Solving SVP in 2^n Time Using Discrete Gaussian Sampling

Divesh Aggarwal
Daniel Dadush
Oded Regev
Noah Stephens-Davidowitz

Before We Start

I'm going to talk about an exact algorithm. To break crypto, you only need to approximate SVP to within some polynomial factor.

(The fastest algorithm to provably break crypto runs in $2^{0.4n}$ time [Sch87, GN08, LWXZ11].)

Before We Start

This algorithm is easy to understand. If you aren't following, that is my fault. So, please interrupt me frequently.

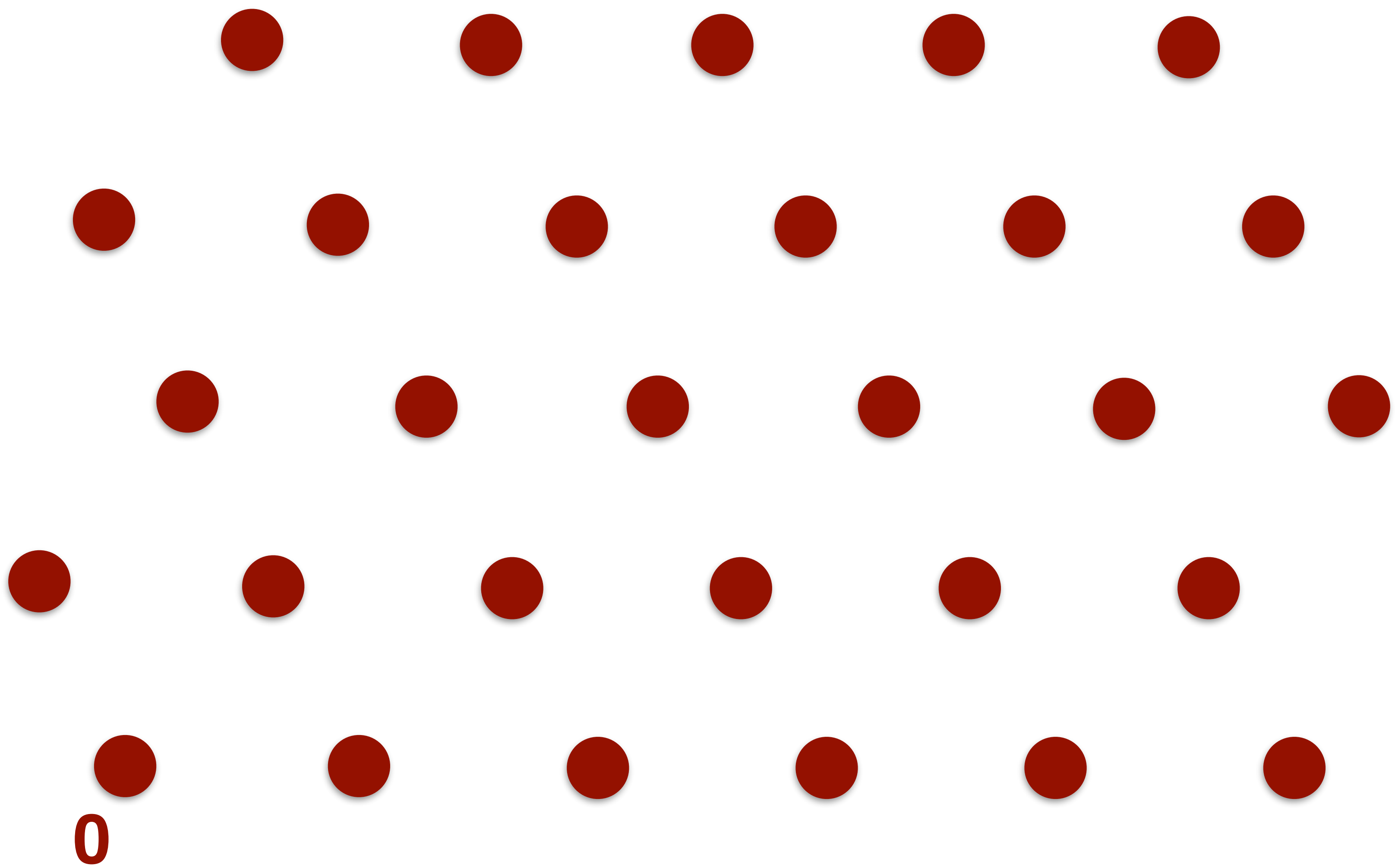
Lattices

Lattices

- $\mathcal{L}$ is a discrete set of vectors in $\mathbb{R}^n$

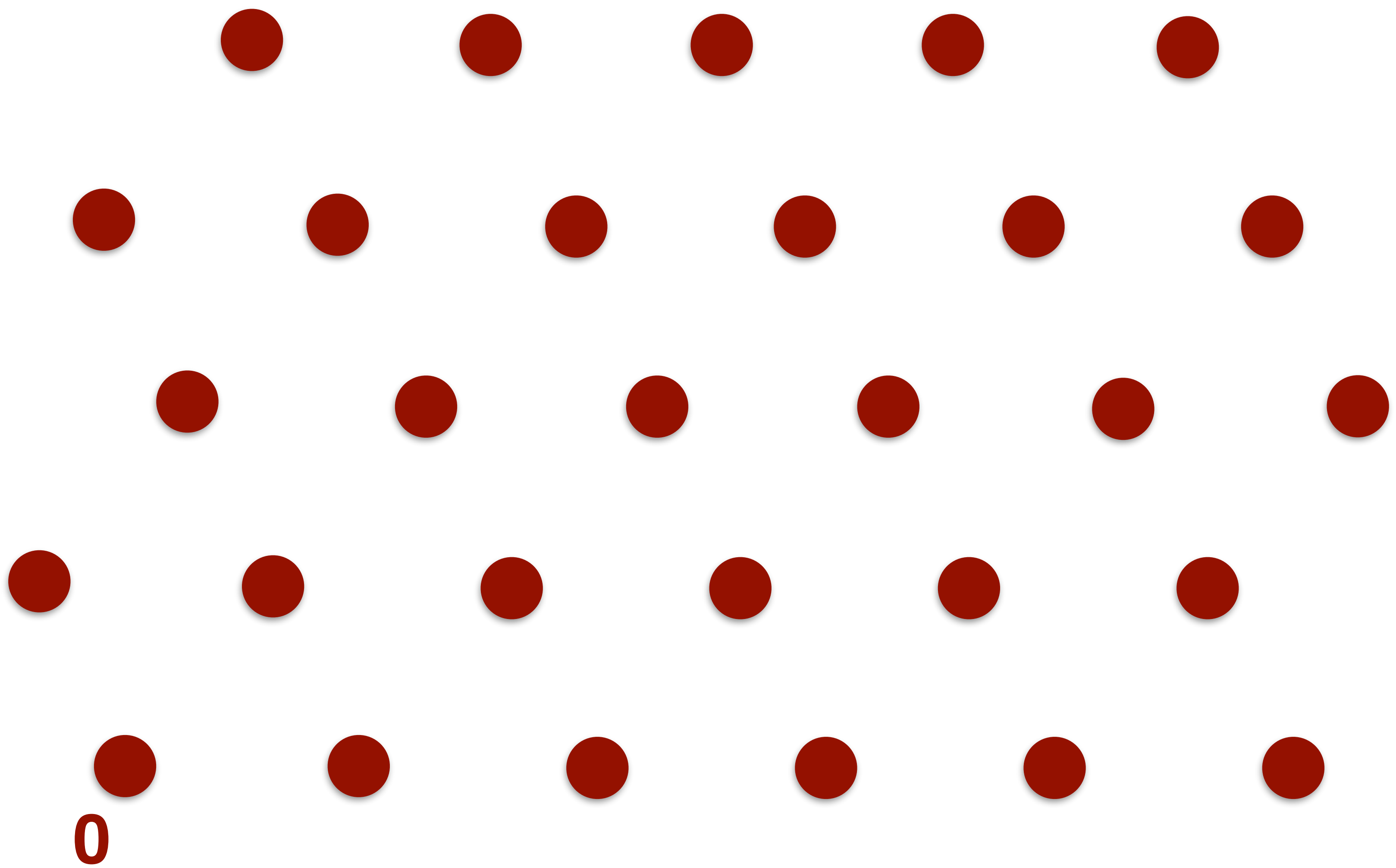
Lattices

- $\mathcal{L}$ is a discrete set of vectors in $\mathbb{R}^n$



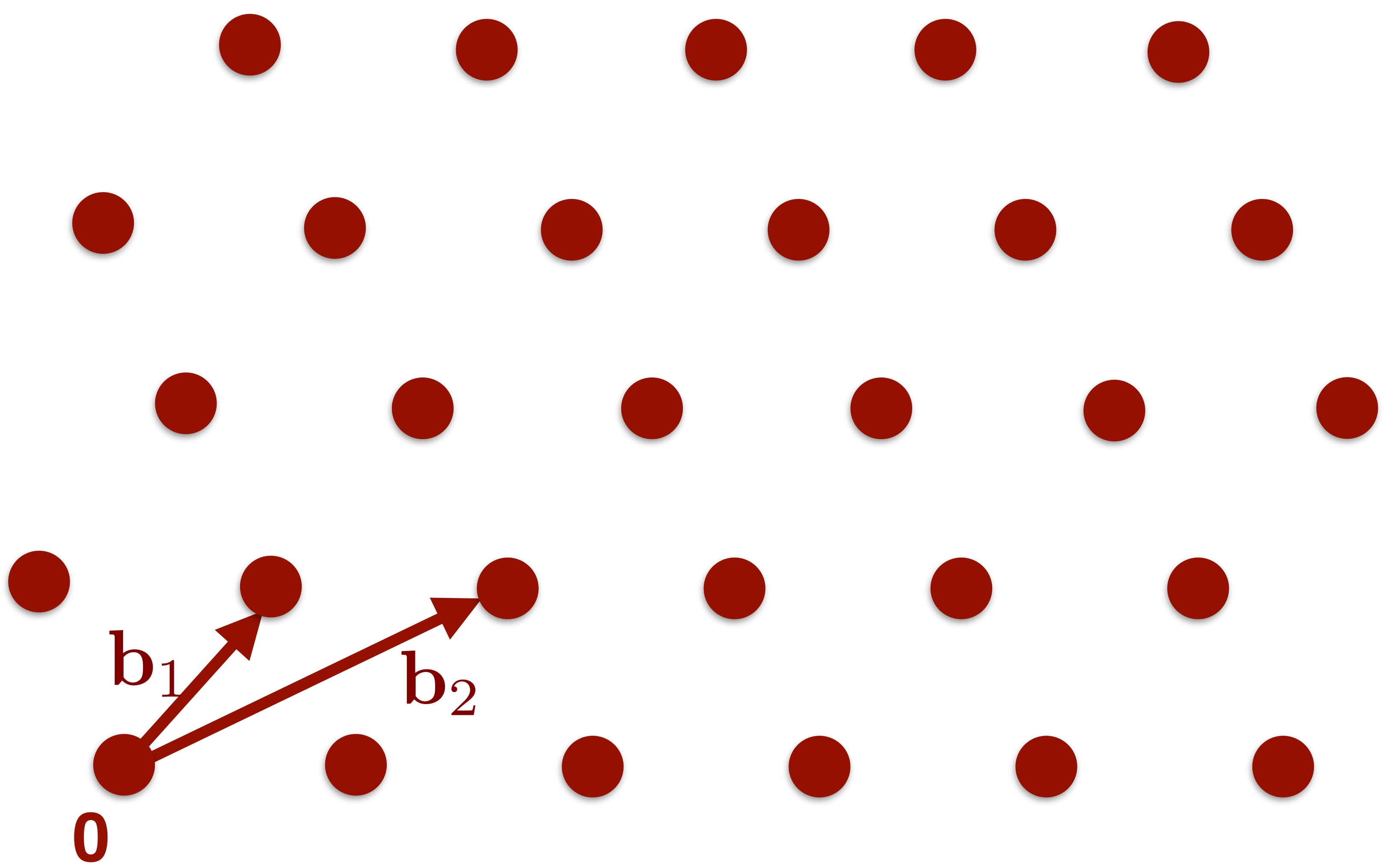
Lattices

- $\mathcal{L}$ is a discrete set of vectors in $\mathbb{R}^n$
- Specified by a basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$, linearly independent vectors



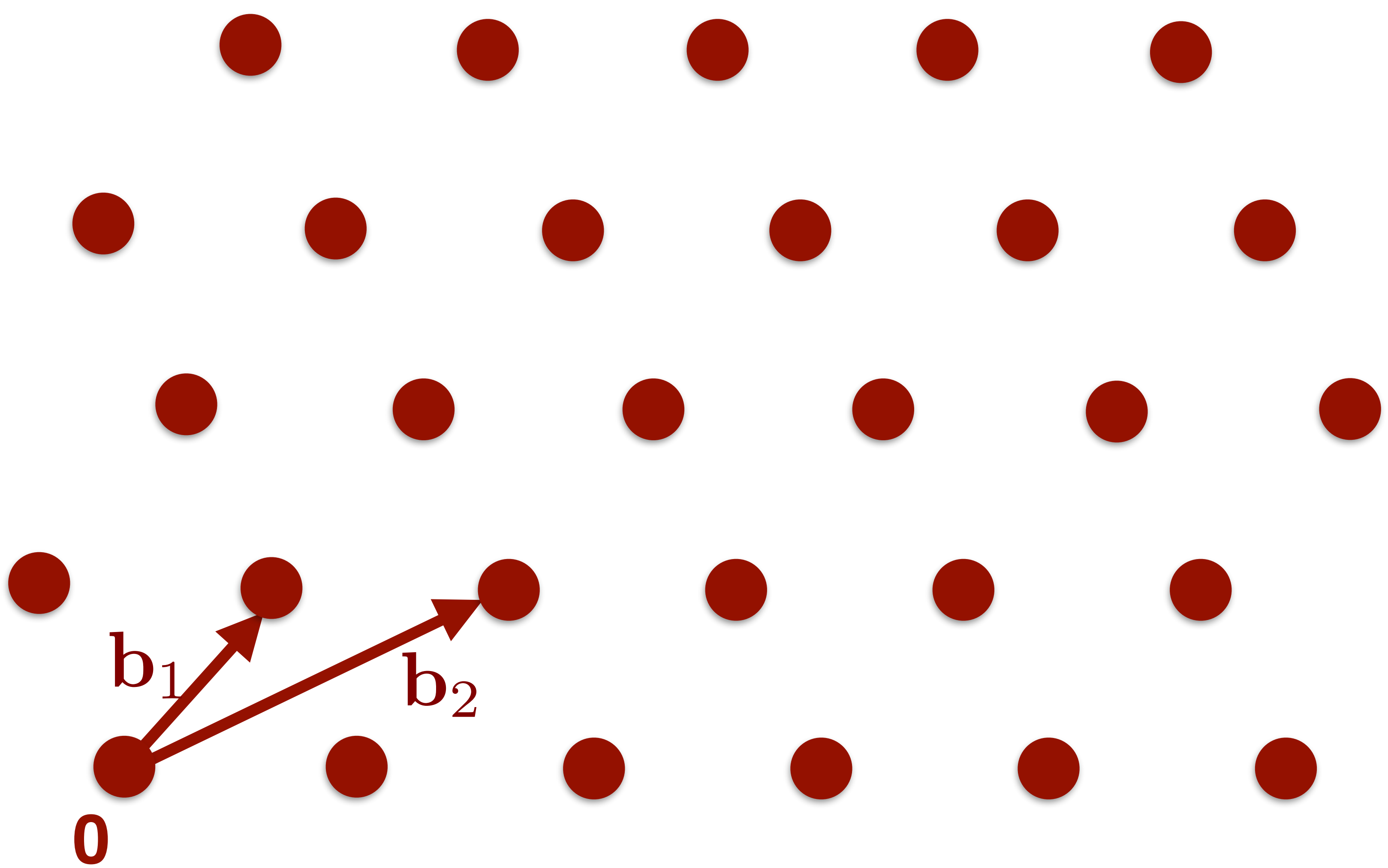
Lattices

- $\mathcal{L}$ is a discrete set of vectors in $\mathbb{R}^n$
- Specified by a basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$, linearly independent vectors

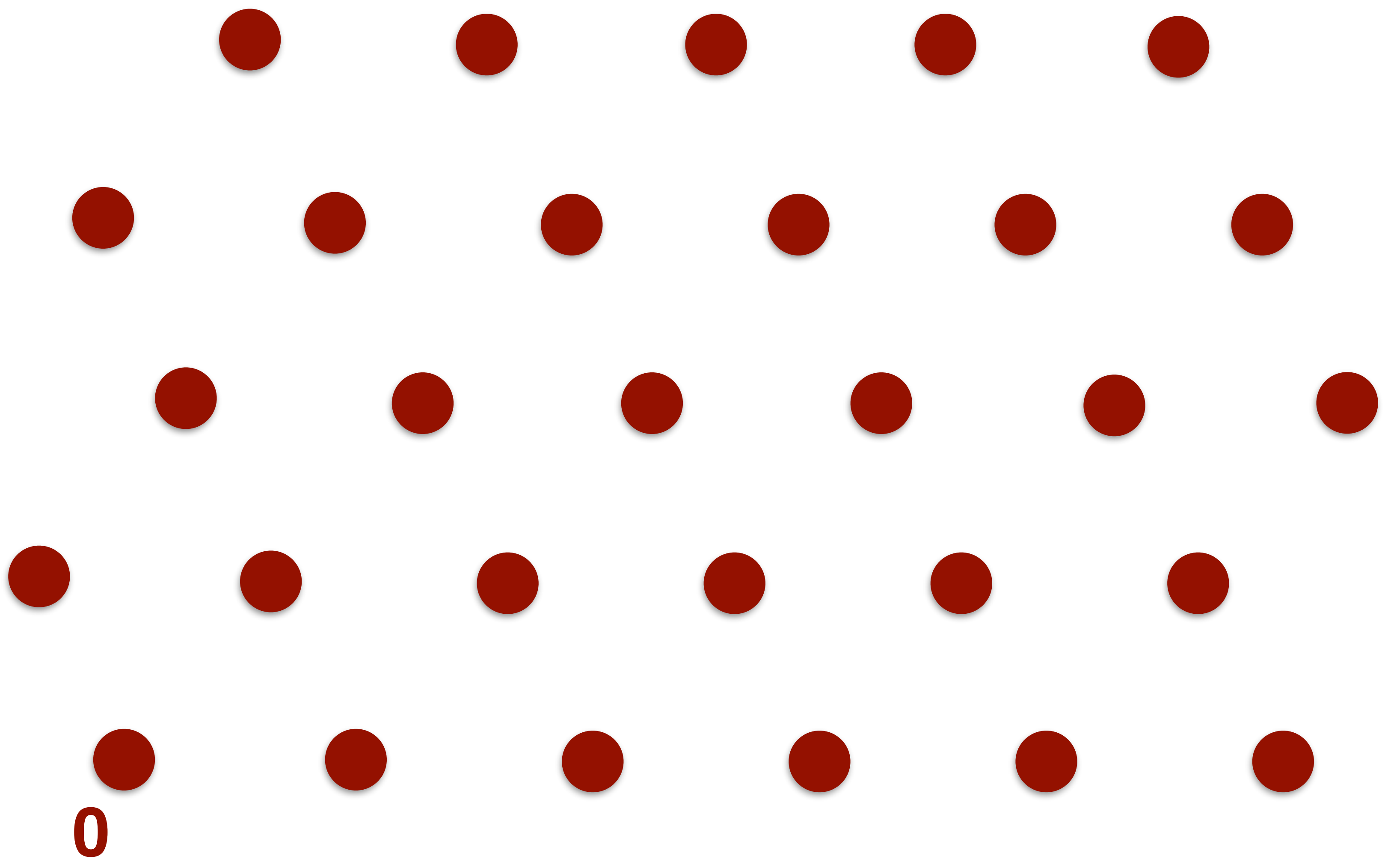


Lattices

- $\mathcal{L}$ is a discrete set of vectors in $\mathbb{R}^n$
- Specified by a basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$, linearly independent vectors
- $\mathcal{L} = \{a_1\mathbf{b}_1 + \cdots + a_n\mathbf{b}_n \mid a_i \in \mathbb{Z}\}$

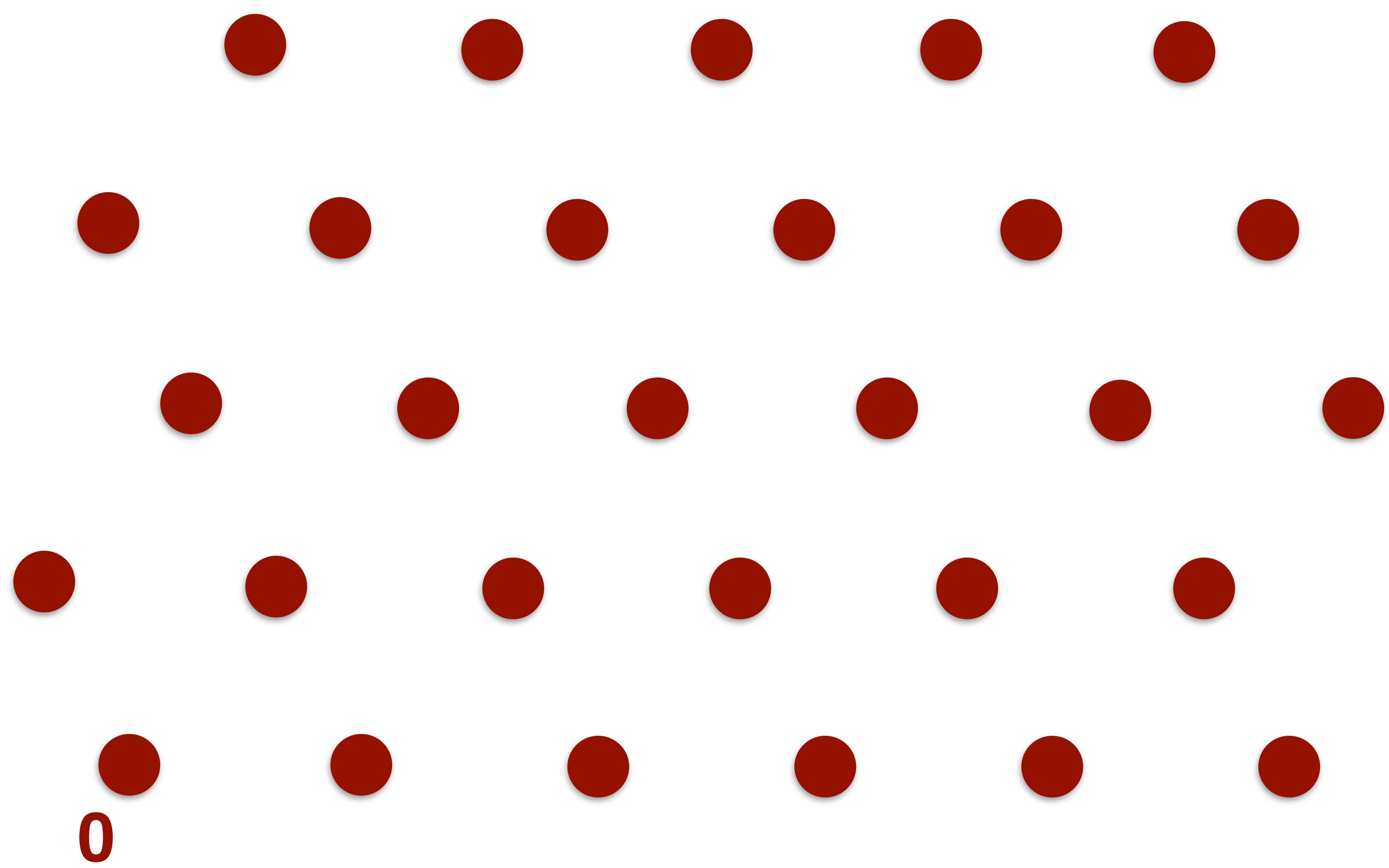


The Shortest Vector Problem



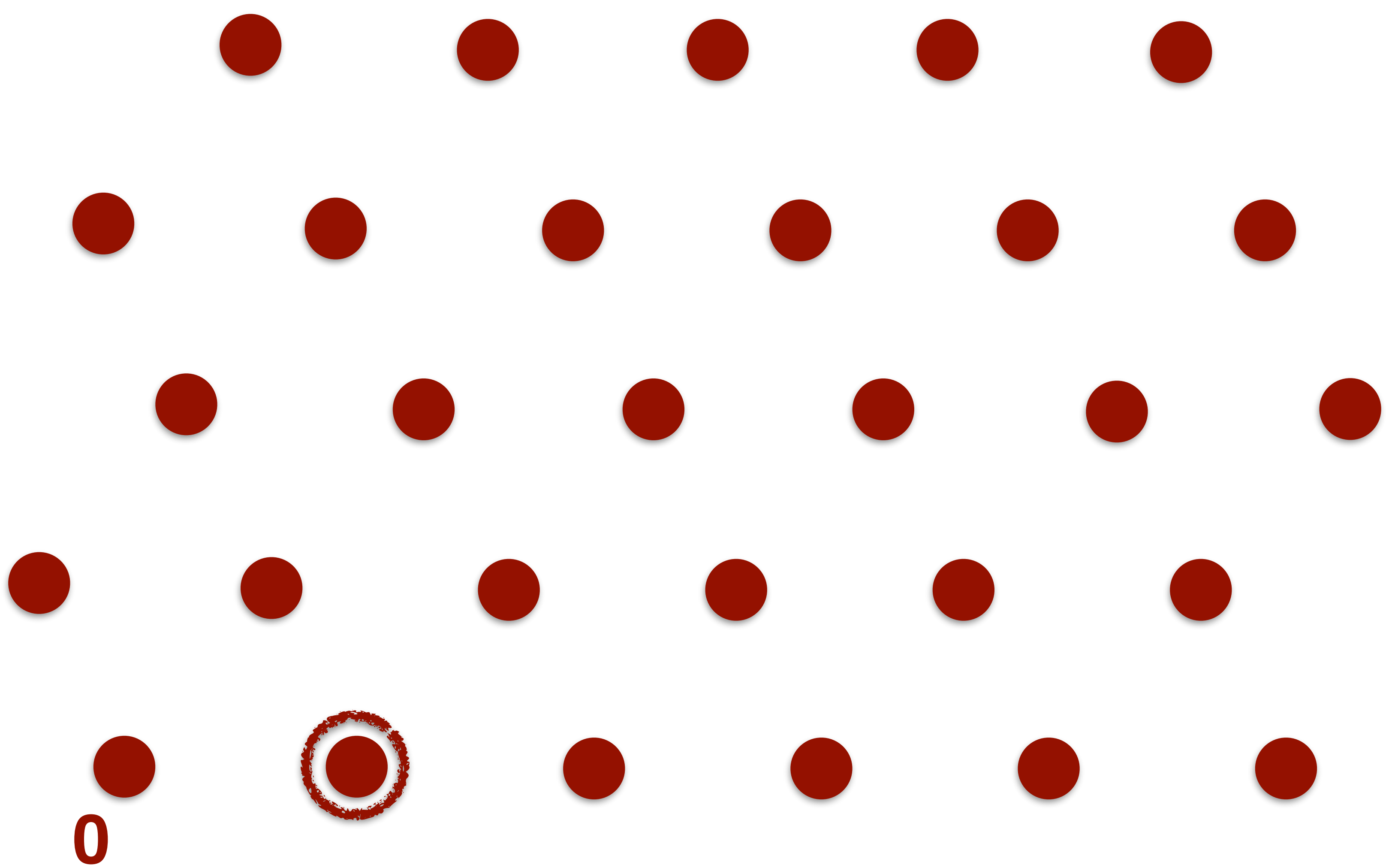
The Shortest Vector Problem

- $\text{SVP}(\mathcal{L}) =$ shortest non-zero $\mathbf{y} \in \mathcal{L}$



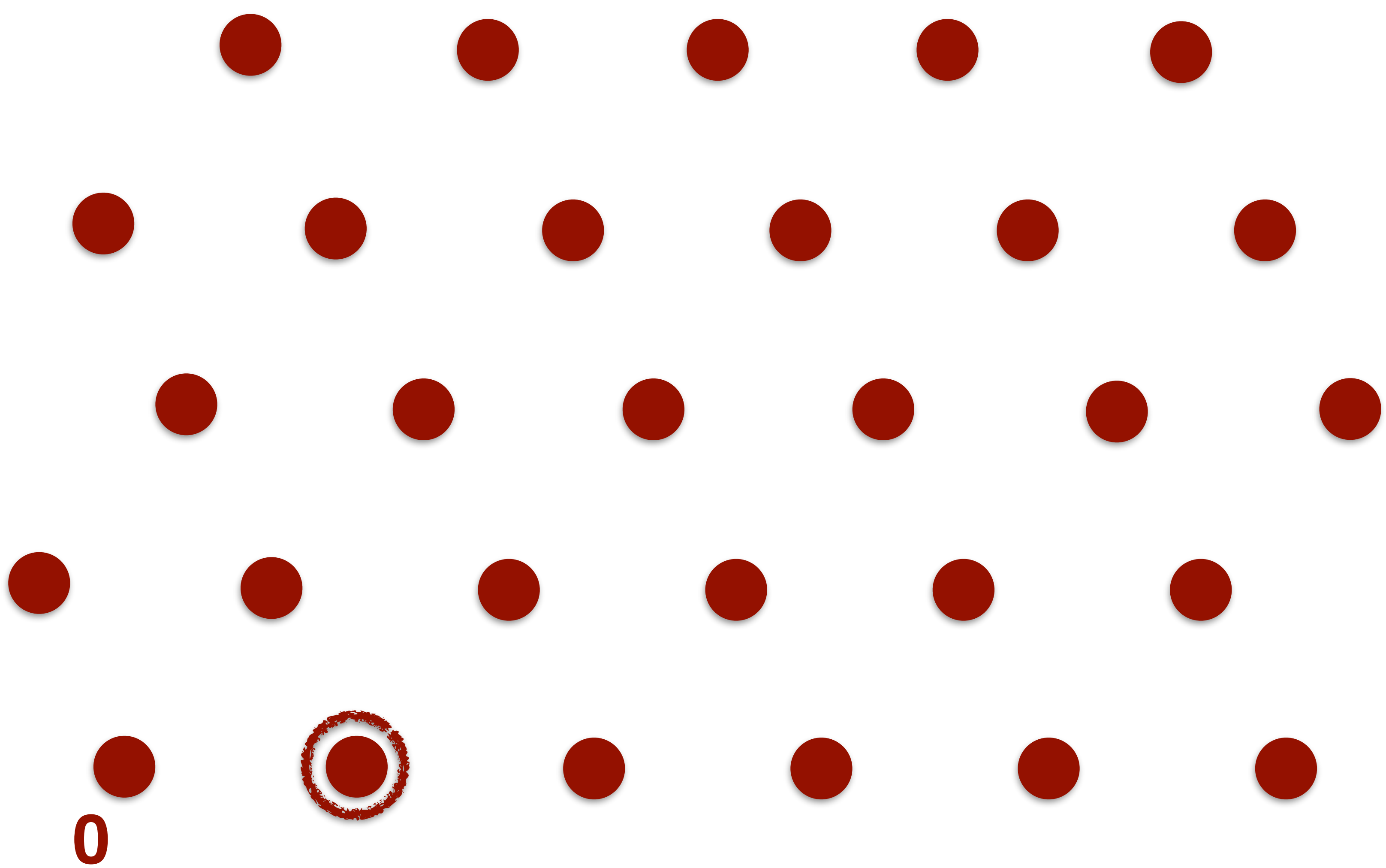
The Shortest Vector Problem

- $\text{SVP}(\mathcal{L}) =$ shortest non-zero $\mathbf{y} \in \mathcal{L}$



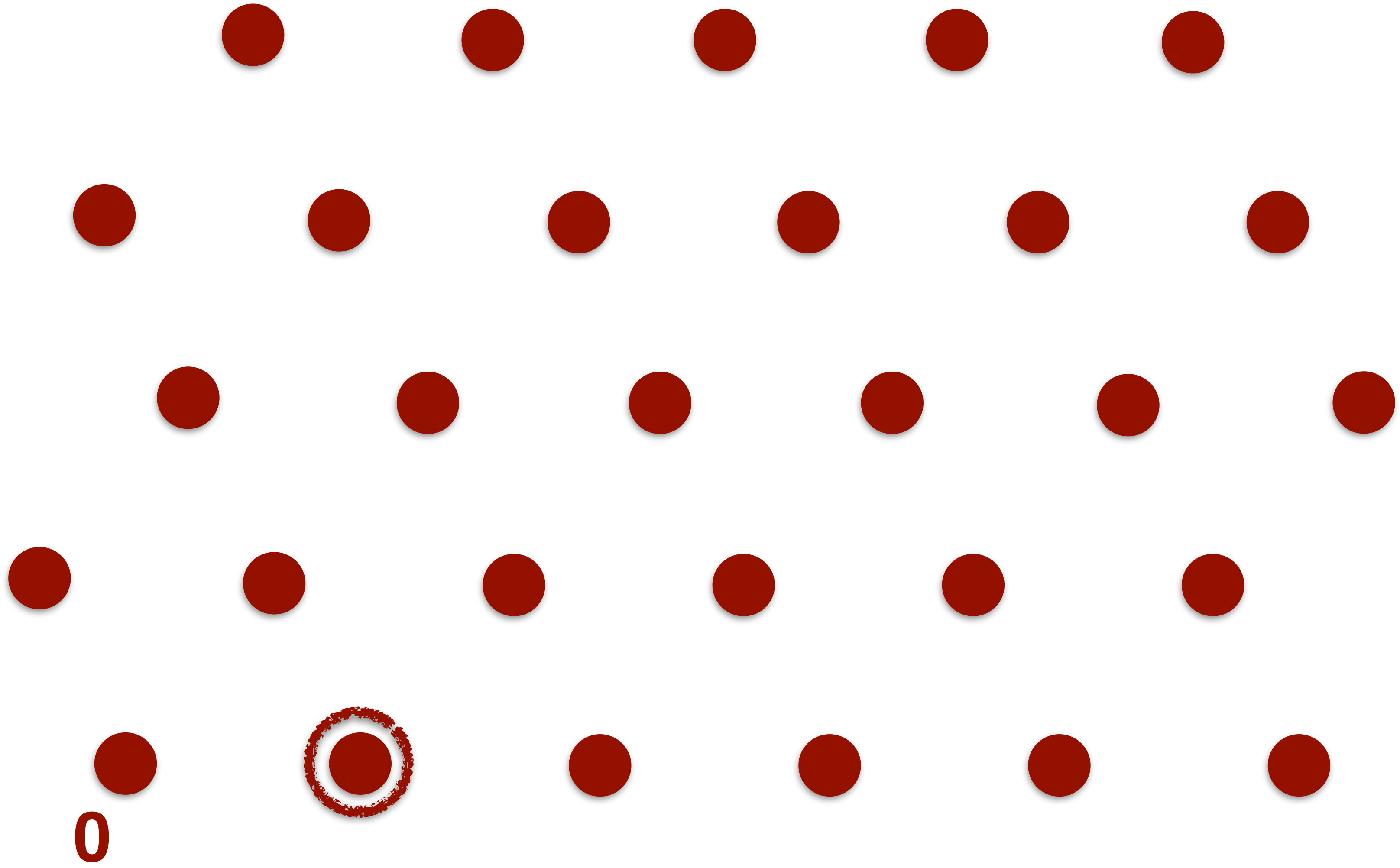
The Shortest Vector Problem

- $\mathrm{SVP}(\mathcal{L}) =$ shortest non-zero $\mathbf{y} \in \mathcal{L}$
- NP-hard (even to approximate).



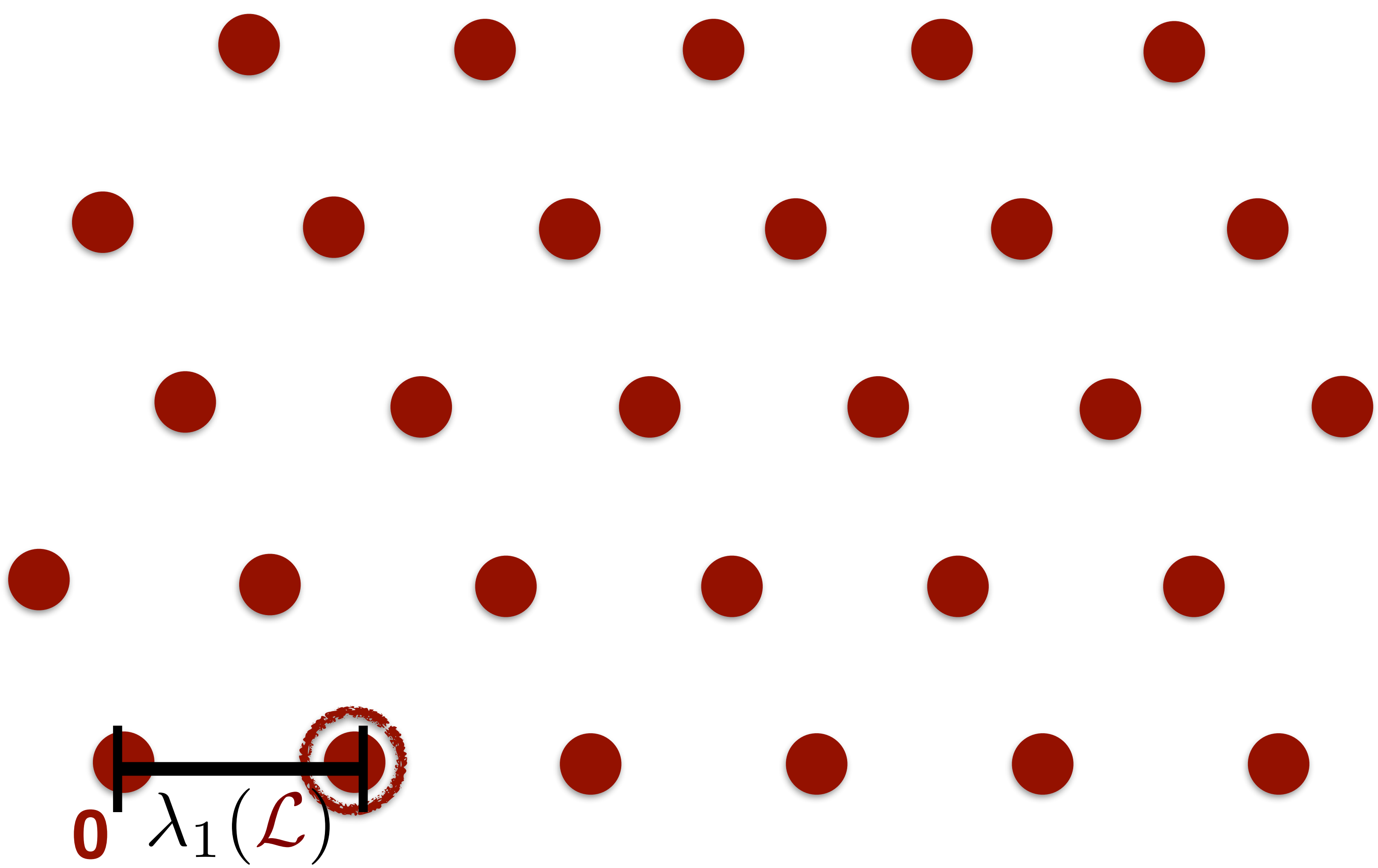
The Shortest Vector Problem

- $\text{SVP}(\mathcal{L}) =$ shortest non-zero $\mathbf{y} \in \mathcal{L}$
- NP-hard (even to approximate).
- $\lambda_1(\mathcal{L}) = ||\text{SVP}(\mathcal{L})||$



The Shortest Vector Problem

- $\text{SVP}(\mathcal{L}) =$ shortest non-zero $\mathbf{y} \in \mathcal{L}$
- NP-hard (even to approximate).
- $\lambda_1(\mathcal{L}) = ||\text{SVP}(\mathcal{L})||$



Progress on SVP

Progress on SVP

	Time	Space

Progress on SVP

	Time	**Space**
[Kan86] (Enumeration)	$n^{O(n)}$	$\mathrm{poly}(n)$

Progress on SVP

	Time	Space
[Kan86] (Enumeration)	$n^{O(n)}$	$\mathrm{poly}(n)$
[AKS01] (Sieving)	$2^{O(n)}$	$2^{O(n)}$

Progress on SVP

	Time	Space
[Kan86] (Enumeration)	$n^{O(n)}$	$\mathrm{poly}(n)$
[AKS01] (Sieving)	$2^{O(n)}$	$2^{O(n)}$
[NV08, PS09, MV10a, …]	$2^{2.465n+o(n)}$	$2^{1.233n+o(n)}$

Progress on SVP

	Time	Space
[Kan86] (Enumeration)	$n^{O(n)}$	$\text{poly}(n)$
[AKS01] (Sieving)	$2^{O(n)}$	$2^{O(n)}$
[NV08, PS09, MV10a, …]	$2^{2.465n+o(n)}$	$2^{1.233n+o(n)}$
[MV10b] (Voronoi cell, deterministic, CVP)	$2^{2n+o(n)}$	$2^{n+o(n)}$

Progress on SVP

	Time	**Space**
[Kan86] (Enumeration)	$n^{O(n)}$	$\mathrm{poly}(n)$
[AKS01] (Sieving)	$2^{O(n)}$	$2^{O(n)}$
[NV08, PS09, MV10a, …]	$2^{2.465n+o(n)}$	$2^{1.233n+o(n)}$
[MV10b] (Voronoi cell, deterministic, CVP)	$2^{2n+o(n)}$	$2^{n+o(n)}$
This work (Discrete Gaussian sampling)	$2^{n+o(n)}$	$2^{n+o(n)}$

Our Algorithm

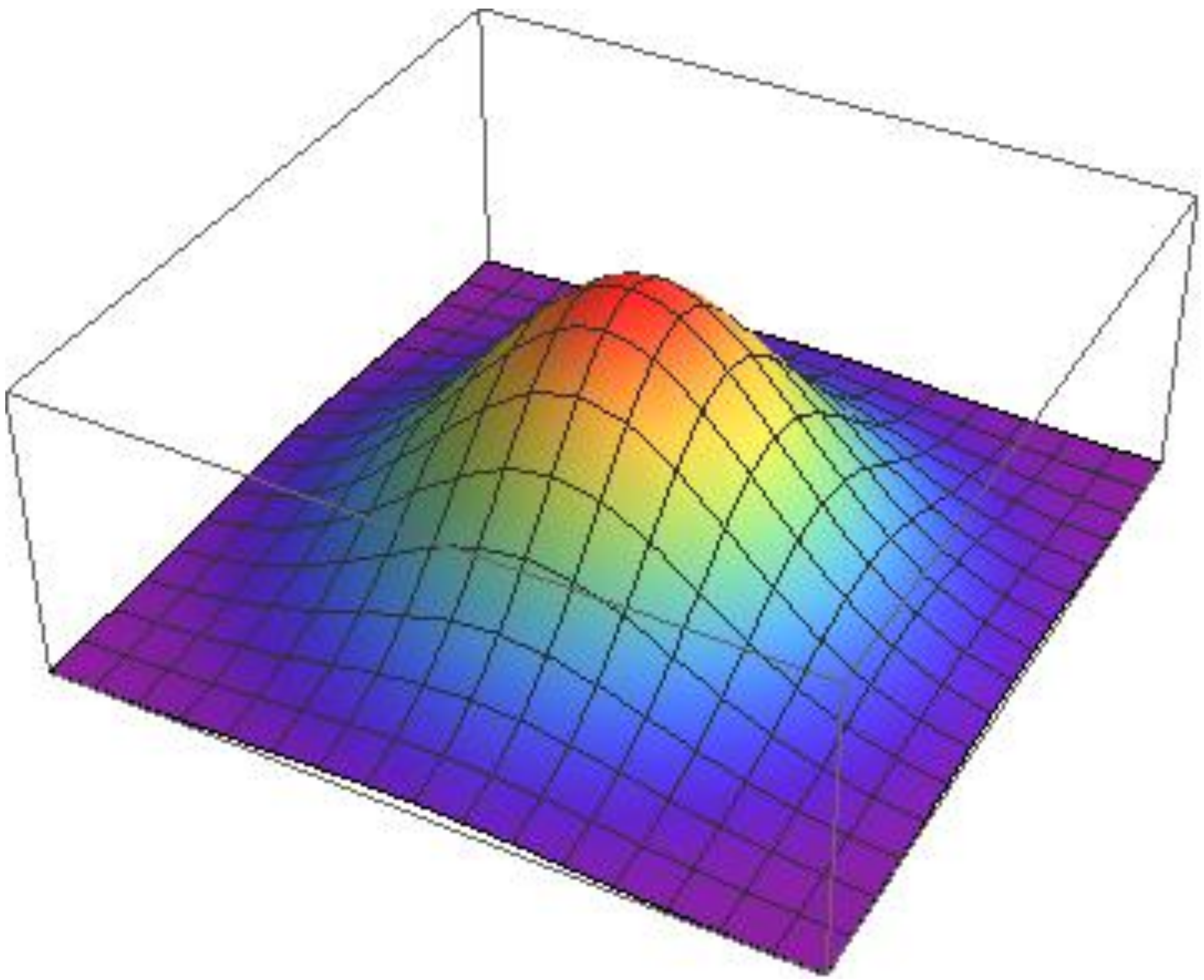
Gaussian Distribution

Gaussian Distribution

$$\mathsf{Gauss}(s) := \Pr[\mathbf{x}] \propto e^{-\|\mathbf{x}\|^2/s^2}$$

Gaussian Distribution

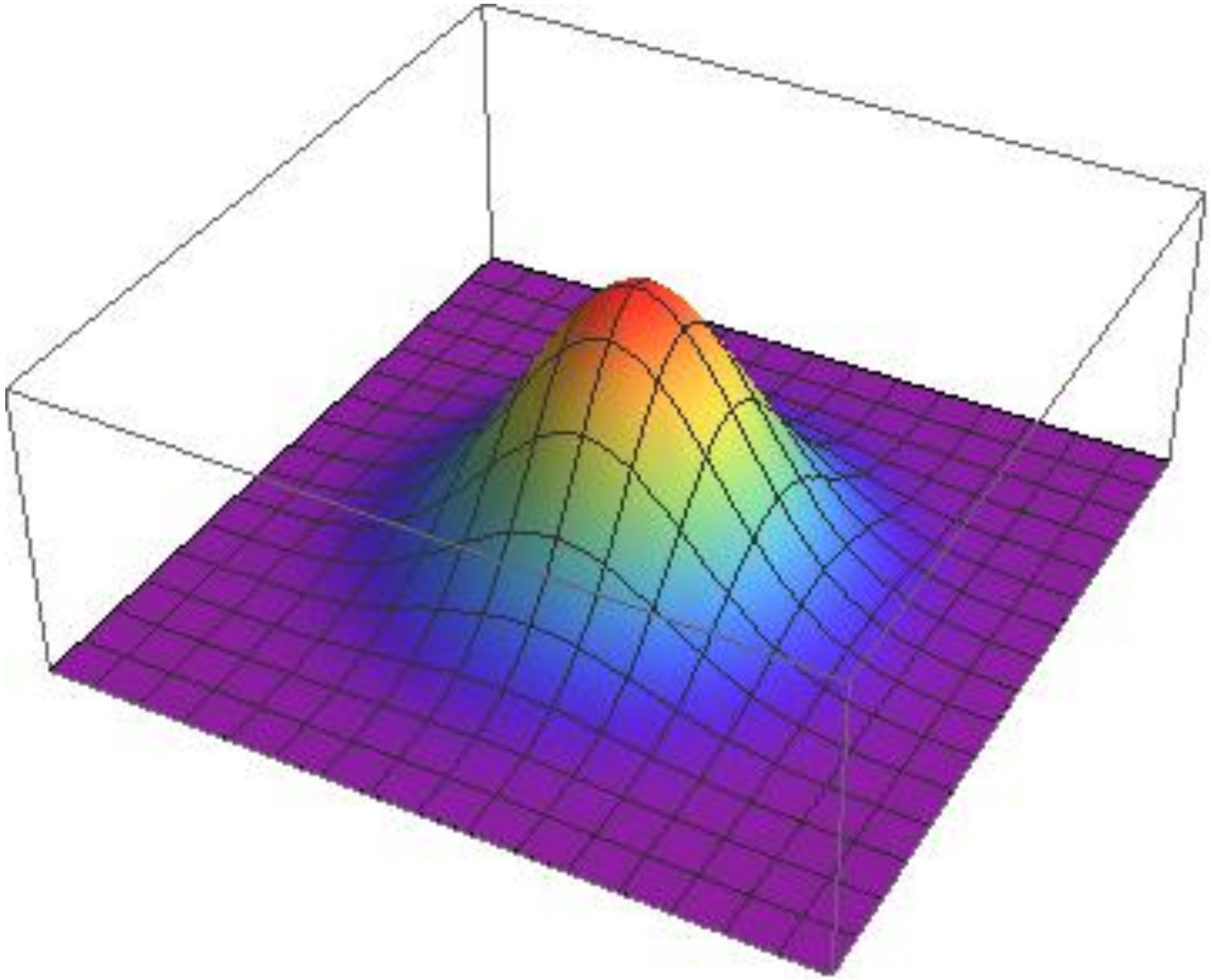
$$\text{Gauss}(s) := \Pr[\mathbf{x}] \propto e^{-\|\mathbf{x}\|^2/s^2}$$



$s = 20$

Gaussian Distribution

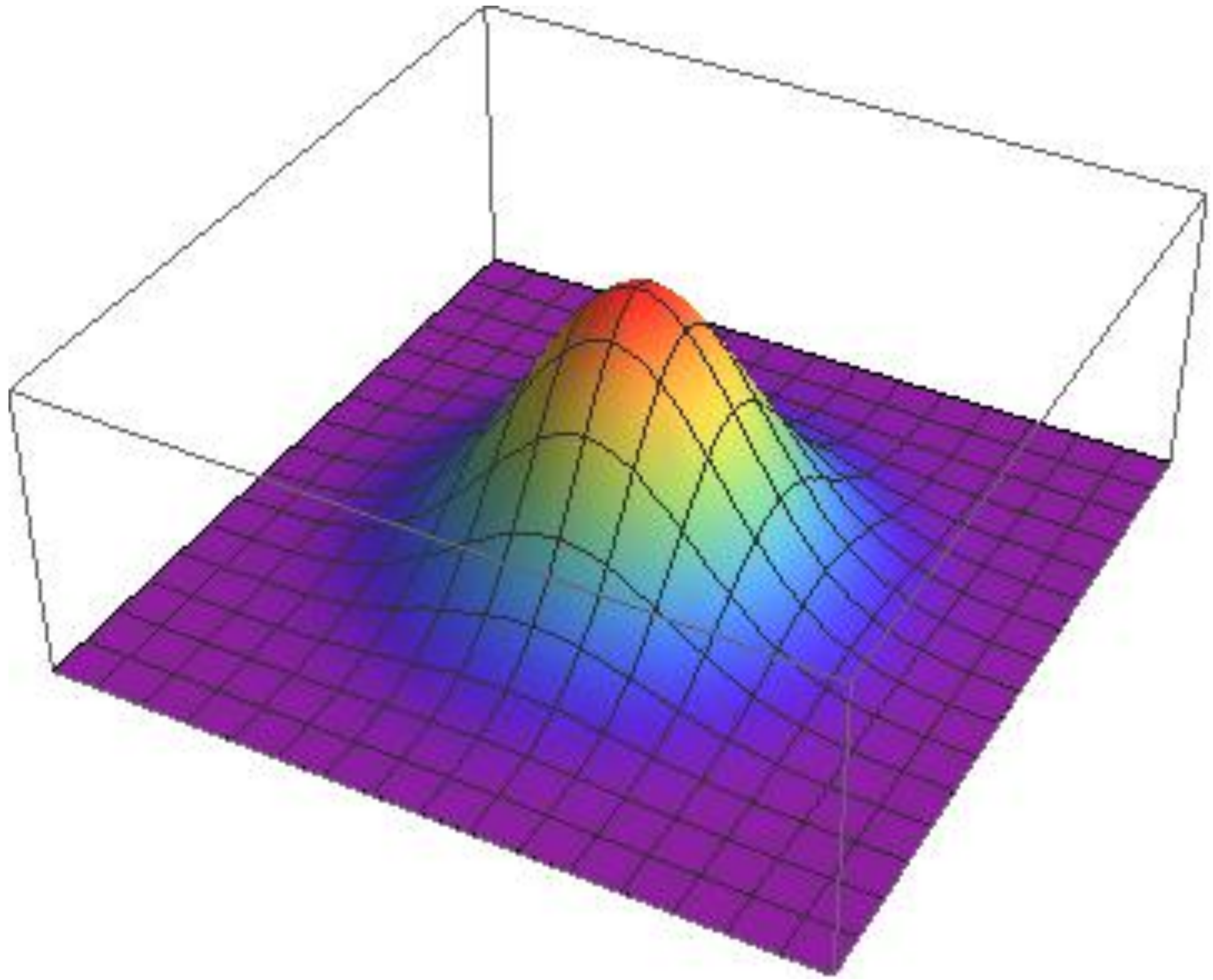
$$\text{Gauss}(s) := \Pr[\mathbf{x}] \propto e^{-\|\mathbf{x}\|^2/s^2}$$



$s = 10$

Gaussian Distribution

$$\text{Gauss}(s) := \Pr[\mathbf{x}] \propto e^{-\|\mathbf{x}\|^2/s^2}$$



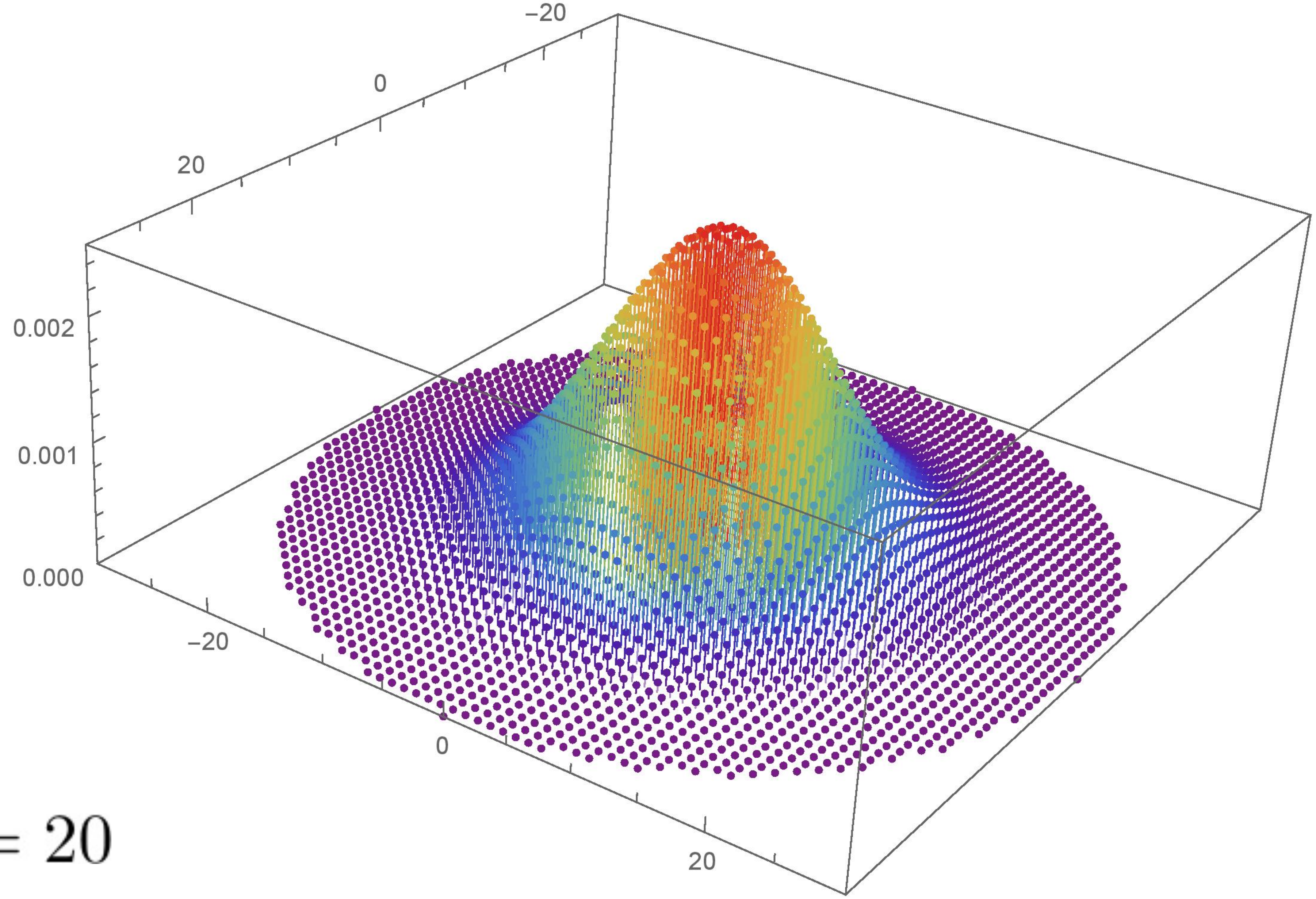
$s = 10$

Discrete Gaussian Distribution

$$D_{\mathcal{L},s} := \Pr[\mathbf{y}] \propto e^{-\|\mathbf{y}\|^2/s^2}$$

Discrete Gaussian Distribution

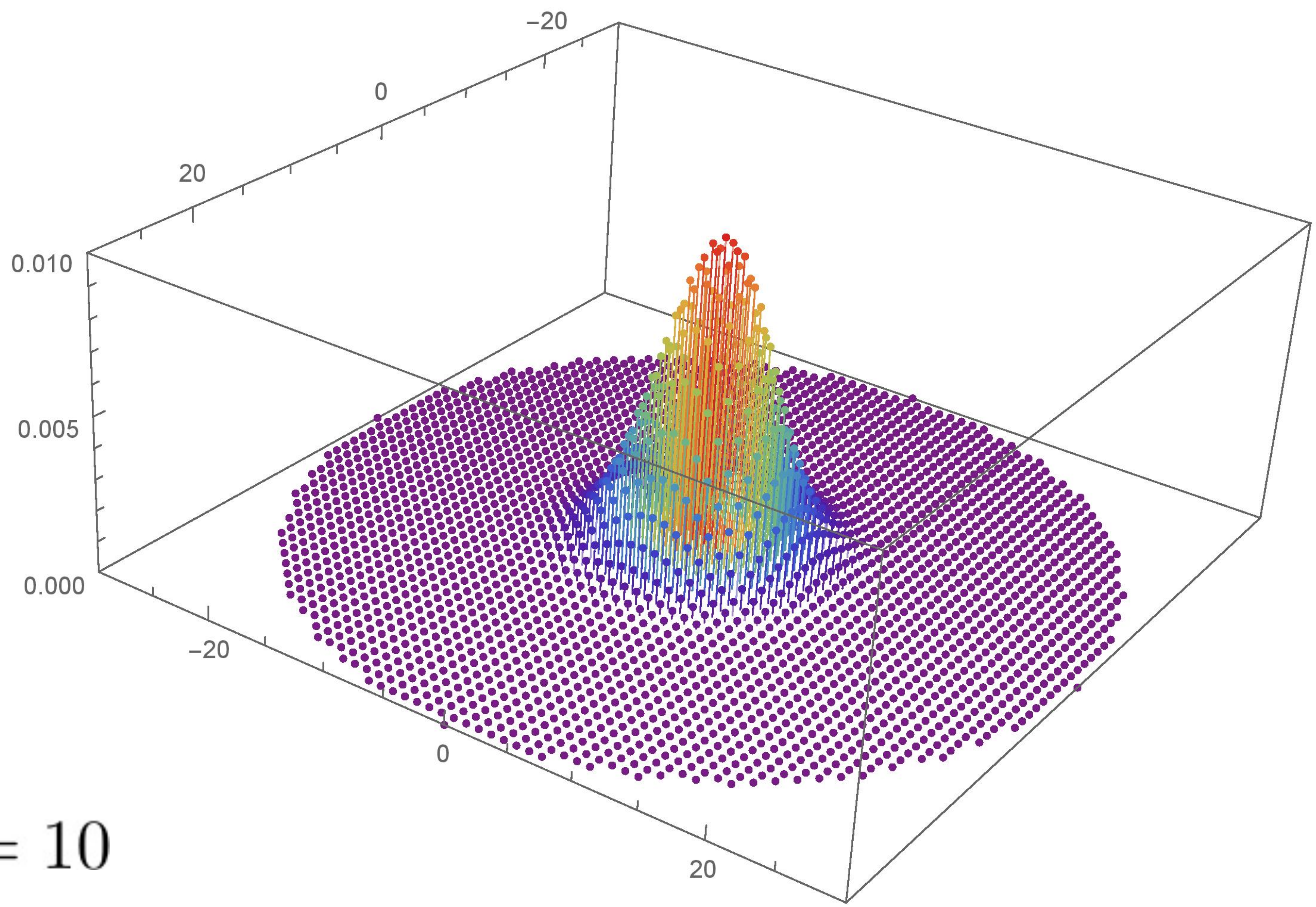
$$D_{\mathcal{L},s} := \Pr[\mathbf{y}] \propto e^{-\|\mathbf{y}\|^2/s^2}$$



$s = 20$

Discrete Gaussian Distribution

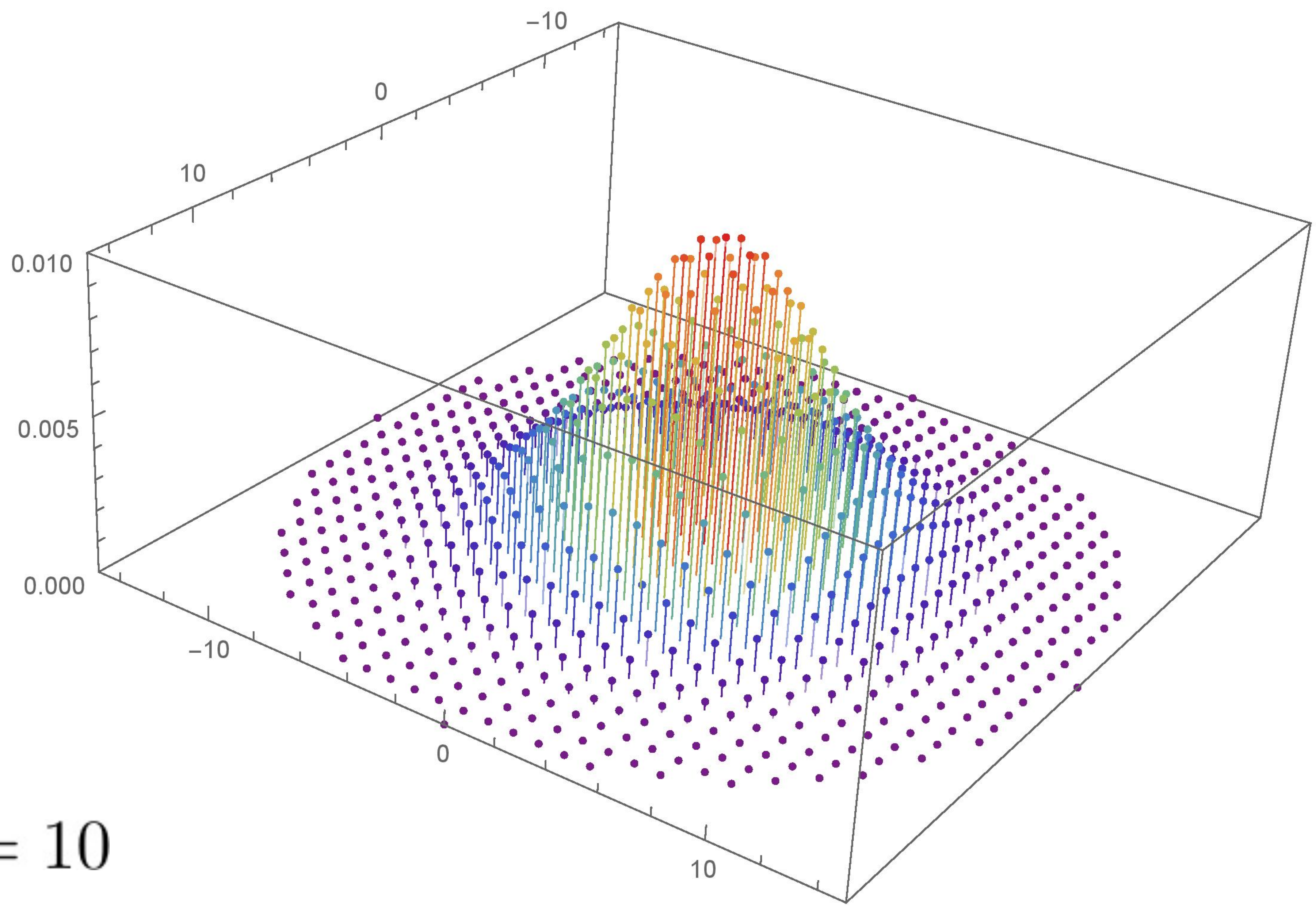
$$D_{\mathcal{L},s} := \Pr[\mathbf{y}] \propto e^{-\|\mathbf{y}\|^2/s^2}$$



$s = 10$

Discrete Gaussian Distribution

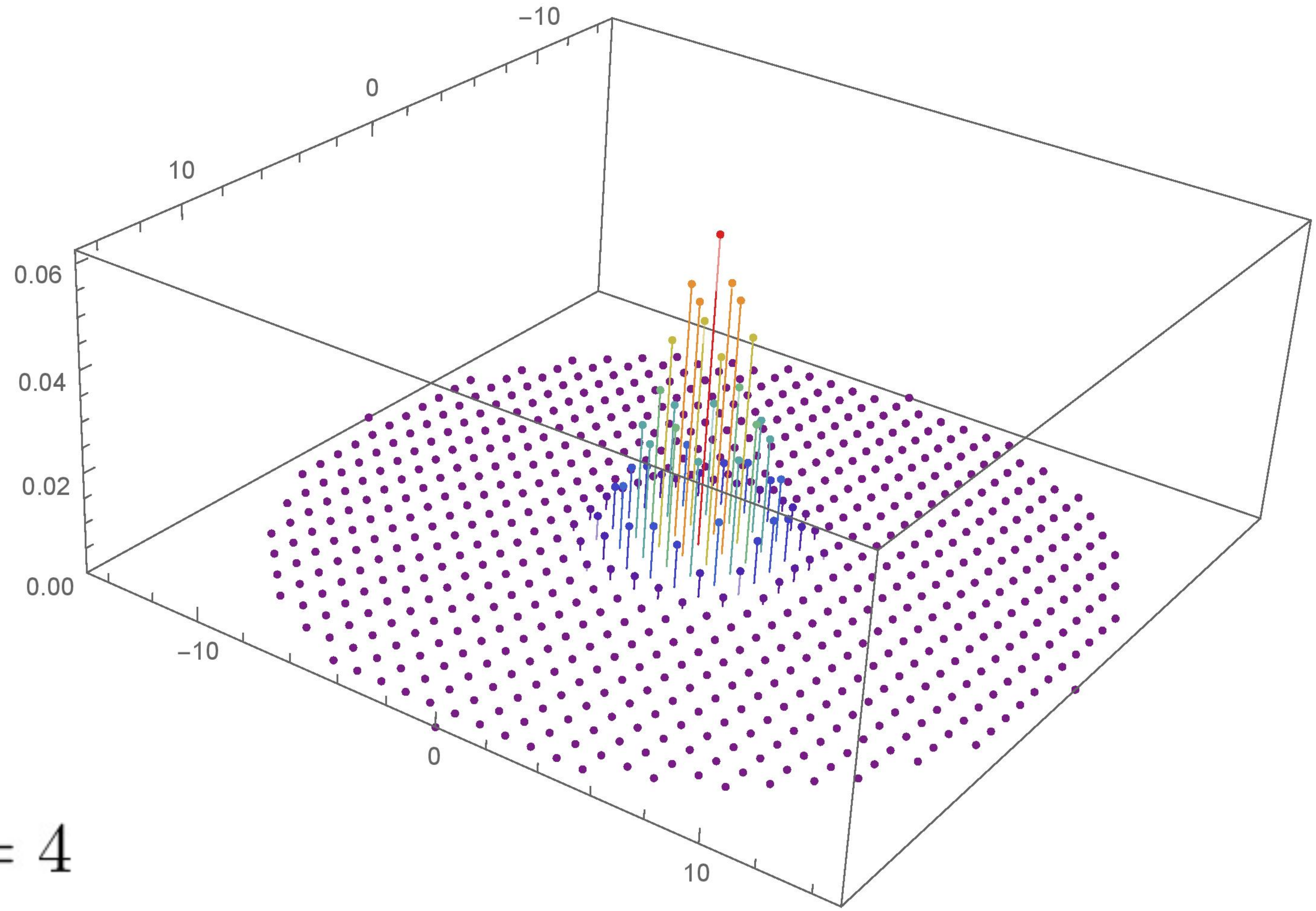
$$D_{\mathcal{L},s} := \Pr[\mathbf{y}] \propto e^{-\|\mathbf{y}\|^2/s^2}$$



$s = 10$

Discrete Gaussian Distribution

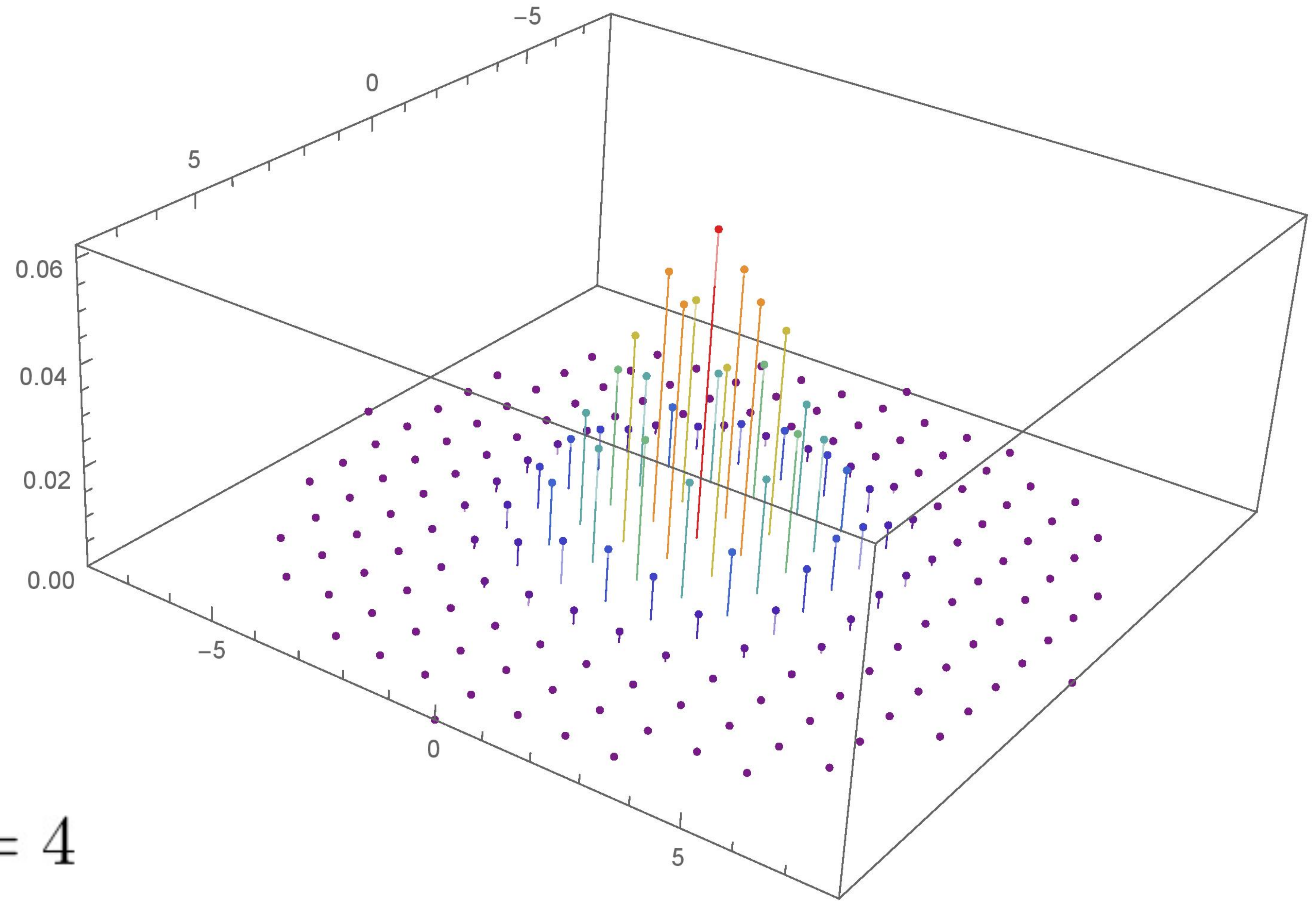
$$D_{\mathcal{L},s} := \Pr[\mathbf{y}] \propto e^{-\|\mathbf{y}\|^2/s^2}$$



$s = 4$

Discrete Gaussian Distribution

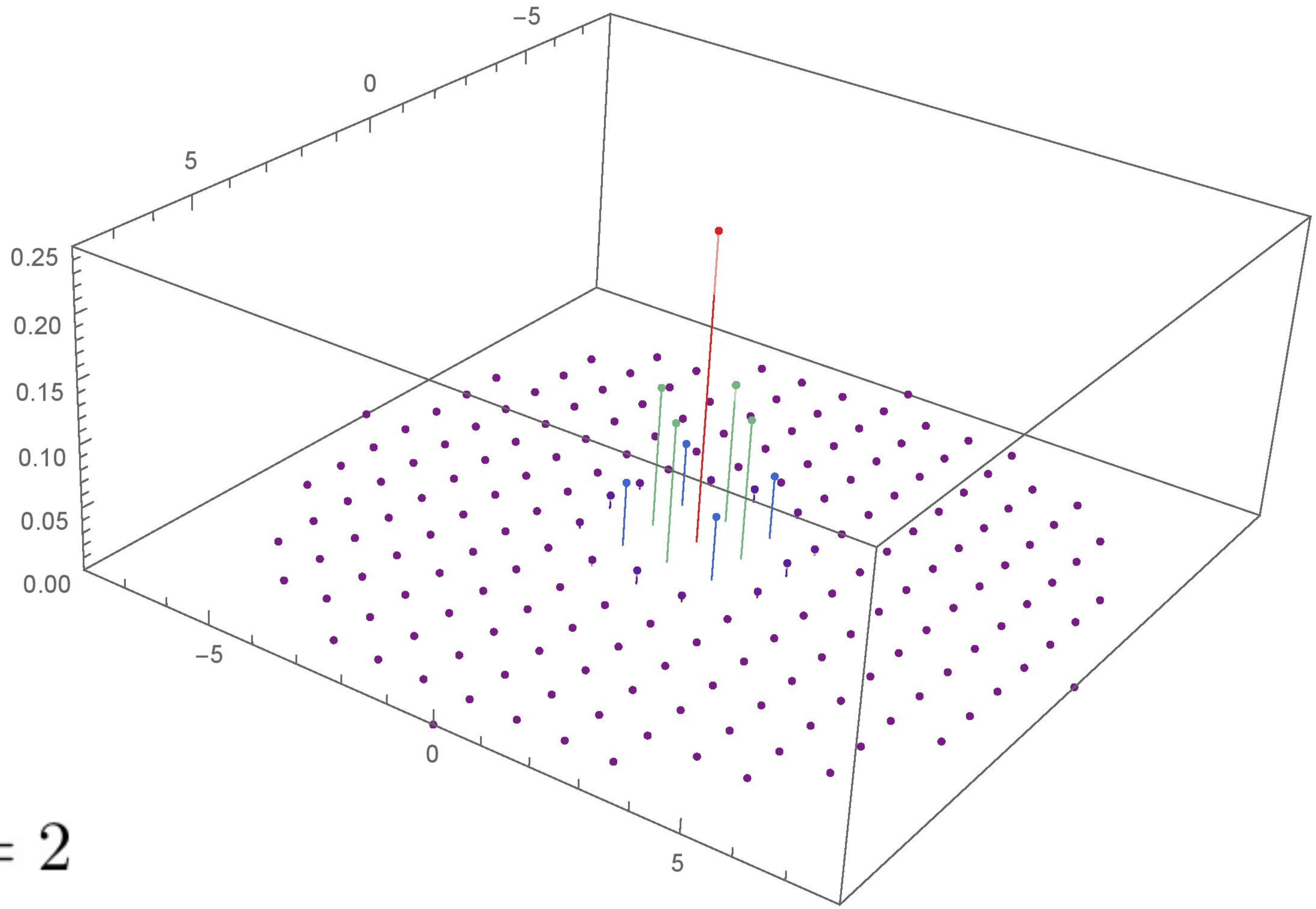
$$D_{\mathcal{L},s} := \Pr[\mathbf{y}] \propto e^{-\|\mathbf{y}\|^2/s^2}$$



$s = 4$

Discrete Gaussian Distribution

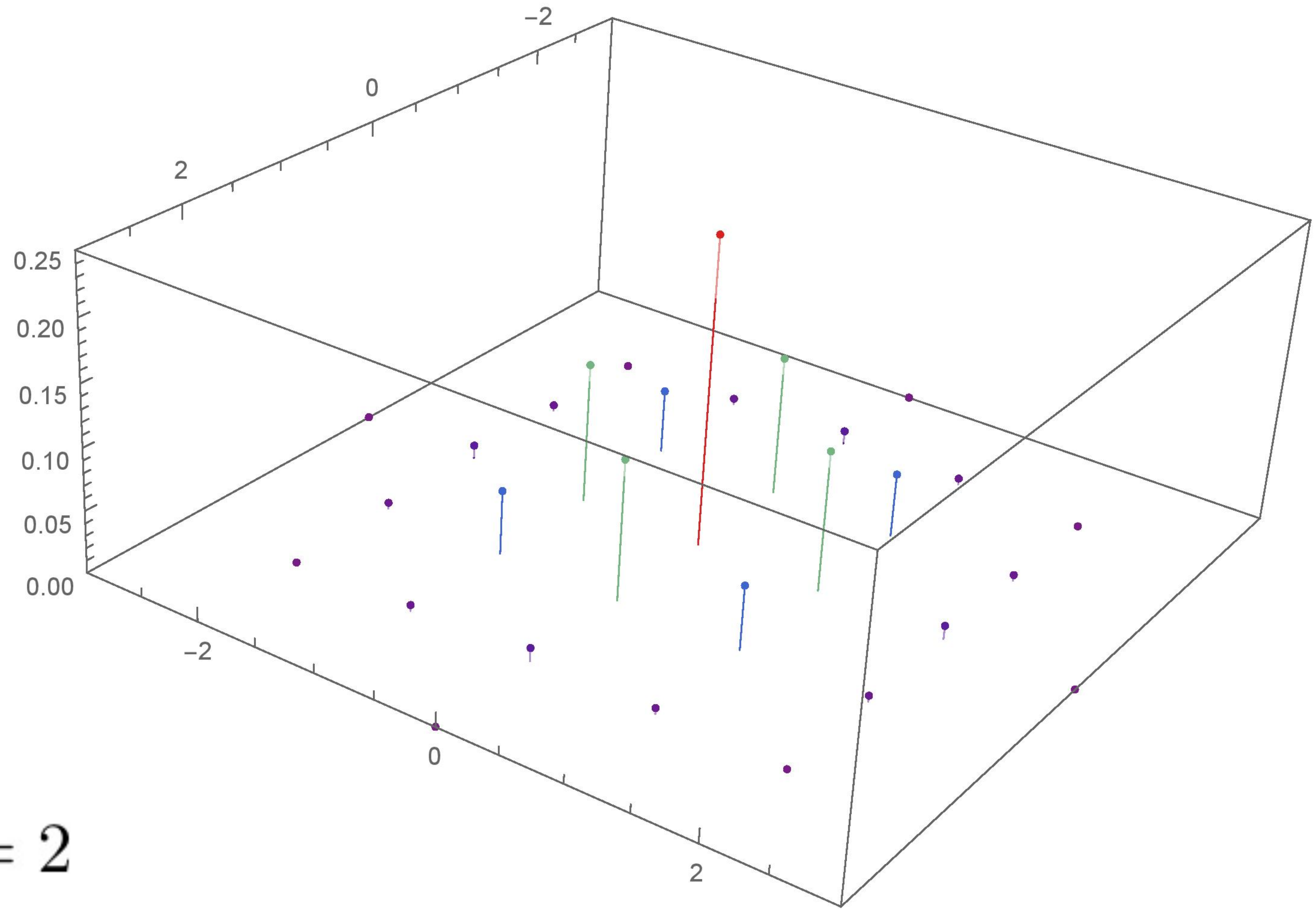
$$D_{\mathcal{L},s} := \Pr[\mathbf{y}] \propto e^{-\|\mathbf{y}\|^2/s^2}$$



$s = 2$

Discrete Gaussian Distribution

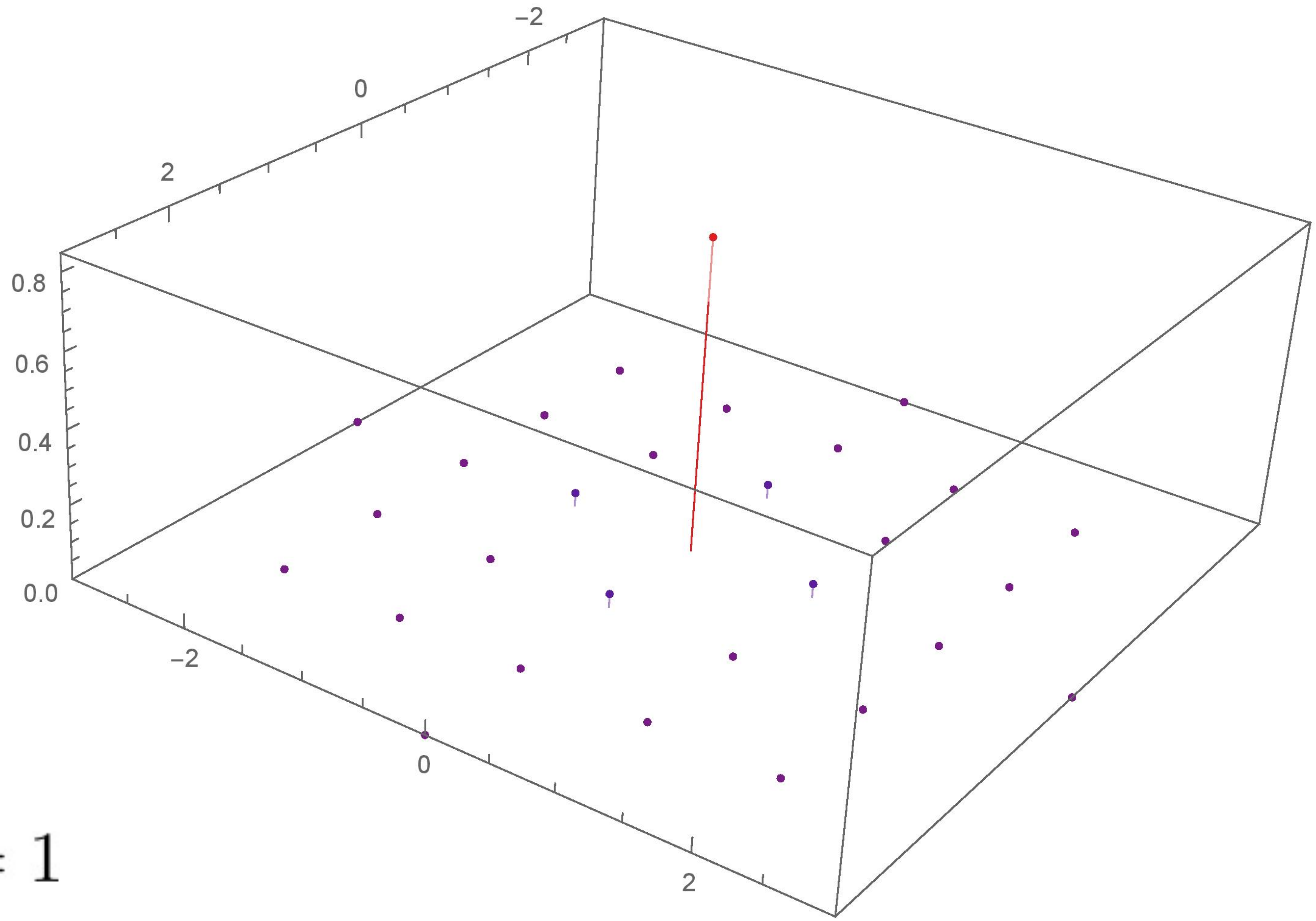
$$D_{\mathcal{L},s} := \Pr[\mathbf{y}] \propto e^{-\|\mathbf{y}\|^2/s^2}$$



$s = 2$

Discrete Gaussian Distribution

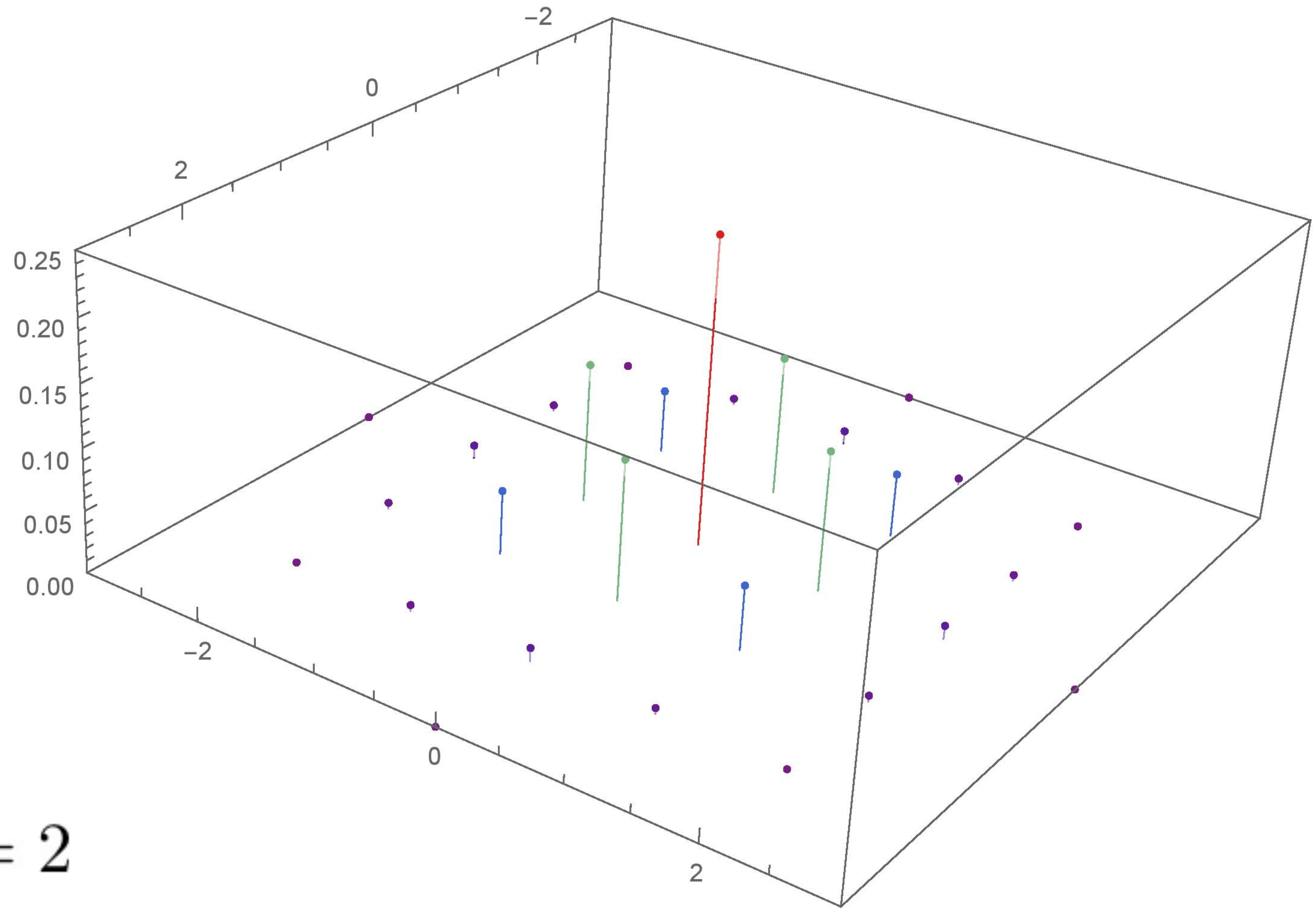
$$D_{\mathcal{L},s} := \Pr[\mathbf{y}] \propto e^{-\|\mathbf{y}\|^2/s^2}$$



$s = 1$

Discrete Gaussian Distribution

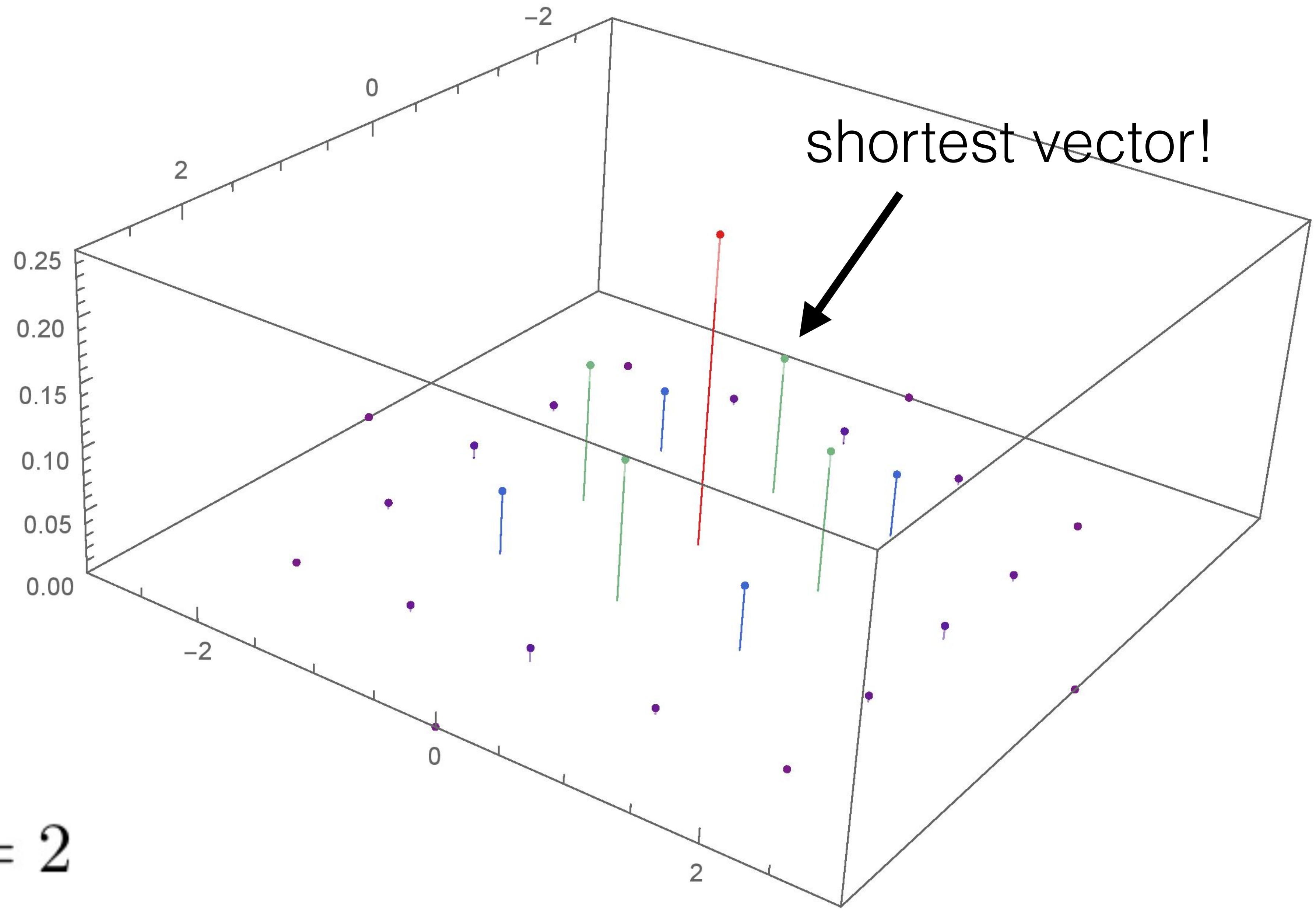
$$D_{\mathcal{L},s} := \Pr[\mathbf{y}] \propto e^{-\|\mathbf{y}\|^2/s^2}$$



$s = 2$

Discrete Gaussian Distribution

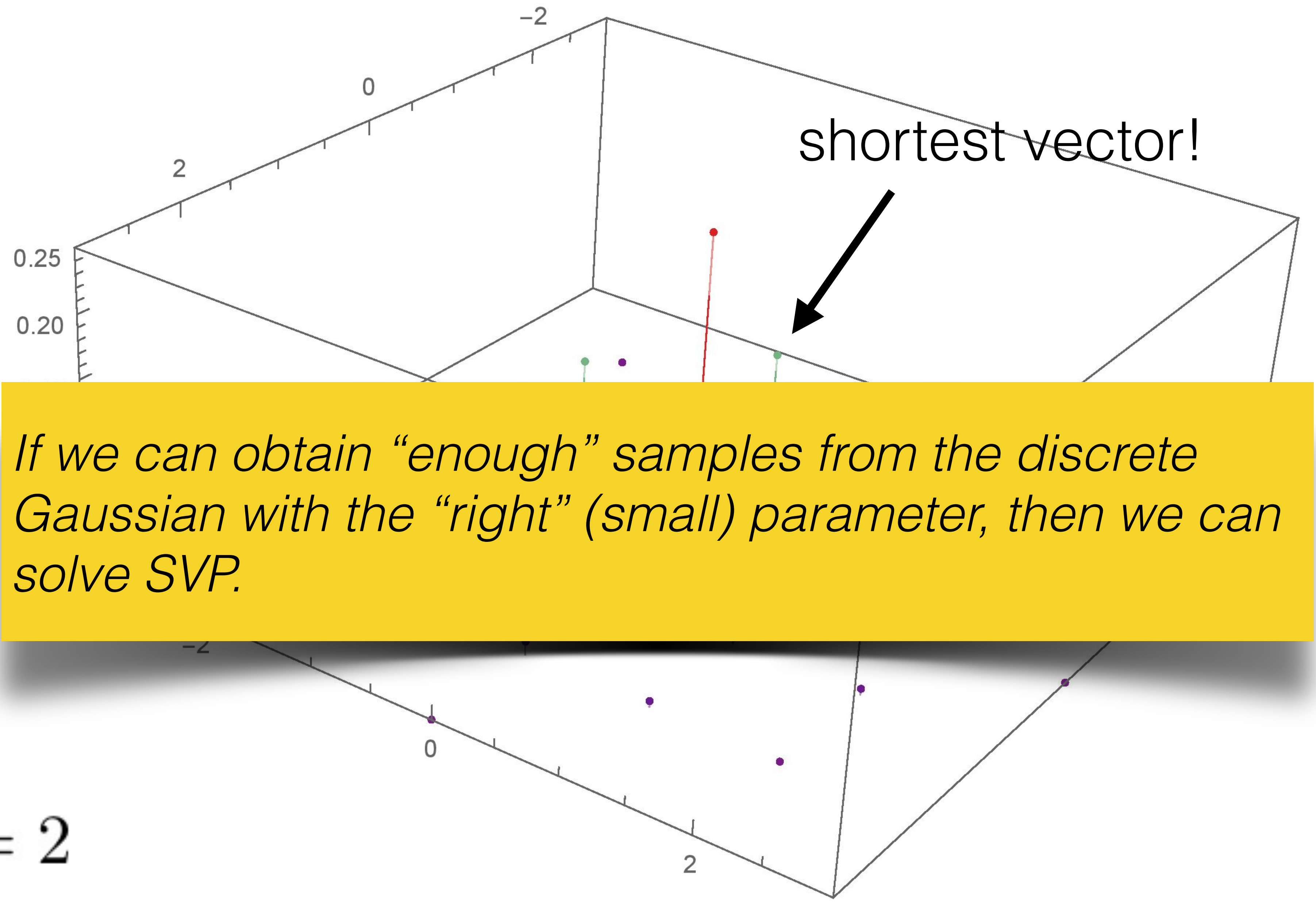
$$D_{\mathcal{L},s} := \Pr[\mathbf{y}] \propto e^{-\|\mathbf{y}\|^2/s^2}$$



$s = 2$

Discrete Gaussian Distribution

$$D_{\mathcal{L},s} := \Pr[\mathbf{y}] \propto e^{-\|\mathbf{y}\|^2/s^2}$$



If we can obtain "enough" samples from the discrete Gaussian with the "right" (small) parameter, then we can solve SVP.

$s = 2$

Discrete Gaussian Distribution

We need at most $\approx 1.38^n$ vectors with $s \approx \lambda_1(\mathcal{L})/\sqrt{n}$ [KL78].

Discrete Gaussian Distribution

We need at most $\approx 1.38^n$ vectors with $s \approx \lambda_1(\mathcal{L})/\sqrt{n}$ [KL78].

$D_{\mathcal{L},s}$ is very well-studied for very high parameters $s \gg \lambda_1(\mathcal{L})$, above the “smoothing parameter.”

Discrete Gaussian Distribution

We need at most $\approx 1.38^n$ vectors with $s \approx \lambda_1(\mathcal{L})/\sqrt{n}$ [KL78].

$D_{\mathcal{L},s}$ is very well-studied for very high parameters $s \gg \lambda_1(\mathcal{L})$, above the "smoothing parameter."

[GPV08] show how to sample in this regime in polynomial time.

Discrete Gaussian Distribution

We need at most $\approx 1.38^n$ vectors with $s \approx \lambda_1(\mathcal{L})/\sqrt{n}$ [KL78].

$D_{\mathcal{L},s}$ is very well-studied for very high parameters $s \gg \lambda_1(\mathcal{L})$, above the "smoothing parameter."

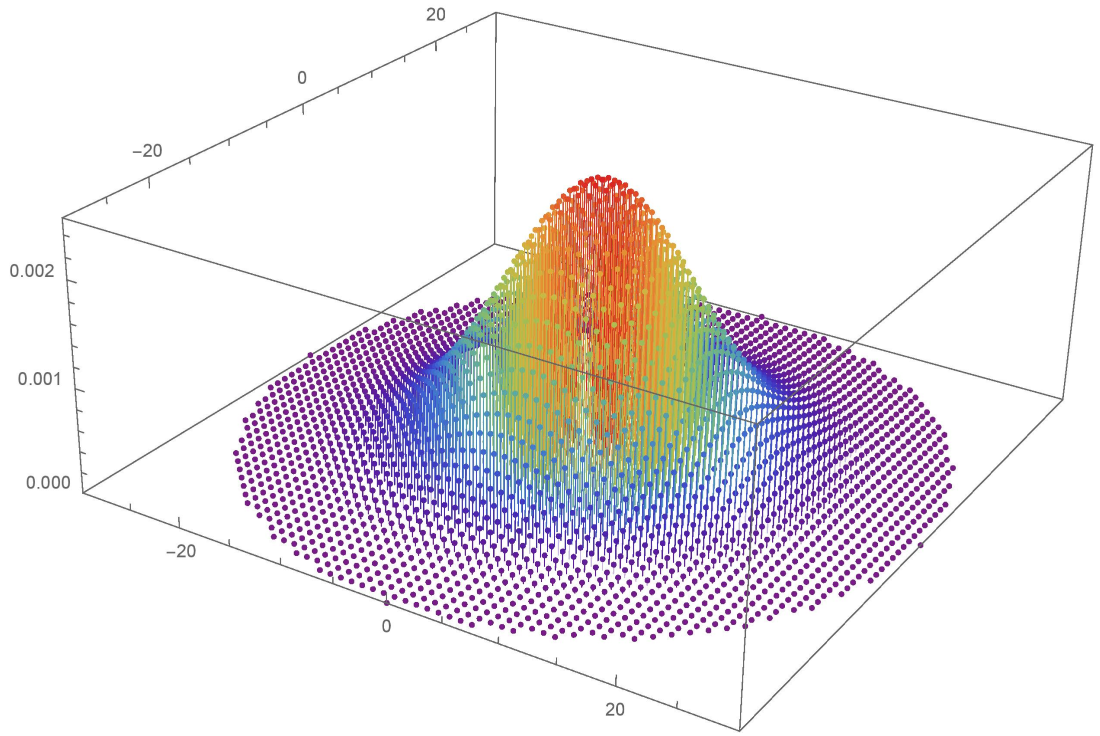
[GPV08] show how to sample in this regime in polynomial time.

(Previously could not do much better, even in exponential time.)

Discrete Gaussian Distribution

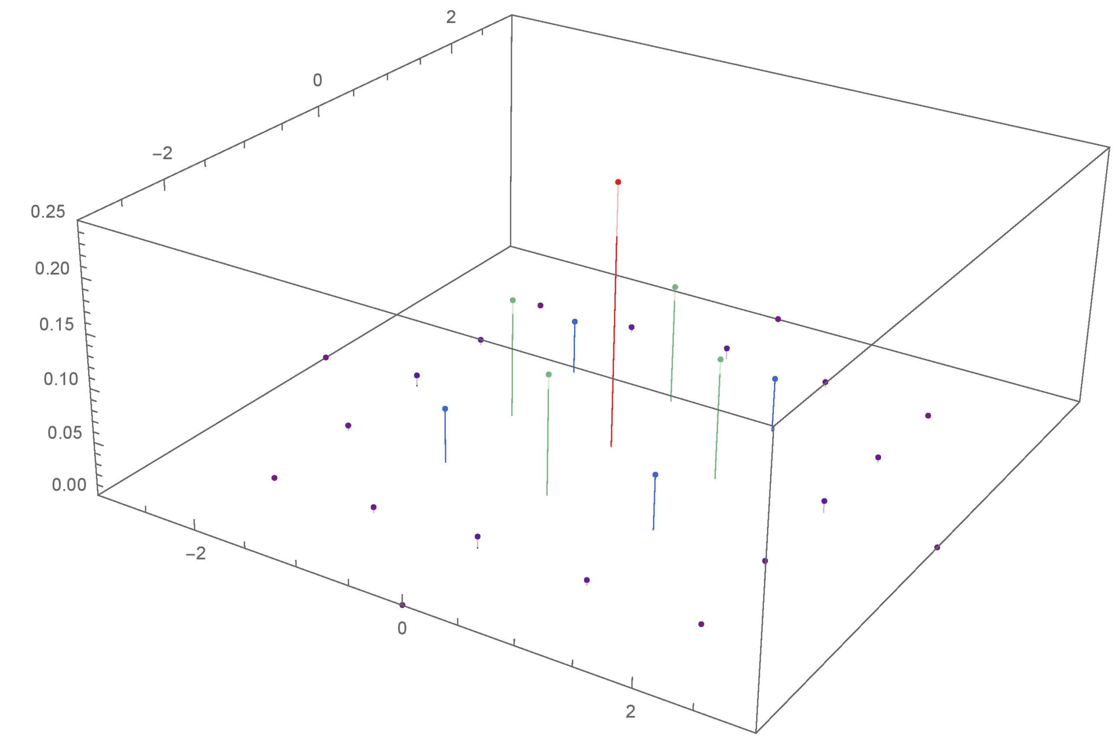
Easy

[GPV08]



$$s \gg \lambda_1(\mathcal{L})$$

Hard

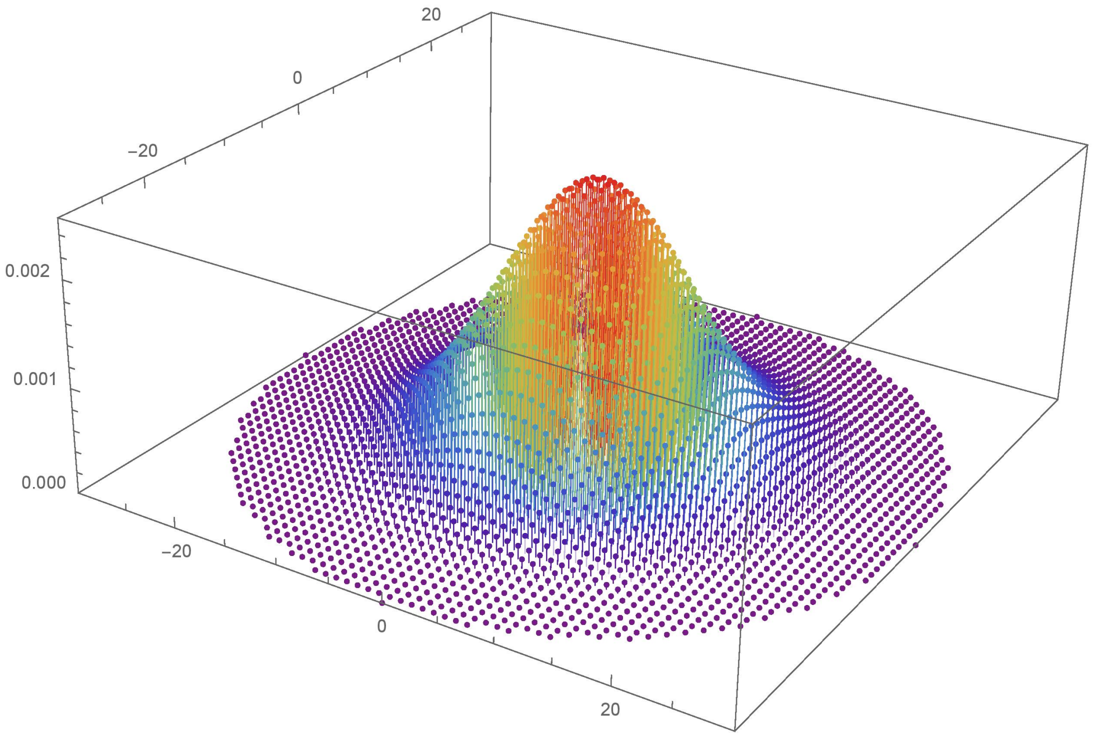


$$s \approx \lambda_1(\mathcal{L})/\sqrt{n}$$

Discrete Gaussian Distribution

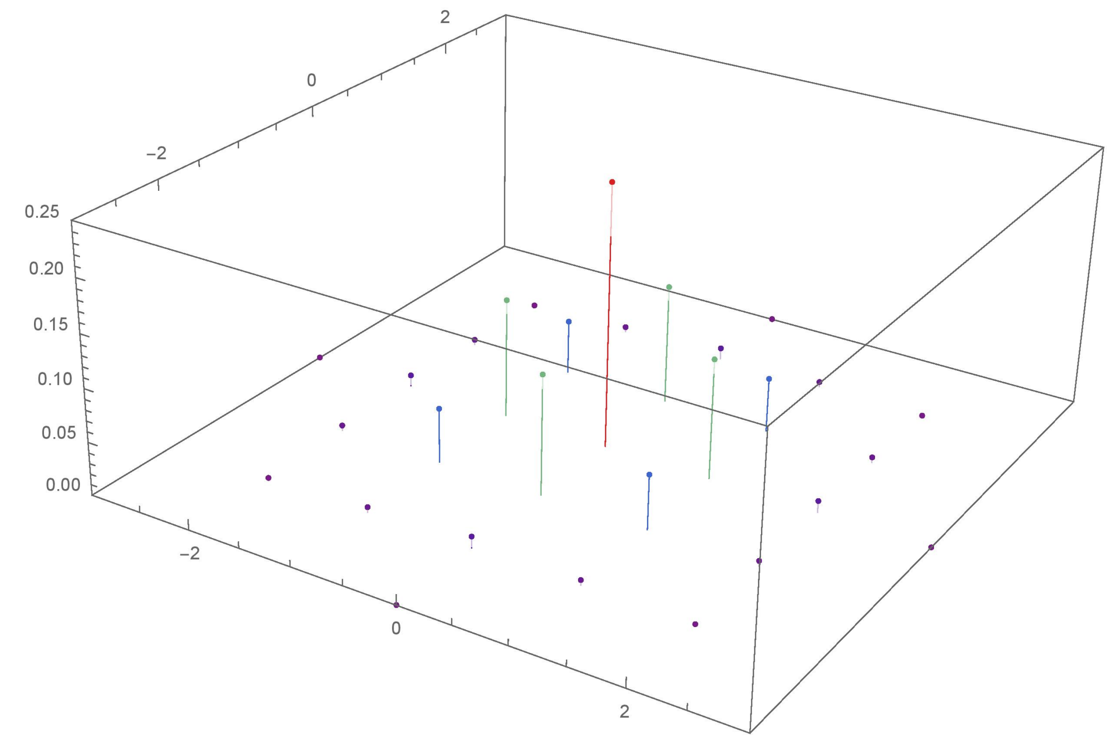
Easy

[GPV08]



$$s \gg \lambda_1(\mathcal{L})$$

Hard



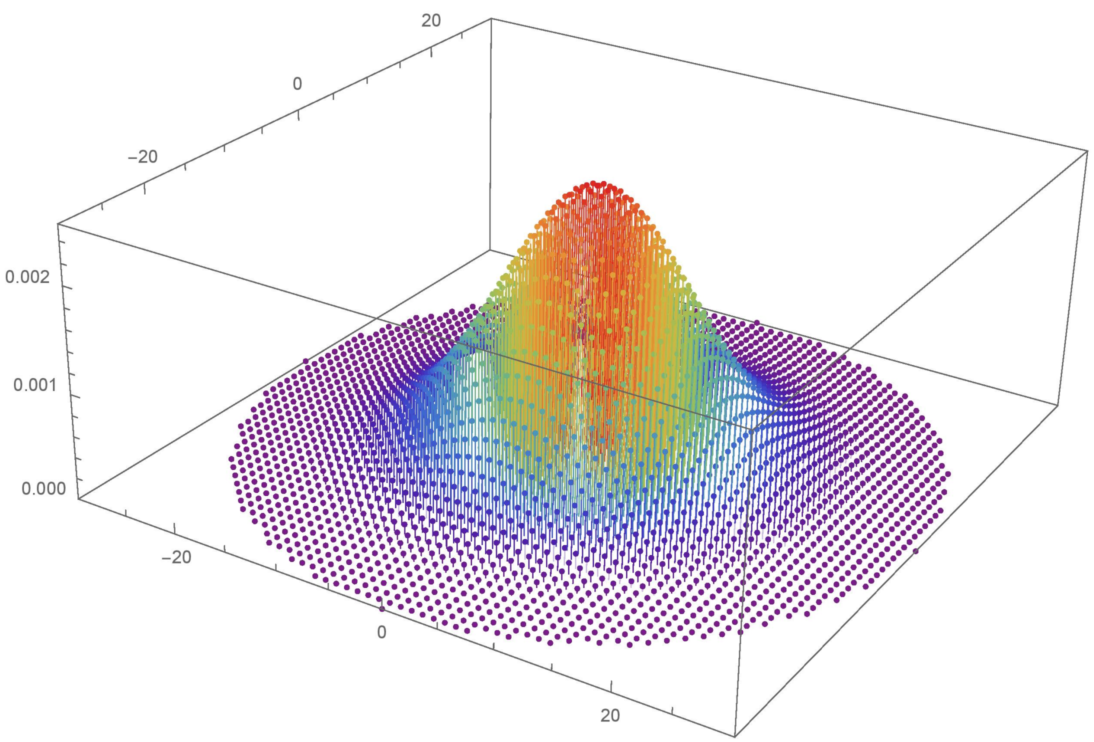
$$s \approx \lambda_1(\mathcal{L})/\sqrt{n}$$

Can we use samples from the LHS to get samples from the RHS?

Discrete Gaussian Distribution

Easy

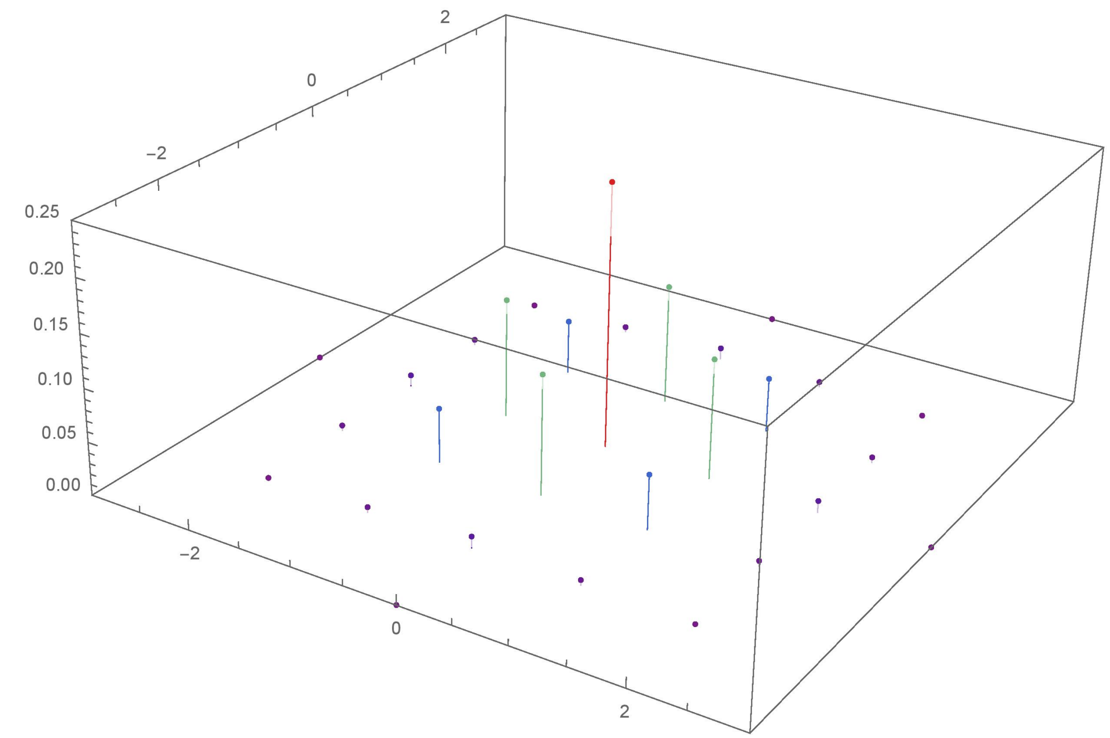
[GPV08]



$s \gg \lambda_1(\mathcal{L})$

Our goal

Hard



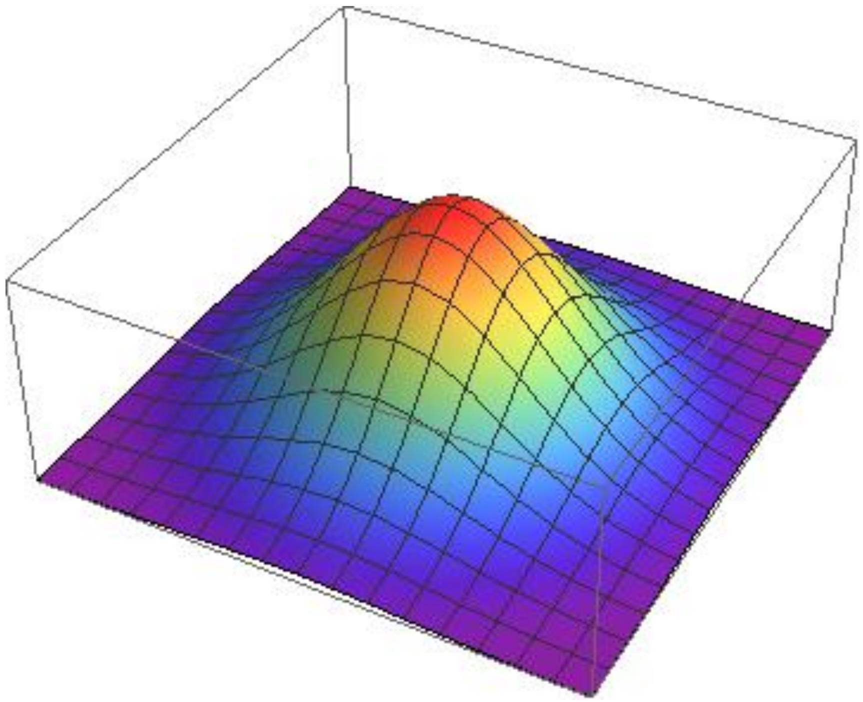
$s \approx \lambda_1(\mathcal{L})/\sqrt{n}$

Can we use samples from the LHS to get samples from the RHS?

Converting Gaussian Vectors

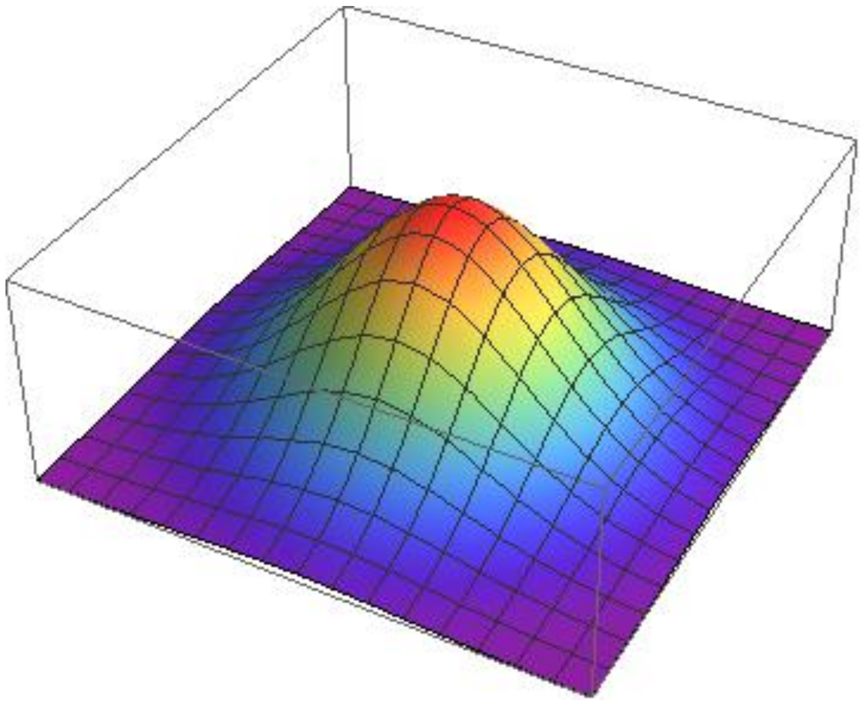
Converting Gaussian Vectors

$$\mathbf{x} \sim \mathsf{Gauss}(s)$$



Converting Gaussian Vectors

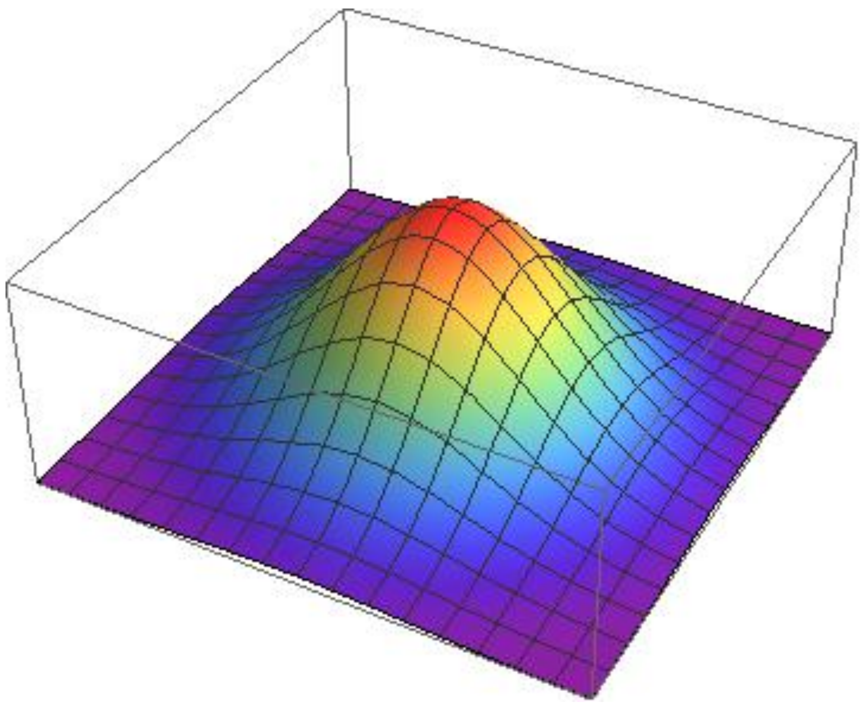
$\mathbf{x} \sim \mathsf{Gauss}(s)$



2

Converting Gaussian Vectors

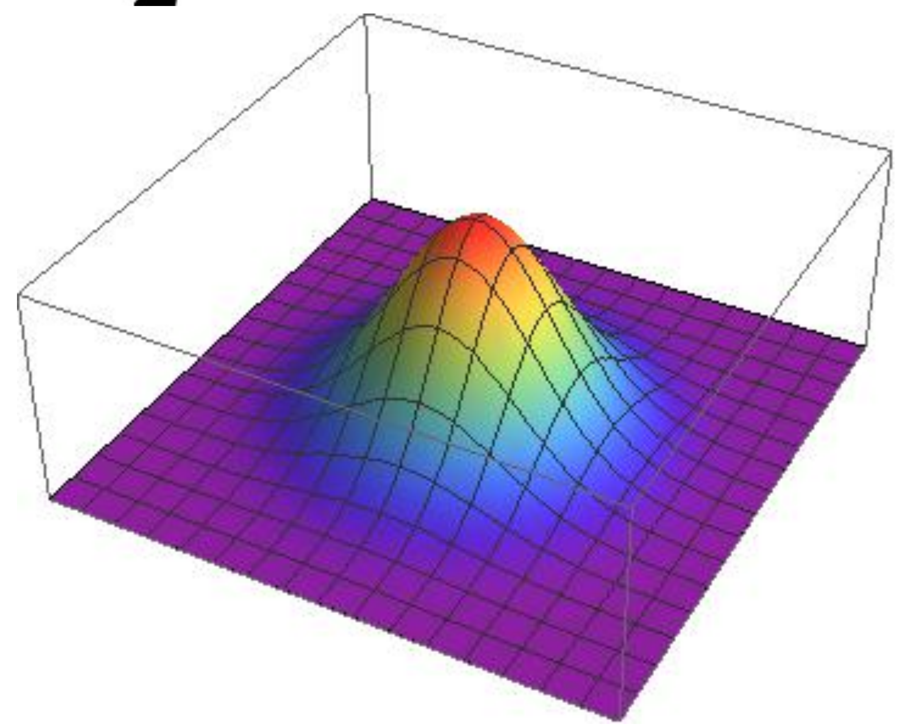
$\mathbf{x} \sim \mathsf{Gauss}(s)$



2

=

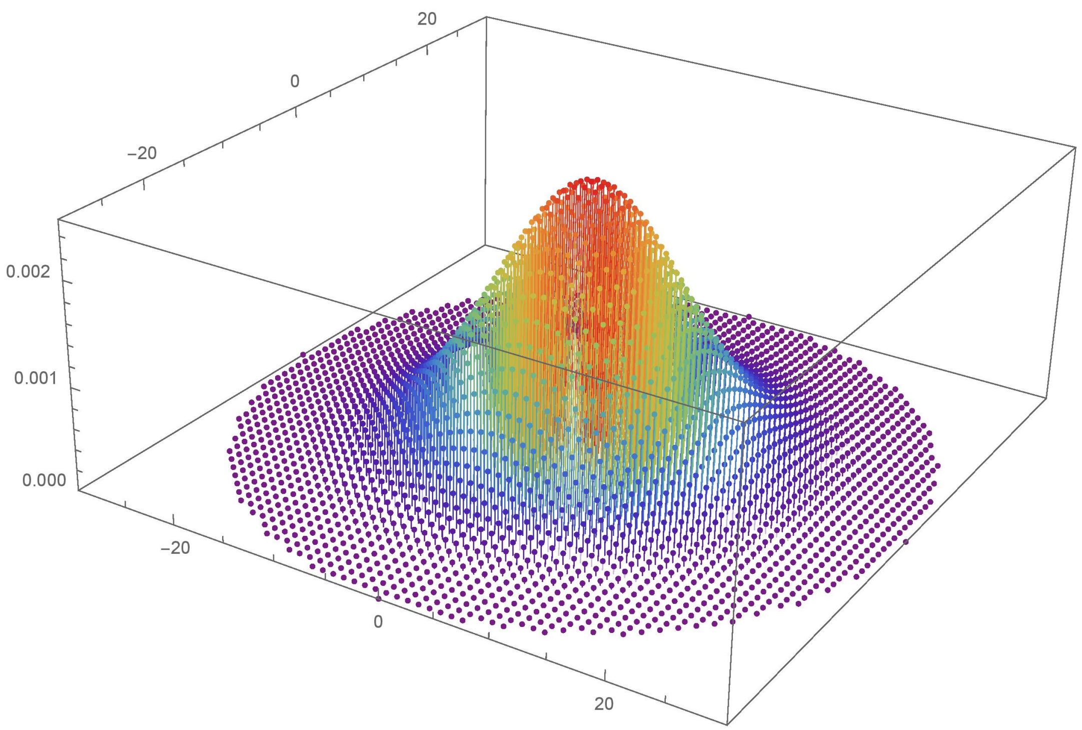
$\frac{\mathbf{x}}{2} \sim \mathsf{Gauss}(s/2)$



Converting Gaussian Vectors

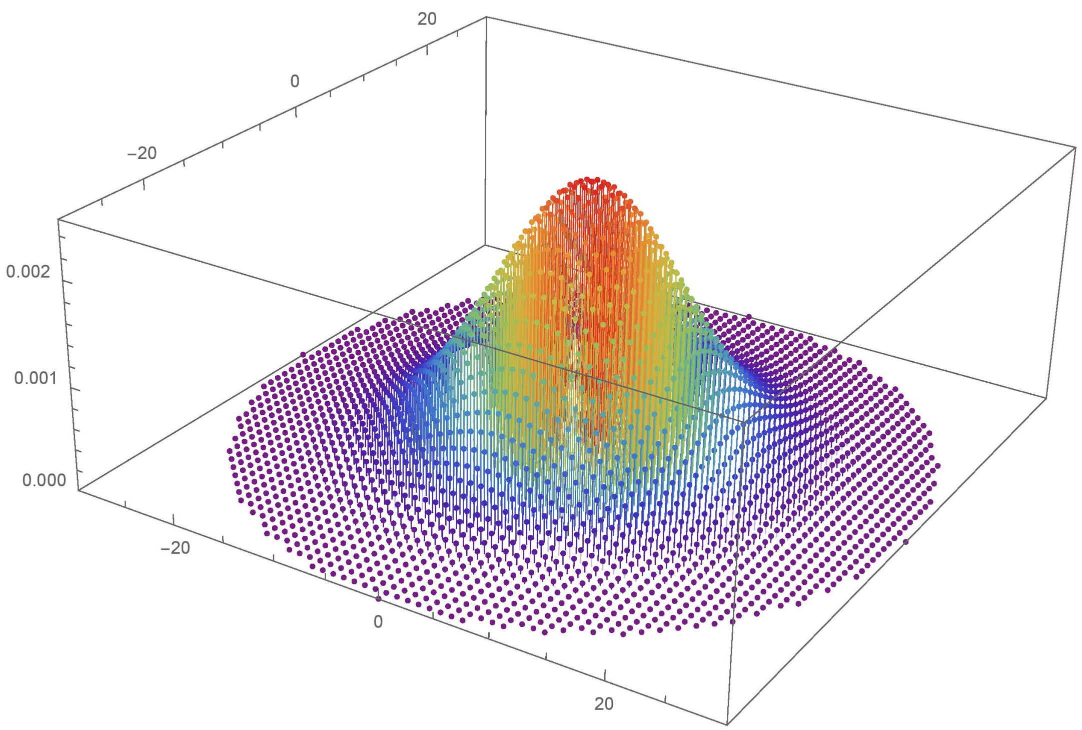
Converting Gaussian Vectors

$\mathbf{y} \sim D_{\mathcal{L},s}$



Converting Gaussian Vectors

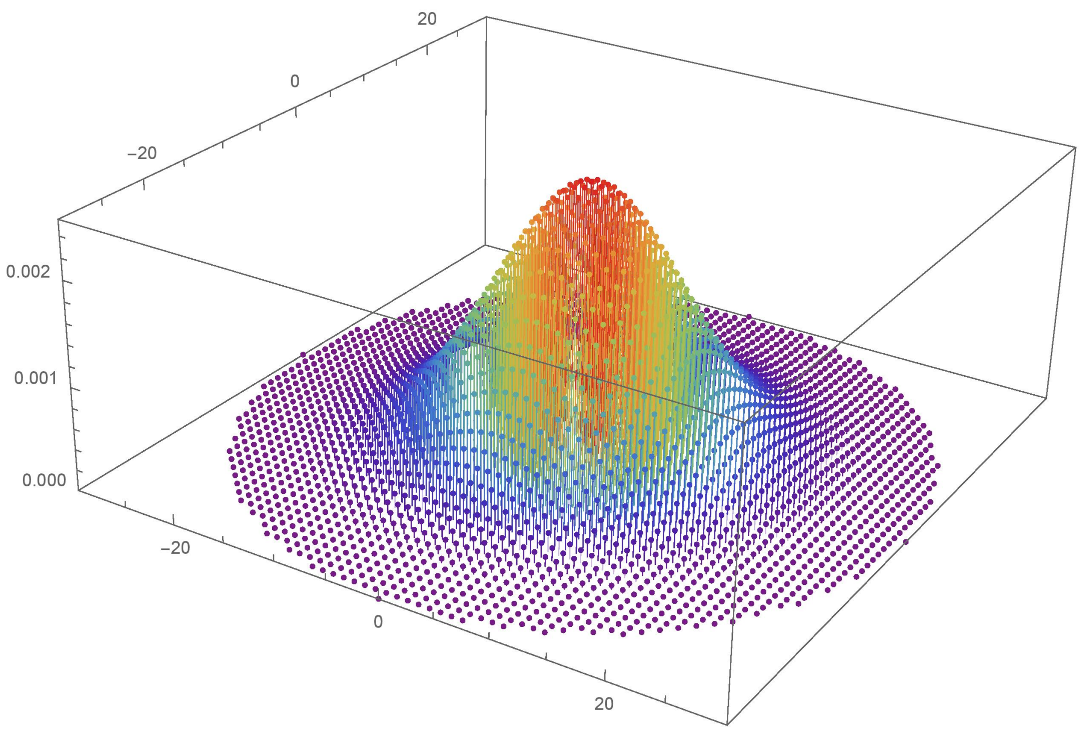
$\mathbf{y} \sim D_{\mathcal{L},s}$



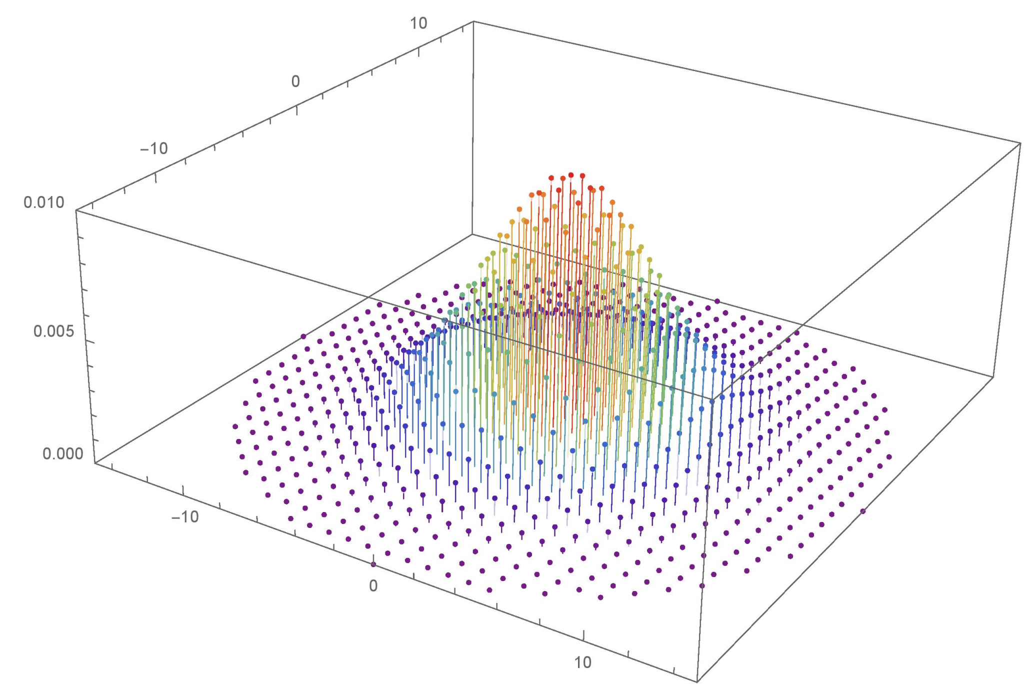
$$\frac{}{2}$$

Converting Gaussian Vectors

$\mathbf{y} \sim D_{\mathcal{L},s}$

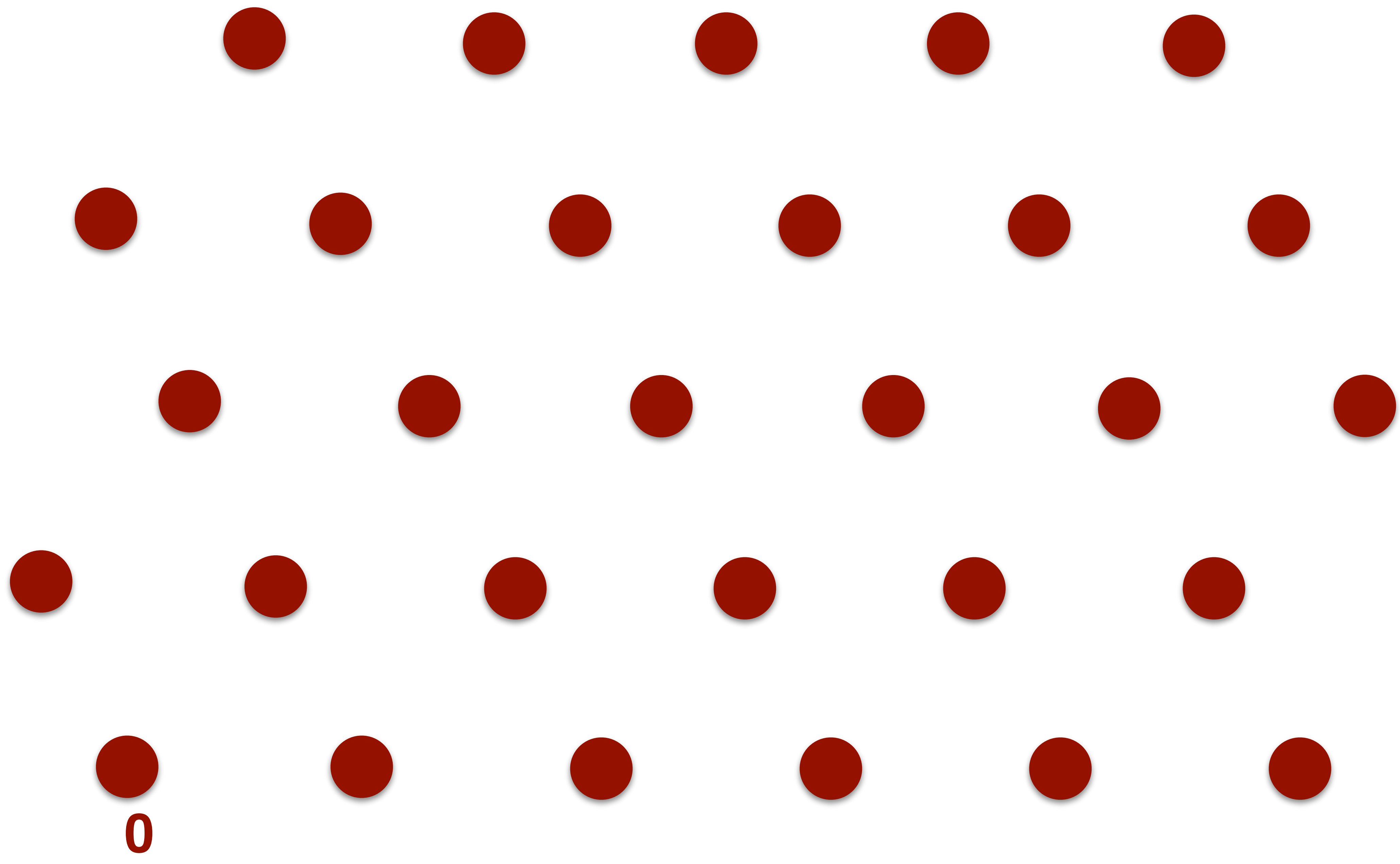


$$\frac{\quad}{2} \stackrel{?}{=}$$

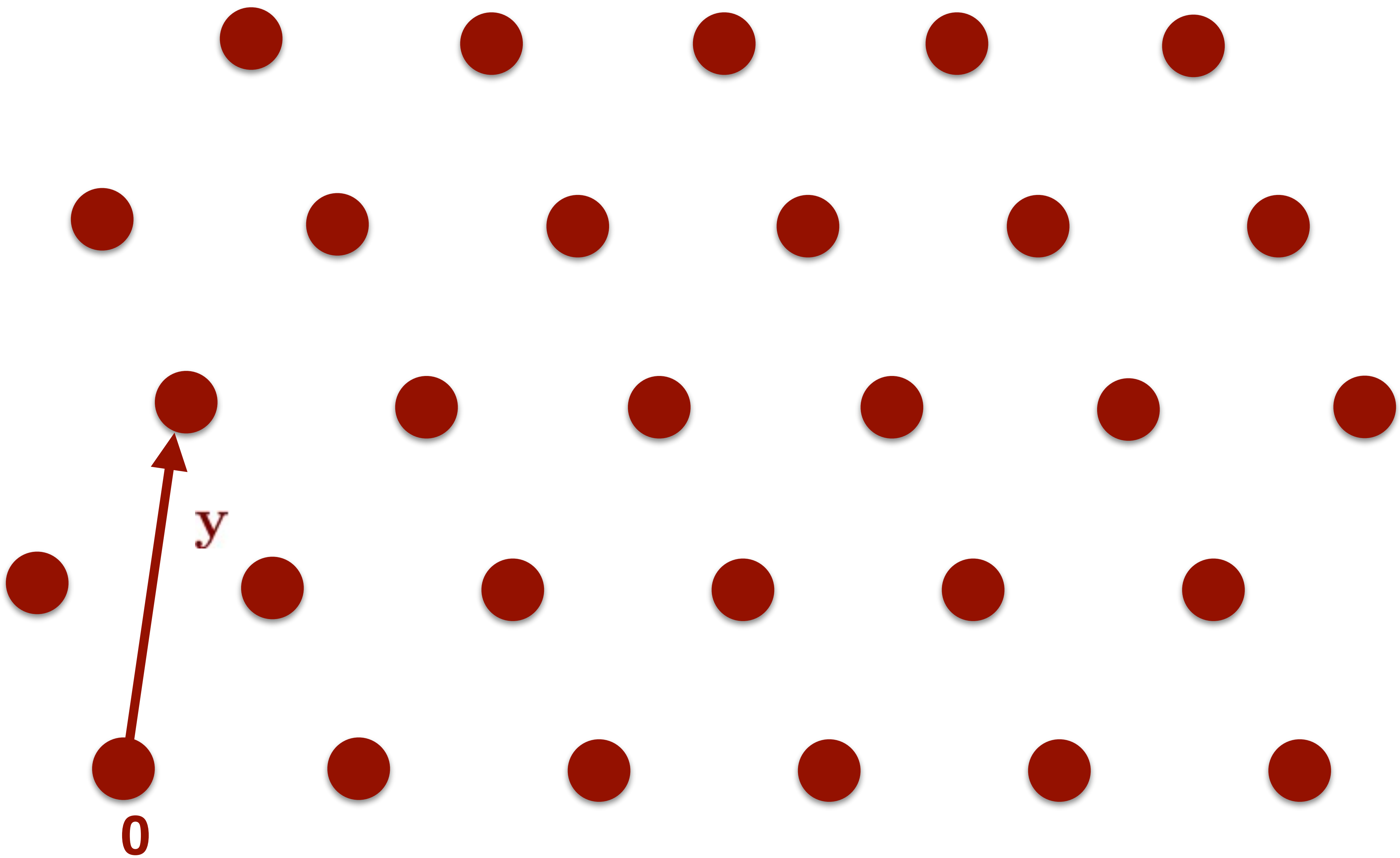


Converting Gaussian Vectors

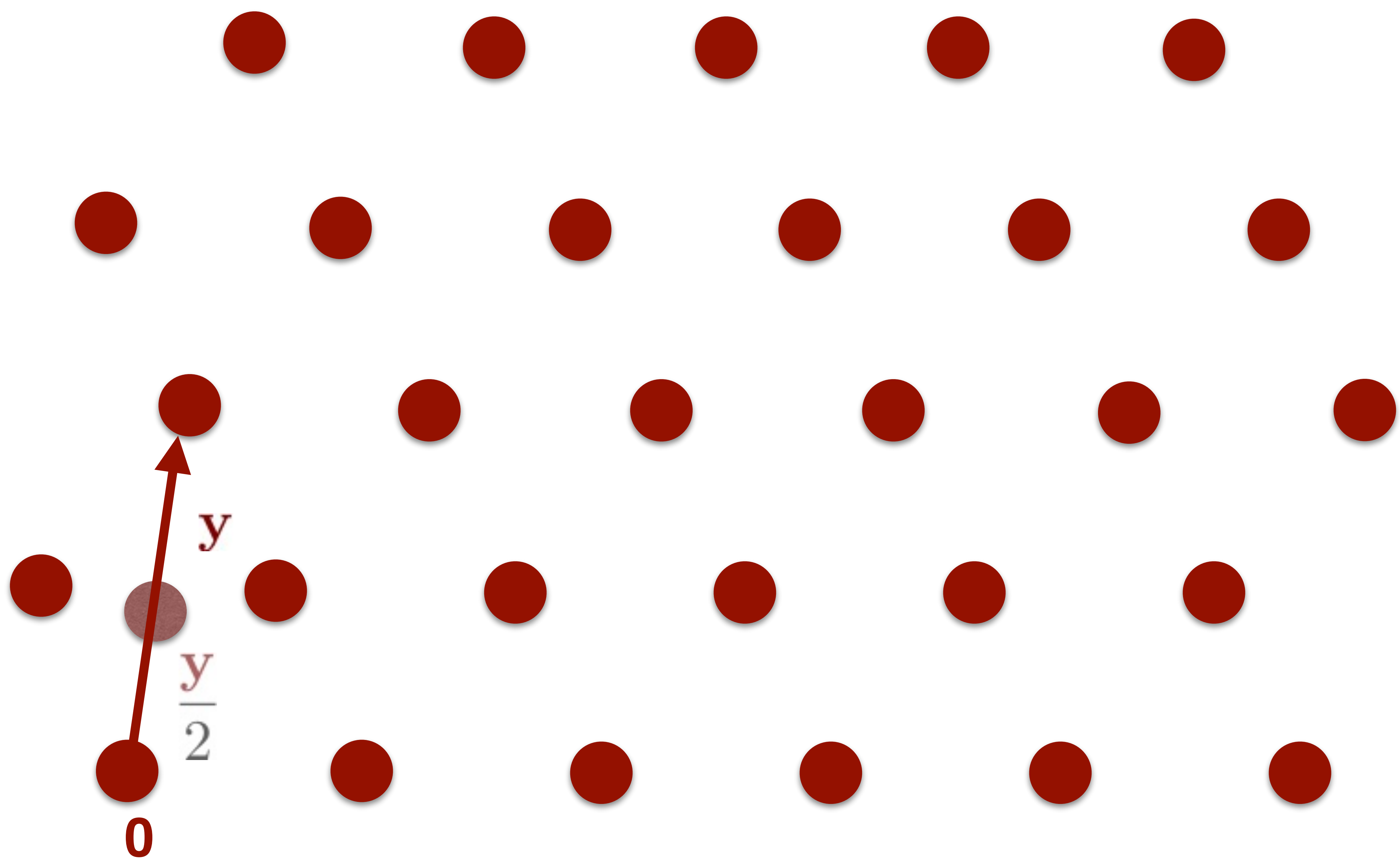
Converting Gaussian Vectors



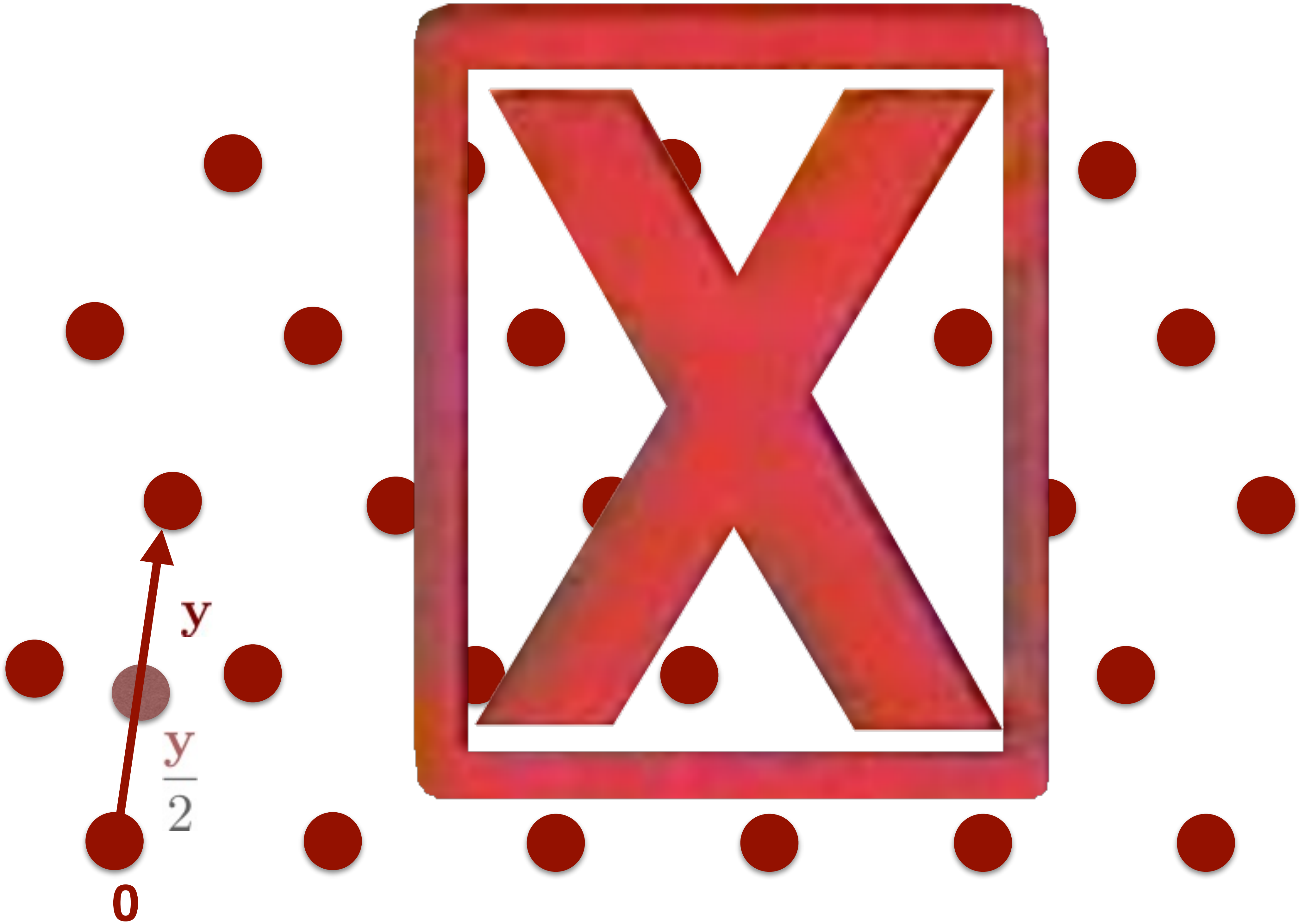
Converting Gaussian Vectors



Converting Gaussian Vectors



Converting Gaussian Vectors



Converting Gaussian Vectors

What if we *condition on* the result being in the lattice?

Converting Gaussian Vectors

What if we *condition on* the result being in the lattice?

$$\Pr_{\mathbf{y} \sim D_{\mathcal{L},s}} \left[\frac{\mathbf{y}}{2} = \mathbf{x} \;\middle|\; \frac{\mathbf{y}}{2} \in \mathcal{L} \right] \propto e^{-4||\mathbf{x}||^2/s^2}$$

Converting Gaussian Vectors

What if we *condition on* the result being in the lattice?

$$\Pr_{\mathbf{y} \sim D_{\mathcal{L},s}} \left[\frac{\mathbf{y}}{2} = \mathbf{x} \;\middle|\; \frac{\mathbf{y}}{2} \in \mathcal{L} \right] \propto e^{-4||\mathbf{x}||^2/s^2}$$

Progress!

Converting Gaussian Vectors

What if we *condition on* the result being in the lattice?

$$\Pr_{\mathbf{y} \sim D_{\mathcal{L},s}} \left[\frac{\mathbf{y}}{2} = \mathbf{x} \;\middle|\; \frac{\mathbf{y}}{2} \in \mathcal{L} \right] \propto e^{-4||\mathbf{x}||^2/s^2}$$

Progress!

Unfortunately, this requires us to throw out a lot of vectors.

Converting Gaussian Vectors

What if we *condition on* the result being in the lattice?

$$\Pr_{\mathbf{y} \sim D_{\mathcal{L},s}} \left[\frac{\mathbf{y}}{2} = \mathbf{x} \;\middle|\; \frac{\mathbf{y}}{2} \in \mathcal{L} \right] \propto e^{-4||\mathbf{x}||^2/s^2}$$

Progress!

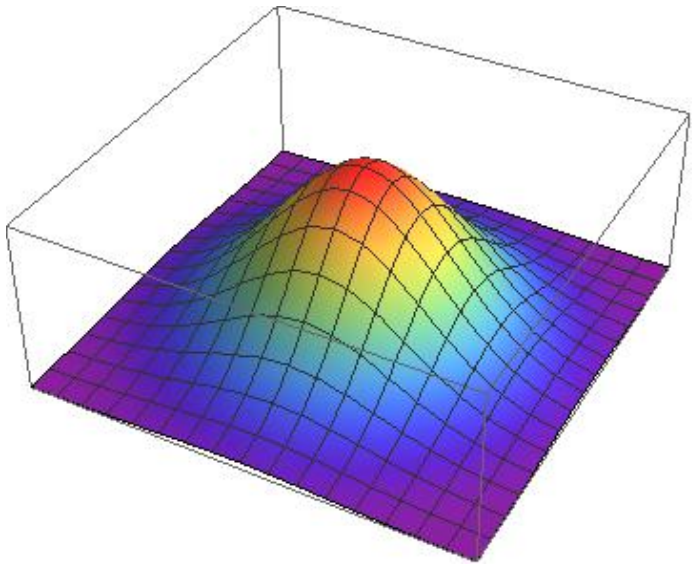
Unfortunately, this requires us to throw out a lot of vectors.

We only keep one from every $\approx 2^n$ vectors each time we do this, leading to a very slow algorithm!

Converting Gaussian Vectors

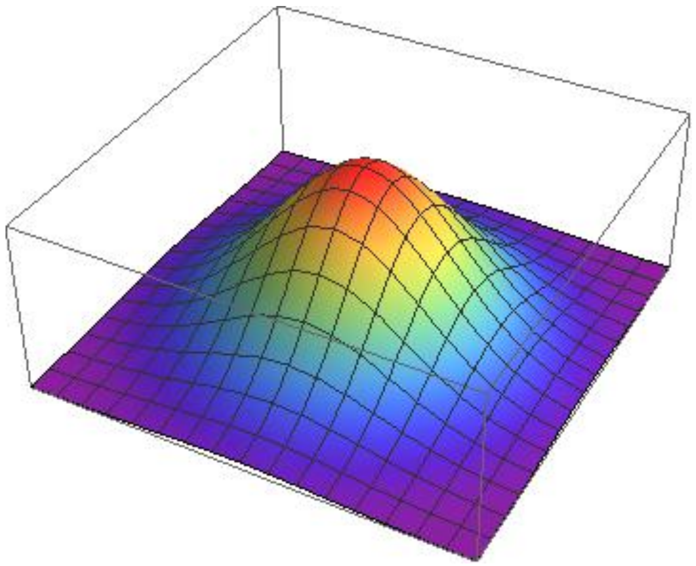
Converting Gaussian Vectors

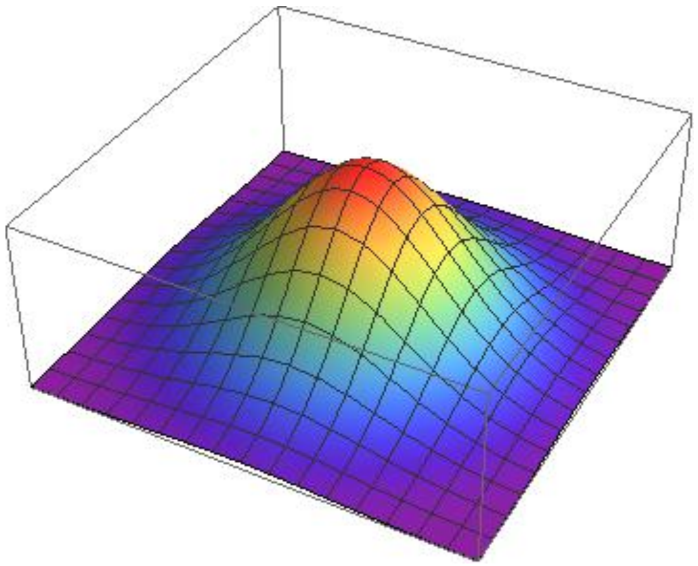
$\mathbf{x}_1 \sim \mathsf{Gauss}(s)$



Converting Gaussian Vectors

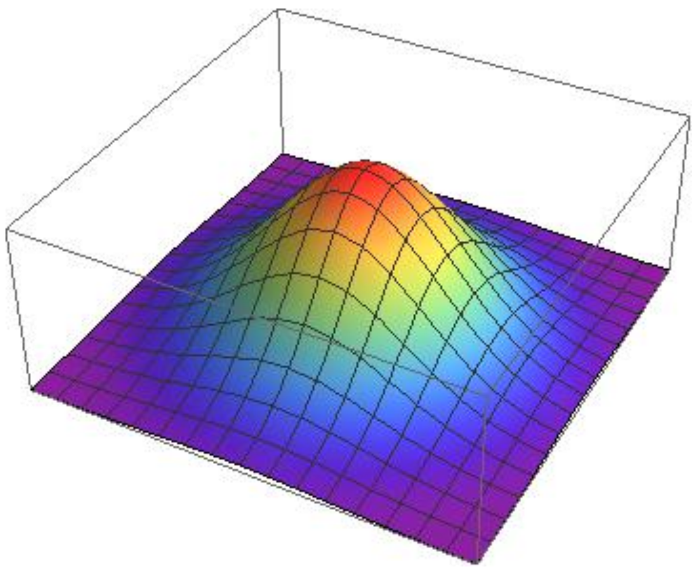
$\mathbf{x}_1 \sim \mathsf{Gauss}(s)$ $\mathbf{x}_2 \sim \mathsf{Gauss}(s)$



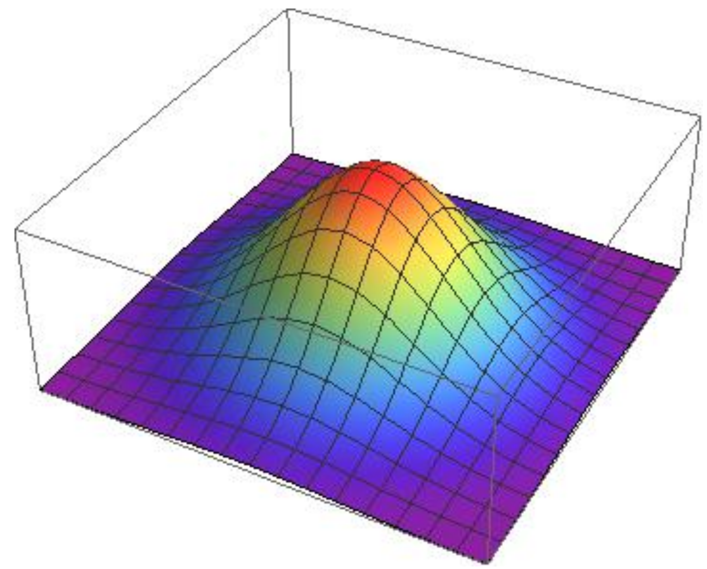


Converting Gaussian Vectors

$\mathbf{x}_1 \sim \text{Gauss}(s)$ $\mathbf{x}_2 \sim \text{Gauss}(s)$



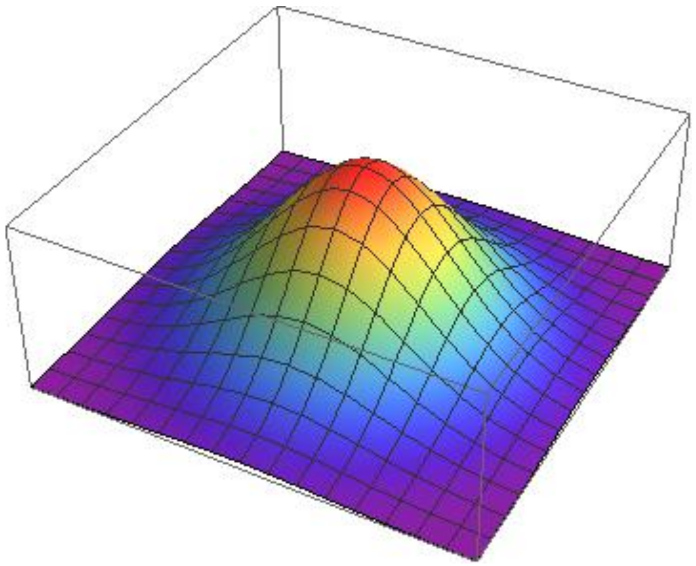
$+$



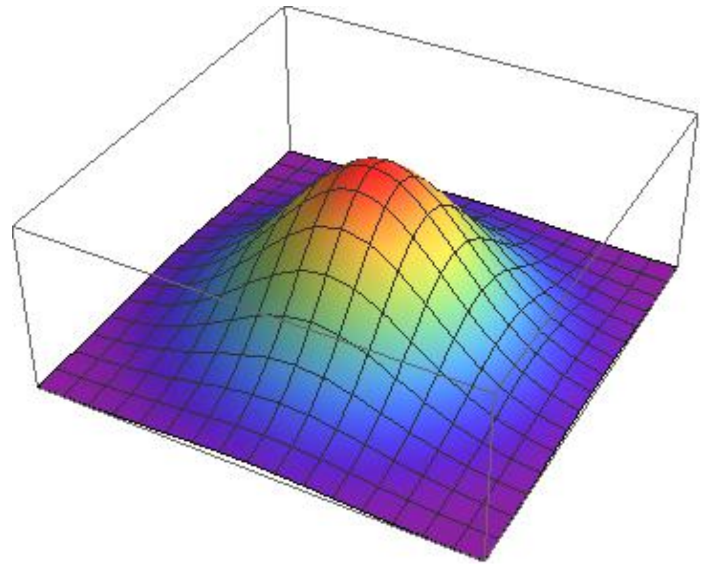
2

Converting Gaussian Vectors

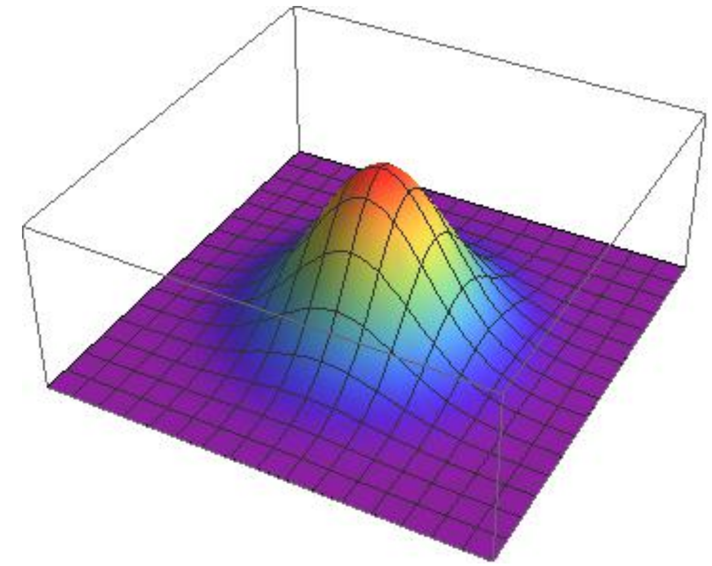
$\mathbf{x}_1 \sim \mathsf{Gauss}(s)$ $\mathbf{x}_2 \sim \mathsf{Gauss}(s)$ $\frac{\mathbf{x}_1 + \mathbf{x}_2}{2} \sim \mathsf{Gauss}(s/\sqrt{2})$



+



=



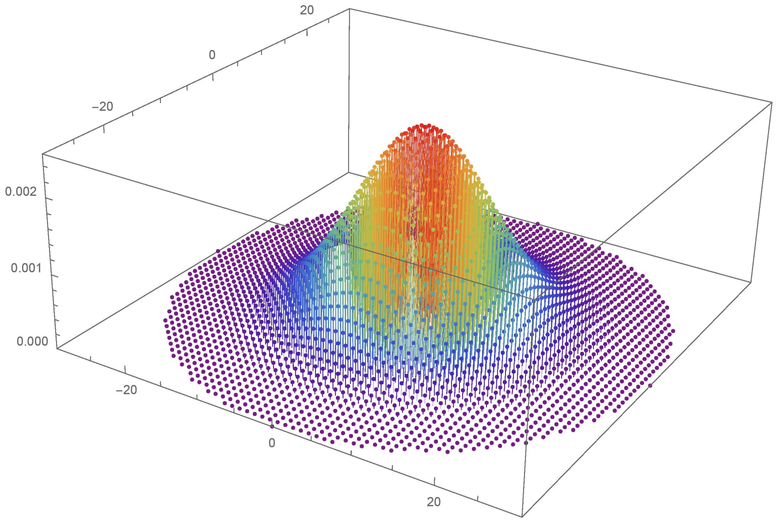
———————————————

2

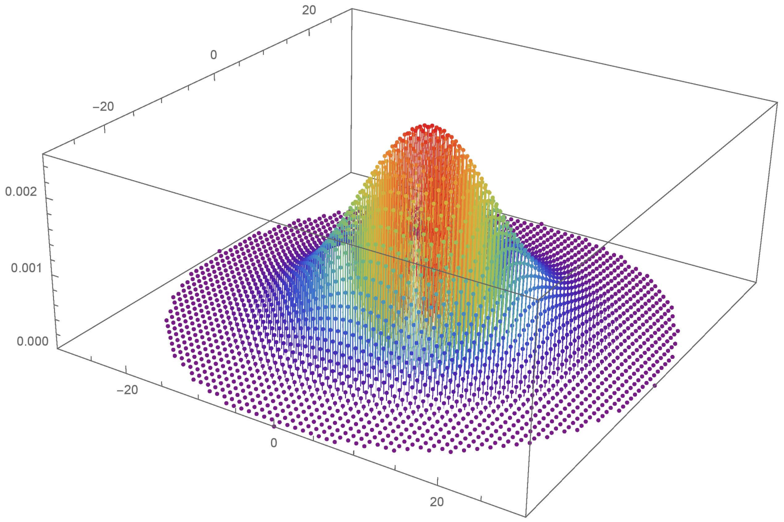
Converting Gaussian Vectors

Converting Gaussian Vectors

$\mathbf{y}_1 \sim D_{\mathcal{L},s}$

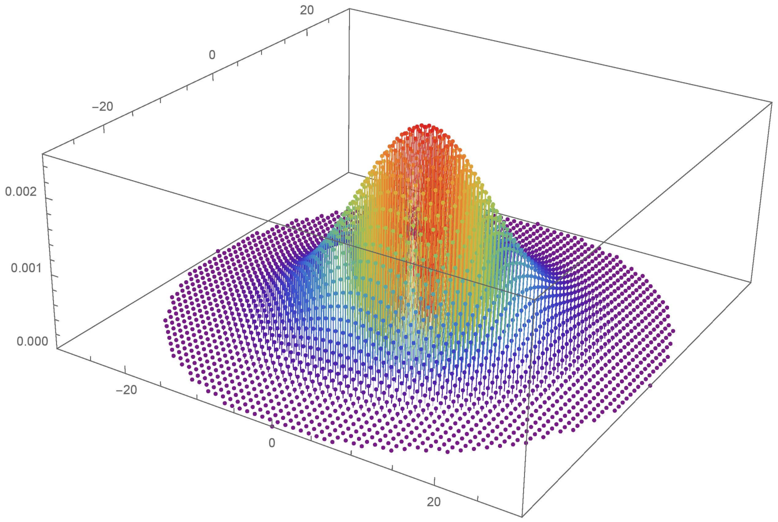


$\mathbf{y}_2 \sim D_{\mathcal{L},s}$

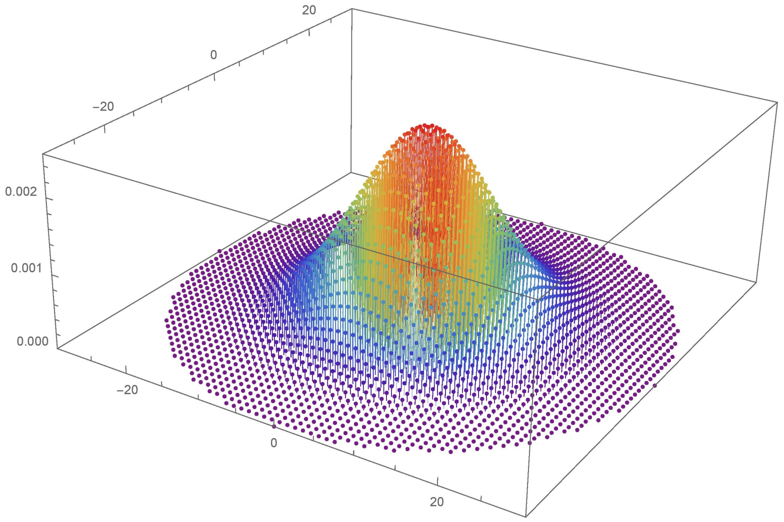


Converting Gaussian Vectors

$\mathbf{y}_1 \sim D_{\mathcal{L},s}$ $\mathbf{y}_2 \sim D_{\mathcal{L},s}$



$+$

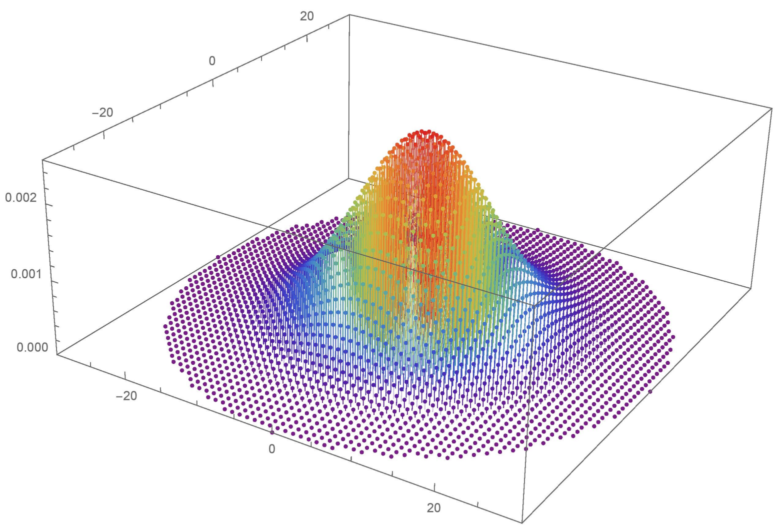


$\overline{}$

2

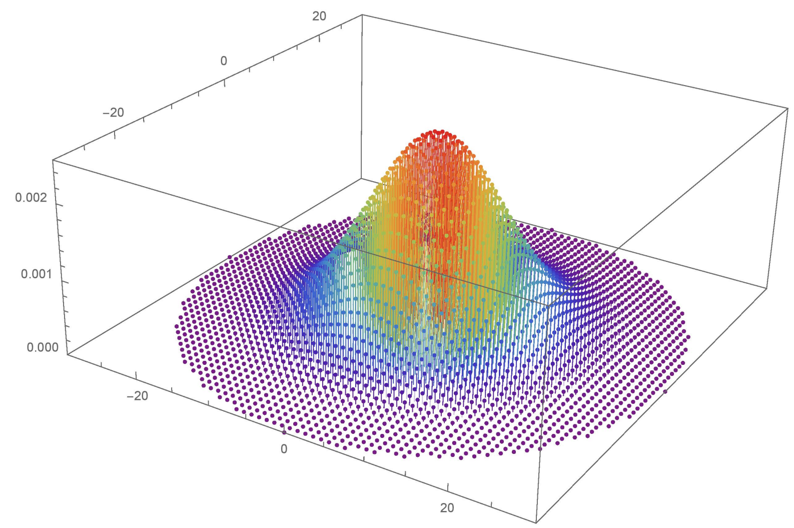
Converting Gaussian Vectors

$$\mathbf{y}_1 \sim D_{\mathcal{L},s}$$



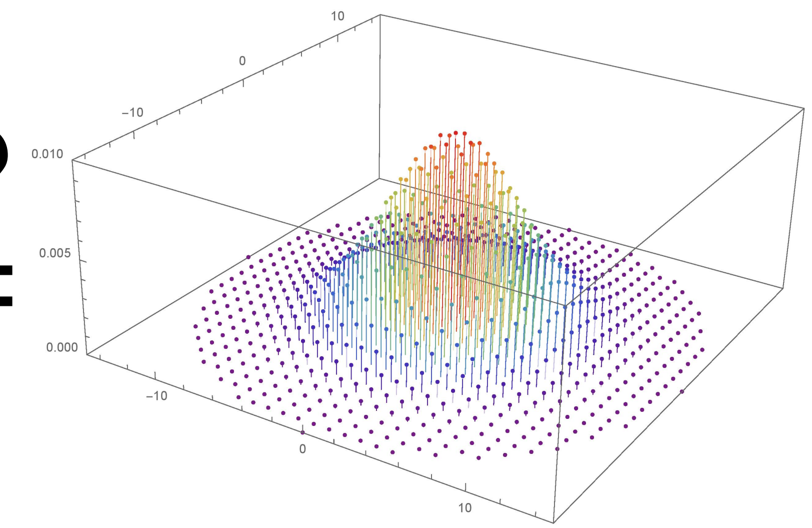
$+$

$$\mathbf{y}_2 \sim D_{\mathcal{L},s}$$



$\overset{?}{=}$

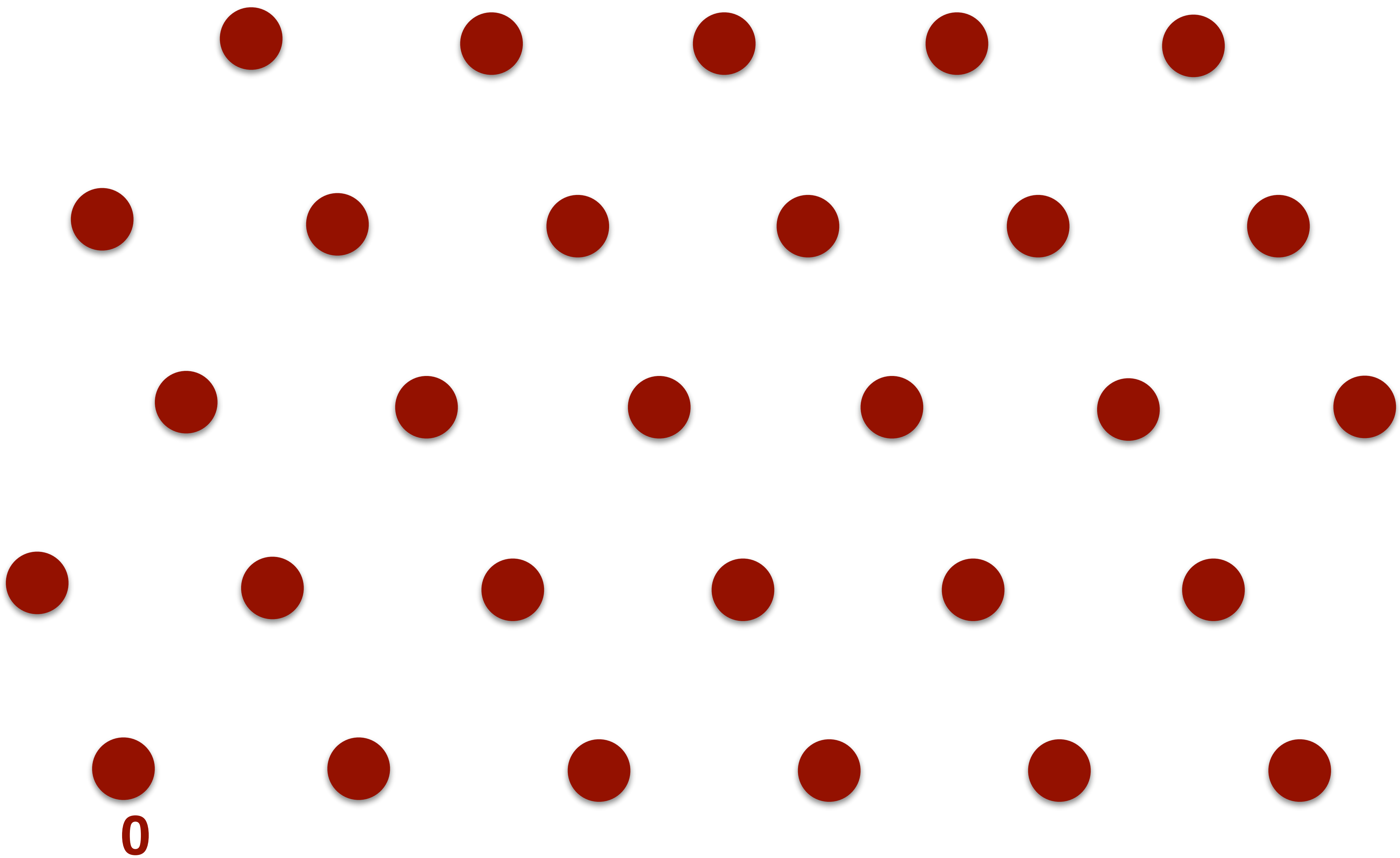
$$\frac{\mathbf{y}_1 + \mathbf{y}_2}{2} \sim D_{\mathcal{L},s/\sqrt{2}}$$



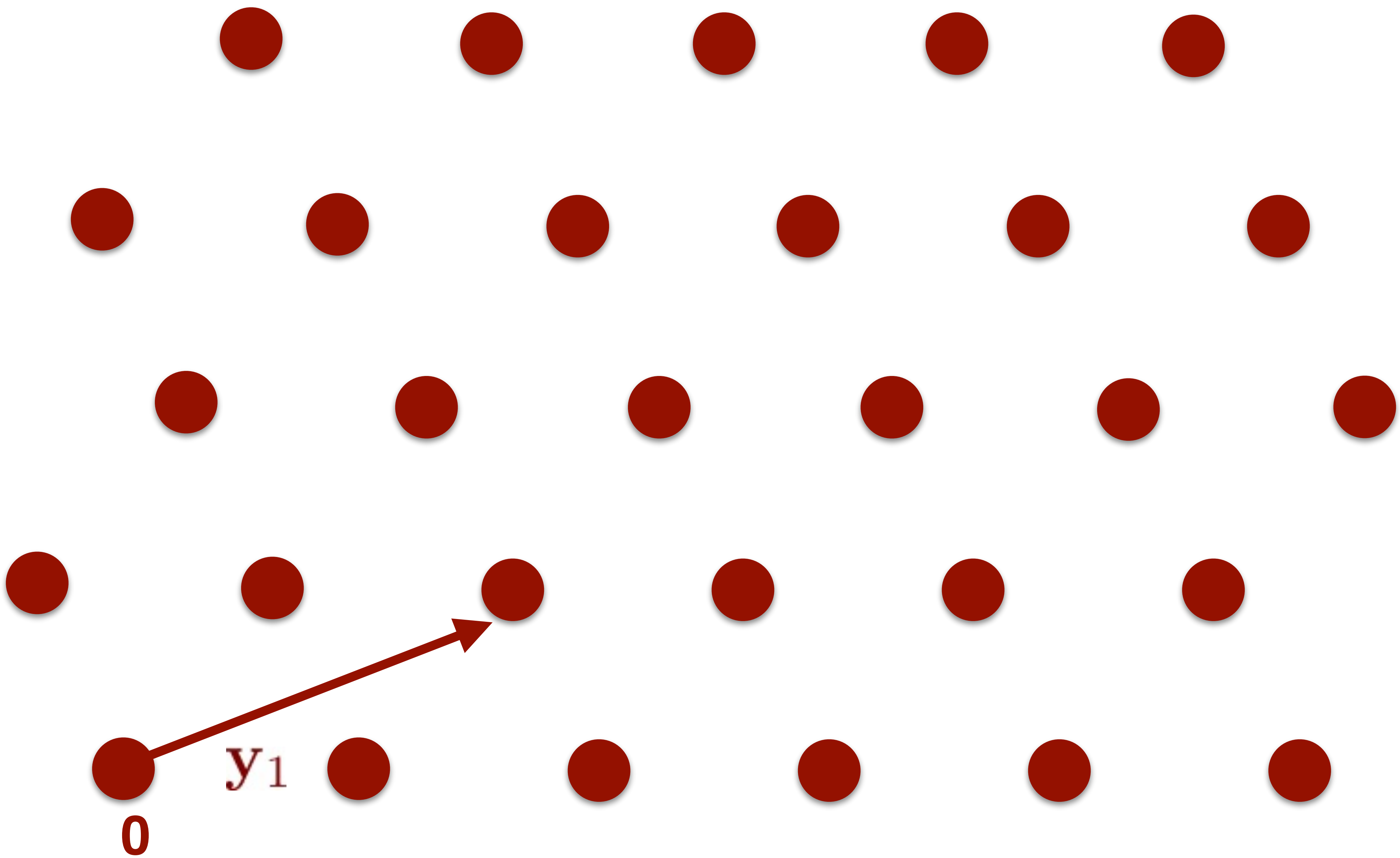
2

Converting Gaussian Vectors

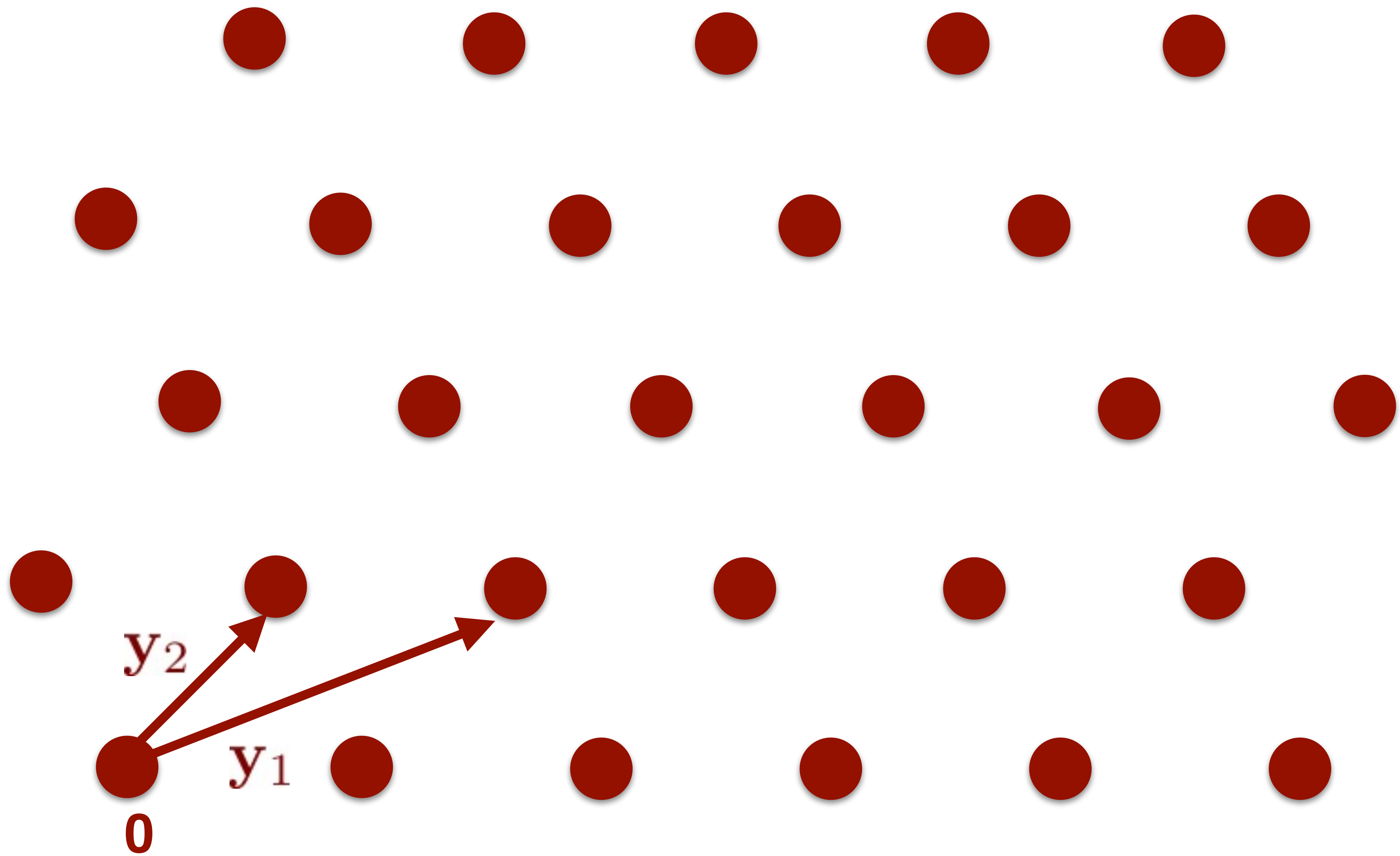
Converting Gaussian Vectors



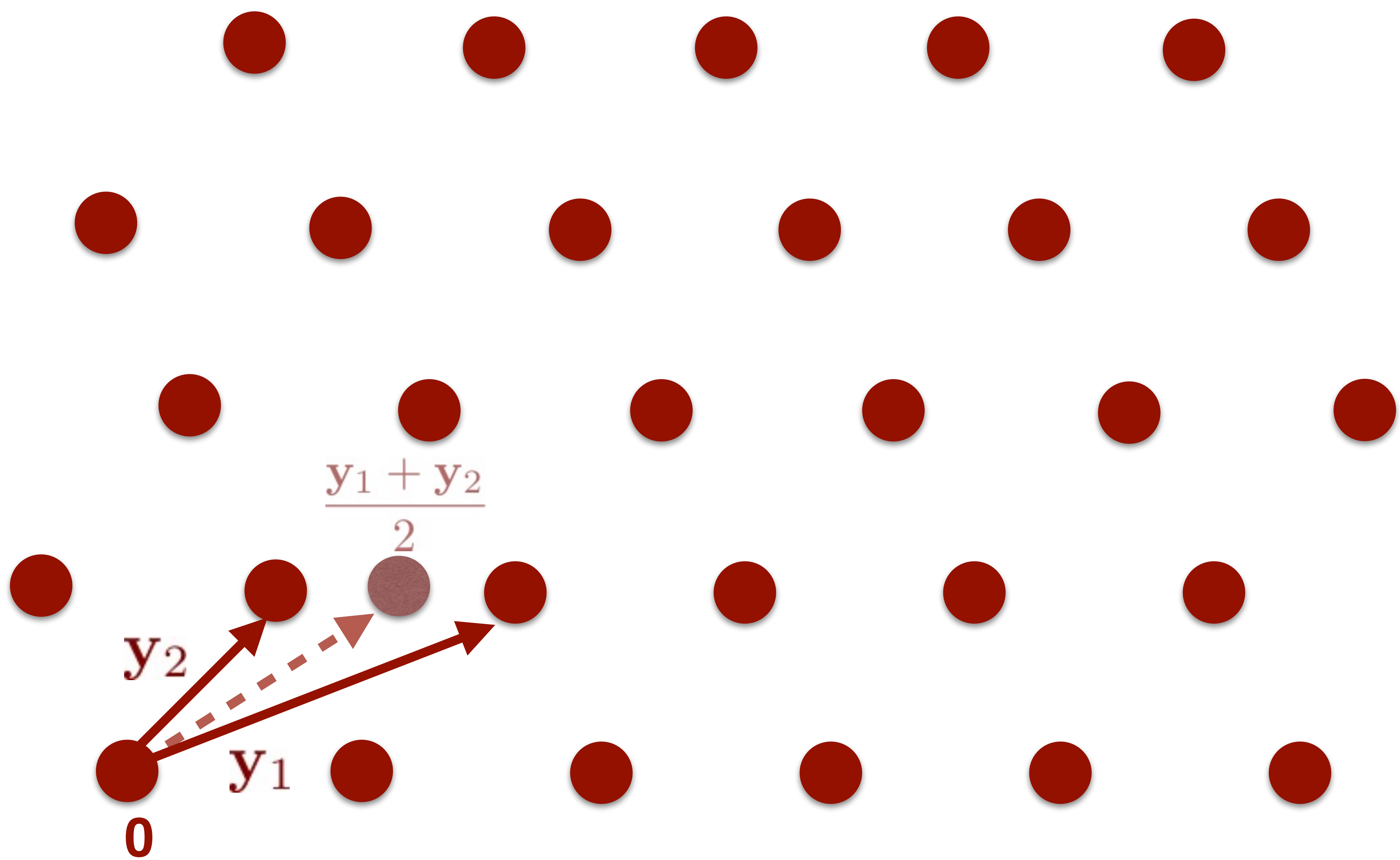
Converting Gaussian Vectors



Converting Gaussian Vectors



Converting Gaussian Vectors



Converting Gaussian Vectors

Converting Gaussian Vectors

What about the average of two discrete Gaussian vectors *conditioned on* the result being in the lattice?

Converting Gaussian Vectors

Converting Gaussian Vectors

When do we have $\frac{\mathbf{y}_1 + \mathbf{y}_2}{2} \in \mathcal{L}$?

Converting Gaussian Vectors

When do we have $\frac{\mathbf{y}_1 + \mathbf{y}_2}{2} \in \mathcal{L}$?

$$\mathbf{y}_1 = a_{1,1}\mathbf{b}_1 + \cdots + a_{1,n}\mathbf{b}_n$$

Converting Gaussian Vectors

When do we have $\frac{\mathbf{y}_1 + \mathbf{y}_2}{2} \in \mathcal{L}$?

$$\mathbf{y}_1 = a_{1,1}\mathbf{b}_1 + \cdots + a_{1,n}\mathbf{b}_n \qquad \mathbf{y}_2 = a_{2,1}\mathbf{b}_1 + \cdots + a_{2,n}\mathbf{b}_n$$

Converting Gaussian Vectors

When do we have $\frac{\mathbf{y}_1 + \mathbf{y}_2}{2} \in \mathcal{L}$?

$$\mathbf{y}_1 = a_{1,1}\mathbf{b}_1 + \cdots + a_{1,n}\mathbf{b}_n \qquad \mathbf{y}_2 = a_{2,1}\mathbf{b}_1 + \cdots + a_{2,n}\mathbf{b}_n$$

$$\frac{\mathbf{y}_1 + \mathbf{y}_2}{2} = \frac{a_{1,1} + a_{2,1}}{2} \cdot \mathbf{b}_1 + \cdots + \frac{a_{1,n} + a_{2,n}}{2} \cdot \mathbf{b}_n$$

Converting Gaussian Vectors

When do we have $\frac{\mathbf{y}_1 + \mathbf{y}_2}{2} \in \mathcal{L}$?

$$\mathbf{y}_1 = a_{1,1}\mathbf{b}_1 + \cdots + a_{1,n}\mathbf{b}_n \qquad \mathbf{y}_2 = a_{2,1}\mathbf{b}_1 + \cdots + a_{2,n}\mathbf{b}_n$$

$$\frac{\mathbf{y}_1 + \mathbf{y}_2}{2} = \frac{a_{1,1} + a_{2,1}}{2} \cdot \mathbf{b}_1 + \cdots + \frac{a_{1,n} + a_{2,n}}{2} \cdot \mathbf{b}_n$$

$$\frac{\mathbf{y}_1 + \mathbf{y}_2}{2} \in \mathcal{L} \iff a_{1,i} \equiv a_{2,i} \mod 2$$

Converting Gaussian Vectors

When do we have $\frac{\mathbf{y}_1 + \mathbf{y}_2}{2} \in \mathcal{L}$?

$$\mathbf{y}_1 = a_{1,1}\mathbf{b}_1 + \cdots + a_{1,n}\mathbf{b}_n \qquad \mathbf{y}_2 = a_{2,1}\mathbf{b}_1 + \cdots + a_{2,n}\mathbf{b}_n$$

$$\frac{\mathbf{y}_1 + \mathbf{y}_2}{2} = \frac{a_{1,1} + a_{2,1}}{2} \cdot \mathbf{b}_1 + \cdots + \frac{a_{1,n} + a_{2,n}}{2} \cdot \mathbf{b}_n$$

$$\frac{\mathbf{y}_1 + \mathbf{y}_2}{2} \in \mathcal{L} \iff a_{1,i} \equiv a_{2,i} \mod 2$$

$$\iff \mathbf{y}_1 \equiv \mathbf{y}_2 \mod 2\mathcal{L}$$

Converting Gaussian Vectors

When do we have $\frac{\mathbf{y}_1 + \mathbf{y}_2}{2} \in \mathcal{L}$?

$\mathbf{y}_1 = a_1$ … $a_{2,n}\mathbf{b}_n$

$\frac{\mathbf{y}_1 \ldots}{}$ … $\mathbf{b}_n$

We have $\frac{\mathbf{y}_1 + \mathbf{y}_2}{2} \in \mathcal{L}$ *if and only if* $\mathbf{y}_1, \mathbf{y}_2$ *are in the same* ***coset*** *of* $2\mathcal{L}$.

(Note that there are 2^n *cosets.)*

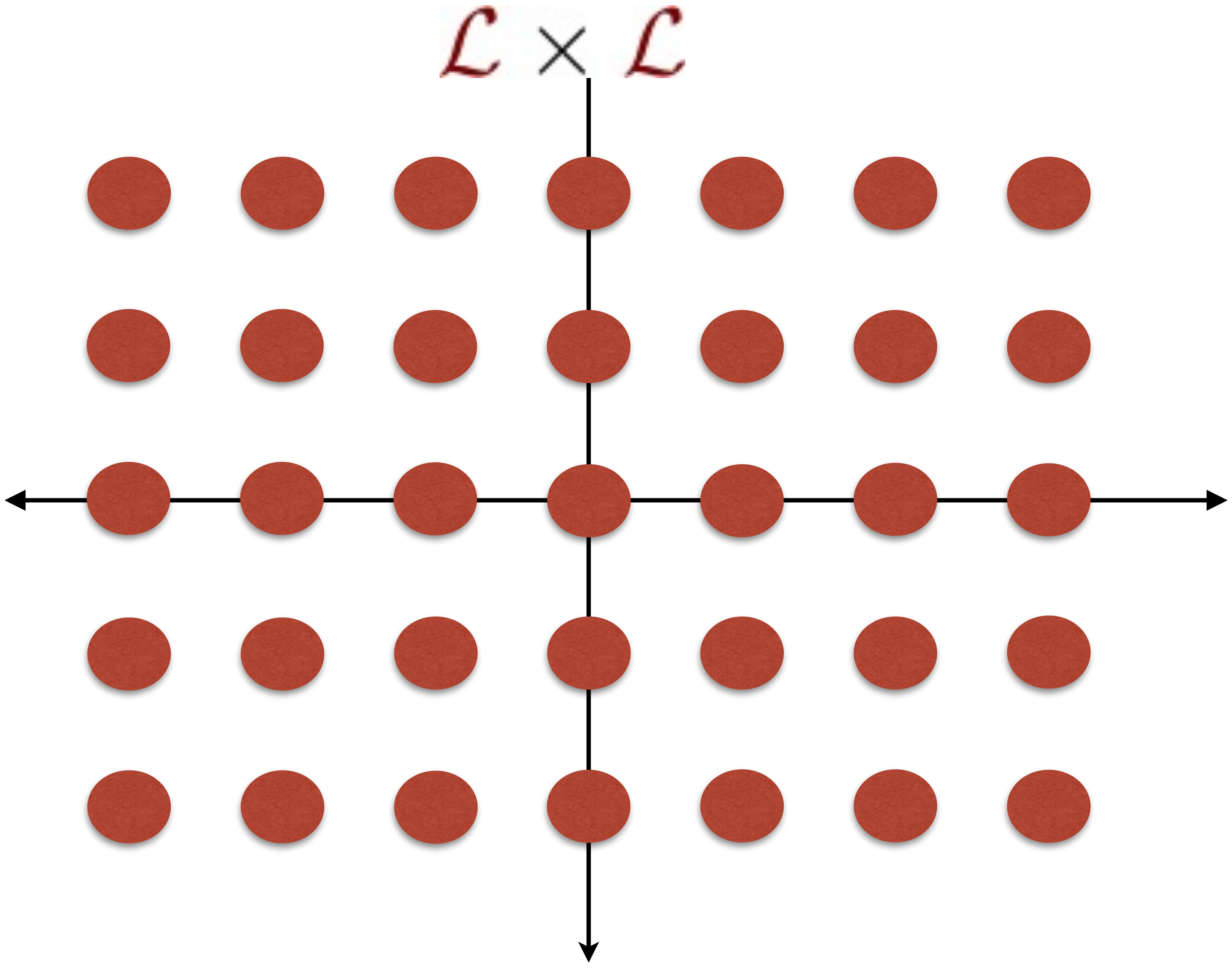
$$\frac{\mathbf{y}_1 + \mathbf{y}_2}{2} \in \mathcal{L} \iff a_{1,i} \equiv a_{2,i} \mod 2$$

$$\iff \mathbf{y}_1 \equiv \mathbf{y}_2 \mod 2\mathcal{L}$$

Converting Gaussian Vectors

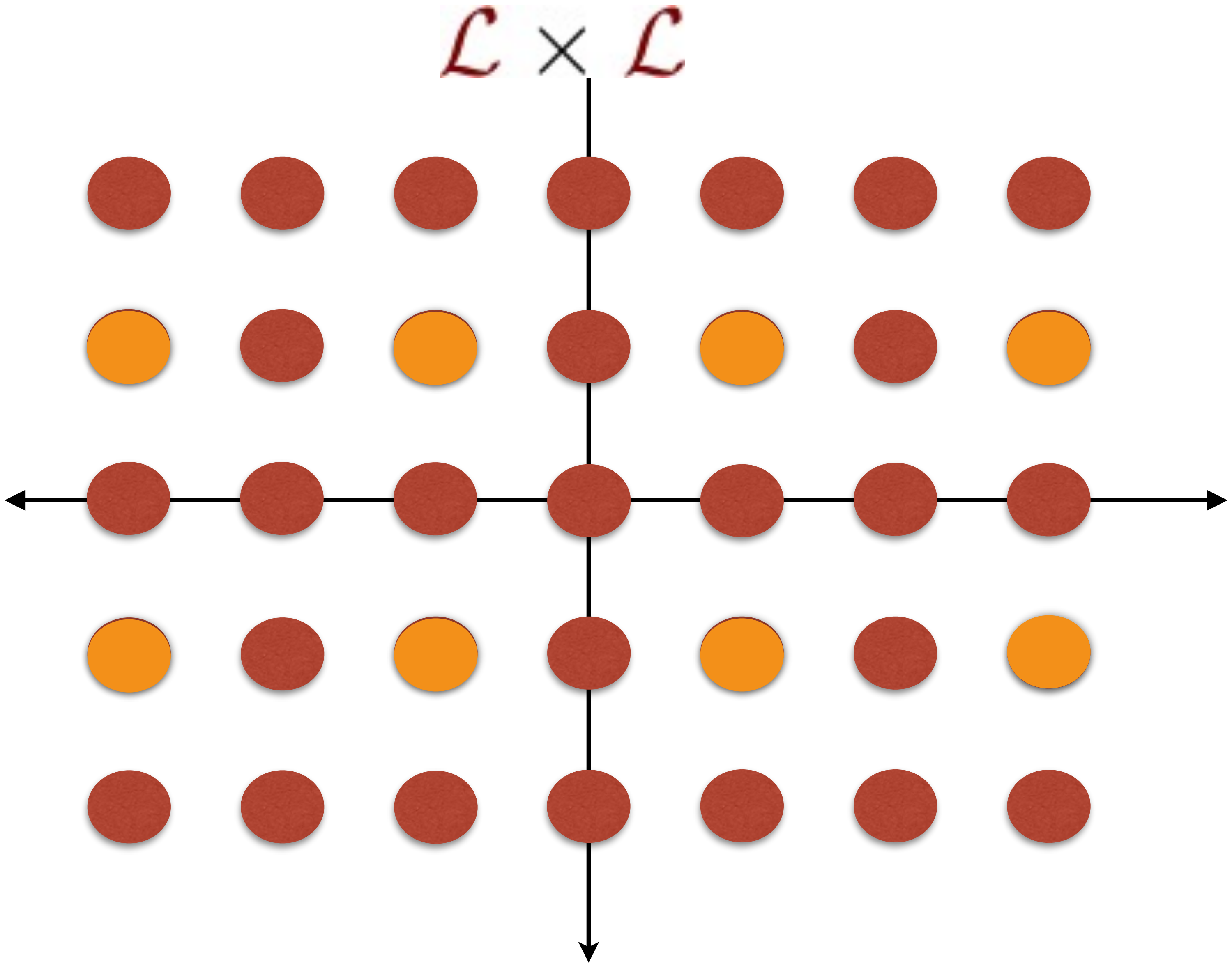
What about the average of two discrete Gaussian vectors *conditioned on* the result being in the lattice?

Converting Gaussian Vectors



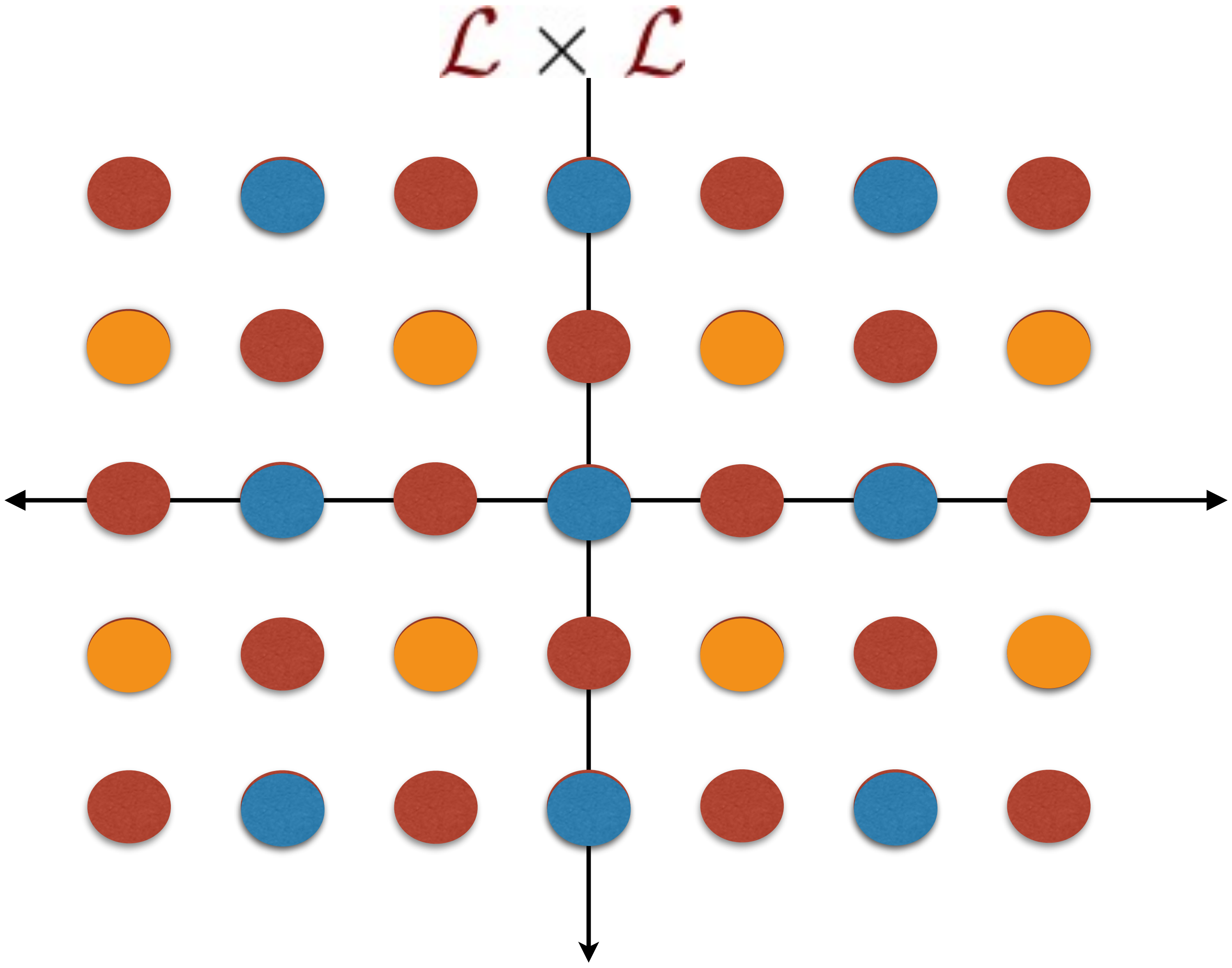
What about the average of two discrete Gaussian vectors *conditioned on* the result being in the lattice?

Converting Gaussian Vectors



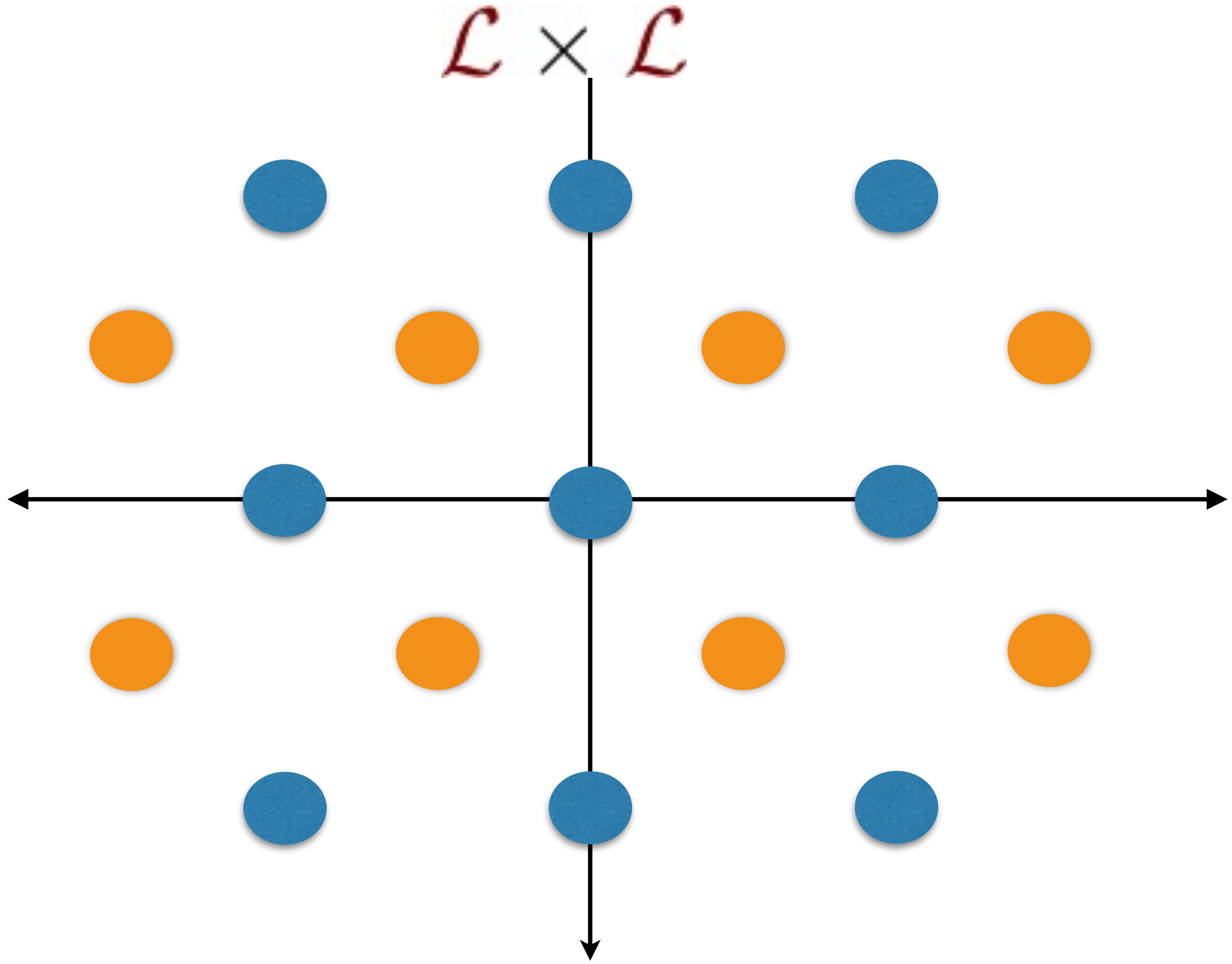
What about the average of two discrete Gaussian vectors *conditioned on* the result being in the lattice?

Converting Gaussian Vectors



What about the average of two discrete Gaussian vectors *conditioned on* the result being in the lattice?

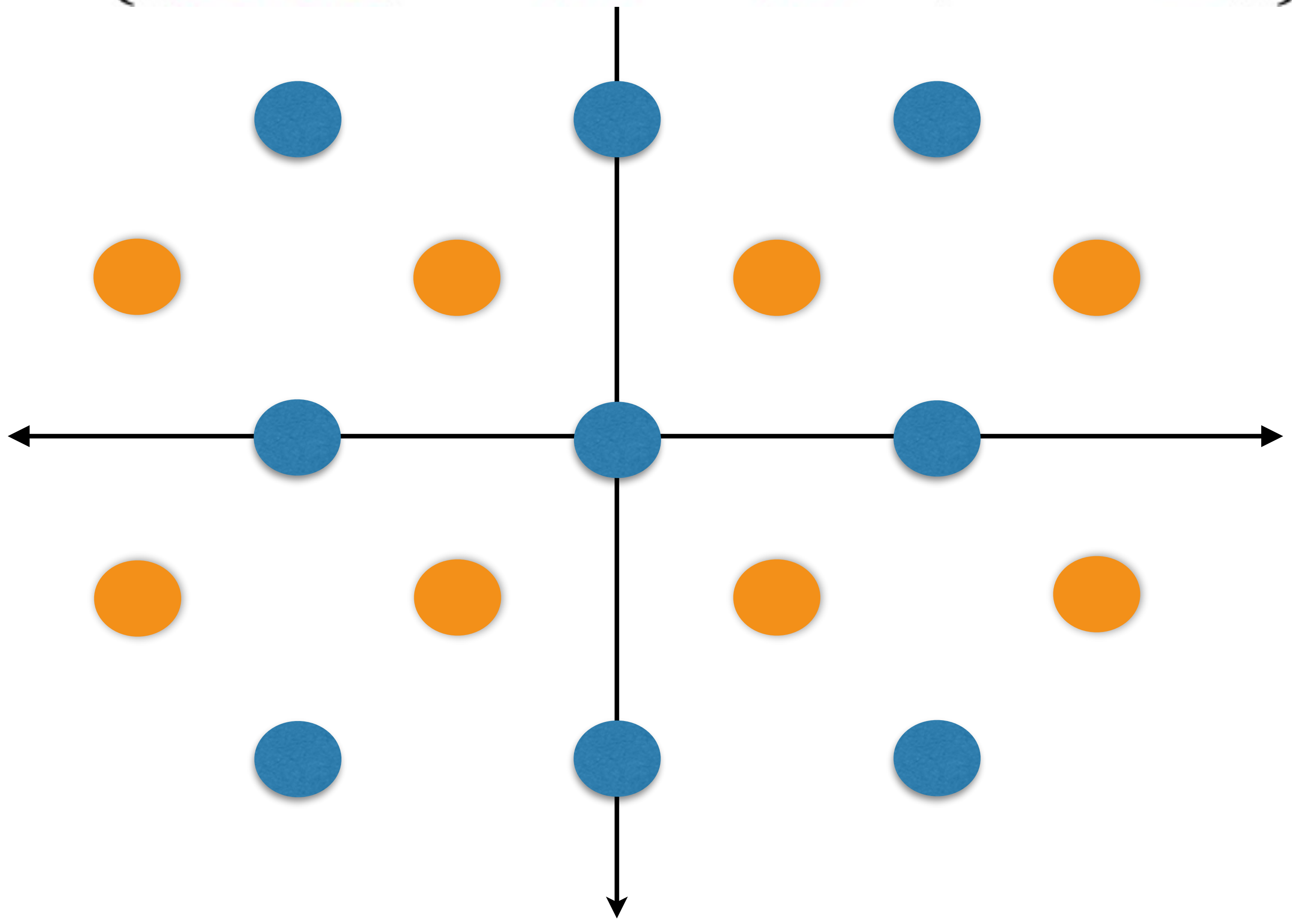
Converting Gaussian Vectors



What about the average of two discrete Gaussian vectors *conditioned on* the result being in the lattice?

Converting Gaussian Vectors

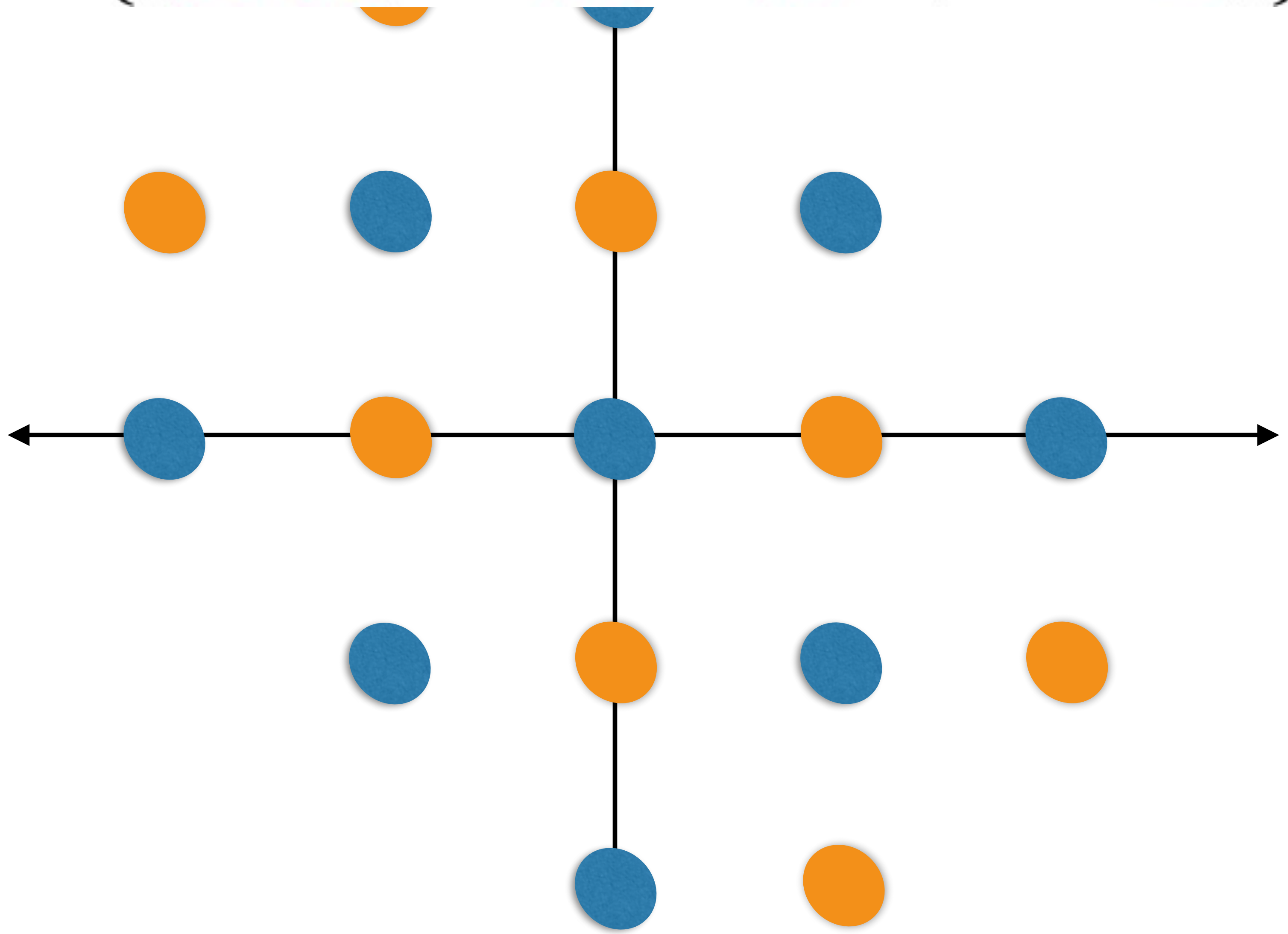
$$\mathcal{L}^\dagger := \{(\mathbf{y_1}, \mathbf{y_2}) \ : \ \mathbf{y_1} \equiv \mathbf{y_2} \pmod{2\mathcal{L}}\}$$



What about the average of two discrete Gaussian vectors *conditioned on* the result being in the lattice?

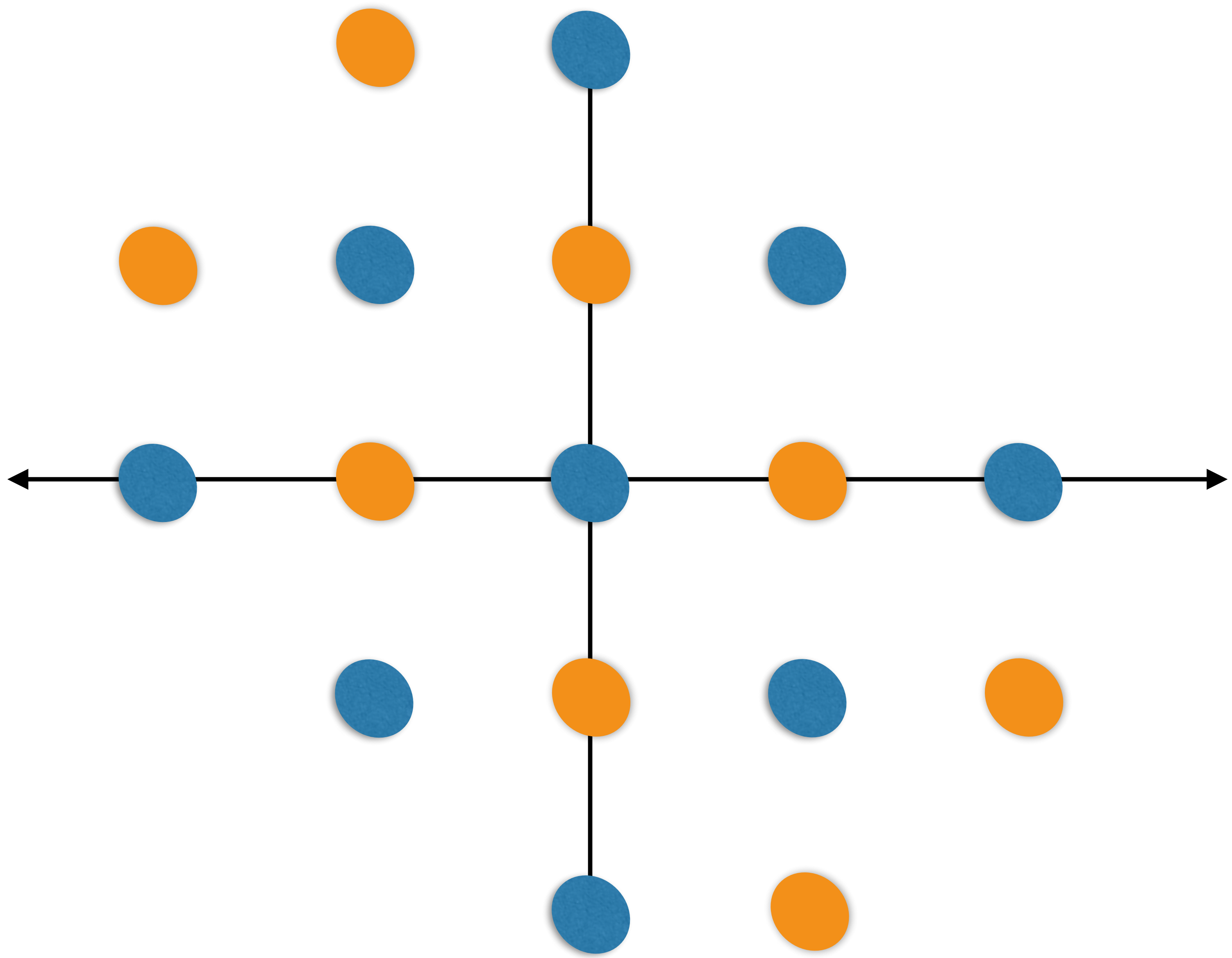
Converting Gaussian Vectors

$$\mathcal{L}^\dagger := \{(\mathbf{y_1}, \mathbf{y_2}) \ : \ \mathbf{y_1} \equiv \mathbf{y_2} \pmod{2\mathcal{L}}\}$$



What about the average of two discrete Gaussian vectors *conditioned on* the result being in the lattice?

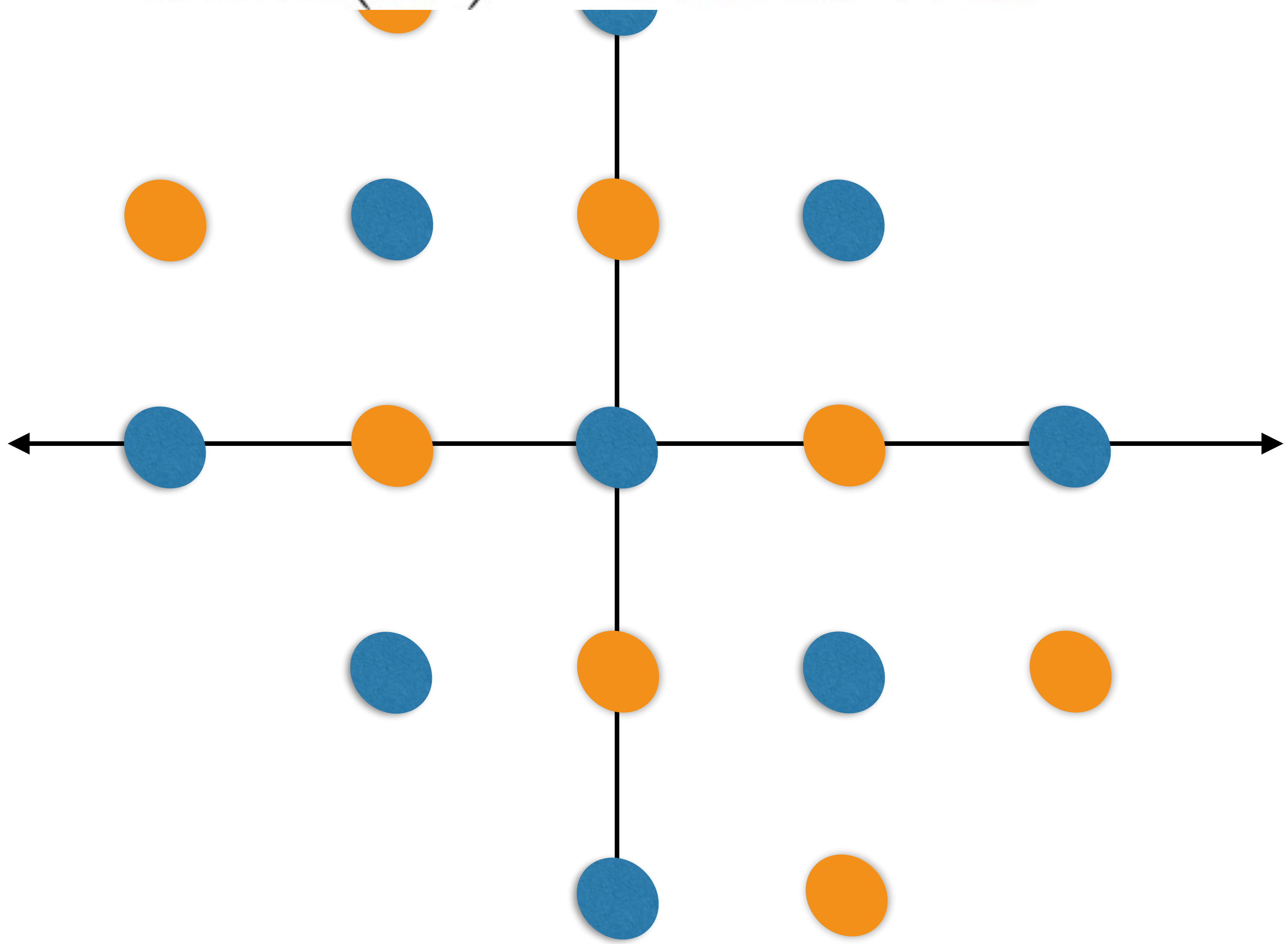
Converting Gaussian Vectors



What about the average of two discrete Gaussian vectors *conditioned on* the result being in the lattice?

Converting Gaussian Vectors

$$\text{rotate}(\mathcal{L}^\dagger) = \sqrt{2}\mathcal{L} \times \sqrt{2}\mathcal{L}$$



What about the average of two discrete Gaussian vectors *conditioned on* the result being in the lattice?

Converting Gaussian Vectors

$$\mathsf{rotate}(\mathcal{L}^{\dagger}) = \sqrt{2}\mathcal{L} \times \sqrt{2}\mathcal{L}$$

Converting Gaussian Vectors

$$\mathsf{rotate}(\mathcal{L}^\dagger) = \sqrt{2}\mathcal{L} \times \sqrt{2}\mathcal{L}$$

$$(\mathbf{y}_1, \mathbf{y}_2) \sim D_{\mathcal{L}^\dagger, s} \Rightarrow \mathsf{rotate}(\mathbf{y}_1, \mathbf{y}_2) \sim D_{\sqrt{2}\mathcal{L} \times \sqrt{2}\mathcal{L}, s}$$

Converting Gaussian Vectors

$$\mathsf{rotate}(\mathcal{L}^\dagger) = \sqrt{2}\mathcal{L} \times \sqrt{2}\mathcal{L}$$

$$(\mathbf{y}_1, \mathbf{y}_2) \sim D_{\mathcal{L}^\dagger, s} \Rightarrow \mathsf{rotate}(\mathbf{y}_1, \mathbf{y}_2) \sim D_{\sqrt{2}\mathcal{L} \times \sqrt{2}\mathcal{L}, s}$$

$$\mathsf{rotate}(\mathbf{y}_1, \mathbf{y}_2) := \left(\frac{\mathbf{y}_1 + \mathbf{y}_2}{\sqrt{2}}, \frac{\mathbf{y}_1 - \mathbf{y}_2}{\sqrt{2}}\right)$$

Converting Gaussian Vectors

$$\text{rotate}(\mathcal{L}^\dagger) = \sqrt{2}\mathcal{L} \times \sqrt{2}\mathcal{L}$$

$$(\mathbf{y}_1, \mathbf{y}_2) \sim D_{\mathcal{L}^\dagger, s} \Rightarrow \text{rotate}(\mathbf{y}_1, \mathbf{y}_2) \sim D_{\sqrt{2}\mathcal{L} \times \sqrt{2}\mathcal{L}, s}$$

$$\text{rotate}(\mathbf{y}_1, \mathbf{y}_2) := \Big(\frac{\mathbf{y}_1 + \mathbf{y}_2}{\sqrt{2}}, \frac{\mathbf{y}_1 - \mathbf{y}_2}{\sqrt{2}}\Big)$$

$$\Big(\frac{\mathbf{y}_1 + \mathbf{y}_2}{2}, \frac{\mathbf{y}_1 - \mathbf{y}_2}{2}\Big) = \frac{\text{rotate}(\mathbf{y}_1, \mathbf{y}_2)}{\sqrt{2}} \sim D_{\mathcal{L} \times \mathcal{L}, s/\sqrt{2}}$$

Converting Gaussian Vectors

$$\mathsf{rotate}(\mathcal{L}^\dagger) = \sqrt{2}\mathcal{L} \times \sqrt{2}\mathcal{L}$$

$$(\mathbf{y}_1, \mathbf{y}_2) \sim D_{\mathcal{L}^\dagger, s} \Rightarrow \mathsf{rotate}(\mathbf{y}_1, \mathbf{y}_2) \sim D_{\sqrt{2}\mathcal{L} \times \sqrt{2}\mathcal{L}, s}$$

$$\mathsf{rotate}(\mathbf{y}_1, \mathbf{y}_2) := \Big(\frac{\mathbf{y}_1 + \mathbf{y}_2}{\sqrt{2}}, \frac{\mathbf{y}_1 - \mathbf{y}_2}{\sqrt{2}}\Big)$$

Progress!

$$\Big(\frac{\mathbf{y}_1 + \mathbf{y}_2}{2}, \frac{\mathbf{y}_1 - \mathbf{y}_2}{2}\Big) = \frac{\mathsf{rotate}(\mathbf{y}_1, \mathbf{y}_2)}{\sqrt{2}} \sim D_{\mathcal{L} \times \mathcal{L}, s/\sqrt{2}}$$

Converting Gaussian Vectors

$$\text{rotate}(\mathcal{L}^{\dagger}) = \sqrt{2}\mathcal{L} \times \sqrt{2}\mathcal{L}$$

$$(\mathbf{y}_1, \mathbf{y}_2) \sim D_{\mathcal{L}^{\dagger},s} \Rightarrow \text{rotate}(\mathbf{y}_1, \mathbf{y}_2) \sim D_{\sqrt{2}\mathcal{L} \times \sqrt{2}\mathcal{L},s}$$

If we sample $\mathbf{y_1}, \mathbf{y_2} \sim D_{\mathcal{L},s}$ *,*
then their average will be distributed as $D_{\mathcal{L},s/\sqrt{2}}$*,*
if we condition on the result being in the lattice.

ogress!

$$\left(\frac{\mathbf{y}_1 + \mathbf{y}_2}{2}, \frac{\mathbf{y}_1 - \mathbf{y}_2}{2}\right) = \frac{\text{rotate}(\mathbf{y}_1, \mathbf{y}_2)}{\sqrt{2}} \sim D_{\mathcal{L} \times \mathcal{L},s/\sqrt{2}}$$

Sampling from the Conditional Distribution

Sampling from the Conditional Distribution

$$\Pr_{\mathbf{y}_1, \mathbf{y}_2 \sim D_{\mathcal{L}, s}} \left[\frac{\mathbf{y}_1 + \mathbf{y}_2}{2} = \mathbf{y} \;\middle|\; \frac{\mathbf{y}_1 + \mathbf{y}_2}{2} \in \mathcal{L} \right]$$

Sampling from the Conditional Distribution

$$\Pr_{\mathbf{y}_1,\mathbf{y}_2\sim D_{\mathcal{L},s}}\left[\frac{\mathbf{y}_1+\mathbf{y}_2}{2}=\mathbf{y}\;\middle|\;\frac{\mathbf{y}_1+\mathbf{y}_2}{2}\in\mathcal{L}\right]$$

$$\propto \sum_{\text{coset }\mathbf{c}} \Pr[D_{\mathcal{L},s}\in\mathbf{c}]^2\cdot \Pr_{\mathbf{y}_1,\mathbf{y}_2\sim D_{\mathcal{L},s}}\left[\frac{\mathbf{y}_1+\mathbf{y}_2}{2}=\mathbf{y}\;\middle|\;\mathbf{y}_1,\mathbf{y}_2\in\mathbf{c}\right]$$

Sampling from the Conditional Distribution

$$\Pr_{\mathbf{y}_1,\mathbf{y}_2 \sim D_{\mathcal{L},s}}\left[\frac{\mathbf{y}_1+\mathbf{y}_2}{2} = \mathbf{y} \;\middle|\; \frac{\mathbf{y}_1+\mathbf{y}_2}{2} \in \mathcal{L}\right]$$

$$\propto \sum_{\text{coset } \mathbf{c}} \Pr[D_{\mathcal{L},s} \in \mathbf{c}]^2 \cdot \Pr_{\mathbf{y}_1,\mathbf{y}_2 \sim D_{\mathcal{L},s}}\left[\frac{\mathbf{y}_1+\mathbf{y}_2}{2} = \mathbf{y} \;\middle|\; \mathbf{y}_1, \mathbf{y}_2 \in \mathbf{c}\right]$$

Input: $\approx 2^n$ samples from $D_{\mathcal{L},s}$

Sampling from the Conditional Distribution

$$\Pr_{\mathbf{y}_1,\mathbf{y}_2 \sim D_{\mathcal{L},s}}\left[\frac{\mathbf{y}_1+\mathbf{y}_2}{2} = \mathbf{y} \;\middle|\; \frac{\mathbf{y}_1+\mathbf{y}_2}{2} \in \mathcal{L}\right]$$

$$\propto \sum_{\text{coset } \mathbf{c}} \Pr[D_{\mathcal{L},s} \in \mathbf{c}]^2 \cdot \Pr_{\mathbf{y}_1,\mathbf{y}_2 \sim D_{\mathcal{L},s}}\left[\frac{\mathbf{y}_1+\mathbf{y}_2}{2} = \mathbf{y} \;\middle|\; \mathbf{y}_1,\mathbf{y}_2 \in \mathbf{c}\right]$$

Input: $\approx 2^n$ samples from $D_{\mathcal{L},s}$

1. Separate the vectors into "buckets" according to their coset.

Sampling from the Conditional Distribution

$$\Pr_{\mathbf{y}_1,\mathbf{y}_2\sim D_{\mathcal{L},s}}\left[\frac{\mathbf{y}_1+\mathbf{y}_2}{2}=\mathbf{y} \;\middle|\; \frac{\mathbf{y}_1+\mathbf{y}_2}{2}\in\mathcal{L}\right]$$

$$\propto \sum_{\text{coset }\mathbf{c}} \Pr[D_{\mathcal{L},s}\in\mathbf{c}]^2 \cdot \Pr_{\mathbf{y}_1,\mathbf{y}_2\sim D_{\mathcal{L},s}}\left[\frac{\mathbf{y}_1+\mathbf{y}_2}{2}=\mathbf{y} \;\middle|\; \mathbf{y}_1,\mathbf{y}_2\in\mathbf{c}\right]$$

Input: $\approx 2^n$ samples from $D_{\mathcal{L},s}$

1. Separate the vectors into "buckets" according to their coset.
2. Pair a number of vectors from each coset proportional to $|\{\mathbf{y}\in\mathbf{c}\}|^2$

Sampling from the Conditional Distribution

$$\Pr_{\mathbf{y}_1,\mathbf{y}_2 \sim D_{\mathcal{L},s}}\left[\frac{\mathbf{y}_1+\mathbf{y}_2}{2} = \mathbf{y} \;\middle|\; \frac{\mathbf{y}_1+\mathbf{y}_2}{2} \in \mathcal{L}\right]$$

$$\propto \sum_{\text{coset } \mathbf{c}} \Pr[D_{\mathcal{L},s} \in \mathbf{c}]^2 \cdot \Pr_{\mathbf{y}_1,\mathbf{y}_2 \sim D_{\mathcal{L},s}}\left[\frac{\mathbf{y}_1+\mathbf{y}_2}{2} = \mathbf{y} \;\middle|\; \mathbf{y}_1, \mathbf{y}_2 \in \mathbf{c}\right]$$

Input: $\approx 2^n$ samples from $D_{\mathcal{L},s}$

1. Separate the vectors into "buckets" according to their coset.
2. Pair a number of vectors from each coset proportional to $|\{\mathbf{y} \in \mathbf{c}\}|^2$
3. Output the averages of the pairs.

Sampling from the Conditional Distribution

$$\Pr_{\mathbf{y}_1,\mathbf{y}_2 \sim D_{\mathcal{L},s}}\left[\frac{\mathbf{y}_1+\mathbf{y}_2}{2} = \mathbf{y} \;\middle|\; \frac{\mathbf{y}_1+\mathbf{y}_2}{2} \in \mathcal{L}\right]$$

$$\propto \sum_{\text{coset } \mathbf{c}} \Pr[D_{\mathcal{L}} \ldots]^2 \ldots \Pr\left[\frac{\mathbf{y}_1+\mathbf{y}_2}{\ldots} \ldots \mathbf{y} \;\middle|\; \mathbf{y}_1,\mathbf{y}_2 \in \mathbf{c}\right]$$

Output will be $D_{\mathcal{L},s/\sqrt{2}}$!!!

Input: $\approx 2^n$ samples from $D_{\mathcal{L},s}$

1. Separate the vectors into "buckets" according to their coset.
2. Pair a number of vectors from each coset proportional to $|\{\mathbf{y} \in \mathbf{c}\}|^2$
3. Output the averages of the pairs.

How Many Vectors Do We Get?

How Many Vectors Do We Get?

$$\# \text{ of output vectors} = T \cdot \sum_{\mathbf{c}} |\{\mathbf{y} \in \mathbf{c}\}|^2$$

How Many Vectors Do We Get?

$$\# \text{ of output vectors} = T \cdot \sum_{\mathbf{c}} |\{\mathbf{y} \in \mathbf{c}\}|^2 \;\; = \frac{\sum_{\mathbf{c}} |\{\mathbf{y} \in \mathbf{c}\}|^2}{\max_{\mathbf{c}} |\{\mathbf{y} \in \mathbf{c}\}|}$$

How Many Vectors Do We Get?

$$M := \#\ \text{input vectors}$$

$$\#\ \text{of output vectors} = T \cdot \sum_{\mathbf{c}} |\{\mathbf{y} \in \mathbf{c}\}|^2 = \frac{\sum_{\mathbf{c}} |\{\mathbf{y} \in \mathbf{c}\}|^2}{\max_{\mathbf{c}} |\{\mathbf{y} \in \mathbf{c}\}|}$$

How Many Vectors Do We Get?

$$M := \#\text{ input vectors}$$

$$\#\text{ of output vectors} = T \cdot \sum_{\mathbf{c}} |\{\mathbf{y} \in \mathbf{c}\}|^2 = \frac{\sum_{\mathbf{c}} |\{\mathbf{y} \in \mathbf{c}\}|^2}{\max_{\mathbf{c}} |\{\mathbf{y} \in \mathbf{c}\}|}$$

$$\approx M \cdot \frac{\sum_{\mathbf{c}} \Pr[D_{\mathcal{L},s} \in \mathbf{c}]^2}{\max_{\mathbf{c}} \Pr[D_{\mathcal{L},s} \in \mathbf{c}]}$$

How Many Vectors Do We Get?

$$M := \# \text{ input vectors}$$

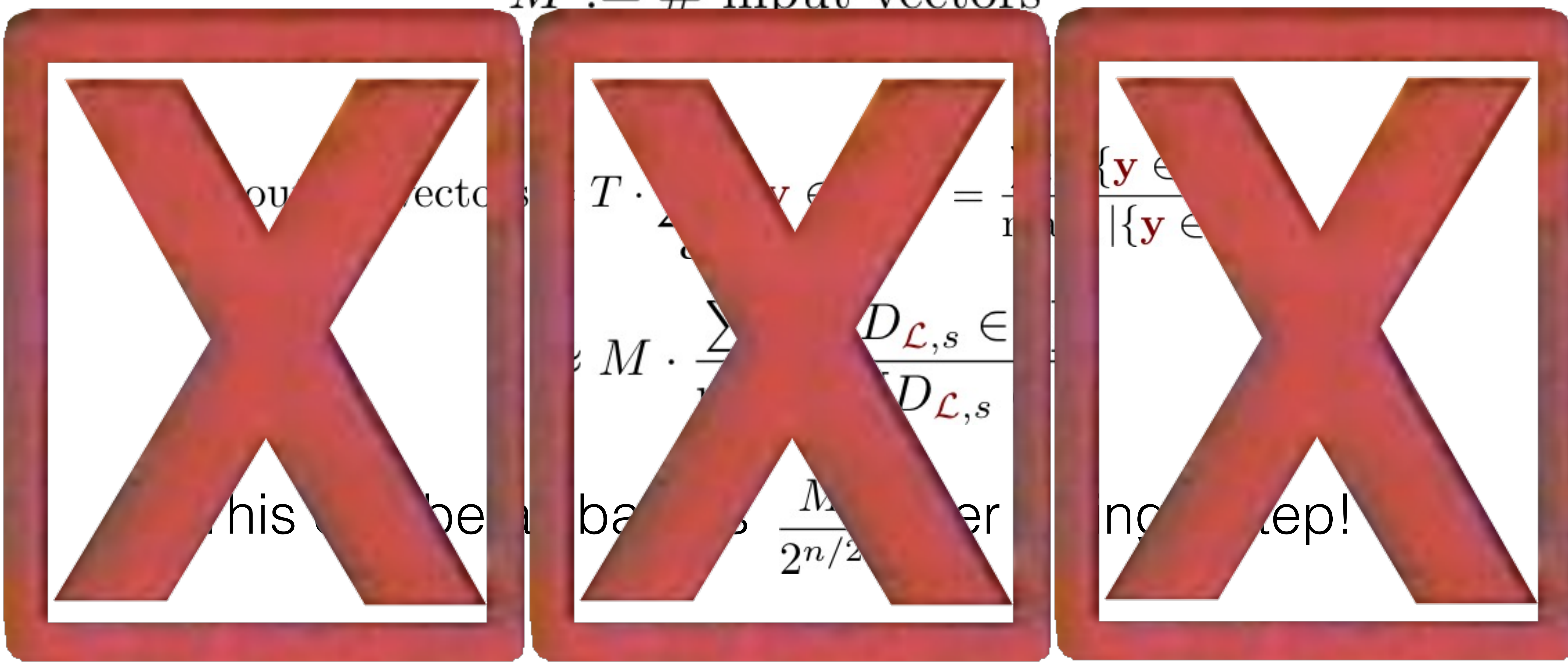
$$\# \text{ of output vectors} = T \cdot \sum_{\mathbf{c}} |\{\mathbf{y} \in \mathbf{c}\}|^2 = \frac{\sum_{\mathbf{c}} |\{\mathbf{y} \in \mathbf{c}\}|^2}{\max_{\mathbf{c}} |\{\mathbf{y} \in \mathbf{c}\}|}$$

$$\approx M \cdot \frac{\sum_{\mathbf{c}} \Pr[D_{\mathcal{L},s} \in \mathbf{c}]^2}{\max_{\mathbf{c}} \Pr[D_{\mathcal{L},s} \in \mathbf{c}]}$$

This can be as bad as $\frac{M}{2^{n/2}}$ after a single step!

How Many Vectors Do We Get?

$$M := \#\text{ input vectors}$$



How Many Vectors Do We Get?

How Many Vectors Do We Get?

$$\#\text{ of output vectors } \approx M \cdot \frac{\sum_{\mathbf{c}} \Pr[D_{\mathcal{L},s} \in \mathbf{c}]^2}{\max_{\mathbf{c}} \Pr[D_{\mathcal{L},s} \in \mathbf{c}]}$$

How Many Vectors Do We Get?

$$\#\text{ of output vectors } \approx M \cdot \frac{\sum_{\mathbf{c}} \Pr[D_{\mathcal{L},s} \in \mathbf{c}]^2}{\max_{\mathbf{c}} \Pr[D_{\mathcal{L},s} \in \mathbf{c}]}$$

$$\sum_{\mathbf{c}} \Pr[D_{\mathcal{L},s} \in \mathbf{c}]^2 = \frac{\rho_s(\mathcal{L}^\dagger)}{\rho_s(\mathcal{L})^2}$$

How Many Vectors Do We Get?

$$\#\text{ of output vectors } \approx M \cdot \frac{\sum_{\mathbf{c}} \Pr[D_{\mathcal{L},s} \in \mathbf{c}]^2}{\max_{\mathbf{c}} \Pr[D_{\mathcal{L},s} \in \mathbf{c}]}$$

$$\sum_{\mathbf{c}} \Pr[D_{\mathcal{L},s} \in \mathbf{c}]^2 = \frac{\rho_s(\mathcal{L}^\dagger)}{\rho_s(\mathcal{L})^2}$$

$$= \frac{\rho_s(\sqrt{2}\mathcal{L} \times \sqrt{2}\mathcal{L})}{\rho_s(\mathcal{L})^2}$$

How Many Vectors Do We Get?

$$\#\text{ of output vectors } \approx M \cdot \frac{\sum_{\mathbf{c}} \Pr[D_{\mathcal{L},s} \in \mathbf{c}]^2}{\max_{\mathbf{c}} \Pr[D_{\mathcal{L},s} \in \mathbf{c}]}$$

$$\sum_{\mathbf{c}} \Pr[D_{\mathcal{L},s} \in \mathbf{c}]^2 = \frac{\rho_s(\mathcal{L}^\dagger)}{\rho_s(\mathcal{L})^2}$$

$$= \frac{\rho_s(\sqrt{2}\mathcal{L} \times \sqrt{2}\mathcal{L})}{\rho_s(\mathcal{L})^2}$$

$$= \frac{\rho_{s/\sqrt{2}}(\mathcal{L})^2}{\rho_s(\mathcal{L})^2}$$

How Many Vectors Do We Get?

How Many Vectors Do We Get?

$$\#\text{ of output vectors } \approx M \cdot \frac{\rho_{s/\sqrt{2}}(\mathcal{L})^2}{\rho_s(\mathcal{L})^2 \max_{\mathbf{c}} \Pr[D_{\mathcal{L},s} \in \mathbf{c}]}$$

How Many Vectors Do We Get?

$$\#\text{ of output vectors } \approx M \cdot \frac{\rho_{s/\sqrt{2}}(\mathcal{L})^2}{\rho_s(\mathcal{L})^2 \max_{\mathbf{c}} \Pr[D_{\mathcal{L},s} \in \mathbf{c}]}$$

$$= M \cdot \frac{\rho_{s/\sqrt{2}}(\mathcal{L})^2}{\rho_s(\mathcal{L})\rho_s(2\mathcal{L})}$$

How Many Vectors Do We Get?

$$\# \text{ of output vectors } \approx M \cdot \frac{\rho_{s/\sqrt{2}}(\mathcal{L})^2}{\rho_s(\mathcal{L})^2 \max_{\mathbf{c}} \Pr[D_{\mathcal{L},s} \in \mathbf{c}]}$$

$$= M \cdot \frac{\rho_{s/\sqrt{2}}(\mathcal{L})^2}{\rho_s(\mathcal{L})\rho_s(2\mathcal{L})}$$

$$= M \cdot \frac{\rho_{s/\sqrt{2}}(\mathcal{L})^2}{\rho_s(\mathcal{L})\rho_{s/2}(\mathcal{L})}$$

How Many Vectors Do We Get?

How Many Vectors Do We Get?

$$\#\text{ of output vectors after } \ell \text{ steps } \approx M \cdot \prod_{i=0}^{\ell} \frac{\rho_{2^{-\frac{i+1}{2}}s}(\mathcal{L})^2}{\rho_{2^{-\frac{i}{2}}s}(\mathcal{L})\rho_{2^{-\frac{i+2}{2}}s}(\mathcal{L})}$$

How Many Vectors Do We Get?

$$\#\text{ of output vectors after } \ell \text{ steps} \approx M \cdot \prod_{i=0}^{\ell} \frac{\rho_{2^{-\frac{i+1}{2}}s}(\mathcal{L})^2}{\rho_{2^{-\frac{i}{2}}s}(\mathcal{L})\rho_{2^{-\frac{i+2}{2}}s}(\mathcal{L})}$$

$$= M \cdot \frac{\rho_{s/\sqrt{2}}(\mathcal{L})}{\rho_s(\mathcal{L})} \cdot \frac{\rho_{2^{-\frac{\ell+1}{2}}s}(\mathcal{L})}{\rho_{2^{-\frac{\ell+2}{2}}s}(\mathcal{L})}$$

How Many Vectors Do We Get?

$$\#\text{ of output vectors after } \ell \text{ steps} \approx M \cdot \prod_{i=0}^{\ell} \frac{\rho_{2^{-\frac{i+1}{2}}s}(\mathcal{L})^2}{\rho_{2^{-\frac{i}{2}}s}(\mathcal{L})\rho_{2^{-\frac{i+2}{2}}s}(\mathcal{L})}$$

$$= M \cdot \frac{\rho_{s/\sqrt{2}}(\mathcal{L})}{\rho_s(\mathcal{L})} \cdot \frac{\rho_{2^{-\frac{\ell+1}{2}}s}(\mathcal{L})}{\rho_{2^{-\frac{\ell+2}{2}}s}(\mathcal{L})}$$

$$\geq M \cdot 2^{-n/2}$$

How Many Vectors Do We Get?

$$\#\text{ of output vectors after } \ell \text{ steps } \approx M \cdot \prod_{i=0}^{\ell} \frac{\rho_{2^{-\frac{i+1}{2}}s}(\mathcal{L})^2}{\rho_{2^{-\frac{i}{2}}s}(\mathcal{L})\rho_{2^{-\frac{i+2}{2}}s}(\mathcal{L})}$$

$$= M \cdot \frac{\rho_{s/\sqrt{2}}(\mathcal{L})}{\rho_s(\mathcal{L})} \cdot \frac{\rho_{2^{-\frac{\ell+1}{2}}s}(\mathcal{L})}{\rho_{2^{-\frac{\ell+2}{2}}s}(\mathcal{L})}$$

$$\geq M \cdot 2^{-n/2}$$

Setting $M \approx 2^n$ gives $\#$ output vectors $\approx 2^{n/2}$

How Many Vectors Do We Get?

$$\#\ \text{of output vectors after } \ell \text{ steps} \approx M \cdot \prod_{i=0}^{\ell} \frac{\rho_{2^{-\frac{i+1}{2}}s}(\mathcal{L})^2}{\rho_{2^{-\frac{i}{2}}s}(\mathcal{L})\rho_{2^{-\frac{i+2}{2}}s}(\mathcal{L})}$$

Recall that we only need 1.38^n samples to solve SVP!

$$= M \cdot \frac{\rho_{s/\sqrt{2}}(\mathcal{L})}{\rho_s(\mathcal{L})} \cdot \frac{\rho_{2^{-\frac{\ell+1}{2}}s}(\mathcal{L})}{\rho_{2^{-\frac{\ell+2}{2}}s}(\mathcal{L})}$$

$$\geq M \cdot 2^{-n/2}$$

Setting $M \approx 2^n$ gives $\#\ \text{output vectors} \approx 2^{n/2}$

How Many Vectors Do We Get?

$$\#\text{ of output vectors after } \ell \text{ steps} \approx M \cdot \prod_{i=0}^{\ell} \frac{\rho_{2^{-\frac{i+1}{2}}s}(\mathcal{L})^2}{\rho_{2^{-\frac{i}{2}}s}(\mathcal{L})\,\rho_{2^{-\frac{i+2}{2}}s}(\mathcal{L})}$$

Recall that we only need 1.38^n samples to solve SVP!

$$= M \cdot \frac{\rho_{s/\sqrt{2}}(\mathcal{L})}{\rho_s(\mathcal{L})} \cdot \frac{\rho_{2^{-\frac{\ell+1}{2}}s}(\mathcal{L})}{\rho_{2^{-\frac{\ell+2}{2}}s}(\mathcal{L})}$$

$$\geq M \cdot 2^{-n/2}$$

Setting $M \approx 2^n$ gives $\#\text{ output vectors} \approx 2^{n/2}$

Final Algorithm

Final Algorithm

$\mathsf{SVPSolver}(\mathcal{L})$

Final Algorithm

$\mathsf{SVPSolver}(\mathcal{L})$

1. Use GPV to get $\approx 2^n$ samples from $D_{\mathcal{L},s}$ with $s \gg \lambda_1(\mathcal{L})$.

Final Algorithm

$\mathsf{SVPSolver}(\mathcal{L})$

1. Use GPV to get $\approx 2^n$ samples from $D_{\mathcal{L},s}$ with $s \gg \lambda_1(\mathcal{L})$.
2. Run the ("squaring") discrete Gaussian combiner on the result repeatedly.

Final Algorithm

SVPSolver($\mathcal{L}$)

1. Use GPV to get $\approx 2^n$ samples from $D_{\mathcal{L},s}$ with $s \gg \lambda_1(\mathcal{L})$.
2. Run the ("squaring") discrete Gaussian combiner on the result repeatedly.
3. Output $\approx 2^{n/2}$ samples from $D_{\mathcal{L},s}$ with $s \approx \lambda_1(\mathcal{L})/\sqrt{n}$.

Final Algorithm

SVPSolver($\mathcal{L}$)

1. Use GPV to get $\approx 2^n$ samples from $D_{\mathcal{L},s}$ with $s \gg \lambda_1(\mathcal{L})$.
2. Run the ("squaring") discrete Gaussian combiner on the result repeatedly.
3. Output $\approx 2^{n/2}$ samples from $D_{\mathcal{L},s}$ with $s \approx \lambda_1(\mathcal{L})/\sqrt{n}$.
4. We can then simply output a shortest non-zero vector from our samples.

Summary of Results

Summary of Results

Discussed in this talk

Summary of Results

Discussed in this talk

- $2^{n+o(n)}$ algorithm for SVP.

Summary of Results

Discussed in this talk

- $2^{n+o(n)}$ algorithm for SVP.
- We actually can sample $2^{n/2}$ vectors from $D_{\mathcal{L},s}$ for any s in time $2^{n+o(n)}$.

Summary of Results

Discussed in this talk

- $2^{n+o(n)}$ algorithm for SVP.
- We actually can sample $2^{n/2}$ vectors from $D_{\mathcal{L},s}$ for any s in time $2^{n+o(n)}$.

Additional results from this work

Summary of Results

Discussed in this talk

- $2^{n+o(n)}$ algorithm for SVP.
- We actually can sample $2^{n/2}$ vectors from $D_{\mathcal{L},s}$ for any s in time $2^{n+o(n)}$.

Additional results from this work

- $2^{n/2+o(n)}$-time algorithm for sampling $2^{n/2}$ vectors above smoothing.

Summary of Results

Discussed in this talk

- $2^{n+o(n)}$ algorithm for SVP.
- We actually can sample $2^{n/2}$ vectors from $D_{\mathcal{L},s}$ for any s in time $2^{n+o(n)}$.

Additional results from this work

- $2^{n/2+o(n)}$-time algorithm for sampling $2^{n/2}$ vectors above smoothing.
  - 1.93-GapSVP.

Summary of Results

Discussed in this talk

- $2^{n+o(n)}$ algorithm for SVP.
- We actually can sample $2^{n/2}$ vectors from $D_{\mathcal{L},s}$ for any s in time $2^{n+o(n)}$.

Additional results from this work

- $2^{n/2+o(n)}$-time algorithm for sampling $2^{n/2}$ vectors above smoothing.
  - 1.93-GapSVP.
  - .422-BDD.

Summary of Results

Discussed in this talk

- $2^{n+o(n)}$ algorithm for SVP.
- We actually can sample $2^{n/2}$ vectors from $D_{\mathcal{L},s}$ for any s in time $2^{n+o(n)}$.

Additional results from this work

- $2^{n/2+o(n)}$-time algorithm for sampling $2^{n/2}$ vectors above smoothing.
  - 1.93-GapSVP.
  - .422-BDD.
  - $\sqrt{n \log n}$ -SIVP.

Summary of Results

Discussed in this talk

- $2^{n+o(n)}$ algorithm for SVP.
- We actually can sample $2^{n/2}$ vectors from $D_{\mathcal{L},s}$ for any s in time $2^{n+o(n)}$.

Additional results from this work

- $2^{n/2+o(n)}$-time algorithm for sampling $2^{n/2}$ vectors above smoothing.
  - 1.93-GapSVP.
  - .422-BDD.
  - $\sqrt{n \log n}$ -SIVP.

Recent addition

Summary of Results

Discussed in this talk

- $2^{n+o(n)}$ algorithm for SVP.
- We actually can sample $2^{n/2}$ vectors from $D_{\mathcal{L},s}$ for any s in time $2^{n+o(n)}$.

Additional results from this work

- $2^{n/2+o(n)}$-time algorithm for sampling $2^{n/2}$ vectors above smoothing.
  - 1.93-GapSVP.
  - .422-BDD.
  - $\sqrt{n \log n}$ -SIVP.

Recent addition

- Sampling from $D_{\mathcal{L},s}$ reduces to SVP. [S15, preprint]

Summary of Results

Discussed in this talk

- $2^{n+o(n)}$ algorithm for SVP.
- We actually can sample $2^{n/2}$ vectors from $D_{\mathcal{L},s}$ for any s in time $2^{n+o(n)}$.

Additional results from this work

- $2^{n/2+o(n)}$-time algorithm for sampling $2^{n/2}$ vectors above smoothing.
  - 1.93-GapSVP.
  - .422-BDD.
  - $\sqrt{n \log n}$ -SIVP.

Recent addition

- Sampling from $D_{\mathcal{L},s}$ reduces to SVP. [S15, preprint]
  - (Not equivalence because the reduction in the other direction requires 1.38^n samples.)

Open Questions/Future Work

- Other uses for discrete Gaussian sampling at arbitrary parameters?
- Faster discrete Gaussian sampling?
- Is centered discrete Gaussian sampling NP-hard? (Conjecture: No. Can we prove it?)
- Lower bounds for CVP/SVP assuming SETH (or something similar)?

Thanks!

Thanks!