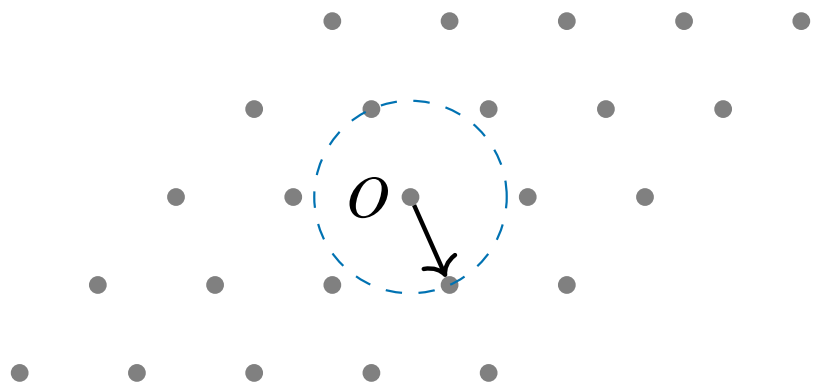
Solving the Shortest Vector Problem in $2^{0.63269n+o(n)}$ time on Random Lattices

Amaury Pouly and Yixin Shen

Univ Rennes, CNRS, Inria, IRISA, Rennes, France

13 May 2026



Shortest Vector Problems

Definition (Shortest Vector Problem, SVP)

On lattice $\mathcal{L}$ output a vector $\mathbf{y} \in \mathcal{L} \setminus \{0\}$ with $\|\mathbf{y}\| \leqslant \lambda_1(\mathcal{L})$.

Shortest Vector Problems

Definition (Shortest Vector Problem, γ-SVP)

On lattice $\mathcal{L}$ output a vector $\mathbf{y} \in \mathcal{L} \setminus \{0\}$ with $\|\mathbf{y}\| \leqslant \gamma \cdot \lambda_1(\mathcal{L})$.

Shortest Vector Problems

Definition (Shortest Vector Problem, γ-SVP)

On lattice $\mathcal{L}$ output a vector $\mathbf{y} \in \mathcal{L} \setminus \{0\}$ with $\|\mathbf{y}\| \leqslant \gamma \cdot \lambda_1(\mathcal{L})$.

- fundamental problem
- building block of lattice reduction algorithms (e.g. BKZ)

Significant gap between provable and heuristic for SVP (2^n vs $2^{0.292n}$)

- provable algorithm work on **all lattices** (worst case)
- heuristic algorithms work for **most lattices** (average case)

Motivation

Bridge the gap between heuristic and provable results: provable resultats for random lattices.

Random Lattices in Cryptography

Lattices in cryptography are random:

- random q-ary:
  - ring: integers, polynomials, modules
  - distribution: uniform, Gaussian
- random real lattices:
  - formally defined using a Haar measure
  - in some sense, the limit of sampling uniformly an integer lattice of fixed volume and rescaling

Random Lattices in Cryptography

Lattices in cryptography are random:

- random q-ary:
  - ring: integers, polynomials, modules
  - distribution: uniform, Gaussian
- random real lattices:
  - formally defined using a Haar measure
  - in some sense, the limit of sampling uniformly an integer lattice of fixed volume and rescaling

Main contribution

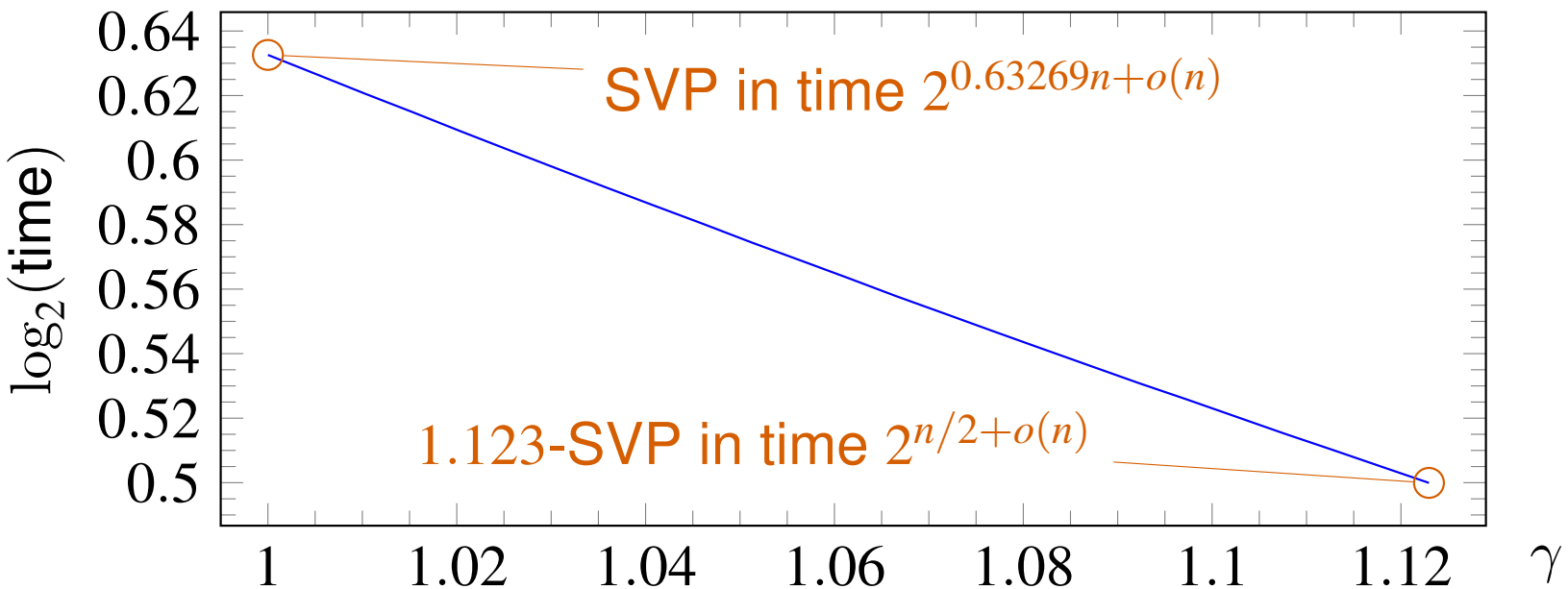
Solve SVP faster on real random lattices using discrete Gaussian sampling.

Why real lattices? $\rightsquigarrow$ Easiest to work with technically.

Contributions

SVP on random lattices

Algorithm that, for every $n \geqslant 1$ and $\gamma \in [1, 1.1230]$, solves γ-SVP on almost all* lattices in time $e^{o(n)}(\frac{\gamma^2}{2}e^{-\gamma^2/2e})^{-n/2}$ and space $2^{n/2+o(n)}$.

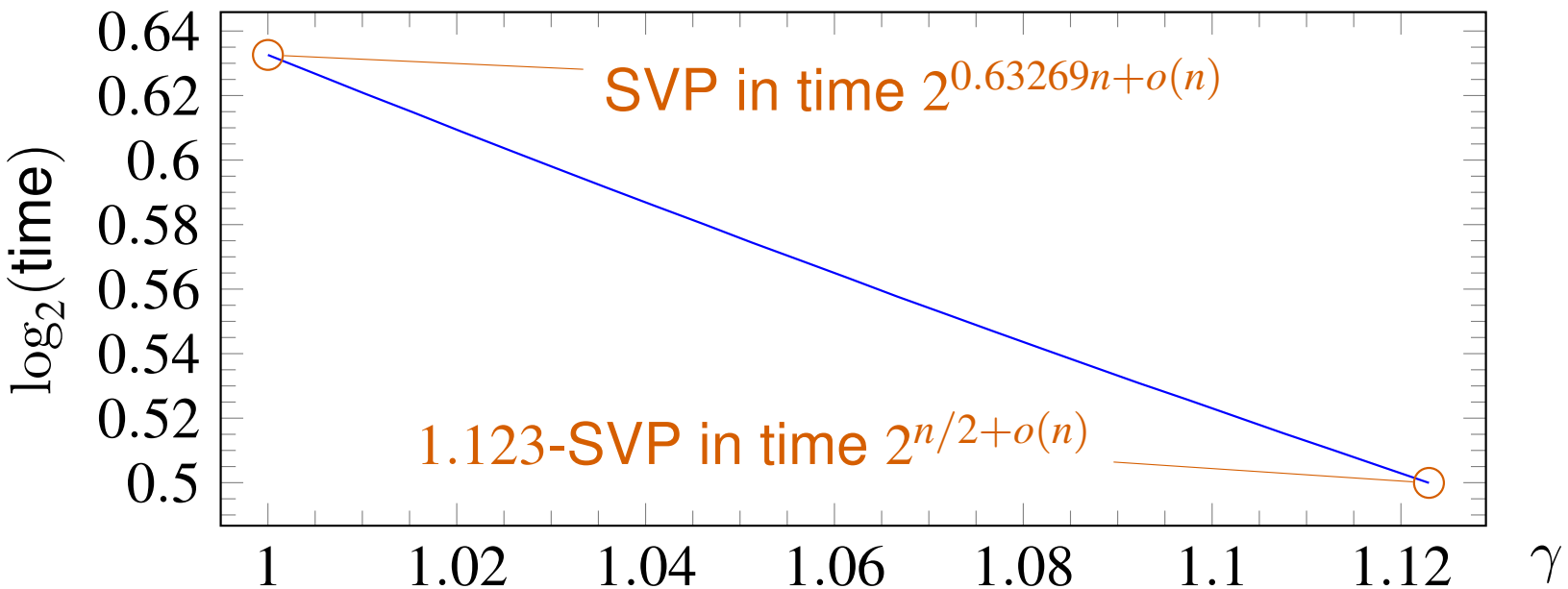


Contributions

SVP on random lattices

Algorithm that, for every $n \geqslant 1$ and $\gamma \in [1, 1.1230]$, solves γ-SVP on almost all* lattices in time $e^{o(n)}(\frac{\gamma^2}{2}e^{-\gamma^2/2e})^{-n/2}$ and space $2^{n/2+o(n)}$.

More generally, trade-off between complexity and fraction of lattices.



*Fraction $1 - 1/\text{poly}(n)$ of real lattices, can do any $1 - \varepsilon$, complexity depends on ε.

Comparison with state of the art

Problem	Time	Reference	Type
SVP	$2^{0.292n+o(n)}$	[BDGL16]	Heuristic (sieving)
SVP	$2^{n+o(n)}$	[ADRS15]	Provable
SVP	$2^{0.63269n+o(n)}$	This work	Provable (random)
$O(1)$-SVP	$2^{0.802n+o(n)}$	[WLW15]	Provable
100-SVP	$2^{0.824n+o(n)}$	[AUV19]†	Provable
1.123-SVP	$2^{n/2+o(n)}$	This work	Provable (random)
$\tilde{O}(\sqrt{n})$-SVP	$2^{n/2+o(n)}$	[ALS21]	Provable

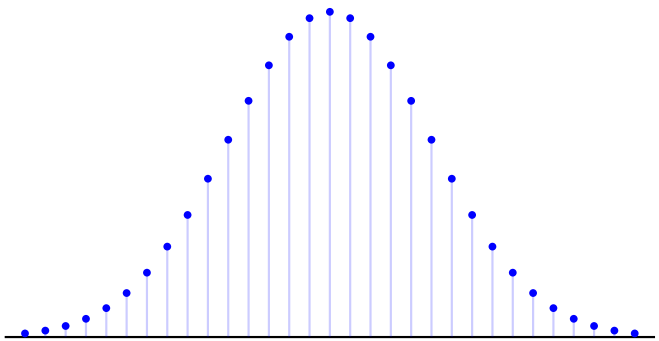
†Constant in [WLW15] analysed by [AUV19], 100-SVP is just one example.

Discrete Gaussian Sampling

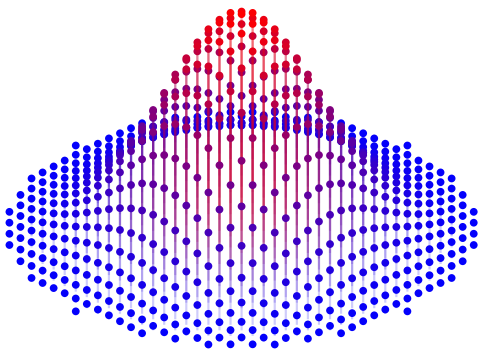
$$\rho_s(\boldsymbol{x}) = \exp\left(-\pi \frac{\|\boldsymbol{x}\|^2}{s^2}\right), \qquad D_{\mathcal{L},s}(\boldsymbol{x}) = \frac{\rho_s(\boldsymbol{x})}{\rho_s(\mathcal{L})}, \qquad \boldsymbol{x} \in \mathbb{R}^n, s > 0.$$

Discrete Gaussian Distribution

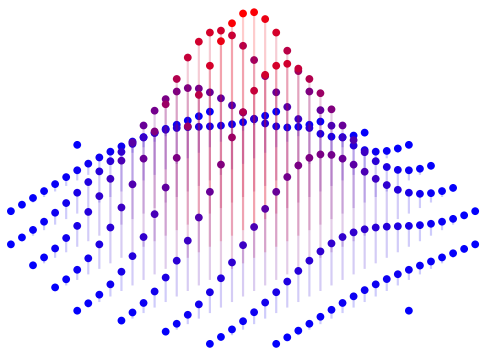
On lattice $\mathcal{L}$ with parameter s: probability of $\boldsymbol{x} \in \mathcal{L}$ is $D_{\mathcal{L},s}(\boldsymbol{x})$.



$\mathcal{L} = \mathbb{Z}, s = 7$



$\mathcal{L} = \mathbb{Z}^2, s = 7$



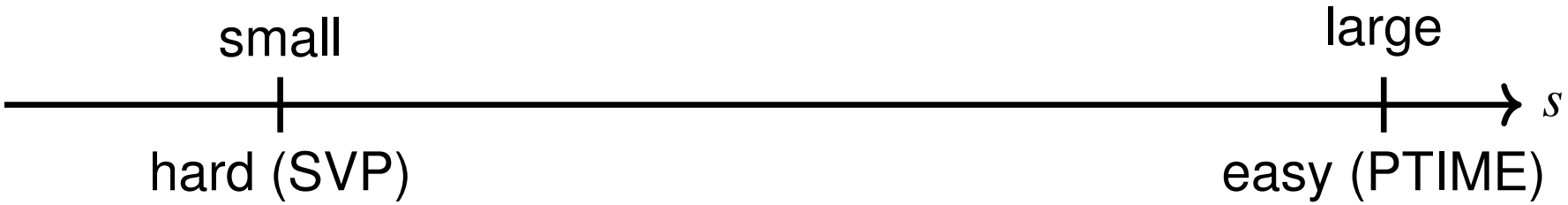
$\mathcal{L} = \mathbb{Z} \times 4\mathbb{Z}, s = 7$

Discrete Gaussian Sampling (DGS)

- **input:** $\mathcal{L}$ and s
- **output:** random $\boldsymbol{x} \in \mathcal{L}$ according to $D_{\mathcal{L},s}$.

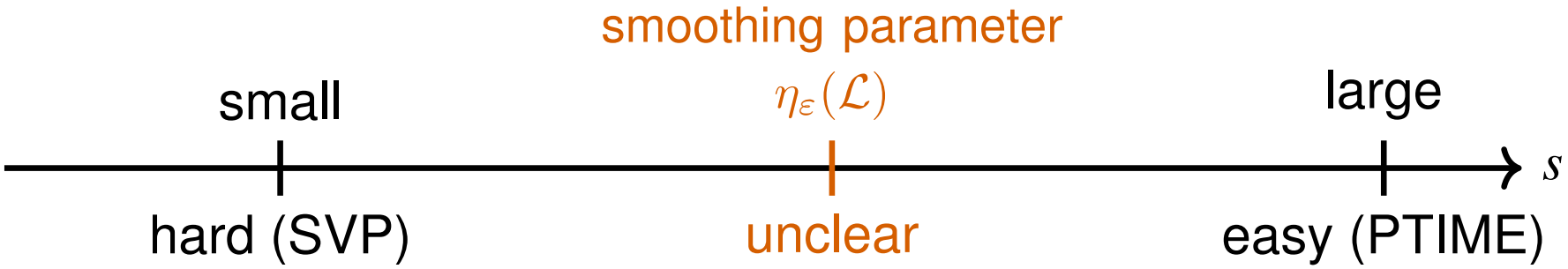
Complexity of Discrete Gaussian Sampling

Sampling from the discrete Gaussian over $\mathcal{L}$ with parameter s:



Complexity of Discrete Gaussian Sampling

Sampling from the discrete Gaussian over $\mathcal{L}$ with parameter s:

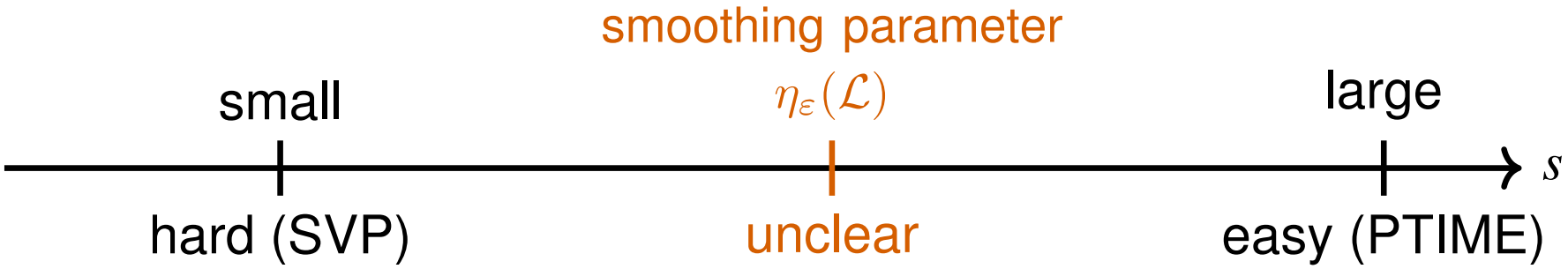


Smoothing parameter

For $\varepsilon > 0$, $\eta_\varepsilon(\mathcal{L}) = \inf\left\{s > 0 : \rho_{1/s}(\widehat{\mathcal{L}}) \leqslant 1 + \varepsilon\right\}$.

Complexity of Discrete Gaussian Sampling

Sampling from the discrete Gaussian over $\mathcal{L}$ with parameter s:



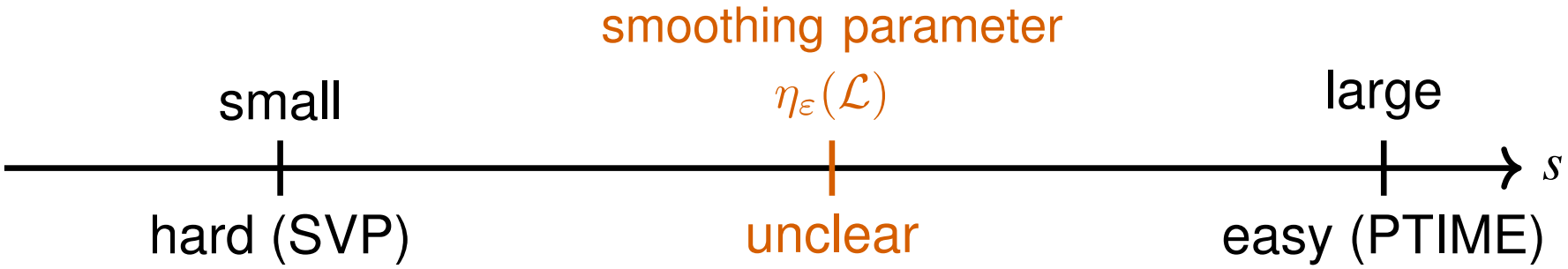
Smoothing parameter

For $\varepsilon > 0$, $\eta_\varepsilon(\mathcal{L}) = \inf\left\{s > 0 : \rho_{1/s}(\widehat{\mathcal{L}}) \leqslant 1 + \varepsilon\right\}$.

- Open problem: $2^{O(n)}$ time, $2^{o(n)}$ space algorithm for $s = \eta_\varepsilon(\mathcal{L})$
- $s \geqslant \eta_\varepsilon(\mathcal{L})$ is useful for hard problems: LWE, SVP, BDD, ...

Complexity of Discrete Gaussian Sampling

Sampling from the discrete Gaussian over $\mathcal{L}$ with parameter s:



Smoothing parameter

For $\varepsilon > 0$, $\eta_\varepsilon(\mathcal{L}) = \inf\left\{s > 0 : \rho_{1/s}(\widehat{\mathcal{L}}) \leqslant 1 + \varepsilon\right\}$.

- Open problem: $2^{O(n)}$ time, $2^{o(n)}$ space algorithm for $s = \eta_\varepsilon(\mathcal{L})$
- $s \geqslant \eta_\varepsilon(\mathcal{L})$ is useful for hard problems: LWE, SVP, BDD, ...

Theorem ([ADRS15])

For any $\mathcal{L} \subset \mathbb{R}^n$ and $s \geq \sqrt{2}\eta_{1/2}(\mathcal{L})$, can get $2^{n/2}$ samples from a distribution $2^{-\Omega(n^2)}$-close to $D_{\mathcal{L},s}$ in expected time $2^{n/2+o(n)}$.

High-level view of the algorithm

Algorithm for γ-SVP

Sample N_γ vectors from $D_{\mathcal{L},\sqrt{2}\eta_{1/2}(\mathcal{L})}$, keep the shortest nonzero.

High-level view of the algorithm

Algorithm for γ-SVP

Sample N_γ vectors from $D_{\mathcal{L},\sqrt{2}\eta_{1/2}(\mathcal{L})}$, keep the shortest nonzero.

Analysis requires:

- $\eta_{1/2}(\mathcal{L})$: smoothing parameter
- nonzero:

$$\Pr_{\mathbf{x}\sim D_{\mathcal{L},s}}[\mathbf{x}=0] = \frac{1}{\rho_s(\mathcal{L})}$$

- N_γ: estimate

$$\Pr_{\mathbf{x}\sim D_{\mathcal{L},s}}[\|\mathbf{x}\| \leqslant r] = \frac{\rho_s(\mathcal{L}\cap B_n(r))}{\rho_s(\mathcal{L})}, \qquad r = \gamma\cdot\lambda_1(\mathcal{L})$$

- $\lambda_1(\mathcal{L})$: length of SVP

High-level view of the algorithm

Algorithm for γ-SVP

Sample N_γ vectors from $D_{\mathcal{L},\sqrt{2}\eta_{1/2}(\mathcal{L})}$, keep the shortest nonzero.

Analysis requires:

- $\eta_{1/2}(\mathcal{L})$: smoothing parameter
- nonzero:

$$\Pr_{\mathbf{x}\sim D_{\mathcal{L},s}}[\mathbf{x}=0] = \frac{1}{\rho_s(\mathcal{L})}$$

- N_γ: estimate

$$\Pr_{\mathbf{x}\sim D_{\mathcal{L},s}}[\|\mathbf{x}\| \leqslant r] = \frac{\rho_s(\mathcal{L}\cap B_n(r))}{\rho_s(\mathcal{L})}, \qquad r = \gamma\cdot\lambda_1(\mathcal{L})$$

- $\lambda_1(\mathcal{L})$: length of SVP

Non-tight estimates in **general**, but can do better for random lattices

Random Real Lattices

High-level intuition:

- Consider lattice basis modulo scale: $\mathrm{vol}(\mathcal{L}) = 1 \rightsquigarrow \mathrm{SL}_n(\mathbb{R})$
- Lattices invariant by unimodular transformations: quotient / $\mathrm{SL}_n(\mathbb{Z})$

Random Real Lattices

High-level intuition:

- Consider lattice basis modulo scale: $\mathrm{vol}(\mathcal{L}) = 1 \rightsquigarrow \mathrm{SL}_n(\mathbb{R})$
- Lattices invariant by unimodular transformations: quotient / $\mathrm{SL}_n(\mathbb{Z})$

Theorem ([Sie45])

There is a unique "natural" probability measure μ_n on $\mathrm{SL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{Z})$.

μ_n usually called the Siegel-Haar measure on $X_n := \mathrm{SL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{Z})$.

Random Real Lattices

High-level intuition:

- Consider lattice basis modulo scale: $\mathrm{vol}(\mathcal{L}) = 1 \rightsquigarrow \mathrm{SL}_n(\mathbb{R})$
- Lattices invariant by unimodular transformations: quotient / $\mathrm{SL}_n(\mathbb{Z})$

Theorem ([Sie45])

There is a unique "natural" probability measure μ_n on $\mathrm{SL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{Z})$.

μ_n usually called the Siegel-Haar measure on $X_n := \mathrm{SL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{Z})$.

Averaging result ([Sie45])

Let $n \geqslant 1$ and f be a Lebesgue integrable function on $\mathbb{R}^n$, then

$$\mathbb{E}_{\mathcal{L}\sim\mu_n}\left[\sum_{\mathbf{x}\in\mathcal{L}\setminus\{0\}} f(\mathbf{x})\right] = \int_{\mathbb{R}^n} f(\mathbf{x})\mathrm{d}\,\lambda(\mathbf{x}).$$

where λ denotes the usual Lebesgue measure on $\mathbb{R}^n$

Averaging results: Gaussian mass

For any $s > 0$,

$$\mathbb{E}_{\mathcal{L}\sim\mu_n}[\rho_s(\mathcal{L})] = 1 + \int_{\mathbb{R}^n} \rho_s(\mathbf{x}) \mathrm{d}\,\lambda(\mathbf{x}) = 1 + s^n.$$

Can obtain a bound on $\rho_s(\mathcal{L})$ and $\eta_\varepsilon(\mathcal{L})$ using Markov's inequality.

Averaging results: Gaussian mass

For any $s > 0$,

$$\mathbb{E}_{\mathcal{L}\sim\mu_n}[\rho_s(\mathcal{L})] = 1 + \int_{\mathbb{R}^n} \rho_s(\mathbf{x}) \mathrm{d}\,\lambda(\mathbf{x}) = 1 + s^n.$$

Can obtain a bound on $\rho_s(\mathcal{L})$ and $\eta_\varepsilon(\mathcal{L})$ using Markov's inequality.

Similar results for other models:

Model	**Method**	**Ref**
q-ary, Gaussian entries	estimate λ_1, bound η_ε	[KNSW20]
q-ary, uniform entries	Siegel-like* method	[LLBS14]
q-ary / cyclotomic field	ad-hoc calculation estimate λ_1, bound η_ε	[CPSWX20; LPR13] [SS11]

*A generic Siegel-like averaging result for q-ary was already shown in [Loe97].

Averaging results: Gaussian mass

For any $s > 0$,

$$\mathbb{E}_{\mathcal{L}\sim\mu_n}[\rho_s(\mathcal{L})] = 1 + \int_{\mathbb{R}^n} \rho_s(\mathbf{x}) \mathrm{d}\,\lambda(\mathbf{x}) = 1 + s^n.$$

Can obtain a bound on $\rho_s(\mathcal{L})$ and $\eta_\varepsilon(\mathcal{L})$ using Markov's inequality.

Similar results for other models:

Model	**Method**	**Ref**
q-ary, Gaussian entries	estimate λ_1, bound η_ε	[KNSW20]
q-ary, uniform entries	Siegel-like* method	[LLBS14]
q-ary / cyclotomic field	ad-hoc calculation estimate λ_1, bound η_ε	[CPSWX20; LPR13] [SS11]

However, Markov inequality is not very tight...

*A generic Siegel-like averaging result for q-ary was already shown in [Loe97].

Averaging results: variance

The averaging result of Siegel is not always sufficient. A higher-order version was shown* by Mac Beath and Rogers [MR58]. However the statement is complicated.

Corollary ([MR58])

Let $n \geqslant 2$ and f be Lebesgue integrable on $\mathbb{R}^n$, then

$$\mathbb{V}_{\mathcal{L}\sim\mu_n}\left[\sum_{\mathbf{x}\in\mathcal{L}} f(\mathbf{x})\right] = \frac{1}{\zeta(n)} \sum_{\alpha\in\mathbb{N}\setminus\{0\}} \sum_{\beta\in\mathbb{Z}\setminus\{0\}} \int_{\mathbb{R}^n} f(\alpha\mathbf{x}) f(\beta\mathbf{x}) \mathrm{d}\,\lambda(\mathbf{x}).$$

*There is an error in the original proof of Rogers, noticed and fixed in [Kim24].

Gaussian mass and smoothing parameter

Theorem (Gaussian mass, simplified)

For any $s > 0$ and $\alpha > 0$

$$\Pr_{\mathcal{L}\sim\mu_n}[|\rho_s(\mathcal{L}) - 1 - s^n| > \alpha] \leqslant \frac{2^{-n/2}s^n}{\alpha^2}.$$

Gaussian mass and smoothing parameter

Theorem (Gaussian mass, simplified)

For any $s > 0$ and $\alpha > 0$

$$\Pr_{\mathcal{L}\sim\mu_n}[|\rho_s(\mathcal{L}) - 1 - s^n| > \alpha] \leqslant \frac{2^{-n/2}s^n}{\alpha^2}.$$

More generally: concentration bound on $\rho_s(\mathcal{L} \cap B_n(r))$ for any $r > 0$

Gaussian mass and smoothing parameter

Theorem (Gaussian mass, simplified)

For any $s > 0$ and $\alpha > 0$

$$\Pr_{\mathcal{L}\sim\mu_n}[|\rho_s(\mathcal{L}) - 1 - s^n| > \alpha] \leqslant \frac{2^{-n/2}s^n}{\alpha^2}.$$

More generally: concentration bound on $\rho_s(\mathcal{L} \cap B_n(r))$ for any $r > 0$

Corollary (Smoothing parameter, simplified)

For any $\varepsilon > 0$, let $s_\varepsilon = \left(\frac{\varepsilon+1+\sqrt{2\,\varepsilon+1}}{\varepsilon^2}\right)^{1/n}$. Then

$$\Pr_{\mathcal{L}\sim\mu_n}[\eta_\varepsilon(\mathcal{L}) > s_\varepsilon] \leqslant 2^{-n/2}.$$

Open question: smoothing parameter

For any $\varepsilon > 0$, almost all lattices $\mathcal{L}$ satisfy that

$$\eta_\varepsilon(\mathcal{L}) \leqslant \left(\frac{\varepsilon + 1 + \sqrt{2\,\varepsilon + 1}}{\varepsilon^2}\right)^{1/n} \sim_{\varepsilon \to 0} 2^{1/n} \varepsilon^{-2/n}$$

Open question: smoothing parameter

For any $\varepsilon > 0$, almost all lattices $\mathcal{L}$ satisfy that

$$\eta_\varepsilon(\mathcal{L}) \leqslant \left(\frac{\varepsilon + 1 + \sqrt{2\,\varepsilon + 1}}{\varepsilon^2}\right)^{1/n} \sim_{\varepsilon \to 0} 2^{1/n} \varepsilon^{-2/n}$$

Combine with the bound on $\lambda_1(\mathcal{L})$:

$$\lambda_1(\mathcal{L}) \eta_\varepsilon(\widehat{\mathcal{L}}) \leqslant \sqrt{\tfrac{n}{2\pi e}} \cdot \varepsilon^{-2/n} \tag{1}$$

Open question: smoothing parameter

For any $\varepsilon > 0$, almost all lattices $\mathcal{L}$ satisfy that

$$\eta_\varepsilon(\mathcal{L}) \leqslant \left(\frac{\varepsilon + 1 + \sqrt{2\,\varepsilon + 1}}{\varepsilon^2}\right)^{1/n} \sim_{\varepsilon \to 0} 2^{1/n} \varepsilon^{-2/n}$$

Combine with the bound on $\lambda_1(\mathcal{L})$:

$$\lambda_1(\mathcal{L}) \eta_\varepsilon(\widehat{\mathcal{L}}) \leqslant \sqrt{\tfrac{n}{2\pi e}} \cdot \varepsilon^{-2/n} \tag{1}$$

Compare with the unconditional result of [ADRS15]:

$$\lambda_1(\mathcal{L}) \eta_\varepsilon(\widehat{\mathcal{L}}) < \sqrt{\frac{\beta(\mathcal{L})^2 n}{2\pi e}} \cdot \varepsilon^{-1/n} \tag{2}$$

where $\beta(\mathcal{L}) \leqslant 2^{0.401}$ is the generalized kissing number [ACKS21].

Open question: smoothing parameter

For any $\varepsilon > 0$, almost all lattices $\mathcal{L}$ satisfy that

$$\eta_\varepsilon(\mathcal{L}) \leqslant \left(\frac{\varepsilon + 1 + \sqrt{2\,\varepsilon + 1}}{\varepsilon^2}\right)^{1/n} \sim_{\varepsilon \to 0} 2^{1/n} \varepsilon^{-2/n}$$

Combine with the bound on $\lambda_1(\mathcal{L})$:

$$\lambda_1(\mathcal{L}) \eta_\varepsilon(\widehat{\mathcal{L}}) \leqslant \sqrt{\tfrac{n}{2\pi e}} \cdot \varepsilon^{-2/n} \tag{1}$$

Compare with the unconditional result of [ADRS15]:

$$\lambda_1(\mathcal{L}) \eta_\varepsilon(\widehat{\mathcal{L}}) < \sqrt{\frac{\beta(\mathcal{L})^2 n}{2\pi e}} \cdot \varepsilon^{-1/n} \tag{2}$$

where $\beta(\mathcal{L}) \leqslant 2^{0.401}$ is the generalized kissing number [ACKS21].

Discrepancy:

- $\varepsilon^{-2/n}$ in our case,
- $\varepsilon^{-1/n}$ in [ACKS21].

Good:

- suggest $\beta(\mathcal{L}) \approx 1$ for random $\mathcal{L}$

Conclusion and future work

Study of real random lattices:

- probabilistic bounds on $\rho_s(\mathcal{L})$, $\eta_\varepsilon(\mathcal{L})$ and $\rho_s(\mathcal{L} \cap B_n(r))$
- time/approx tradeoff for γ-SVP (constant γ regime)
- SVP and $\sqrt{\frac{n}{2\pi e}}$-HSVP in time $2^{0.63269n+o(n)}$
- 1.123-SVP in time $2^{n/2+o(n)}$

Open question: improve bound on η_ε to resolve discrepancy

- use Rogers averaging for higher order, difficult computations
- if we can solve this, can improve BDD results from [ACKS21]

[ACKS21] Divesh Aggarwal, Yanlin Chen, Rajendra Kumar, and Yixin Shen. *Improved (Provable) Algorithms for the Shortest Vector Problem via Bounded Distance Decoding*.

[ADRS15] Divesh Aggarwal, Daniel Dadush, Oded Regev, and Noah Stephens-Davidowitz. *Solving the Shortest Vector Problem in 2^n Time Using Discrete Gaussian Sampling: Extended Abstract*.

[ALS21] Divesh Aggarwal, Zeyong Li, and Noah Stephens-Davidowitz. *A $2^{n/2}$-Time Algorithm for $\sqrt{n}$-SVP and $\sqrt{n}$-Hermite SVP, and an Improved Time-Approximation Tradeoff for (H)SVP*.

[AUV19] Divesh Aggarwal, Bogdan Ursu, and Serge Vaudenay. *Faster Sieving Algorithm for Approximate SVP with Constant Approximation Factors*.

[BDGL16] Anja Becker, Léo Ducas, Nicolas Gama, and Thijs Laarhoven. *New directions in nearest neighbor searching with applications to lattice sieving*.

[CDLP13] Kai-Min Chung, Daniel Dadush, Feng-Hao Liu, and Chris Peikert. *On the Lattice Smoothing Parameter Problem*.

[CPSWX20] Chitchanok Chuengsatiansup, Thomas Prest, Damien Stehlé, Alexandre Wallet, and Keita Xagawa. *ModFalcon: Compact Signatures Based On Module-NTRU Lattices*.

[Kim24] Seungki Kim. *Adelic Rogers integral formula*.

[KNSW20] Elena Kirshanova, Huyen Nguyen, Damien Stehlé, and Alexandre Wallet. *On the smoothing parameter and last minimum of random orthogonal lattices*.

[LLBS14] Cong Ling, Laura Luzzi, Jean-Claude Belfiore, and Damien Stehlé. *Semantically Secure Lattice Codes for the Gaussian Wiretap Channel*.

[Loe97] H.-A. Loeliger. *Averaging bounds for lattices and linear codes*.

[LPR13] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. *A Toolkit for Ring-LWE Cryptography*.

[MR58] A. M. Macbeath and C. A. Rogers. *Siegel's mean value theorem in the geometry of numbers*.

[Rog56] C. A. Rogers. *The Number of Lattice Points in a Set*.

[Sie45] Carl Ludwig Siegel. *A Mean Value Theorem in Geometry of Numbers*.

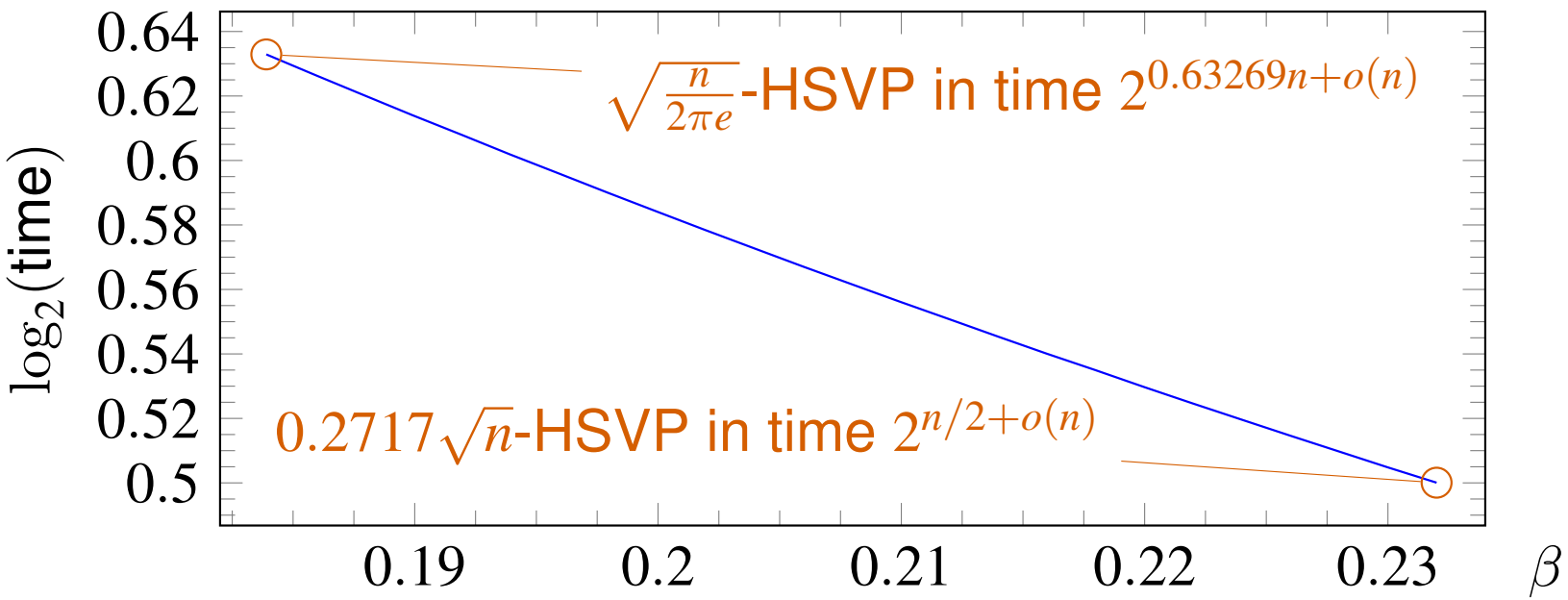
[SS11] Damien Stehlé and Ron Steinfeld. *Making NTRU as Secure as Worst-Case Problems over Ideal Lattices*.

[WLW15] Wei Wei, Mingjie Liu, and Xiaoyun Wang. *Finding Shortest Lattice Vectors in the Presence of Gaps*.

Contributions (cont.)

HSVP on random lattices

Algorithm that, for every $n \geqslant 1$ and $\beta \in [\frac{1}{2e}, 0.2320]$, solves $\sqrt{\frac{n\beta}{\pi}}$-HSVP on almost all lattices in time $e^{o(n)}(\beta e^{1-\beta})^{-n/2}$ and space $2^{n/2+o(n)}$.



GapSVP

Promise version of SVP:

Definition (γ-GapSVP)

On lattice $\mathcal{L}$ and $r > 0$, accept if $\lambda_1(\mathcal{L}) \leqslant r$ and reject if $\lambda_1(\mathcal{L}) \geqslant \gamma r$.

Best provable result: $2^{n/2+o(n)}$-time algorithm for 1.93-GapSVP [ADRS15].

GapSVP

Promise version of SVP:

Definition (γ-GapSVP)

On lattice $\mathcal{L}$ and $r > 0$, accept if $\lambda_1(\mathcal{L}) \leqslant r$ and reject if $\lambda_1(\mathcal{L}) \geqslant \gamma r$.

Best provable result: $2^{n/2+o(n)}$-time algorithm for 1.93-GapSVP [ADRS15].

Random real lattices: concentration bounds on $\lambda_1(\mathcal{L})$.

Corollary (Informal, was already folklore)

There is an algorithm that, for every $\gamma > 1$, $n \geqslant 1$ and on most lattices $\mathcal{L} \subset \mathbb{R}^n$, solves γ-GapSVP in polynomial time.

Algorithm: on input $\mathcal{L} \subseteq \mathbb{R}^n$ and $r > 0$, accept if $\mathrm{vol}(B_n)^{-1/n} < r\sqrt{\gamma}$ and reject otherwise.

Estimating the Smoothing Parameter

- Generic bound [ADRS15]:

$$\sqrt{\frac{\log(1/\varepsilon)}{\pi}} < \lambda_1(\mathcal{L})\eta_\varepsilon(\widehat{\mathcal{L}}) < \sqrt{\frac{\beta(\mathcal{L})^2 n}{2\pi e}} \cdot \varepsilon^{-1/n} \cdot (1 + o(1))$$

where $\beta(\mathcal{L}) \leqslant 2^{0.401}$ is the generalized kissing number of $\mathcal{L}$.

Estimating the Smoothing Parameter

- Generic bound [ADRS15]:

$$\sqrt{\frac{\log(1/\varepsilon)}{\pi}} < \lambda_1(\mathcal{L})\eta_\varepsilon(\widehat{\mathcal{L}}) < \sqrt{\frac{\beta(\mathcal{L})^2 n}{2\pi e}} \cdot \varepsilon^{-1/n} \cdot (1 + o(1))$$

where $\beta(\mathcal{L}) \leqslant 2^{0.401}$ is the generalized kissing number of $\mathcal{L}$.

  - requires to know $\lambda_1(\mathcal{L})$
  - gap between LHS and RHS
  - $\beta(\mathcal{L}) \leqslant 2^{0.401}$ pessimistic (see later)

Estimating the Smoothing Parameter

- Generic bound [ADRS15]:

$$\sqrt{\frac{\log(1/\varepsilon)}{\pi}} < \lambda_1(\mathcal{L})\eta_\varepsilon(\widehat{\mathcal{L}}) < \sqrt{\frac{\beta(\mathcal{L})^2 n}{2\pi e}} \cdot \varepsilon^{-1/n} \cdot (1 + o(1))$$

where $\beta(\mathcal{L}) \leqslant 2^{0.401}$ is the generalized kissing number of $\mathcal{L}$.

  - requires to know $\lambda_1(\mathcal{L})$
  - gap between LHS and RHS
  - $\beta(\mathcal{L}) \leqslant 2^{0.401}$ pessimistic (see later)

Definition (Smoothing Parameter Problem γ-GapSPP$_{\varepsilon_Y,\varepsilon_N}$)

On lattice $\mathcal{L}$: accept if $\eta_{\varepsilon_Y}(\mathcal{L}) \leqslant 1$, reject if $\eta_{\varepsilon_N}(\mathcal{L}) > \gamma$.

- Hard problem [CDLP13]:
  - $(1 + o(1))$-GapSPP$_{\varepsilon,\varepsilon} \in$ DTIME$(2^{O(n)}\text{polylog}(1/\varepsilon))$
  - reduction* from α-BDD to $\sqrt{n}/\alpha$-GapSPP$_{\text{negl}(n),1/\text{poly}(n)}$
  - quantum reduction* from LWE$_\alpha$ to $2\sqrt{n}/\alpha$-GapSPP$_{\text{negl}(n),1/\text{poly}(n)}$

*Result highly simplified for presentation.

Averaging results: higher order

The averaging result of Siegel is not always sufficient.

Generalized averaging result* ([MR58])

Let $1 \leqslant \ell \leqslant n-1$ and f be Lebesgue integrable on $\mathbb{R}^{n\times\ell}$, then

$$\int_{X_n} \sum_{\mathbf{M}\in \mathrm{LI}_{n,\ell}} f(\mathbf{AM})\mathrm{d}\,\mu(\mathbf{A})$$

$$= \zeta(n)\cdots\zeta(n-\ell+1)\int_{X_n}\sum_{\mathbf{P}\in\mathrm{PR}_{n,\ell}} f(\mathbf{AP})\mathrm{d}\,\mu(\mathbf{A}) = \int_{\mathbb{R}^{n\times\ell}} f(X)\mathrm{d}\,\lambda(X).$$

- $\mathrm{LI}_{n,\ell}$: $n\times\ell$ integer matrix, linearly indepependent columns
- $\mathrm{PR}_{n,\ell}$: $n\times\ell$ integer matrix, primitive†

*There is an error in the original proof of Rogers, noticed and fixed in [Kim24].

†Can be extended to form an integer basis of $\mathbb{Z}^n$.

HSVP: formal result

Theorem (HSVP)

There is a randomized algorithm that for every $n \geqslant 2$ *and* $\beta \in (0, \frac{n-2}{2n})$ *and on a fraction at least* $1 - 2^{1-n/2}(1+o(1)) - (2e\beta)^{-n/2}O(n^{3/2})$ *of random lattices* $\mathcal{L}$ *according to* μ_n*, outputs in time* $e^{o(n)}(\beta e^{1-\beta})^{-n/2} + 2^{n/2+o(n)}$ *and space* $2^{n/2+o(n)}$ *a nonzero vector of* $\mathcal{L}$ *of length at most* $s_{1/2}\sqrt{\frac{n\beta}{\pi}}$ *with probability at least* $1/2$*, where* $s_{1/2} = (6+4\sqrt{2})^{1/n} = 1 + o(1)$

Corollary (HSVP)

There is a randomized algorithm that for every $n \geqslant 2$ *and* $\beta \in [\frac{1}{2e}, 0.2320]$*, solves* $(1+o(1))\sqrt{\frac{n\beta}{\pi}}$*-HSVP in time* $e^{o(n)}(\beta e^{1-\beta})^{-n/2}$ *and space* $2^{n/2+o(n)}$ *with probability at least* $1/2$ *on a fraction at least* $1 - e^{o(n)}(2e\beta)^{-n/2}$ *of random lattices according to* μ_n*.*

SVP: formal result

Theorem (γ-SVP ($\gamma > 1$))

There is a randomized algorithm that for every $n \geqslant 1$, $\gamma \in (1, 1.1230]$ and $\beta \in [\frac{1}{2e}, \frac{\gamma^2}{2e})$, solves γ-SVP in time $e^{o(n)}(\beta e^{1-\beta})^{-n/2}$ and space $2^{n/2+o(n)}$ with probability at least $1/2$ on a fraction at least $1 - O(n^{3/2})(2e\beta)^{-n/2} - O(n^{-1/2})\left(\frac{2e\beta}{\gamma^2}\right)^{n/2}$ of random lattices $\mathcal{L}$ according to μ_n.

Theorem (SVP ($\gamma = 1$))

There is a randomized algorithm that for every $n \geqslant 1$ and $\alpha > 2^{1/n}$, and on a fraction at least $1 - 2^{1-n/2}(1 + o(1)) - \frac{2\alpha^n A(n)}{(\alpha^n - 2)^2}$ of random lattices $\mathcal{L}$ according to μ_n, outputs in time $2^{\tau n + o(n)}$ and space $2^{n/2+o(n)}$ a shortest nonzero vector of $\mathcal{L}$ with probability at least $1/2$, where $\tau = \frac{1}{2} + \frac{\alpha^2}{4e \ln 2}$ and $A(n) = 1 + 2^{1-n}(1 + o(1))$.

SVP: almost all lattices

Corollary (γ-SVP on almost all lattices ($\gamma > 1$))

There is a randomized algorithm that for every $\gamma \in (\frac{1}{0.99}, \sqrt{2e\beta_{\max}}]$ *and* $n \geqslant 1$ *solves* γ*-SVP in time* $\left(0.1821\gamma^2 e^{1-0.1821\gamma^2}\right)^{-n/2} e^{o(n)}$ *and space* $2^{n/2+o(n)}$ *with probability at least* $1/2$ *on a fraction at least* $1 - 0.99^{n/2+o(n)}$ *of random lattices* $\mathcal{L}$ *according to* μ_n.

Corollary (SVP on almost all lattices ($\gamma = 1$))

There is a randomized algorithm that for every $n \geqslant 70$*, solves SVP in time* $2^{0.635n+o(n)}$ *with probability at least* $1/2$ *on a fraction at least* $1 - 0.99^{n/2}$ *of random lattices* $\mathcal{L}$ *according to* μ_n.

SVP: most lattices

Corollary (γ-SVP on most lattices ($\gamma > 1$))

For every $k > 0$, there is a randomized algorithm that for every $\gamma \in (1, \sqrt{2e\beta_{\max}}]$ and $n \geqslant -\frac{k}{\ln \gamma} W_{-1}(-\frac{\ln \gamma}{k})$ solves γ-SVP in space $2^{n/2+o(n)}$ and time $e^{o(n)}(\frac{2}{\gamma^2}e^{\gamma^2/2e})^{n/2}$ with probability at least $1/2$ on a fraction at least $1 - O(n^{-k})$ of random lattices $\mathcal{L}$ according to μ_n.

Corollary (SVP on most lattices ($\gamma = 1$))

There is a randomized algorithm that for every $k \in \mathbb{N}$ and $n \geqslant 1$, solves SVP in time $2^{(\frac{1}{2}+\frac{1}{4e\ln 2})n+o(n)} = 2^{0.63269n+o(n)}$ with probability at least $1/2$ on a fraction at least $1 - 2n^{-k}(1 + o(1))$ of random lattices $\mathcal{L}$ according to μ_n.