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 25.09.2017

Abstract. We factor an integer $N$ by enumeration algorithms that find vectors of the prime number lattice $L(B_{n,c})$ close to a specific target vector $N$, 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. We consider extensions to large $N$.

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

1 Introduction and survey

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, PÖHST [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 $B = [b_1, ..., b_n] \in \mathbb{Z}^{n \times n}$ 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 $b$ that behaves randomly (SA) under the volume heuristics in polynomial time if $rd(L) = o(n^{-1/4})$ holds for the relative density $rd(L)$ of $L$, defined in section 2. It follows that the maximal SVP-time of ENUM under linear pruning for lattices of dim. $n$ is $2^\frac{\delta}{2} + o(n)$. Cor. 3 translates Prop. 1 from SVP to CVP proving pol. time under similar conditions as Prop. 1 if $\|L - t\| \lesssim \delta_1$ holds for the target vector $t$.

Sections 5 and 6 study factoring integers $N$ by approximate CVP solutions for the prime number lattice $L(B_{u,c})$ and a target vector $N$, 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 $\frac{1}{2}N^\delta \leq v \leq N^\delta, |u-vN| \leq p_n^\delta$. We can efficiently enumerate these $p_n$-smooth triples by the CVP-algorithm for the prime number lattice $L(B_{u,c})$, target vector $N$, 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 $B = [b_1, ..., b_n] \in \mathbb{R}^{m \times n}$ be a basis matrix consisting of $n$ linearly independent column vectors $b_1, ..., b_n \in \mathbb{R}^m$. They generate the lattice $L(B) = \{Bx \mid x \in \mathbb{Z}^n\}$ consisting of all integer linear combinations of $b_1, ..., b_n$, the dimension of $L$ is $n$. The determinant of $L$ is $\det L = (\det B^tB)^{1/2}$ for any basis matrix $B$ and the transpose $B^t$ of $B$. The length of $b \in \mathbb{R}^m$ is $\|b\| = (b^t b)^{1/2}$. 
Let $\lambda_1, \ldots, \lambda_n$ denote the successive minima of $L$ and $\lambda_1 = \lambda_1(L)$ is the length of the shortest nonzero vector of $L$. The Hermite constant $\gamma_n$ is the minimal $\gamma$ such that $\lambda_1^2 \leq \gamma (\det L)^{2/n}$ holds for all lattices of dimension $n$. Let $B = QR \in \mathbb{R}^{n \times n}$, $R = [r_{i,j}]_{1 \leq i,j \leq n} \in \mathbb{R}^{n \times n}$ the unique QR-factorization: $Q \in \mathbb{R}^{n \times n}$ is isometric (with pairwise orthogonal column vectors of length 1) and $R \in \mathbb{R}^{n \times n}$ 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 $B$. The orthogonal projection $b_i^r$ of $b_i$ in $\text{span}(b_1, \ldots, b_{i-1})$ has length $r_{i,i} = ||b_i^r||$, $r_{1,1} = ||b_1||$. 

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

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

Obviously, LLL-bases satisfy $r_{i,i}^2 \leq \alpha r_{i+1,i}^2 + r_{i+1,i+1}^2$ 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. $\alpha^{-i+1} \leq ||b_i||^2 \lambda_i^{-2} \leq \alpha^{n-1}$ for $i = 1, ..., n$.
4. $||b_1||^2 \leq \alpha^{\frac{n-1}{2}} (\det L)^{2/n}$.

A basis $B = QR \in \mathbb{R}^{n \times n}$ is an HKZ-basis (Hermite, Korkine, Zolotareff) if $|r_{i,j}| / r_{i,i} \leq \frac{1}{4}$ for all $j \geq i$, and if each diagonal entry $r_{i,i}$ of $R = [r_{i,j}] \in \mathbb{R}^{n \times n}$ is minimal under all unitary transformations of $B$ to $BT$, $T \in \text{GL}_n(\mathbb{Z})$ that preserve $b_1, \ldots, b_{i-1}$.

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

A famous problem is the shortest vector problem (SVP): Given a basis of $L$ find a shortest nonzero vector of $L$, i.e., a vector of length $\lambda_1$. Closest vector problem (CVP): Given a basis of $L$ and a target $t \in \text{span}(L)$ find a closest vector $b^* \in L$ such that $||t - b^*|| = ||t - L|| =_{def} \min \{||t - b|| \mid b \in L\}$.

The efficiency of our algorithms depends on the lattice invariant $rd(L) := \lambda_1 \gamma_n^{-1/2} (\det L)^{-1/n}$ which we call the relative density of $L$. Note that $rd(L) = \lambda_1 / \max \lambda_1(L')$ holds for the maximum of $\lambda_1(L')$ over all lattices $L'$ of dim $L = \dim L'$ and det $L = \det L'$. Clearly $0 < rd(L) \leq 1$ holds for all $L$, and $rd(L) = 1$ if and only if $L$ has maximal density. Lattices of maximal density and $\gamma_n$ 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 $b$ rather fast by performing the stages in order of decreasing success rate.

Let $B = [b_1, ..., b_n] = QR \in \mathbb{Z}^{n \times n}$, $R = [r_{i,j}]_{1 \leq i,j \leq n} \in \mathbb{R}^{n \times n}$ be the given basis of $L = (L \langle b \rangle)$. Let $\pi_t : \text{span}(b_1, ..., b_n) \to \text{span}(b_1, ..., b_{t-1})^\perp = \text{span}(b_t, ..., b_n)$ for $t = 1, ..., n$ denote the orthogonal projections and let $L_t = L(b_1, ..., b_{t-1})$. Let $\lambda_t^2$ of $L$ be given, otherwise we use some close $A > \lambda_t^2$.

The success rate of stages. At stage $u = (u_1, ..., u_n)$ of Enum for SVP of $L$ a vector $b = \sum_{i=1}^n u_i b_i \in L$ is given such that $||u_{t-1}(b)||^2 \leq \lambda_{t-1}^2$. (When $\lambda^2$ is unknown we use instead some $A > \lambda_t^2$.) Stage $u$ calls the substages $(u_1, ..., u_n)$ such that $||u_{t-1}(\sum_{i=1}^{n-t} u_i b_i)||^2 \leq \lambda_{t-1}^2$. We have $||u_{t-1}(u_i b_i)||^2 = ||\zeta_i + \sum_{j=t+1}^n u_j b_j||^2 + ||\pi_1(b)||^2$, where $\zeta_i := b - \pi_t(b) \in \text{span} L_t$ is $b$'s orthogonal projection in $\text{span} L_t$. Stage $u$ and its substages enumerate the intersection $B_{t-1}(\zeta_t, b_t) \cap L_t$ of the sphere $B_{t-1}(\zeta_t, b_t) \subset \text{span} L_t$ with radius $\rho_t := (\lambda_t^2 - ||\pi_1(b)||^2)^{1/2}$ and center $\zeta_t$. The GAUSSIAN volume heuristics estimates $|B_{t-1}(\zeta_t, b_t) \cap L_t|$ for $t = 1, ..., n$ to

$$|B_{t-1}(\zeta_t, b_t) \cap L_t| \approx \frac{\pi^{d/2}}{(t-1)!} \left(\frac{2\pi e}{t+1}\right)^{t+1/2} \sqrt{\pi(t-1)}$$

Here $vol B_{t-1}(\zeta_t, b_t) = \nu_{t-1} b_t^{-1}$. $\nu_{t-1} = \pi^{d/2} / (t-1)! \approx \left(\frac{2\pi e}{t+1}\right)^{t+1/2}/\sqrt{\pi(t-1)}$ is the volume of the unit sphere of dimension $t-1$ and det $L_t = r_{1,1} \cdots r_{1-t,-1}$. If $\zeta_t \mod L_t$ is uniformly distributed
the expected size of this intersection satisfies \( E_t \left( \# (B_{t-1} (\zeta_t, \varrho_t) \cap L_t) \right) = \beta_t (u) \). This holds because \( 1 / \det L_t \) is the number of lattice points of \( L_t \) per volume in \( \text{span} \ L_t \).

The success rate \( \beta_t \) has been used in [SH95] to speed up \( \text{Enum} \) by cutting stages of very small success rate. \( \text{New Enum} \) first performs all stages with sufficiently large \( \beta_t \) giving priority to small \( t \) and can collect during this process the unperformed stages in the list \( L \). For instance it first performs all stages with \( \beta_t \geq -s + \lfloor \lg \lg t \rfloor \), i.e. \( \beta_t \geq 2^{-s + \lfloor \lg \lg t \rfloor} \), where \( \lg := \log_2 \). Thereafter \( \text{New Enum} \) increases \( s \) to \( s + 1 \). So far our experiments simply perform all stages with \( \beta_t \geq 2^{-s} \).

If \( \lambda_2^2 \) is unknown we can use instead \( A := \frac{3}{4} (\det B^t B)^{1/\alpha} \) as \( A > \lambda_2^2 \) holds for \( n \geq 10 \) where \( \gamma_n < n/4 \).

### Outline of New Enum

<table>
<thead>
<tr>
<th>INPUT</th>
<th>BKZ-basis ( B = QR \in Z^{n \times n}, R = [r_{ij}] \in R^{n \times n} ) for block size 32.</th>
</tr>
</thead>
<tbody>
<tr>
<td>OUTPUT</td>
<td>a sequence of ( b \in L(B) ) of decreasing length terminating with ( | b | = \lambda_1 ).</td>
</tr>
</tbody>
</table>

1. Start at level \( s := \lfloor \lg \lg n \rfloor \), \( L := \emptyset \). If \( \lambda_2^2 \) is unknown then use some \( A > \lambda_2^2 \).
2. Let \( \text{New Enum} \) perform all stages \( u = (u_1, ..., u_n) \) with \( \beta_t (u) \geq 2^{-s + \lfloor \lg \lg t \rfloor} \).
   
   Upon entry of stage \((u_1, ..., u_n)\) compute \( \beta_t (u) \). If \( \beta_t (u) < 2^{-s + \lfloor \lg \lg t \rfloor} \) then store \((u_1, ..., u_n)\) in the list \( L \) of delayed stages.
   
   Otherwise perform stage \((u_1, ..., u_n)\), setting \( t := t - 1 \), \( u := -\sum_{i=1}^{n} u_i r_{i,t}/r_{i,t} \) and go to stage \((u_1, ..., u_n)\). If for \( t = 1 \) some \( b \in L - 0 \) of length \( \| b \|^2 \leq A \) has been found, give out \( b \) and decrease \( A := \| b \|^2 - 1 \).
3. \( s := s + 1 \). IF \( L \neq \emptyset \) THEN perform all stages \( u = (u_1, ..., u_n) \) of \( L \) with \( \beta_t (u) \geq 2^{-s + \lfloor \lg \lg t \rfloor} \) ELSE terminate.

### Running in linear space.

If instead of storing the list \( L \) we restart \( \text{New Enum} \) in step 3 on level \( s + 1 \) then \( \text{New Enum} \) runs in linear space and its running time increases at most by a factor \( n \).

### Practical optimization.

\( \text{New Enum} \) computes \( R, \beta_t, V_t, \varrho_t, c_t \) in floating point and \( b, \| b \|^2 \) in exact arithmetic. The final output \( b \) has length \( \| b \| = \lambda_1 \), but this is only known when the more expensive final search does not find a vector shorter than the final \( b \).

### Reason of efficiency.

For short vectors \( b = \sum_{i=1}^{n} u_i b_i \in L \setminus 0 \) the stages \( u = (u_1, ..., u_n) \) have large success rate \( \beta_t (u) \). On average \( \| x_i (b) \|^2 \approx \frac{2}{2^n} \lambda_2^2 \) holds for a random \( b \in R B_n (0, \lambda) \) of length \( \lambda_1 \). Therefore \( q_t^2 = A - \| x_t (b) \|^2 \) and \( \beta_t (u) \) are large. \( \text{New Enum} \) tends to output very short lattice vectors first.

\( \text{New Enum} \) is particularly fast for small \( \lambda_1 \). The size of its search space is approximates \( \lambda_1^4 V_n \), and it is by Prop. 1 heuristically polynomial if \( rd (L) = o (n^{-1/4}) \). Having found \( b' \) \( \text{New Enum} \) proves \( \| b' \| = \lambda_1 \) in exponential time by a complete exhaustive enumeration.

### Notation.

We use the following function \( c_t : Z^{n-t+1} \rightarrow R : \)

\[
c_t (u_1, ..., u_n) = \| x_t (\sum_{i=1}^{n} u_i b_i) \|^2 = \sum_{i=1}^{n} \sum_{j=1}^{n} u_i r_{i,j}^2 + c_{t+1} (u_{t+1}, ..., u_n). \]

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

\[-y_t, -\lfloor y_t \rfloor - \zeta_t, -\lfloor y_t \rfloor + \zeta_t, -\lfloor y_t \rfloor - 2 \zeta_t, -\lfloor y_t \rfloor + 2 \zeta_t, ... \]

Let \( \text{sign} (0) := 1 \) and let \( \lfloor r \rfloor \) denote a nearest integer to \( r \in R \). The iteration does not decrease \( |u_t + y_t| \) and \( c_t (u_1, ..., u_n) \), it does not increase \( y_t \) and \( \beta_t \). \( \text{Enum} \) performs the stages \((u_1, ..., u_n)\) for fixed \( u_{t+1}, ..., u_n \) in order of increasing \( c_t (u_1, ..., u_n) \) and decreasing success rate \( \beta_t \). The center \( \zeta = b - \pi_t (b) = \sum_{i=1}^{n} u_i (b_i - \pi_t (b_i)) \in \text{span} (L_t) \) changes continously within \( \text{New Enum} \).
Algorithm BKZ Enum adapted from [SH95]

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

1. FOR $i = 1, \ldots, n$ DO $c_i := u_i := y_i := 0$, $u_i := 1$, $t := t_{\text{max}} := 1$, $\tilde{c}_i := c_i := \|\mathbf{b}_i\|^2$. (Here $c_i$ is always holds for the current $t$, $\tilde{c}_i$ is the current minimum of $c_i$)
2. WHILE $t \leq n$ #perform stage $(u_i, \ldots, u_n)$:
   
   $c_i := c_{i+1} + (u_i - y_i)^2r_{i,t}^2$
   
   IF $c_i < \tilde{c}_i$ and $t > 1$ THEN [$t := t - 1$, $\nu_t := 1$, $y_t := \sum_{i=1}^{t_{\text{max}}} u_i r_{i,t}/r_{i,t}$
   $u_t := -[y_t]$, $\tilde{c}_i := \text{sign}(u_t - y_t)$] ELSE IF $c_i < \tilde{c}_i$ and $t = 1$ THEN $\tilde{c}_i := c_i$, $b := \sum_{i=1}^{n} u_i b_i$, $t := t + 1$
   $t_{\text{max}} := \max(t, t_{\text{max}})$, IF $t = t_{\text{max}}$ THEN $u_t := u_t + 1$, $\nu_t := 1$
   ELSE $u_t := -[y_t] + [\nu_t/2](-1)^{\nu_t}c_t$, $\nu_t := \nu_t + 1$.

3. output $b$

New Enum for SVP

INPUT $\mathbf{B}$-basis $\mathbf{B} = QR \in \mathbb{Z}^{m \times n}, \mathbf{R} = [r_{i,j}] \in \mathbb{R}^{n \times n}$ of block size $32$, $s = \lfloor \log_2 n \rfloor$.
OUTPUT a sequence of $\mathbf{b} \in \mathcal{L}(\mathbf{B})$ such that $\|\mathbf{b}\|$ decreases to $\lambda_1$.

1. $L := \emptyset$, $t := t_{\text{max}} := 1$, FOR $i = 1, \ldots, n$ DO $c_i := u_i := y_i := 0$, $u_i := u_i := 1$, $c_i := r_{i,1}$, $A := \frac{1}{8} (\det \mathbf{B}^2)^{1/8}$ ($c_i$ is always holds for the current $t$)
2. WHILE $t \leq n$ #perform stage $(u_i, \ldots, u_n)$:
   
   $c_i := c_{i+1} + (u_i - y_i)^2r_{i,t}^2$
   
   IF $c_i < A$ THEN $\text{GO TO 2.1}$
   $y_t := \text{det}(A - c_i)^{1/2}$, $\beta_t := V_{t-1}^{-1}(-r_{1,1}^{-1}\cdots r_{t-1,1}^{-1})$
   $t = 1$ THEN [$b := \sum_{i=1}^{n} u_i b_i$]
   IF $\|\mathbf{b}\|^2 < A$ THEN output $b$, $A := \|\mathbf{b}\|^2 - 1$, GO TO 2.1
   IF $\beta_t \geq 2^{-s}[[\log \left|\mathbf{b}\right|]]$ THEN [$t := t - 1$, $y_t := \sum_{i=1}^{n} u_i r_{i,t}/r_{i,t}$, $u_t := -[y_t]$, $\tilde{c}_i := \text{sign}(u_t - y_t)$, $\nu_t := \nu_t + 1$]
   $A := \text{GO TO 2}$
   ELSE store $(u_1, \ldots, u_n, y_t, c_t, \nu_t, \beta_t, A)$ in $L$

2.1. $t := t + 1$, $t_{\text{max}} := \max(t, t_{\text{max}})$

IF $t = t_{\text{max}}$ THEN $u_t := u_t + 1$, $\nu_t := 1$, $y_t := 0$
ELSE $u_t := -[y_t] + [\nu_t/2](-1)^{\nu_t}c_t$, $\nu_t := \nu_t + 1$.

3. $s := s + 1$, perform step 2 for all delayed stages $(u_1, \ldots, u_n, y_1, c_1, \nu_1, \beta_1, A)$ of $L$

Delay new stages with $\beta_t < 2^{-s}[[\log \left|\mathbf{b}\right|]]$ and store them in $L$

4. IF $L \neq \emptyset$ THEN GO TO 3 ELSE terminate.

Step 2 that is called in step 3 for a stage $u_i := (u_i, \ldots, u_n, \cdots) \in L$ does not perform any stage $u_i$ with $t'' > t$ because stage $u_{i+1}$ has already been performed by 2.1 immediately after storing $u_i$ in $L$ and no stage $u_i$, $t'' > t + 1$ gets performed before step 3 performed all stages in $L$. Increasing $t$ to go from $u_i$ to $u_{i+1}$ for the same $u_{i+1}, \ldots, u_n$ requires a step 3 performing all stages stored in $L$ including those that get stored in $L$ during step 3.

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 $\|\mathbf{t} - \mathbf{b}\|^2 \leq \frac{1}{4} \sum_{i=1}^{n} r_{i,t}^2$ in polynomial time for an LLL-basis $\mathbf{B} = QR$, $\mathbf{R} = [r_{i,j}]$.

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

Optimal value of $\bar{A}$. If the distance $\|\mathbf{t} - \mathcal{L}\|$ or a close upper bound of it is known then we choose $\bar{A}$ to be that close upper bound. This prunes away many irrelevant stages. At stage $(u_1, \ldots, u_n)$ New Enum searches to extend the current $\mathbf{b} = \sum_{i=1}^{n} u_i \mathbf{b}_i \in \mathcal{L}$ to some $\mathbf{b}' = \sum_{i=1}^{n} u_i \mathbf{b}_i \in \mathcal{L}$ such that $\|\mathbf{t} - \mathbf{b}'\|^2 < \bar{A}$. The expected number of such $\mathbf{b}'$ is for random $\mathbf{t}$:

$\bar{\beta}_t = V_{t-1}^{-1} / \det \mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_{t-1})$ for $\bar{\beta}_t := (\bar{A} - \|\pi(\mathbf{t} - \mathbf{b})\|^2)^{1/2}$.

Previously, stage $(u_1, \ldots, u_n)$ determines $u_\ell$ to yield the next integer minimum of
c_i((\tau_i - u_1, \ldots, \tau_i - u_n)) := ||\pi_i(t - b)||^2 = (\sum_{i=1}^{n}(\tau_i - u_i)) + c_{i+1}(\tau_{i+1} - u_{i+1}, \ldots, \tau_n - u_n).

Given u_{i+1}, \ldots, u_n, ||\pi_i(t - b)||^2 is minimal for u_i = [-\tau_i - \sum_{i=1}^{n}(\tau_i - u_i))r_{i,1}/r_{i,t}].

**New Enum for CVP**

**INPUT** BKZ-basis B = QR ∈ Z^{m×n} of block size 32, R = [r_{i,j}] ∈ R^{n×n}, s = ⌊lg lg t⌋, t = \sum_{i=1}^{n} \tau_i b_i ∈ \text{span}(L), \tau_i, \ldots, \tau_n ∈ Q, ∅ ∈ Q such that ||t - L(B)||^2 < A

**OUTPUT** A sequence of b = \sum_{i=1}^{n} u_i b_i ∈ L(B) such that ||t - b|| decreases to ||t - L||.

1. t := n, L := ∅, y_n := \tau_n, u_n := [y_n], c_{n+1} := 0,
   (c_i = c_i(\tau_i - u_1, \ldots, \tau_i - u_n) always holds for the current t, u_1, \ldots, u_n)
2. WHILE t ≤ n #perform stage (u_1, ..., u_n):
   \[ c_i := c_{i+1} + (u_i - y_i)^2 r_{t,i}^2, \]
   IF \( c_i ≥ A \) THEN GO TO 2.1,
   \[ \bar{y}_i := (\bar{A} - c_i)^{1/2}, \bar{b}_i := \frac{V_{t-1}^{-1} b_i}{(r_{t,1}\cdots r_{t,1}^{-1})}, \]
   IF t = 1 THEN \{ output b := \sum_{i=1}^{n} u_i b_i, \bar{A} := ||t - b||^2, GO TO 2.1 \}
   IF \( \bar{b}_i ≥ 2^{t-t+1}/(\bar{y}_t t) \) THEN \[ t := t - 1, y_i := \tau_i + \sum_{i=1}^{n}(\tau_i - u_i)r_{t,i}/r_{t,i}, \]
   \[ u_i := [y_i], \nu_i := \text{sign}(u_i - y_i), \nu_i := 1, \text{ GO TO 2 } \]
   ELSE store (u_1, ..., u_t, y_{t+1}, c_{t+1}, A) in L,
2.1. t := t + 1, u_i := [y_i] + [u_i/2] c_{i+1}, \nu_i := \nu_i + 1, \nu_i := -\nu_i \]
3. s := s + 1, perform step 2 for all delayed stages (u_1, ..., u_n, ...) of L.
   Delay new stages with \( \bar{b}_i < 2^{t-t+1}/(\bar{y}_t t) \) and store them in L.
4. IF L ≠ ∅ 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 b′ ∈ L(B) with ||b′|| = λ_1. Finding an unproved shortest vector b′ is easier than proving ||b|| = λ_1. New Enum finds an unproved shortest lattice vector b′ in polynomial time under the following conditions and assumptions:

- the given lattice basis B = [b_1, ..., b_n] and the relative density rd(L) of L(B) satisfy
  \[ rd(L) ≤ (\sqrt{2π} ||b||) \]
  i.e., both b_1 and rd(L) are sufficiently small.

**GSA:** The basis B = QR, R = [r_{i,j}]_{i≤j≤n} satisfies \( r_{t,i}/r_{t-i,1} = q \) for 2 ≤ i ≤ n for some q > 0.

**SA:** There is a vector b′ ∈ L(B) such that ||b|| = λ_1 and ||π_i(b)||^2 ≤ \( \frac{n+i+1}{n} \lambda_i^2 \) for t = 1, ..., n.

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

- the vol. heur. is close: \( M_{ij} := ||b_{j+1}|| \cap π_j(L) ≈ \frac{V_{i+1}^{j+1} b_{j+1}}{\text{det} π_j(L)} \) for \( b_{j+1} = \frac{n+i+1}{n} \lambda_i^2 \).

**Remarks.** 1. If GSA holds with q ≥ 1 the basis B satisfies \( ||b|| ≤ \frac{1}{2} \sqrt{3} + 3 \lambda_i \) for all i and \( ||b_1|| = \lambda_1 \). Therefore, q ≤ 1 unless \( ||b_1|| = \lambda_1 \). GSA means that the reduction of the basis is "locally uniform", i.e., the \( t_{i,j}^2 \) form an arithmetic series. It is easier to work with the idealized property that all \( t_{i,j}/t_{i-1,j} \) are equal. In practice \( t_{i,i}/r_{i-1,i} \) slightly increases on 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 B is sufficiently small. GSA has been used in [S03, NS06, GN08, S07, N10] and in the security analysis of NTRU in [H07, HIHW09].

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

\[ \text{Pr}(||π_1(b)||^2 ≤ \frac{n+i+1}{n} \lambda_i^2) \text{ for } t = 1, ..., n \]

for random b′ ∈ span(L) with ||b'|| = λ_1. Lange [La13, Kor. 4.3.2] proves that the prob. 1/n increases to 1 − e^{−d^2} by increasing \( n+i+1 \) of linear pruning to \( \frac{n+i+1}{d/\sqrt{n}} \). Linear pruning means to cut off all stages (u_1, ..., u_n) that satisfy \( ||π_i(\sum_{i=1}^{n} u_i b_i)||^2 > \frac{n+i+1}{d/\sqrt{n}} \lambda_i^2 \). 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_1, ..., 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 \( \#_n := \#(B_i(\zeta_i, q_n) \cap \mathcal{L}) \), and similar for \( \#_i := \#(B_i(\zeta_i, q_i) \cap \pi_{r_n-i+1}(\mathcal{L})) \), are for fixed \( n, q_n \) very close for large radius \( q_n \), but can differ considerably for small \( q_n \) since \( \#_n \) can change a lot with the actual center \( \zeta_i \) of the sphere. For small \( q_n \) the minimum of \( \#_n \) can be very small and then the average value for random center \( \zeta_i \) 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 \( \#_n, \#_i \) its success rate \( \beta_t \) frequently overestimates the success rate for the actual \( \zeta_i \). A cut of the smallest (resp. closest) lattice vector by New Enum in case that it underestimates \( \#_i \) can nearly be excluded if stages are only cut for very small \( \beta_t \).

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

\[
\| \mathbf{b}_t \| / \lambda_1 = \| \mathbf{b}_t \| / (r_d(\mathcal{L}) \sqrt{\det(\mathcal{L})}) = q \frac{\lambda_1}{\sqrt{n}} \sqrt{\det(\mathcal{L})}.
\]

Therefore \( r_d(\mathcal{L}) \sqrt{\det(\mathcal{L})} / \| \mathbf{b}_t \| / \lambda_1 \leq 1 \) implies under GSA that \( \det(\mathcal{L}) \geq 1 \) and \( q \geq 1 \) and thus \( \| \mathbf{b}_t \| = \lambda_1 \). Hence \( r_d(\mathcal{L}) > \frac{\lambda_1}{\sqrt{n}} \sqrt{\det(\mathcal{L})} \) holds under GSA if \( \| \mathbf{b}_t \| > \lambda_1 \).

Our time bounds must be multiplied by the work load per stage, a modest polynomial factor covering the steps performed at stage \((u_1, \ldots, u_n)\) of ENUM before going to a subsequent stage.

**Proposition 1.** Let the basis \( \mathbf{B} = \mathbf{QR}, \mathbf{R} \in \mathbb{R}^{n \times n} \) of \( \mathcal{L} \) satisfy \( r_d(\mathcal{L}) \leq \left( \frac{1}{2} \sqrt{\frac{e}{\pi n}} \right)^{\frac{1}{2}} \) and GSA 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.** For simplicity we assume that \( \lambda_1 \) is known. Pruning all stages \((u_1, \ldots, u_n)\) that satisfy \( \| \pi_t(\sum_{i=1}^n u_i b_i) \| > \sqrt{n} \mathbf{q}^\frac{1}{2} \sqrt{\det(\mathcal{L})} \) does not cut off any shortest lattice vector \( \mathbf{b}' \) that satisfies SA. The volume heuristics approximates the number \( \mathcal{M}_t^q \) of performed stages \((u_1, \ldots, u_n)\) to

\[
\mathcal{M}_t^q := \# B_{n-t+1}(0, q_t) \cap \pi_t(\mathcal{L}) \approx \left( \frac{n-t+1}{n} \lambda_1 \right)^{n-t+1} \frac{1}{(n-t+1)} \frac{\sqrt{n}}{\sqrt{n}} \frac{V_{n-t+1}}{q^t \cdots r_{n,n}} \frac{t}{t+1}.
\]

For \( t = 1 \) this yields \( \frac{q^t}{n} - \frac{1}{n} = \delta(\mathcal{L}) / n = \lambda_1 / (r_1, 1) \sqrt{\det(\mathcal{L})} \). Combining (4.1) with this equation and \( \gamma_n < \frac{1}{n} \) which holds for \( n > n_0 \), we get

\[
\mathcal{M}_t^q \lesssim \left( \frac{\lambda_1}{r_1, 1} \sqrt{\frac{e}{\pi n}} \right)^{n-t+1} \frac{q^t}{n} \frac{1}{\sqrt{n}}
\]

Evaluating this upper bound for \( r_d(\mathcal{L}) \leq \left( \frac{\lambda_1}{r_1, 1} \sqrt{\frac{e}{\pi n}} \right)^{\frac{1}{2}} \) yields

\[
\mathcal{M}_t^q \lesssim \left( \frac{\lambda_1}{r_1, 1} \sqrt{\frac{e}{\pi n}} \right)^{n-t+1} \frac{q^t}{n} \frac{1}{\sqrt{n}} \frac{1}{\sqrt{n}} \frac{1}{\sqrt{n}}
\]

This approximate upper bound has for \( t \leq n \) its maximum 1 at \( t = n \). This proves Prop. 1. \( \square \)

**Extension of Prop. 1 to GSA_{m,q}-bases.** i.e. lattice bases that satisfy for some \( m, 1 \leq m \leq n \):

\[
r_{1,i}/r_{1,i-1} = \begin{cases} q & \text{for } i \leq m \leq m, \\ 1 & \text{for } i > m \end{cases}, \quad r_{1,i}/r_{2} = \begin{cases} q^{i-1} & \text{for } i \leq m \\ q^{m-i} & \text{for } i > m \end{cases}
\]

This increases \( r_{i,i}/r_{i-1,i-1} \) of GSA for \( i \geq m \); 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 GSA_{m,q}-basis, \( r_d(\mathcal{L}(\mathbf{B})) \leq \frac{1}{\sqrt{m}} \left( \frac{\lambda_1}{r_1, 1} \sqrt{\frac{e}{\pi n}} \right)^{\frac{m}{n}} \) 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.
Proposition 3. 
Proof. We modify the proof of Prop. 1 and concentrate on \( t \geq m \) since \( \mathcal{M}_t^\rho \) has its maximum for \( t \geq m \). Then we have for \( t \geq m \)
\[
\left( r_{t-1} \cdots r_{n-1} \right) / r_{t-1}^{m-1} = q^{(n-t+1) 2^m - 1}
\]
\[
(\det L)^{1/n} / r_{t-1} = q^{\sum_{i=1}^{m-1} i-1/n + m-1/n - m/n} = \frac{2^m}{r_{t-1} \sqrt{\pi n} rd(L)}
\]
where \( \sum_{i=1}^{m-1} i/n + m-1/n - m/n = \frac{(m+1)m}{4n} - m - \frac{1}{2}(1 - \frac{m}{2}) = \frac{m-1}{2}(1 - \frac{m}{2n}) \). Hence
\[
\mathcal{M}_t^\rho \approx \left( \frac{2^m}{r_{t-1} \sqrt{\pi n}} \right)^{n-t+1} / q^{(n-t+1) m-1/n} = \left( \frac{2^m}{r_{t-1} \sqrt{\pi n}} \right)^{n-t+1} \left( \frac{2}{r_{t-1} \sqrt{\pi n}} \right) \frac{1}{\sqrt{n} rd(L)}
\]
Evaluating \( \frac{2}{r_{t-1} \sqrt{\pi n}} \sqrt{n} rd(L) \) for \( rd(L) \leq \frac{1}{2} \left( \frac{2^m}{r_{t-1} \sqrt{\pi n}} \right)^{m/n} \) and \( \gamma_n \leq \frac{n}{2} \), we get
\[
\mathcal{M}_t^\rho \approx \left( \frac{2}{r_{t-1} \sqrt{\pi n}} \right)^{(1-1/n)(1-1/n)} {n-1} = \left( \frac{2}{r_{t-1} \sqrt{\pi n}} \right)^0 = 1
\]
In particular \( \mathcal{M}_t^\rho \approx 1 \) holds for all \( t \geq m \) if \( rd(L) \leq \frac{1}{2} \left( \frac{2}{r_{t-1} \sqrt{\pi n}} \right)^{m/n} \) and \( \gamma_n \leq \frac{n}{2} \).

Prop. 2 handles the case that \( r_{i,i} \) decreases uniformly for \( i \leq m \) with an abrupt stop at \( i = m \). Prop. 3 assumes a lattice basis of dimension \( n \) that satisfies for some \( 0 < q < 1 \) that
\[
r_{i+1,i+1} = q^{-1/n} i \] for \( i = 1, \ldots, n-1 \) (4.3)
Hence \( r_{i,j} / r_{t-1} = q^{-1/n} \sum_{i=1}^{j-1} 1/n \) 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 \( \mathbf{B} = \mathbf{QR} R \in \mathbb{R}^{n \times n} \) be a basis of lattice \( L \) satisfying (4.3), \( n > 4\pi \frac{1}{n} \) and \( rd(L) \leq \left( \frac{2}{r_{t-1} \sqrt{\pi n}} \right)^{1/2} \) and let \( L \) have a shortest lattice vector \( \mathbf{b'} \) that satisfies \( \text{SA} \). Then \( \text{ENUM} \) with linear pruning finds such \( \mathbf{b'} \) under the volume heuristics in polynomial time.

Proof. Defining the proofs of Prop. 1, 2 we have \( \frac{r_{j,j} \cdots r_{n,n}}{r_{t-1}^{m-1}} = q^{\sum_{j=1}^{n} j-1/n} \), where
\[
\sum_{j=1}^{n} j-1/n = \sum_{j=1}^{n} j - 1 - \frac{(j-1)j}{2n} = \frac{n^2(n+1)}{2} - \frac{n(n+1)(2n+1)}{12n}
\]
Hence
\[
\left( \frac{2}{r_{t-1} \sqrt{\pi n} rd(L)} \right)^n = \det L / r_{t-1}^{m/n} = q^{n^2/n + O(n)}
\]
This bounds the number \( \mathcal{M}_t^\rho \) of performed stages \( (u_t, \ldots, u_n) \) under linear pruning to
\[
\mathcal{M}_t^\rho \approx \left( \frac{2}{r_{t-1} \sqrt{\pi n}} \right)^{n-t+1} / \left( r_{t-1} \cdots r_{n,n} \right) = \left( \frac{2}{r_{t-1} \sqrt{\pi n}} \right)^{n-t+1} q^{-n^2/3 - \frac{t^2(t-3n)}{6}} \]
\[
= \left( \frac{2}{r_{t-1} \sqrt{\pi n}} \right)^{n-t+1} \left[ \left( \det(L) / r_{t-1} \right) \right]^{1/n} - n^2/3 - \frac{t^2(t-3n)}{6} \]
\[
= \left( \frac{2}{r_{t-1} \sqrt{\pi n}} \right)^{n-t+1} \left[ \left( 1 - \right) \right]^{1/n} + \frac{t^2(t-3n)}{6} + O(1)
\]
(4.2)
We get for \( rd(L) \leq \left( \frac{2}{r_{t-1} \sqrt{\pi n}} \right)^{1/2} \) and \( \gamma_n < \frac{n}{2} \) that \( r_{i,i} \sqrt{\pi n} rd(L) / \lambda_1 \leq \left( \frac{2}{r_{t-1} \sqrt{\pi n}} \right)^{1/2} \) and thus
\[
\mathcal{M}_t^\rho \approx \left( \frac{2}{r_{t-1} \sqrt{\pi n}} \right)^{n-t+1} \left( r_{i,i} \sqrt{\pi n} rd(L) / \lambda_1 \right)^{1/2} \]
For \( n > 2\pi \) this upper bound \( \mathcal{H}_t \) of \( \mathcal{M}_t^\rho \) is monotonous decreasing in \( t \leq n \). This holds because the exponent of \( \left( \frac{2}{r_{t-1} \sqrt{\pi n}} \right)^{1/2} \) is monotonous increasing in \( t \) and \( \frac{2}{r_{t-1} \sqrt{\pi n}} < 1 \). Hence for \( n > 4\pi \)
\[
\mathcal{M}_t^\rho \approx \left( \frac{2}{r_{t-1} \sqrt{\pi n}} \right)^{n/2 + O(1/n)} 2^{n/2} = o(1).
\]
In practice all relevant bases satisfy some slightly modified version of \( \text{GSA} \). The main problem for the fast \( \text{SVP} \) algorithms for them is to find a sufficiently short \( \mathbf{b}_1 \in L \). 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 \( \text{NEW ENUM} \) with pruning and arranged to enumerate smallest vectors first.

The \( \gamma \)-unique \( \text{SVP} \) is to solve \( \text{SVP} \) for a lattice \( L \) of dim. \( n \) where all vectors \( \mathbf{b} \in L \) of length \( 0 < ||\mathbf{b}|| < \gamma \lambda_1 \) are parallel to each other. Minkowski's second theorem shows for such \( L \) with successive minima \( \lambda_1, \ldots, \lambda_n \) that
\[
\lambda_2 \gamma^{-n} < \lambda_1 \cdots \lambda_n \leq \gamma_n^{n/2} \det L \] and thus
\[ \lambda_k^2 < \gamma^{-2+2/n} \gamma_n (\det L)^{2/n} \text{ hence } \quad r_d(L) < \gamma^{-1+1/n}. \]

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

1. \( a = 1.5, k = 24, \gamma_{24} = 4 \) for all \( n \leq 245 \)
2. \( a = 1, k = 24, \gamma_{24} = 4 \) for all \( n \leq 140 \)

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

SVP-time bound for \( rd(L) \leq 1 \) under linear pruning. (4.2) proves for \( r_d(L) \leq 1 \) that

\[ M_r^o \lesssim \left( \frac{\sqrt{2\pi} \cdot \lambda_{1/n}}{\pi} \right)^{n - \frac{(t-1)(t-2)}{2} + n + t - 1} 2 \cdot \frac{n + t + 1}{n}. \]

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

\[ n^{O(1)} \left( \frac{\sqrt{2\pi} \cdot \lambda_{1/n}}{\pi} \right)^{\frac{n^2}{2}} 2^{n^4} = n^{\frac{n}{8} + o(n)}. \]

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

**Theorem 1.** Given a lattice basis \( \mathbf{B} \in \mathbb{Z}^{m \times n} \) satisfying GSA and \( \|\mathbf{b}_1\| \leq \sqrt{\pi} n^{h_1} \lambda_1 \) for some \( b \geq 0 \), New ENUM solves SVP and proves to have found a solution in time \( 2^{O(n)}(n^{\frac{n}{8} + rd(L)}))^{\frac{n}{8} + o(n)}. \)

Theorem 1 is proven in [S10], it does not assume \( \text{SA} \) and the vol. heuristic. Recall from remark 4 that \( n^{\frac{n}{8} + \nu rd(L)} \geq 1 \) holds under GSA. For \( b = o(1) \) Thm. 1 shows the SVP-time bound \( n^{\frac{n}{8} + o(n)} \) which beats \( n^{\frac{n}{8} + o(n)} \) from HANROT, STEIGLE [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 \( n^{\frac{n}{8} + o(n)} \) for solving CVP by KANNAN’S CVP-algorithm [Ka87]. Minimizing \( \|\mathbf{b}\| \) for \( \mathbf{b} \in L \setminus \{0\} \) and minimizing \( \|\mathbf{t} - \mathbf{b}\| \) for \( \mathbf{b} \in L \) require nearly the same work if \( \|\mathbf{t} - L\| \approx \lambda_1 \). In fact the proof of Theorem 1 yields:

**Corollary 1.** [S10] Given a basis \( \mathbf{B} = [\mathbf{b}_1, \ldots, \mathbf{b}_n] \) satisfying GSA, \( \|\mathbf{b}_1\| \leq \sqrt{\pi} n^{h_1} \lambda_1 \) with \( b \geq 0 \) and \( \mathbf{t} \in \text{span}(L) \) with \( \|\mathbf{t} - L\| \leq \lambda_1 \), New ENUM solves this CVP in time \( 2^{O(n)}(n^{\frac{n}{8} + rd(L)}))^{\frac{n}{8}}. \)

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

**CA:** \[ \|\pi_t(\mathbf{t} - \mathbf{b})\|^2 \lesssim \frac{n+1}{n} \|\mathbf{t} - L\|^2 \text{ holds for } t = 1, \ldots, n \text{ and some } \mathbf{b} \in L \text{ closest to } \mathbf{t}. \]

CA translates the assumption \( \text{SA} \) from SVP to CVP. CA holds with probability \( 1/n \) for random \( \mathbf{b} \in \text{span}(L) \) such that \( \|\mathbf{t} - \mathbf{b}\| = \|\mathbf{t} - L\| \) [GRN10]. 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 \( \|\pi_t(\mathbf{t} - \mathbf{b})\|^2 \lesssim \frac{n+1}{n} \|\mathbf{t} - L\|^2 (1 + 1/\sqrt{\pi}) \) for \( t = 1, \ldots, n \).

**Corollary 2.** [S10] Given a basis \( \mathbf{B} = [\mathbf{b}_1, \ldots, \mathbf{b}_n] \in \mathbb{Z}^{m \times n} \) of \( L \) that satisfies GSA, \( \|\mathbf{b}_1\| = O(\lambda_1) \) and \( rd(L) \leq \left( \frac{1}{\sqrt{2\pi}} \right)^{\frac{n}{8}} \). Let some lattice vector \( \mathbf{b} \) that is closest to the target vector \( \mathbf{t} \) satisfy CA then NEW ENUM finds for random \( \mathbf{t} \) in average time \( n^{O(1)} t_{E_b}(\|\mathbf{t} - L\|/\lambda_1)^n). \)
Cor. 2 eliminates the volume heuristics for a random target vector $t$. Prop. 1 translates into

**Corollary 3.** Let a basis $B = [b_1, ..., b_n] \in \mathbb{Z}^{n \times n}$ of $\mathcal{L}$ be given satisfying GSA, $\|b_i\| = O(\lambda_1)$ and $\text{rd}(\mathcal{L}) \leq (\frac{1}{\|b_1\|} \sqrt{2\pi})^{\frac{1}{2}}$. Let some $b \in \mathcal{L}$ closest to the target vector $t$ satisfy CA and let $\|t - \mathcal{L}\| \lesssim \lambda_1$ then ENUM with linear pruning for CVP finds $b$ 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" $\prod_{i \geq 1} \lambda_i$ for $\lambda_i = \|b_i^*\|/(\text{det} \mathcal{L})^{1/n}$ 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 pairs of $p_n$-smooth integers $u, |u - v N|$. We call such $(u, v)$ a fac-relation.

**The classical factoring method.** Given $n + 1$ fac-relations $(u_j, v_j)$ we have for $p_0 := -1$

$$u_j = \prod_{i \geq 1} p_i^{e_{i,j}}, \quad u_j - v_j = \prod_{i \geq 0} p_i^{e_{i,j}} \quad \text{with} \quad e_{i,j}, e_{i,j}' \in \mathbb{N}. \quad (5.1)$$

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

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

solves $X^2 = 1 \mod N$ by $X = \sum_{i = 0}^{n} p_i^{e_{i,j} - e_{i,j}'} \mod N$. In case that $X \neq \pm 1 \mod N$ this yields two non-trivial factors gcd($X \pm 1, N$) $\not\in \{1, N\}$ 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 $u, |u - v N|$. This factoring method goes back to Morrison & Brillhart [MB75] and let to the first factoring algorithm in subexponential time by J. Dixon [D81].

We construct $p_n$-smooth triples $u, v, |u - v N|$ from CVP solutions for the prime number lattice $\mathcal{L}(B_{n, \varepsilon})$ with basis $B_{n, \varepsilon} = [b_1, ..., b_n] \in \mathbb{R}^{(n+1) \times n}$ and target vector $N_0 = \mathbb{R}^{n+1}$ for some $\varepsilon > 0$:

$$B_{n, \varepsilon} = \begin{bmatrix} \sqrt{\ln p_1} & 0 & 0 & \cdots & 0 \\ 0 & \sqrt{\ln p_2} & \sqrt{\ln p_3} & \cdots & \sqrt{\ln p_n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \sqrt{\ln p_n} \end{bmatrix}, \quad N_0 = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ \sqrt{N \ln N} \end{bmatrix}, \quad (5.3)$$

$$\left(\text{det} \mathcal{L}(B_{n, \varepsilon})\right)^{2/n} = \left(\prod_{i = 1}^{n} \ln p_i\right) \left(1 + N^{2c} \sum_{i = 1}^{n} \ln p_i\right),$$

$$\left(\text{det} \mathcal{L}(B_{n, \varepsilon})\right)^{2/n} = \ln p_n \cdot N^{2c/n} \cdot (1 \pm o(1))$$

$$\text{det} \mathcal{L}(B_{n, \varepsilon}, N_0) \approx \ln p_n^{n^n / N^{2n}} \ln N$$

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

$$u = \prod_{i \geq 1} p_i^{e_i}, \quad v = \prod_{i \geq 0} p_i^{e_i} \in \mathbb{N} \quad \text{denoting} \quad \mathbf{b} \sim (u, v).$$

Clearly $uv$ is square-free if and only if $e_1, ..., e_n \in \{0, \pm 1\}$. Let $\hat{z}_b := N^{c} \ln \frac{1}{p}, \hat{z}_{b, N_0} := N^{c} \ln \frac{1}{p N}$ denote the last coordinates of $\mathbf{b}$ and $\mathbf{b} - N_0$. As a factor $p_i^{e_i}$ of $uv$ contributes $e_i \ln p_i$ to $\ln u$ and $e_i' \ln p_i$ to $\|\mathbf{b}\|^2$ we have $\|\mathbf{b}\|^2 \geq \ln uv + \hat{z}_b^2$ with equality if and only if $uv$ is square-free. Similarly

**Fact 1.** $\|\mathbf{b} - N_0\|^2 \geq \ln uv + \hat{z}_{b, N_0}^2$ holds for $(u, v) \sim \mathbf{b} \in \mathcal{L}(B_{n, \varepsilon})$ with equality iff $uv$ is square-free. Hence $\|\mathcal{L}(B_{n, \varepsilon}) - N_0\|^2$ is close to $\ln uv + \hat{z}_{b, N_0}^2$ if $uv$ is nearly square-free.

**Lemma 1.** Let $(u, v) \sim \mathbf{b} \in \mathcal{L}(B_{n, \varepsilon})$ satisfy $\frac{1}{2} N^3 \leq v \leq N^3$, and $|u - v N| = o(v N)$. Then

1. $\|\mathbf{b} - N_0\|^2 \geq (2\delta + 1 - o(1)) \ln N + \hat{z}_{b, N_0}^2$.
2. $|\hat{z}_{b, N_0}| = N^{c} \ln \frac{|u - v N|}{p N} (1 \pm o(1))$. 

9
Proof. Clearly $0 \leq \delta \ln N - \ln v \leq \ln 2$ and thus for $n, N \to \infty$ we have $\ln v = \delta \ln N (1 - o(1))$, $\ln u = \ln(\ln N)(1 - o(1))$ and $\ln u v = (2\delta - o(1)) \ln N$. Then 1 follows from Fact 1 and this upper bound if $w$ is nearly square-free. Moreover $\ln(1 + \frac{u v \ln N}{\ln u v N}) = \frac{u v \ln N}{\ln u v N} (1 \pm o(1))$ holds due to $|u - v N| = o(v N)$ and thus $|\Delta_{n, v N}| = N^{\frac{\ln u v N}{\ln N} (1 \pm o(1))}$ which proves 2. □

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. $\lambda_1^2 > 2c \ln N + 1 - \frac{1}{2} N^{-\epsilon} + \Theta(N^{-2\epsilon})$ holds for the lattice $L(B_{n, c})$ for $N^e \geq 10^3$.

Proof. Let $b = B_{n, c} u \neq 0$ be a shortest vector of $L(B_{n, c})$, corresponding to $(u, v)$. Let $u > v$, otherwise change $u$ into $-u$. Then $\ln \frac{z}{v}$ minimizes for some $u \geq v + 1$. Hence

$$
\ln \frac{z}{v} \geq \ln(1 + 1/v) > \ln(1 + 1/\sqrt{uv}) \\
\geq \ln(1 + 1/v) > \ln(1 + 1/\sqrt{uv}) > v
$$

Hence $\lambda_2^2 > \ln uv + N^{2\epsilon} \ln^2(\frac{z}{v}) \geq \ln uv + N^{2\epsilon} \frac{1}{v}(1 - \frac{1}{2\sqrt{uv}})^2 =: f(\sqrt{uv})^2$ where $N^{\ln \frac{z}{v}} = \lambda_h$ is the last coordinate of $b$. We abbreviate $h := \sqrt{uv}$. The derivative $\frac{df(\lambda)}{d\lambda}(\lambda) = h^{-9}[2h^4 + N^{2\epsilon}(-2h^2 + 3h - 1)]$ is zero for some $h$ with $N - 0.751 < h < N^e - 0.75$ and this $h$ determines the minimal value $f(\lambda)$ of $f$. Then the Lemma follows from

$$
f(N^e - \epsilon) = \ln(N^e - \epsilon)^2 + \frac{N^{2\epsilon}}{(N^e - \epsilon)^2}(1 - \frac{1}{2(N^e - \epsilon)})
$$

If $p_m$-smooth $u, v$ exist such that $u = v + 1$, we are square-free, $u = O(N)$ then $\lambda_2^2 > 2c \ln N + O(1)$. Otherwise $\lambda_1^2$ increases by the minimum of $\lambda_2^2 > N^{2\epsilon} \ln^2(\frac{z}{v})$ for $p_m$-smooth $v < u$ of order $u = O(N^e)$. Let $\Psi(X, y)$ denote the number of integers in $[1, X]$ that are $y$-smooth. DICKMAN [1930] shows

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

(5.4)

$\rho(\epsilon)$ is the Dickman $\rho$-function, see [G08] for a recent survy. It is known that $\rho(\epsilon) = 1$ for $0 \leq \epsilon \leq 1$, $\rho(\epsilon) = 1 - \ln z$ for $1 \leq \epsilon \leq 2$

(5.5)

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

$$
\Psi(y^e, y)^{-\epsilon} = \rho(\epsilon)(1 + O(\frac{\ln(+1)}{\ln y}))
$$

(5.6)

holds uniformly for $1 \leq y \leq y^{1/2-\epsilon}$, $y \geq 2$ if and only if the Riemann Hypothesis is true.

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

$$
\Phi(N, p_n, \sigma) = \Theta(2p_n^\sigma \rho(\frac{\ln(N p_n^\sigma)}{\ln p_n^\sigma})^2(\sigma))
$$

(5.7)

uniformly holds for $\frac{\ln N}{\ln p_n} + \sigma \leq p_n^{1/2-\epsilon}$ if the $p_n$-smoothness events of $u, v, |u - v N|$ are nearly statistically independent. We will use (5.7) in a range where $\frac{\ln N}{\ln p_n} + \sigma < p_n^{1/4}$ and we will neglect the $\Theta(1)$-factor of (5.7).

Proof of (5.7). There are $2p_n^\sigma$ pairs of integers $u, v$ such that $0 < u, v < u - v N \leq p_n^\sigma$. Clearly $u \leq N p_n^\sigma \leq p_n^\sigma$ holds for $z = \frac{\ln(N p_n^\sigma)}{\ln p_n^\sigma} + \sigma$. Then (5.6) for $y = p_n^\sigma = (N + 1)p_n^\sigma$ shows that the fraction of $u$ that are $p_n$-smooth is $\rho(z)(1 + O(\frac{\ln(+1)}{\ln y}))$ if $\frac{\ln N}{\ln p_n} + \sigma \leq p_n^{0.4}$. Moreover (5.6) for $y = p_n^\sigma \leq p_n^\sigma$ shows that the fraction of $0 < u < p_n^\sigma$ that are $p_n$-smooth is $\rho(\sigma)(1 + O(\frac{\ln(+1)}{\ln y}))$ if $\sigma \leq p_n^{0.4}$. Therefore the statistical independence of the $p_n$-smoothness events of $u, v, |u - v N|$ implies (5.7) if $\ln(z + 1) = O(\ln p_n)$ holds for both $\rho$-values. The latter holds due to $\frac{\ln N}{\ln p_n} + \sigma \leq p_n^{0.4}$.

Example factoring. Let $N = 1000000980001501 \approx 10^{14}$ and $n = 90, p_{90} = 463, c = 1/2$. (5.7) shows that there are $\Theta(6.4 \cdot 10^7)$ fac-relations such that $v, |u - v N| \leq 463^3$ 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 $\beta_i \geq 2^{-14}$. 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 $[B_{n,c}, N_{c}]$ that are multiples of $N^c$. However the average time for constructing a fac-relation decreased from 6.5 to 6.08 seconds.

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

LOOP. In each round the vectors of the reduced basis of $L(B_{n,c})$ and the shifted $N_{c}$ are randomly scaled as follows. For $i = 1, \ldots, n$ with probability 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 $N_{c}$. New Enum always decreases $\tilde{A}$ to the square distance to $N_{c}$ of the closest found lattice vector. Whenever a fac-relation has been found New Enum stops further decreasing $\tilde{A}$ for this round and continues to enumerate all $b \in L(B_{n,c})$ such that $\|b - N_{c}\|^2 \leq \tilde{A}$. Random scalings per round let each round produce fac-relations 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 $v, |u - vN| \leq p_{30}^2$.

| Round | $u$ | $v$ | $|u - vN|$ |
|-------|-----|-----|------------|
| 6     | 19 · 29² · 31 · 73 · 109 · 139 · 211 · 359 | 415 | 2² · 11 · 37 · 439 |
| 6     | 29 · 37 · 83 · 139 · 191 · 269 · 307 · 443 | 865 | 2 · 11 · 239 · 383 |
| 12    | 2 · 3 · 17² · 103 · 263 · 317 · 379 · 443 | 25  | 13 · 173 |
| 14    | 2 · 5 · 47 · 83 · 157 · 179 · 307 · 331 · 421 | 469 | 19 · 43 · 373 |
| 19    | 7² · 13 · 41 · 43 · 107 · 109 · 113 · 131 · 409 · 461 | 365571 | 2⁴ · 5 · 11² · 197 · 433 |
| 19    | 2 · 7 · 13 · 31 · 107 · 127 · 149 · 179 · 383 · 397 · 439 | 1364927 | 3 · 5 · 11 · 61 · 337 · 419 |
| 21    | 43 · 131 · 193 · 307 · 353 · 401 · 439 | 28829 | 2 · 3² · 5² · 13 · 41 · 107 |
| 30    | 19 · 31 · 53 · 61 · 67 · 131 · 163 · 241 · 313 | 2055 | 2² · 59 · 71 · 89 |
| 31    | 13² · 17 · 101 · 137 · 199 · 229 · 277 · 331 | 1661 | 2⁶ · 3 · 19 · 233 |
| 33    | 19 · 101 · 107 · 127 · 131 · 179 · 191 · 211 · 379 | 93398 | 3³ · 13 · 29 · 109 · 167 |

A. Schickedarz improved in 2015 Charlet’s program and found for $N = 1000000890015001 \approx 10^{134}$, $n = 90, p_{90} = 463, c = 1/2$ and pruned to stages with $\beta_i \geq 2^{-14}$ 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 $L(B_{n,c})$ 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 $\tilde{A}$ has been decreased. But for $N \approx 10^{20}$ this program took for $n = 150, c = 1/2$ about 34.5 seconds per fac-relation and factored $N$ in 86 minutes.

Alternatively we can find more fac-relations in fewer scaling rounds by decreasing $\tilde{A}$ only to $\|b - N_{c}\|^2(1 + \epsilon)$ for the closest found $b \in L(B_{n,c})$. This larger final $\tilde{A}$ increases all final success rates $\beta_i$ and extends the final enumeration of $b$ with $\|b - N_{c}\|^2 \leq \tilde{A}$. We should experimentally choose $\epsilon$ to maximize the number of fac-relations 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 fac-relations to large $v$. This is necessary for factoring $N \gg 10^{14}$ because $\psi(N, n, \sigma)$ gets small for $\sigma = 3$. Let $\psi_{N,n,\delta}$ 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 $|u - vN| \leq p_n^2$ and $\frac{1}{2}N^\delta < v \leq N^\delta$. Neglecting for large $y = p_n$ the $O(\frac{\ln(y+x+1)}{\ln y})$-term of (5.6), the number of $p_n$-smooth $v \in [\frac{1}{2}N^\delta, N^\delta]$ is $\psi(N^\delta, p_n) - \psi(N^\delta/2, p_n) \approx N^\delta (\rho(z_v) - \frac{1}{2} \rho(z_v'))$ for $z_v = \frac{\ln N}{\ln p_n}, z_v' = z_v - \frac{\ln z_v}{\ln p_n}$. 

11
Hence random \( v \in R \left[ \frac{1}{2}N^4, N^4 \right] \) are \( p_n \)-smooth with probability close to \( 2(\rho(z_n) - \frac{1}{2}\rho(z_n')) \). For the number of \( p_n \)-smooth \( u \in \left[ \frac{1}{2}N^{1+\delta}, N^{1+\delta} \right] \) we replace \( \delta > 1 + \delta \), \( z_n = \frac{(1+\delta)\ln N}{\ln p_n} \); \( z_n = z_n - \frac{\ln 2}{\ln p_n} \).

Then random \( u \in R \left[ \frac{1}{2}N^{1+\delta}, N^{1+\delta} \right] \) are \( p_n \)-smooth with probability close to \( 2(\rho(z_n) - \frac{1}{2}\rho(z_n')) \).

Let \#N,\( n, \delta \) denote the number of \( p_n \)-smooth triplets \((u, v, u - vN)\) with \( u \in \left[ \frac{1}{2}N^{1+\delta}, N^{1+\delta} \right] \), \( v \in \left[ \frac{1}{2}N^{\delta}, N^{\delta} \right] \) and \( |u - vN| \leq p_n \). We get

\[
\#N, n, \delta \approx 4N^{\delta}p_n^{\delta} \rho(3) \left( \rho(z_n) - \frac{1}{2}\rho(z_n') \right) \left( \rho(z_n) - \frac{1}{2}\rho(z_n') \right)
\]

assuming that for random \( u, v, \frac{1}{2}N^{\delta} \leq v \leq N^{\delta} \) and \( u \in \left[ \frac{1}{2}N^{1+\delta}, N^{1+\delta} \right] \) such that \( |u - vN| \leq p_n \) the \( p_n \)-smoothness events for \( u, v \) and \( |u - vN| \leq p_n \) are nearly statistically independent. We compute the \( \rho(z) \) values for integers \( z = 2, ..., 200 \) via [Sage] and interpolate \( \rho(z) \approx \rho([z]) \approx \rho([z]/\rho([z])) \).

**Corollary 4.** Let \( c = \delta + 1 - \frac{3\ln p_n}{\ln N} \) \( p_n = N^{o(1)} \) and let \( ||b - N||^2 \approx (||C(B_{n,c}) - N||^2)^2 \) for a nearly square-free \((u, v) \sim b \in \mathcal{L}(B_{n,c}) \) such that \( \frac{1}{2}N^{\delta} \leq v \leq N^{\delta} \) and \( |u - vN| \leq p_n \). Then \( \|b - N\|^2 \lesssim \lambda_1^2(L) - \ln N \).

**Proof.** As \((u, v) \sim b \) is nearly square-free the bound on \( \|b - N\|^2 \) of Lemma 1 is sharp and thus

\[
\|b - N\|^2 \lesssim (2\delta + 1 + o(1))\ln N + \delta^2 \ln N - C - N
\]

\[
\lesssim (2\delta + 1 + o(1))\ln N + N^{2(\delta-1)-\delta}|u - vN|^2(1 + o(1))
\]

\[
\lesssim (2\delta + 1 + o(1))\ln N + 1 < \lambda_1^2(L) - \ln N + o(1),
\]

the latter because \( |u - vN| \leq p_n \), \( N^{2(\delta-1)-\delta} \leq p_n^6 \) and \( \lambda_1^2(L) > 2c\ln N + 1 - o(1) \geq (2\delta + 2)\ln N + 1 - o(1) \) holds by Lemma 2.

**Consequences.** Cor. 4 shows for \( c = \delta + 1 - \ln p_n^6/\ln N \) that we can enumerate the square-free \((u, v) \) of \( b \in REL(N, \delta) \) by approximate CVP-solutions minimizing \( ||C(B_{n,c}) - N|| \) or by approximate SVP-solutions of \( \mathcal{L}' := \mathcal{L}(B_{n,c}, N) \). Also SVP-solutions for \( \mathcal{L}' \) most likely provides a relation (5.1), possibly with \( N \) of \( N^c \) of \( N \) replaced by \( N^a \), \( a \in N \), most likely \( a = 1 \). Cor. 4 also holds with \( p_n \) replaced by any \( p_n' \) with \( \rho(\sigma) > 0 \). Note that \( |u - vN| \) smaller than \( p_n \) is \( p_n \)-smooth with probability \( \rho(\sigma) \) and \( \rho(3) \approx 0.0846 \) is reasonably large for practical use. Cor. 4 also shows that Cor. 3 extends

Prop. 1 in case that \( rd(L) \lesssim \left( \frac{1}{|b_n|} \sqrt{\frac{p_n}{\ln 2}} \right)^2 \) to CVP of \( \mathcal{L} = \mathcal{L}(B_{n,c}) \) with target vector \( N_c \).

Cor. 4 shows under reasonable conditions that \( \min_{b \in L} ||b - N||^2 \lesssim \lambda_1^2(L) - \ln N \). So we have \( \lambda_1^2(L) \leq ||b - N||^2 \lesssim \lambda_1^2(L) - \ln N \). Assuming that the upper bound of Lemma 2 is sharp we have \( \lambda_1^2(L) = 2c\ln N + 1 - o(1) \leq (2\delta + 2)\ln N(1 + o(1)) \) for \( c = \delta + 1 - \ln p_n/\ln N \) and \( p_n = N^{o(1)} \) and thus \( \lambda_1^2(L) \leq (2\delta + 1)\ln N(1 + o(1)) \), hence \( rd(L) \leq \left( \frac{2\delta + 1 + \ln N}{\gamma_{n,c}p_n^{1/2}} \right)^2 / N^{\pi/\tau} \) and we calculate upper bounds for \( rd(L) \) values of table 1 from this bound. For \( n \leq 256 \) we use for \( \gamma_{n+1} \) the maximal known values of \( \lambda_1/\det(L)^{1/4} \) for lattices \( L \) of dim. \( n + 1 \), see \( \delta \) of [CS98] and for larger \( n \) the MINKOWSKI, HLAWKA lower bound \( \gamma_{n+1} \geq \frac{n+1}{2\pi^2} \).

<table>
<thead>
<tr>
<th>( N )</th>
<th>( 10^{14} )</th>
<th>( 10^{20} )</th>
<th>( 2^{100} )</th>
<th>( 2^{200} )</th>
<th>( 2^{400} )</th>
<th>( 2^{800} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( n )</td>
<td>( 48 )</td>
<td>100</td>
<td>256</td>
<td>1350</td>
<td>7850</td>
<td>41300</td>
</tr>
<tr>
<td>( p_n )</td>
<td>223</td>
<td>541</td>
<td>1619</td>
<td>11149</td>
<td>80173</td>
<td>496919</td>
</tr>
<tr>
<td>( \delta )</td>
<td>0.35</td>
<td>0.55</td>
<td>0.71</td>
<td>1.2</td>
<td>1.57</td>
<td>2.1</td>
</tr>
<tr>
<td>#N,( n, \delta )</td>
<td>126</td>
<td>215</td>
<td>392</td>
<td>1608</td>
<td>10131</td>
<td>42806</td>
</tr>
<tr>
<td>( c = \delta + 1 - \frac{3\ln p_n}{\ln N} )</td>
<td>0.8468</td>
<td>1.1400</td>
<td>1.3902</td>
<td>1.9983</td>
<td>2.4478</td>
<td>3.029</td>
</tr>
<tr>
<td>( \ln(N^{\delta}/p_n^6) )</td>
<td>-4.9</td>
<td>6.4</td>
<td>27</td>
<td>138</td>
<td>401</td>
<td>1125</td>
</tr>
<tr>
<td>( rd(L) )</td>
<td>0.48</td>
<td>0.574</td>
<td>0.39</td>
<td>0.61</td>
<td>0.42</td>
<td>0.32</td>
</tr>
</tbody>
</table>

Table 1: parameters \( n, p_n, \delta, c = \delta + 1 - \frac{3\ln p_n}{\ln N}, rd(L') \)

\( \delta \) of table 1 nearly maximizes \#N,\( n, \delta \) and \( n \) is nearly minimal such that \#N,\( n, \delta \) clearly surpasses \( n \). Table 1 shows that \( \ln(N^{\delta}/p_n^6) \approx 1 \) for \( N \geq 10^{20} \); also that \( rd(L') \approx n^{-1/4} \) and therefore ENUM with linear pruning unlikely solves SVP for \( \mathcal{L}' := \mathcal{L}(B_{n,c}, N) \) in pol. time, as Prop. 1 does not apply. \( n = 48, 100 \) for \( N \approx 10^{14}, 10^{20} \) yield \#N,\( n, \delta \geq n \) and should beat the choice of \( n = 90, 130 \) for \( N \approx 10^{44}, 10^{50} \) of the given experiments.

Our prime base is much smaller than the prime base for the quadratic sieve which uses for \( N \approx 2^{400} \) that \( p_n \approx c^{1/2}(N^{\ln 3/\ln 2} \approx 1.53 \cdot 10^{12} \approx p_n^{2^{400}} \), see [CP01, section 6.1].

ENUM with linear pruning solves SVP of \( \mathcal{L} \) of dim \( \mathcal{L} = n \) by (4.4) in worst case heuristic time \( n^{1/8+o(1)} \). New ENUM solves SVP much faster. Short vectors are found much faster if available.
stages with large success rate are always performed first and if stages with very small success rate are cut. Our experiments show that New Enum for $N \approx 10^{14}, 10^{20}$ and $n = 90, 150$ finds vectors in $\mathcal{L}(B_{n,c})$ close to $N$ in polynomial time.

Next we study the success rate $\beta_t$ of stages $(u_1, \ldots, u_n)$ that are near the limit of linear pruning $||\pi_t(\sum_{i=1}^n u_i b_i)||^2 \approx \frac{n_{\pi_t} \lambda^2}{2}$. Following the proof of Prop. 1 the volume heuristic is: 

$$V_t - \left(\lambda_1^{-1/2} n\right) = \frac{\gamma}{(\lambda_1^{-1/2} n)^{2/3}} \approx \left(\frac{\lambda_1^{-1}}{\alpha n}\right)^{2/3}./(\gamma t)$$. 

Hence stage $(u_1, \ldots, u_n)$ has the success rate 

$$\beta_t \approx \left(\frac{\lambda_1^{-1}}{\alpha n}\right)^{2/3} / (\gamma t)$$

where $r_1 \cdots r_{n-t-1} = 1$. We denote to $\mathcal{L}(B_{n,c})$ and we due to GSA that 

$$r_{t+1} \cdots r_{n-t-1} = r_t^{-1} q^{-1} \approx (\lambda_1^{-1}(2/3))^{-1/2} / (\gamma t)$$

where $\mathcal{L}(B_{n,c}) \approx N'(n) \sqrt{n} \sqrt{n} / (1 - \alpha(n))$. 

Thus New Enum performs under linear pruning many stages with unreasonable small success rate.

Outline of the CVP-algorithm for $B_{n,c}, N_c$ using New Enum without scaling. Let $B = QR = B_{n,c} \cdot T = [b_1, \ldots, b_n] \in \mathbb{Z}_{(n+1) \times n}$ be a BKZ-basis of $\mathcal{L}(B_{n,c})$, $|\det(T)| = 1$. For $u = (u_1, \ldots, u_n) \in \mathbb{Z}^n$ we denote $u' = (u_1', \ldots, u_n') = Tu$ so that $b = B_{n,c} u' = B u \sim (u; v)$ where $u = \Pi_{u_i = 0} u_i \in \mathbb{H}$. We replace the input $N_c$ by its projection $\tau(N_c) = \sum_{t=1}^\tau b_t \in \text{span}(\mathcal{L}), \tau : \mathbb{R}_{n+1} \to \text{span}(\mathcal{L})$ satisfies $N_c - \tau(N_c) \in \mathcal{L}^t$. Then $\tau(N_c) = d B_{n,c} \cdot 1 = d B_T \cdot t$ holds for $d = \ln(N/N - 2c + \sum_{k=1}^n \ln p_k), t = (1, \ldots, 1) \in \mathbb{Z}^n$.

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

**INPUT** B, R = \{r_{ij}\} \in \mathbb{R}_{(n+1) \times n}, B_{n,c}, c, T, \tau_1, \ldots, \tau_n, A \in \mathbb{Q}$ s.t. $||\mathcal{L} - N|| \approx A, ||\mathcal{L} - N|| \equiv A, s = [\log n].$

**OUTPUT** A sequence of $\mathbb{Z}^n$, $u_i \in \mathbb{Z}$ where $||\mathbb{B} - N||$ decreases to $||\mathcal{L} - N||$. 

1. $t = n, L = \emptyset, y_1 \equiv \tau_n, u_n \equiv [y_n], \hat{c}_{n+1} = 0,$ 

$\hat{u} := (0, \ldots, 0, u_n) \in \mathbb{Z}^n, b := B - \cdot u' \equiv T \cdot u.$

2. **WHILE** $t \leq n$ 

# perform stage $(l, u_1, \ldots, u_n, y_1)$: 

$$||\hat{c}_t || \approx \hat{c}_{t+1} + (u_t - y_l) / 2 t^2,$$

**IF** $\hat{c}_t \geq A$ **THEN** $\text{GO TO 2.1}$ \# this cuts the present stage, 

$$\hat{y}_t := (A - \hat{c}_t) / 2, \hat{y}_t := V_t^{-1} \hat{y}_t^{-1} / (r_1 \cdots r_{n-t-1}),$$

**IF** $t = 1$ **THEN** output $b, A := \hat{c}_t \equiv ||b - \tau(N_c)||^2,$ update all stored $\hat{y}_t, \hat{y}_t$ to the new $\hat{c}_t, \hat{y}_t \to 2^{s-1} [\log s^t]$. 

**IF** $\hat{y}_t < 2^{-1} [\log s^t]$ **THEN** $\text{store the stage and } \hat{y}_t, \hat{y}_t$ in $L$, GO TO 2.1

3. $s := s + 1$, perform all delayed stages $(u_1, u_2, \ldots, u_n, y_1), \hat{c}_t, \hat{y}_t, \hat{A}$ of $L$ on level $s$. 

Delay new stages with $\hat{y}_t < 2^{-1} [\log s^t]$ and store them in $L$.

**4.** **IF** $s < s_{\max}$ **THEN** $s := s + 1, \text{GO TO 3}$ ELSE terminate.

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

$$||\pi_t(\mathbb{B} - \tau(N_c))||^2 \leq \frac{n_{\pi_t} \lambda^2}{2(2 - 1)} \ln N + \frac{2 \ln N}{2(2 - 1)}$$

This clearly holds for $t = n + 1$. If it holds at $t = 1$ then $||\mathbb{B} - \tau(N_c)||$ and $u - v N$ are so small that they can provide a relation (5.1). We denote $\hat{c}_t \equiv \hat{c}_t \tau_1 \cdots \tau_n - u_n \equiv ||\pi_t(\mathbb{B} - \tau(N_c))||^2.$

Recall that $\hat{y}_t := V_t^{-1} \hat{y}_t^{-1} / (r_1 \cdots r_{n-t-1})$ for $\hat{y}_t := (A - \hat{c}_t)^2/2(2 - 1)$ where $A \geq ||\mathcal{L} - \tau(N_c)||^2$. The success rate $\hat{y}_t$ increases as $\hat{c}_t$ decreases. The stored stages with small success rate $\hat{y}_t$ will be done
after all stages with higher success rate $\hat{\beta}_i$. They can be cut off if $\hat{\beta}_i$ is extremely small or if to stages with higher success rate $\hat{\beta}_i$ have been stored and the algorithm runs out of storage space. For the corresponding SVP-algorithm for $\mathcal{L}$ we initially replace $\mathcal{B}_{n,c}$ by $[N,e,\mathcal{B}_{n,c}]$.

Iterative increase of $c$ so that vectors $b \in \mathcal{L}(\mathcal{B}_{n,c})$ close to $N_e$ yield distinct fac-relations.

Cor. 4 shows that $\|b - N_e\|^2 \leq N^2 \ln N$ holds for $c = \delta + 1 - \ln p_n/\ln N$ if $b \sim (u,v)$ and $1/2N^2 \leq v \leq N^2$ and $|u - vN| \leq p_n^2$. Such $b$ are particularly close to $N_e$ and yield a relation (5.1) if $|u - vN| = p_n^2$, which happens with probability $\rho(3)$.

We get distinct fac-relations from $c$ and $c' \geq c + \ln 2/\ln N$. By Lemma 1 the vectors $b \in \mathcal{L}(\mathcal{B}_{n,c})$, $b \sim (u,v)$ that are close to $N_e$ satisfy $|u - vN| = N^c|\ln - N| + o(1)$. So $|u - vN| \leq p_n^2 = N^c(1)$ implies $v \geq N^{-c - 1} - c(1 - o(1))$ for $c > 1$. Therefore both $v$ and $u/N$ increase proportionate to $N^{-c - 1}$. Thus $v$ is $\rho(3)$ close to $N_e$ shows $v \geq N^{-c - 1}$ and $v'$ of $(u',v') \sim b'$ close to $N_e$ satisfies $v' \geq N^{-c - 1} \geq N^{-c - 1}$. Hence $\text{Rel}_{N,n,c}(\text{Rel}_{N,n,c}) \equiv 0$ if $\delta \geq \delta + \ln 2/\ln N$. So we iteratively increase $\delta$ and $c$ to $\delta' := \delta + \ln 2/\ln N$ and $c' := c + \ln 2/\ln N$ per round so that $\delta$ passes the area for which $\#N_{n,c}$ is nearly maximal. Then the $b$ close to $N_e$ yield distinct fac-relations per round. To approximate the time to get about $\alpha$ fac-relations we simply transform a reduced basis of $(\mathcal{L}(\mathcal{B}_{n,c}))$ to a reduced basis of $(\mathcal{L}(\mathcal{B}_{n,c}))$ by multiplying the last coordinates of the $b_i$ of $\mathcal{B}_{n,c}$ and of $N_e$ by $N^{-c - c}$ and we do not adjust the success rate $\hat{\beta}_i$ to small increases of $c$.

By iteratively increasing $c$ we can in table 1 decrease $\dim \mathcal{L}(\mathcal{B}_{n,c}) = 41350$ for $N \approx 2^{8300}$ to $n = 40000$. This decreases $\#X_{n,2.1}$ from 49591 to 717. So we find about 700 relations (5.1) by minimizing $\|\mathcal{L}(\mathcal{B}_{n,c}) - N_e\|$ for $c = 2 - 3 - \ln p_n/\ln N$. Thereafter we iteratively increase $c$ to $c' = c + \ln 2/\ln N$ until we found about 40000 relations (5.1) in $U_{n,c}^1 = \text{Rel}_{N,n,2+i,\ln 2/\ln N}$.

Iteratively increasing $c$ is much better than randomly scaling the basis vectors of $(\mathcal{L}(\mathcal{B}_{n,c}))$ to generate distinct fac-relations per round. For large $N$ only a very small fractions of rounds of random scaling generate fac-relations because random scaling handicaps to many relations (5.1) by increasing their distance to $N_e$.

Improving New Enum by continued fractions (CF). A. Schickedanz [S16] has extended New Enum by continued fractions. Take $b = \sum_{j=1}^n u_jb_j \in \mathcal{L}(\mathcal{B}_{n,c})$ at stage $(1, u_1, ..., u_n)$ and $(u,v) \sim b$, $u = \prod_{j>0} p_j^{u_j}$ and compute the regular CF $b_0^{(N)} = b_0^{(N)}$ of $b := \frac{k}{\ell} = \frac{b_0^{(N)}}{b_0^{(N)}}$ with denominators $t_i \leq p_n$. This starts with $a_0 = [\delta, a_1 = 1/|\delta|$ and iterates $a_{i+1} := 1/(a_i - |\alpha_i|)$ as long as $a_i > |\alpha_i|$. Then $k_0$ is given by $k_1 = |\alpha_0| + a_k - h_{i-1} + h_{i-2}$ and $k_i = |\alpha_i|k_{i-1} + h_{i-2}$ where $(h_{i-1}, k_{i-1}, h_0, k_0) = (1, 0, 1, 1)$ and $h_1 = 1, k_1 = |\alpha_1|$, hence $k_i \geq \prod_{j=0}^i |\alpha_j|$. Each $k_0^{(N)} = \prod_{j=0}^i |\alpha_j|$ is a best approximation under all rational approximations $k_0^{(N)}$ of $|\delta|$ with denominators $|\delta| \leq k_i$. Lagrange has proved that $|||\delta| - \frac{k_i}{\ell_i^{(N)}}| \leq \frac{1}{\ell_i^{(N)}}$.

Lemma 3. $|u_i - v_iN| \leq N/k_{i+1}$ holds for $u_i := uk_i$ and $v_i := \frac{k_i}{\ell_i^{(N)}} |k_i + \text{sign}(\delta)h_i|$, where $|u_i - v_iN|$ yields a relation (5.1) if $k_i$ and $|u_i - v_iN|$ are $p_n$-smooth.

Proof. $|u_i - v_iN| = |(u - \frac{k_i}{\ell_i^{(N)}} N)| k_i - \text{sign}(\delta) h_i|N| = |(\frac{v_i}{\ell_i^{(N)}} - \frac{k_i}{\ell_i^{(N)}})Nk_i| = |\delta - \text{sign}(\delta) \frac{k_i}{\ell_i^{(N)}} Nk_i| \leq \frac{k_i}{\ell_i^{(N)}}$ since $|||\delta| - \frac{k_i}{\ell_i^{(N)}}| \leq \frac{1}{\ell_i^{(N)}}$ 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 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 $\alpha_i = |\alpha_i|$ and $\alpha_i = |\alpha_i|$. 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 $v_i > N^2$.

The first 10 of the 14,000 relations found for $N \approx 10^{14}$ via continued fractions for just one scaling

\begin{align*}
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 \cdot 463 \\
v &= 508169841668914465884296878342775 \\
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
\end{align*}
Let \( \alpha \) denote \( \ln \ln N \in \mathbb{N} \). For large \( N \), \( \alpha \) is \( \approx \ln \ln N \approx N^{1/3} \). Then \( \alpha \) takes on large values for \( N \geq 10^{20} \). Theorem 2 shows that there are exponentially many \( p_{\alpha} \)-smooth \( u, v \) such that \( |u - vN| = 1, \frac{1}{2}N^{\alpha} \leq v \leq N^{\alpha} \). Theorem 3 shows that the number of solutions is \( \#M_{N, n, \delta} \geq N^{\delta} \) for \( \delta > 0 \). Clearly every \( (u, v) \in M_{N, n, \delta} \) yields a relation (5.2) because \( |u - vN| = 1 \) and \( uv \) is \( p_{\alpha} \)-smooth. Theorem 2 shows that \#\( M_{N, n, \delta} \geq N^{\delta} \) is exponential in the bit length \( k \) of \( N \).

**Theorem 2.** Let \( \alpha \geq 1.01 \frac{\ln N}{\ln \ln N} \) and \( 0 < \epsilon < \delta < \alpha \ln \ln N \). Assume the events that \( u, v \) is \( p_{\alpha} \)-smooth are nearly statistically independent for random \( v \), \( \frac{1}{2}N^{\alpha} \leq v \leq N^{\alpha} \) under the equation \( |u - vN| = 1 \), then \#\( M_{N, n, \delta} \geq N^{\delta} \) holds for sufficiently large \( N \).
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 $\lambda_2^2 = 2c\ln N (1 + o(1))$ and $rd(\mathcal{L}) = o(n^{-1/4})$. If a reduced version of the basis $B_{n,c}$ is given that satisfies GSA and $\|b\|^2 = O(2c \ln N)$ and if some vector $\tilde{b} \in \mathcal{L}(B_{n,c})$ closest to $N_c$ of (5.3) satisfies CA then New Enum finds $\tilde{b}$ 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 $n^{O(1)}(R_{\xi}/\lambda)^n$ where $R_{\xi} = \max_{w \in \text{span}(\mathcal{L})} |\mathcal{L} - u|$ is the covering radius of $\mathcal{L}$. The factor $(R_{\xi}/\lambda)^n$ overestimates New Enum’s running time since New Enum essentially enumerates only lattice points in a ball of radius $\|\mathcal{L} - N_c\| < \lambda_1 < R_{\xi}$.

Proof. We first prove that $\lambda_1^2 = 2c\ln N (1 + o(1))$ for $\mathcal{L} := \mathcal{L}(B_{n,c})$ and $N \to \infty$. We denote $\bar{M}_{n,c} = \{ (u,v) \in \mathbb{N}^2 : |u - v| = 1, \frac{1}{2} N^c \leq v \leq N^c \}$.

Following the proof of Theorem 2 for $\delta = c$ we see that $\# M_{n,c} \geq N^c (z^c)^{-2c} - o(c)$ holds for $z = \frac{\ln N}{\alpha \ln \ln N}$. Recall that $(u,v) \in \bar{M}_{n,c}$ defines a vector $b \sim (u,v)$ in $\mathcal{L}$. Hence $\ln \bar{M}_{n,c} \geq \ln N (c - \frac{2c}{\alpha} + o(1)) = \Theta(\ln N)$, since $\alpha > 2$ due to $1 < (\ln N)^{\alpha/2-1}$. Let $\mathcal{L}(B_{n,c}) \supseteq \{ b \sim (u,v) \in \bar{M}_{n,c} \}$ and let $wuv$ be essentially square-free except for a few small primes. We see from $\frac{1}{2} N^c \leq u \leq N^c$ and $u = v \pm 1$ that $\|b\|^2 = \ln u v (1 + o(1)) + \tilde{d}_u^2 \leq 2c \ln N (1 + o(1)) + 2c$, where $\ln u \leq \ln N \leq 2 \ln v \leq c \ln N$. Moreover $\tilde{d}_u^2 = N^{2c} \ln^2 u/v$ where $|\ln(u/v)| = |\ln(1 + \frac{w}{u})| \leq \frac{1}{2} (1 + o(1)) \leq 2N^{-\alpha} (1 + o(1))$ holds for large $N$. Hence $\tilde{d}_u^2 \leq 4(1 + o(1))$ 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 $\|b\|^2/\lambda_1^2 = 1 + o(1)$.

Next we bound $rd(\mathcal{L}) = \mathcal{L}(B_{n,c})$. Using $\gamma_1 = \frac{n}{2c\ln N}$ we get $\gamma_1 (\det L)^{1/2} \geq \frac{\gamma_1}{n \ln p_n} (p_n \pm 1) \geq N^{2c}$, and thus $rd(\mathcal{L}) = \lambda_1 / (\sqrt{\det L}) \geq (\frac{c}{2} \frac{2c \ln N}{n \ln p_n})^{1/2} (N^{c/n} (1 + o(1)))$.

Moreover $c \leq (\ln N)^{\alpha/2-1} = \sqrt{\ln N}/\ln N$ implies $N^{c/n} = c^{(1)}(1 + o(1))$ and $N^{c/n} - 1 = 1 + o(1)$. Hence $rd(\mathcal{L}) = (\frac{c}{2} \frac{2c \ln N}{n \ln p_n})^{1/2} (1 + o(1)) = O(p_n^{1/4}) = o(n^{-1/4})$. Since $p_n = O(n \ln p_n)$ and $c < (\ln N)^{\alpha/2-1}$ and $\ln N = n^{\alpha/2}$ and $\alpha > 2$. 16
Following the proof of Prop. 1 and Cor. 3 New Enum for CVP finds for \( p_n = (\ln N)^{\alpha} \) some \( b \in \mathcal{L}(B_{n,c}) \) that minimizes \( \|b - Nc\| \) in polynomial time, without proving correctness of the minimization. This proves the polynomial time bound. \( \square \)

References


[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