lambda_1 \leq 4^{\frac{n-1}{23}} < n^{5.44}$ for $n \leq 570$.

Prop. 2 shows for $rd(\mathcal{L}) \leq 1$ the heuristic **SVP** time bound $\big(\frac{r_{1,1}}{\lambda_1}\sqrt{\frac{2n}{e\pi}}\big)^{\frac{m}{2n}\frac{n-m+1}{1-m/2n}}$ for all $\mathbf{GSA}_{\mathbf{m},\mathbf{q}}$-bases. This time bound takes its maximum $\big(\frac{r_{1,1}}{\lambda_1}\sqrt{\frac{2n}{e\pi}}\big)^{(3-2\sqrt{2})n+o(n)}$ near $m = (2-\sqrt{2})n$. Suppose we can reduce the given basis of $\mathcal{L}$ in time $n^{o(n)}$ so that $||\mathbf{b}_1|| = r_{1,1} \leq n^\varepsilon\sqrt{\frac{e\pi}{2}}\lambda_1$. Then Prop. 2 yields the **SVP** time bound $n^{(\varepsilon+1/2)(3-2\sqrt{2})n+o(n)}$. This time bound beats for $\varepsilon \leq 1/2$ the record **SVP** time bound $n^{\frac{n}{2e}+o(n)}$ of Hanrot, Stehle [HS07] because $3-2\sqrt{2} \approx 0.17528 < 0.18397 \approx \frac{1}{2e}$. For $\varepsilon = o(1)$ this time bound is at most $n^{\frac{n}{4e}+o(n)}$.

Theorem 1. *Given a lattice basis $\mathbf{B} \in \mathbb{Z}^{m\times n}$ satisfying* **GSA** *and $\|\mathbf{b}_1\| \leq \sqrt{e\pi}\, n^b\, \lambda_1$ for some $b \geq 0$,* 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]. Recall from remark 4 that $n^{\frac{1}{2}+b}rd(\mathcal{L}) \geq 1$ holds under **GSA** for $\|\mathbf{b}_1\| \leq \sqrt{e\pi}\, n^b\, \lambda_1$ or else $\|\mathbf{b}_1\| = \lambda_1$. 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**, *$\|\mathbf{b}_1\| \leq \sqrt{e\pi}\, n^b\lambda_1$ with $b \geq 0$ and $\mathbf{t} \in \mathrm{span}(\mathcal{L})$ with $\|\mathcal{L} - \mathbf{t}\| \leq \lambda_1$,* New Enum *solves this* **CVP** *in time $2^{O(n)}(n^{\frac{1}{2}+b}rd(\mathcal{L}))^{\frac{n}{4}}$.*

Corollary 1 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 translates the assumption **SA** from **SVP** to **CVP**:

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

CA holds with probability $1/n$ for random $\ddot{\mathbf{b}} \in \text{span}(\mathcal{L})$ 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 $rd(\mathcal{L}) \le \left(\frac{\lambda_1}{\|\mathbf{b}_1\|}\sqrt{\frac{e\,\pi}{2\,n}}\right)^{\frac{1}{2}}$. 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 $rd(\mathcal{L}) \le \left(\frac{\lambda_1}{\|\mathbf{b}_1\|}\sqrt{\frac{e\,\pi}{2\,n}}\right)^{\frac{1}{2}}$. 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 $\mathbf{B}$ 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 $\mathbf{B}$ 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. A classical method factors N via $n+O(1)$ modular equations $\prod_{i=1}^n p_i^{e_i} = \pm\prod_{i=1}^n p_i^{e_i'} \mod N$. We construct such modular equations 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 $c > 0$:

$$\mathbf{B}_{n,c} = \begin{bmatrix} \sqrt{\ln p_1} & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \sqrt{\ln p_n} \\ N^c \ln p_1 & \cdots & N^c \ln p_n \end{bmatrix}, \qquad \mathbf{N}_c = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ N^c \ln N \end{bmatrix}, \tag{5.1}$$

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

as the prime number theorem implies $\prod_{i=1}^n \ln p_i^{1/n}/\ln p_n = 1 - o(1)$ for $n \to \infty$. We use that $o(1) \to 0$ for $n, N \to \infty$.

Outline of the factoring method. We compute vectors $\mathbf{b} = \sum_{i=1}^n e_i\mathbf{b}_i \in \mathcal{L}(\mathbf{B}_{n,c})$ close to $\mathbf{N}_c$ such that $|u - vN| \le p_n^{O(1)}$ factorizes as $|u - vN| = \prod_{i=1}^n p_i^{e_i'}$. This yields a non-trivial relation

$$u = \prod_{e_i>0} p_i^{e_i} = \pm\prod_{i=1}^n p_i^{e_i'} \mod N. \tag{5.2}$$

We write $n+1$ such relations with $p_0 = -1$ as $\prod_{i=0}^n p_i^{e_{i,j}-e_{i,j}'} = 1 \mod N$ for $j = 1, ..., n+1$. Any solution $t_1, ..., t_{n+1} \in \{0,1\}$ of the equations

$$\sum_{j=1}^{n+1} t_j(e_{i,j} - e_{i,j}') = 0 \mod 2 \quad \text{for } i = 0, ..., n \tag{5.3}$$

solves $X^2 = 1 \mod N$ by $X = \prod_{i=0}^n p_i^{\frac{1}{2}\sum_{j=1}^{n+1} t_j(e_{i,j}-e_{i,j}')} \mod N$. 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 (5.3) 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 vectors $\mathbf{b} \in \mathcal{L}(\mathbf{B}_{n,c})$ for which $|u - vN|$ factorizes over $p_1, ..., p_n$. This factoring method goes back to Morrison & Brillhart [MB75] and let to the first factoring algorithm in subexponetial time by J. Dixon [D81].

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 integers

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

Clearly uv is square-free if and only if $e_1, ..., e_n \in \{0, \pm 1\}$. 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 $\|\mathbf{b}\|^2 \geq \ln uv + \hat{z}_{\mathbf{b}}^2$ with equality if and only if uv is square-free. Similarly

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

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

Proof. Clearly $|u - vN| = o(vN)$ and $\frac{1}{2}N^\delta \leq v \leq N^\delta$ implies $|\frac{u-vN}{vN}| = o(1)$ and $\frac{1}{2}N^{1+\delta}(1 - o(1)) \leq u \leq N^{1+\delta}(1 + o(1))$. Hence $\ln uv = (2\delta + 1) \ln N \pm o(1)$ proving **1** by Fact 1. The upper bound **1** is sharp if uv is square-free. Moreover $\ln(1 + \frac{u-vN}{vN}) = \frac{u-vN}{vN}(1 \pm o(1)) = \pm o(1)$ and thus $|\hat{z}_{\mathbf{b}-\mathbf{N}_c}| = N^c \frac{|u-vN|}{vN}(1 \pm o(1)) = N^{c-1-\delta}|u - vN|(1 \pm o(1))$ which proves **2.** □

Lemma 5.3 of [M02] 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 $N^c \geq 10^3$.*

Proof. Let $\mathbf{b} = \mathbf{B}_{n,c}\mathbf{u} \neq \mathbf{0}$ 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 $u \geq v + 1$. Hence

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

Hence $\lambda_1^2 \geq \ln uv + N^{2c} \ln^2(\frac{u}{v}) > \ln uv + N^{2c}\frac{1}{uv}(1 - \frac{1}{2\sqrt{uv}})^2 =: f(\sqrt{uv})^2$ 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

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

An integer is called *y-smooth*, if it has no prime factor larger than y. If p_n-smooth u, v exist such that $u = v + 1$, $u = O(N^c)$, uv is square-free then $\lambda_1^2 = 2c \ln N + O(1)$. Otherwise λ_1^2 increases by the minimum of $\hat{z}_{\mathbf{b}}^2 \geq N^{2c} \ln^2(\frac{u}{v})$ 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] has shown for any fixed $z > 0$

$$\lim_{y \to \infty} \Psi(y^z, y) y^{-z} = \rho(z). \tag{5.5}$$

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

$$\begin{aligned} \rho(z) &= 1 - \ln z \quad \text{for} \quad 1 \leq z \leq 2 \\ \rho(z) &= \big(\tfrac{e \pm o(1)}{z \ln z}\big)^z = 1/z^{z + o(z)} \text{ for } z \to \infty \end{aligned} \tag{5.6}$$

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

$$\Psi(y^z, y) y^{-z} = \rho(z)\big(1 + O\big(\tfrac{\ln(z+1)}{\ln y}\big)\big) \tag{5.7}$$

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 (5.7) that

$$\Phi(N, p_n, \sigma) = O(2p_n^{2\,\sigma}\, \rho\big(\tfrac{\ln(Np_n^\sigma)}{\ln p_n}\big)\rho^2(\sigma)) \tag{5.8}$$

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 (5.8) in a range where $\frac{\ln N}{\ln p_n} + \sigma < p_n^{0.4}$ and we will neglect the $O(1)$-factor of (5.8).

Proof of (5.8). 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 (5.7) 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 (5.7) 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 (5.8) 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 $n = 90$, $p_{90} = 463$. (5.8 shows that there are $\Theta(6.4 \cdot 10^5)$ relations (5.2) such that $v, |u - vN| \le 463^3$ are p_n-smooth. Here we use the values $\rho(8.25) \approx 1.38 \cdot 10^{-8}$ and $\rho(3) \approx 4.86 \cdot 10^{-2}$ from [G08, table 1]. M. Charlet has constructed several hundreds such relations (5.2) for the above N. For this N the following program is particular efficient for $N^c = 10^{10}$, $c \approx 5/7$ and pruned to stages with success rate $\ddot{\beta}_t \ge 2^{-14}$. For the first time this recommends to use $c < 1$ as well as relatively small prime bases and to use extreme pruning.

A program for finding relations (5.2) 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. (This nearly excludes the "scaled" primes p_i to appear as factors of uv in relations (5.2) 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. But whenever a relation (5.2) has been found New Enum stops further decreasing $\ddot{A}$ for this round. Whenever a new closer lattice vector is found it is checked whether it yields a relation (5.2). The scaling per rround makes sure that the algorithm produces distinct relations (5.2). This program has been implemented by M. Charlet.

Performance. The program of Charlet found in 2012 in one run of 15 minutes and 350 rounds 136 relations. On average it found a relation every 6.6 seconds. This amounts to a factoring time of 10 minutes. Here are the first 10 of these example relations, they mostly satisfy $|u - vN| \le p_{90}^3$.

round	u	v	$\lvert u - vN\rvert$
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	$3^3 \cdot 13 \cdot 29 \cdot 109 \cdot 167$

Note that $|u - vN|$ increases with v proportionally to $\sqrt{v}$, $|u - vN| \sim \sqrt{v}$.

M. Charlet's program, improved in 2014 by A. Schickedan, found for $N = 100000980001501 \approx 10^{14}$, $n = 90$, $p_{90} = 463$, $c = 1/2$ and pruned to stages with $\ddot{\beta}_t \geq 2^{-14}t$ 99 relations (5.2) in 32 seconds. This factors $N \approx 10^{14}$ in 32 seconds. However for $N \approx 10^{20}$ this program took for $n = 150$, $c = 1/2$ about 34.5 seconds per relation (5.2).and factors N in 86 minutes.

Extending the search of relations (5.2) to large v. This is necessary for factoring $N \gg 10^{14}$ because the $\Phi(N, n, \sigma)$ values get to small for $\sigma = 3$. Let $rel_{N,n,\delta}$ denote the set of relations (5.2) consisting of p_n-smooth $u, v, |u - vN|$ such that $|u - vN| \leq p_n^3$ and $\frac{1}{2}N^\delta \leq v \leq N^\delta$ and let $\#_{N,n,\delta} = card(rel_{N,n,\delta})$. Using (5.7) we neglect the $O(\frac{\ln z+1}{\ln y})$-term of (5.7). The number of p_n-smooth $v \in [\frac{1}{2}N^\delta, N^\delta]$ is $\Psi(N^\delta, p_n) - \Psi(N^\delta/2, p_n) \approx N^\delta\big(\rho(z_v) - \frac{1}{2}\rho(z'_v)\big)$ for $z_v = \frac{\delta \ln N}{\ln p_n}$ $z'_v = z_v - \frac{\ln 2}{\ln p_n}$. Similarly the number of p_n-smooth $u \in [\frac{1}{2}N^{1+\delta}, N^{1+\delta}]$ is $\Psi(N^{1+\delta}, p_n) - \Psi(N^{1+\delta}/2, p_n) \approx N^{1+\delta}\big(\rho(z_u) - \frac{1}{2}\rho(z'_u)\big)$ for $z_u = \frac{(1+\delta)\ln N}{\ln p_n}$, $z'_u = z_u - \ln 2/\ln p_n$. Hence random $v \in_R [\frac{1}{2}N^\delta, N^\delta]$ is p_n-smooth with probability close to $2(\rho(z_v) - \frac{1}{2}\rho(z'_v))$, and random $u \in_R [\frac{1}{2}N^{\delta+1}, N^{\delta+1}]$ is 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 $v, u, |u - vN|$ with $\frac{1}{2}N^\delta$, the number of $v \in [\frac{1}{2}N^\delta, N^\delta]$ and $2p_n^3$ the number of non zero $u - vN \in [-p_n^3, p_n^3]$. We have 3 factors 2 and one factor 1/2. This yields

$$\#_{N,n,\delta} \approx 4\, N^\delta p_n^3\, \rho(3)\big(\rho(z_u) - \tfrac{1}{2}\rho(z'_u)\big)\big(\rho(z_v) - \tfrac{1}{2}\rho(z'_v)\big) \tag{5.9}$$

assuming that for random u, v, $\frac{1}{2}N^\delta \leq v \leq N^\delta$ and $u \in [\frac{1}{2}N^{1+\delta}, N^{1+\delta}]$ such that $|u - vN| \leq p_n^3$ the p_n-smoothness events for u, v and $|u - vN|$ are nearly statistically independent. Hahn has computed the $\rho(z)$ values for $z = 2, .., 200$ via [Sage] and we interpolate these values for arbitrary z_u, z_v.

For the following statstic we have chosen n, δ for N so that $\#_{N,n,\delta} \gg n$ and $\#_{N,n,\delta}$ is nearly maximal for the given N, n.

$N \approx$	10^{14}	10^{20}	2^{100}	2^{200}	2^{400}	2^{800}
n	90	150	300	1500	8200	42000
p_n	463	863	1987	12553	84127	506131
δ	0.75	0.78	0.8	1.15	1.65	2.095
$\#_{N,n,\delta}$	$1.55 \cdot 10^5$	$6.4 \cdot 10^4$	$9 \cdot 10^3$	$1.46 \cdot 10^4$	$5 \cdot 10^4$	$8.2\, n$

Our prime base is much smaller than the prime base for the quadratic sieve QS. QS requires for $N \approx 2^{400}$ that $p_n \geq e^{1/2\sqrt{lnNlnlnN}} \approx 2 \cdot 10^8$ whereas our $p_{8200} = 84127$.

Corollary 4. *Let $\mathbf{b} \in \mathcal{L}(\mathbf{B}_{n,c})$, $\mathbf{b} \sim (u, v) \in rel_{N,n,\delta}$, uv squarefree and $p_n^3 = o(N)$. Then we have for $c = \delta + 1 - \frac{3\ln p_n}{\ln N}$ that $||\mathbf{b} - \mathbf{N}_c||^2 = (2\delta + 1)\ln N + 1 \pm o(1)$.*

Proof. Lemma 1 part **1** shows $||\mathbf{b} - \mathbf{N}_c||^2 = (2\delta + 1)\ln N \pm o(1) + \hat{z}^2_{\mathbf{b}-\mathbf{N}_c}$ Moreover Lemma 1, part **2** shows that

$$|\hat{z}_{\mathbf{b}-\mathbf{N}_c}| = N^{c-1-\delta}|u - vN|(1 \pm o(1))$$
$$\leq N^{c-1-\delta}p_n^3(1 \pm o(1)) = N^0(1 \pm o(1)) = 1 \pm o(1)$$

for $c = \delta + 1 - \frac{3\ln p_n}{\ln N}$ which proves the claim. □

Consequences. Cor. 4 shows that we can enumerate the square-free $(u, v) \in rel_{N,n,\delta}$ by applying the **CVP** algorithm to an unscaled **BKZ**-reduced basis of $\mathcal{L}(\mathbf{B}_{n,c})$ and the target vector $\mathbf{N}_c$, setting $c := \delta + 1 - \frac{3\ln p_n}{\ln N}$, and fixing the upper bound A of $||\mathbf{b} - \mathbf{N}_c||^2$ to $A := (2\delta + 1)\ln N + 1$. This way the enumeration also covers many $\mathbf{b} \in \mathcal{L}(\mathbf{B}_{n,c})$ of non square-free $(u, v) \in rel_{N,n,\delta_-}$ for the $\delta_- < \delta$.

Theorem 3 proves for $p_n = (\ln N)^\alpha$, $\alpha > 2$ that $rd(\mathcal{L}(\mathbf{B}_{n,c}) = o(n^{-1/4})$. Hence Prop. 1 shows that **CVP** runs under heuristic assumptions, including the volume heuristics, in polynomial time. Fixing the initial A increases the running time but preserves the pol. time bound of Prop. 1.

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 (5.10) as t decreases to 1.

$$||\pi_t(\,\mathbf{b} - \tau(\mathbf{N}_c))\,||^2 \le \tfrac{n-t+1}{n}(2c-1)\ln N + \hat{z}^2_{\mathbf{b}-\tau(\mathbf{N}_c)} \quad \text{for } \mathbf{b} = \mathbf{Bu} \sim (u,v) \tag{5.10}$$

(5.10) clearly holds for $t = n+1$. If (5.10) holds at $t = 1$ then $||\,\mathbf{b} - \tau(\mathbf{N}_c)||$ and $|u - vN|$ are so small that they can provide a relation (5.2). 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 $\ddot{\beta}_t := V_{t-1}\ddot{\rho}_t^{t-1}/(r_{1,1}\cdots r_{t-1,t-1})$ for $\ddot{\rho}_t := (\ddot{A} - \ddot{c}_t)^{1/2}$ 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 (5.2)
`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_{max}.
`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. $s := 10$, $t := n$, $L := \emptyset$, $y_n := \tau_n$, $u_n := \lceil y_n \rfloor$, $\ddot{c}_{n+1} := 0$,
   # $\ddot{c}_t = c_t(\tau_t - u_t,...,\tau_n - u_n)$ *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*
   $\ddot{\rho}_t := (\ddot{A} - \ddot{c}_t)^{1/2}$, $\ddot{\beta}_t := V_{t-1}\ddot{\rho}_t^{t-1}/(r_{1,1}\cdots r_{t-1,t-1})$,
   `IF` $t = 1$ `THEN` [output $\mathbf{b}$, $\ddot{A} := \ddot{c}_1 = \|\mathbf{b} - \tau(\mathbf{N}_c)\|^2$, `GO TO 2.1`]
   `IF` $\ddot{\beta}_t < 2^{-s}t$ `THEN` [store the current stage in L `GO TO 2.1`]
   [$t := t-1$, $y_t := \tau_t + \sum_{i=t+1}^n (\tau_i - u_i)r_{t,i}/r_{t,t}$, $\sigma_t := sign(u_t - y_t)$
   $u_t := \lceil y_t \rfloor$, $\nu_t := 1$, $u'_i := u'_i + t_{i,t}u_i$ for $i = 1,...,n$, GO TO 2.]
2.1. `IF` $t < n$ `THEN` $t := t+1$, $u_t := \lceil y_t \rfloor + \lceil \nu_t/2 \rceil \sigma_t, \nu_t := \nu_t + 1, \sigma_t := -\sigma_t$.]]
3. perform and eliminate all undone stages of L on level s; hereby update $\ddot{A}$, delay all new stages with $2^{-s_{max}}t' \le \ddot{\beta}_{t'} < 2^{-s}t'$, $t' \le t$ and store them in L.
4. `IF` $s < s_{max}$ `THEN` $s := s+1$ `GO TO 3`

For the corresponding **SVP**- algorithm 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. A. Schickedanz has extended the New Enum algorithm for **CVP** by continued fractions (CF). At stage $(t, u_t, ..., u_n)|$ with $t = 1$ take $\mathbf{b} = \sum_{j=1}^n u_j\mathbf{b}_j \in \mathcal{L}(\mathbf{B}_{n,c})$ and the corresponding $(u,v) \sim \mathbf{b}$, $u = \prod_{u_j>0} p_j^{u_j}$ and compute all CF $\frac{h_i}{k_i}$ of $|\delta| := |\frac{u}{N} - \lceil \frac{u}{N} \rfloor|$ with denominators $k_i \lesssim p_n^3$.

The CF-algorithm starts with $\alpha_1 = 1/|\delta|$ and iterates $\alpha_{i+1} := 1/(\alpha_i - \lfloor \alpha_i \rfloor)$ for $i \ge 1$ 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 $k_i \ge \prod_{j=1}^i \lfloor \alpha_j \rfloor$ and thus each $k_1,...,k_i$ increases with $\alpha_1 = 1/|\delta|$. 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* $u_i := uk_i$ *and* $v_i := \lceil \frac{u}{N} \rfloor k_i + sign(\delta)h_i$

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

Note that $|u_i - v_i N|$ yields a relation (5.2) if k_i and $|u_i - v_i N|$ are p_n-smooth. This way CF improves the **CVP**- minimization of $||\mathcal{L}(\mathbf{B}_{n,c}) - \mathbf{N}_c||$ towards smaller values $|u_i - v_i N|$. CF's provide relations (5.2) with extremely large v_i that need not be p_n-smooth. The number of such relations with possibly p_n-unsmooth v_i increases rapidly with the bit length of v_i.

For $N \approx 10^{14}$ and $c = 1.4$ his program found 14.000 relations (5.2) 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 $N \approx 10^{14}$ have extremely large $v \gtrsim N^2$ and thus

$$||\mathbf{b} - \mathbf{N}_c||^2 \ge \ln(v^2 N) > 5 \ln N \quad \text{holds for } \mathbf{b} \sim (u, v).$$

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

$u = 29 \cdot 89 \cdot 101 \cdot 103 \cdot 109 \cdot 127 \cdot 163 \cdot 167 \cdot 179 \cdot 227 \cdot 257 \cdot 337 \cdot 401 \cdot 409 \cdot 431 \cdot 449 \cdot 457 \cdot 461^2 \cdot 463$
$v = 508169841688914466658429687834277 5$
$|u - vN| = 2^6 \cdot 13 \cdot 157$

$u = 3 \cdot 5^2 \cdot 31 \cdot 101 \cdot 109 \cdot 157^2 \cdot 167^2 \cdot 229^2 \cdot 257 \cdot 263 \cdot 347 \cdot 349 \cdot 383 \cdot 389 \cdot 409 \cdot 439 \cdot 449 \cdot 457 \cdot 461 \cdot 463$
$v = 884490004923637711487480829355666391349$
$|u - vN| = 2 \cdot 19 \cdot 79 \cdot 113$

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

$u = 3 \cdot 43 \cdot 47^2 \cdot 73^2 \cdot 101 \cdot 131 \cdot 157 \cdot 163^2 \cdot 167 \cdot 257 \cdot 263 \cdot 269^2 \cdot 409 \cdot 431 \cdot 449 \cdot 457 \cdot 461 \cdot 463$
$v = 39337475528468020686337374289751504$
$|u - vN| = 13 \cdot 199$

$u = 3^2 \cdot 23 \cdot 37 \cdot 43 \cdot 59 \cdot 107 \cdot 157 \cdot 163 \cdot 167 \cdot 179 \cdot 197 \cdot 229 \cdot 257 \cdot 313 \cdot 331 \cdot 379 \cdot 389 \cdot 409 \cdot 431 \cdot 449 \cdot 463$
$v = 11321734931742829267171708121 6913$
$|u - vN| = 2 \cdot 227 \cdot 311 \cdot 461$

$u = 2^2 \cdot 5^2 \cdot 43 \cdot 47 \cdot 67 \cdot 109 \cdot 137 \cdot 163 \cdot 167 \cdot 229 \cdot 257 \cdot 331 \cdot 389^2 \cdot 409 \cdot 439 \cdot 449 \cdot 457 \cdot 463$
$v = 11319792636755003652478470489 73$
$|u - vN| = 83 \cdot 157 \cdot 317$

$u = 2^5 \cdot 519^2 \cdot 61 \cdot 101 \cdot 103 \cdot 107 \cdot 157^2 \cdot 163 \cdot 257 \cdot 281 \cdot 313 \cdot 331^2 \cdot 389 \cdot 409 \cdot 449 \cdot 457 \cdot 463$
$v = 58984548393612475183212130454 67$
$|u - vN| = 7 \cdot 13^3 \cdot 53$

$u = 2 \cdot 5^3 \cdot 7 \cdot 19^2 \cdot 59 \cdot b79^2 \cdot 89 \cdot 113 \cdot 137 \cdot 197 \cdot 263 \cdot 313 \cdot 313 \cdot 389^2 \cdot 431 \cdot 439 \cdot 449 \cdot 457 \cdot 463$
$v = 46796679363237306922702876263 1303$
$|u - vN| = 11 \cdot 97 \cdot 359$
$u = 5^2 \cdot 13 \cdot 19^2 \cdot 59 \cdot 101^2 \cdot 197 \cdot 293 \cdot 313 \cdot 331 \cdot 347 \cdot 389 \cdot 409 \cdot 439 \cdot 449 \cdot 457 \cdot 461 \cdot 463$
$v = 44822761096730397041527718 36$
$|u - vN| = 3^2 \cdot 7^3 \cdot 71 \cdot 307$

$u = 17 \cdot 19^2 \cdot 43 \cdot 47 \cdot 73 \cdot 103 \cdot 109 \cdot 113 \cdot 257 \cdot 263 \cdot 281 \cdot 313 \cdot 317 \cdot 347^2 \cdot 431 \cdot 449 \cdot 457 \cdot 463$
$v = 11345728555987513969922762 7406$
$|u - vN| = 3 \cdot 5^2 \cdot 13^2 \cdot 23 \cdot 89 \cdot 199$

The **CVP** - algorithm has been used for $c = 1.4$. Large c increase the distance $||\mathcal{L}(\mathbf{B}_{n,c}) - \mathbf{N}_c||$ and also increase v of $\mathbf{b} \sim (u, v)$ because $||\mathcal{L}(\mathbf{B}_{n,c}) - \mathbf{N}_c||^2 \approx 2\ln(v^2 N)$. In fact CF extremely decreases $\hat{z}_{\mathbf{b}-\mathbf{N}_c}$. Note that $|u - vN|$ no more increases with v, the CF stopped this former increase. Interestingly the **CVP**-algorithm only found 78 relations at $t = 1$ before the CF-initiations.

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 (5.2). The latter took 10 hours per found relation on a PC of 1993.

6 Exponentially many factoring relations (5.2) 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 $|u - vN| = 1$, $\frac{1}{2}N^\delta \le v \le N^\delta$. 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 $\delta > 0$

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

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 $\#M_{N,n,\delta} \ge N^\varepsilon = 2^{\varepsilon k}$, it is exponential in the bit length k of N.

Theorem 2. *Let $\alpha \ge 1.01\frac{2\delta+1}{\delta-\varepsilon}$ 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, $\frac{1}{2}N^\delta \le v \le N^\delta$ under the equation $|u - vN| = 1$ then $\#M_{N,n,\delta} \ge N^\varepsilon$ 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

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

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

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

Here N^δ counts twice the number of integers v, $\frac{1}{2}N^\delta \le v \le N^\delta$. 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

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

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, $\frac{1}{2}N^c \le v \le N^c$ 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 (5.1) 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 $R_{\mathcal{L}} = \max_{\mathbf{u}\in\mathrm{span}(\mathcal{L})} \|\mathcal{L}-\mathbf{u}\|$ 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

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

Following the proof of Theorem 2 for $\delta = c$ we see that $\#\widetilde{M}_{N,n,c} \ge N^c(zc)^{-2zc-o(z)}$ 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

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

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 $\frac{1}{2}N^c\le v\le N^c$ and $u=v\pm1$ that

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

where $c\ln N - \ln 2 \le \ln v \le c\ln N$. Moreover $\hat{z}_{\mathbf{b}}^2 = N^{2c}\ln^2(u/v)$ where $|\ln(u/v)| = |\ln(1+\frac{u-v}{v})| \le \frac{1}{v}(1+o(1)) \le 2N^{-c}(1+o(1))$ holds for large N. Hence $\hat{z}_{\mathbf{b}}^2 \le 4(1+o(1))$ and thus $\lambda_1^2 \le 2c\ln N\ (1+o(1))$. On the other hand $\lambda_1^2\ge 2c\ln N$ 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 $\gamma_n \ge \frac{n}{2e\pi}$ we get

$$\gamma_n(\det\mathcal{L})^{\frac{2}{n}} \ge \tfrac{n}{2e\pi}(\ln p_n \pm o(1))\cdot N^{2c/n},\ \text{ and thus}$$

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

Moreover $c\le(\ln N)^{\alpha/2-1} = \sqrt{p_n}/\ln N$ 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. □

Towards factoring integers in pol. time. Theorem 3 shows that we can minimize $||\mathbf{b}-\mathbf{N}_c||$ for $\mathbf{b}\in\mathcal{L}(\mathbf{B}_{n,c})$ under the vol. heuristics and other reasonable assumptions in pol. time. In order to obtain n relations by the **CVP** algorithm we choose δ to maximize $\#_{N,n,\delta}$ forgiven N,n. In fact n must be so large that $\max_\delta \#_{N,n,\delta} > n$.

References

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

[AD97] *M. Ajtai and C. Dwork*, A public key cryptosystem with worst-case average-case equivalence. STOC, 1997, An improved version is described in ECCC 2007, No 97.

[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.

[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 NTRUEncrypt 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.
[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(2004), no 6, pp. 899-942.
[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