

WORST-CASE TO AVERAGE-CASE REDUCTIONS

PHONG NGUYEN

<http://www.di.ens.fr/~pnguyen>

October 2026



TODAY

- SIS and LWE
- Variants of SIS and LWE
- The SIS Worst-Case to Average-Case Reduction
 - Proving that Short Vectors Exist
 - Mordell's Proof
 - The SIS Reduction
 - Sampling Lattice Vectors

SIS AND LWE



THE SIMPLEST HARDEST LATTICES

- Let $G = \mathbf{Z} / q\mathbf{Z}$
 - Pick $g_1, \dots, g_m$ uniformly at random mod q .
 - Goal: Find short $\mathbf{x} = (x_1, \dots, x_m) \in \mathbf{Z}^m$ s.t. $\sum_i x_i g_i \equiv 0 \pmod{q}$.
-
- This is finding a short lattice vector for random lattices L such that $\mathbf{Z}^m / L \sim \mathbf{Z} / q\mathbf{Z}$.
 - The SVP challenges uses such lattices for 10m-bit prime q .

THE SIS PROBLEM (1996): SMALL INTEGER SOLUTIONS

- Let $(G, +)$ be a finite Abelian group: $G = (\mathbb{Z} / q\mathbb{Z})^n$ in [Ajtai96]. View G as a $\mathbb{Z}$ -module.
- Pick $g_1, \dots, g_m$ uniformly at random from G .
- Goal: Find short $(\mathbf{x}_1, \dots, \mathbf{x}_m) \in \mathbb{Z}^m$ s.t. $\sum_i \mathbf{x}_i g_i = 0$,
e.g. $\|\mathbf{x}\| \leq m (\#G)^{1/m}$.
- This is essentially finding a short vector in a (uniform) **random lattice** of $L_m(G) = \{ \text{lattices } L \subseteq \mathbb{Z}^m \text{ s.t. } \mathbb{Z}^m / L \sim G \}$.

WORST-CASE TO AVERAGE-CASE REDUCTION

- [Ajtai96]: If one can efficiently solve SIS for $G=(\mathbb{Z}/q_n\mathbb{Z})^n$ on the average, then one can efficiently find short vectors in **every n-dim** lattice.
- [GINX16]: This can be generalized to any sequence (G_n) of finite abelian groups, provided that **$\#G_n$ is sufficiently large** $\geq n^{\Omega(\max(n, \text{rank}(G)))}$ and m too. Ex: $(\mathbb{Z}/2\mathbb{Z})^n$ is not.

HOW ABOUT BDD/CVP?

THE SIMPLEST HARDEST LATTICES

- Let $G = \mathbb{Z} / q\mathbb{Z}$
 - Pick $g_1, \dots, g_m$ and a target $\vec{t} \in \mathbb{Z}^m$
 - What does it mean to find a close lattice vector to $\vec{t}$? Find $\mathbf{x} = (x_1, \dots, x_m) \in \mathbb{Z}^m$ s.t. $\sum_i x_i g_i \equiv 0 \pmod{q}$ and $\|\vec{x} - \vec{t}\|$ small
- Let $\vec{t} = (t_1, \dots, t_m)$ and $h = \sum_{i=1}^m t_i g_i$
- Then $h \equiv \sum_{i=1}^m (t_i - x_i) g_i$, so we can express h as a small linear combination of $g_1, \dots, g_m$

THE SIMPLEST HARDEST LATTICES

- Let $G = \mathbb{Z} / q\mathbb{Z}$
- Pick $g_1, \dots, g_m$ and h uniformly at random mod q
- Goal: Find short $\mathbf{x} = (\mathbf{x}_1, \dots, \mathbf{x}_m) \in \mathbb{Z}^m$ s.t. $\sum_i \mathbf{x}_i g_i \equiv h \pmod{q}$.
 - This is finding a close lattice vector for random lattices L such that $\mathbb{Z}^m / L \sim \mathbb{Z} / q\mathbb{Z}$.
 - Consider the map $\varphi : (\mathbb{Z} / q\mathbb{Z})^m \rightarrow \mathbb{Z} / q\mathbb{Z}$ defined by $\varphi(x_1, \dots, x_m) = \sum_{i=1}^m x_i g_i$
 - If m is large, then is surjective with high probability. Why?
 - Then we can find efficiently $(t_1, \dots, t_m) \in \mathbb{Z}^m$ s.t. $h \equiv \sum_{i=1}^m t_i g_i$
 - Then we can find a solution $\mathbf{x}$ by finding a lattice point close to $\vec{t} = (t_1, \dots, t_m)$.

THE SIS ONE-WAY FUNCTION

- Let $(G, +)$ be a finite Abelian group
- Pick $g_1, \dots, g_m$ uniformly at random from G .
- Let f : short $(\mathbf{x}_1, \dots, \mathbf{x}_m) \in \mathbb{Z}^m \mapsto \sum_i \mathbf{x}_i g_i \in G$.
 - f is many-to-one.
 - Given $h = \sum_i \mathbf{y}_i g_i \in G$, finding a short $(\mathbf{x}_1, \dots, \mathbf{x}_m) \in \mathbb{Z}^m$ s.t. $h = \sum_i \mathbf{x}_i g_i \in G$ is as hard as SIS.

DUALITY

- Remember the SIS lattice:
 - $g_1, \dots, g_m$ in some finite Abelian group $(G, +)$
 - $L = \{\mathbf{x} = (\mathbf{x}_1, \dots, \mathbf{x}_m) \in \mathbb{Z}^m \text{ s.t. } \sum_i \mathbf{x}_i g_i = 0\}$
- The **dual lattice** of L is related to the dual group $G^\times$ of (additive) characters of G : morphisms from G to $\mathbf{T} = \mathbb{R}/\mathbb{Z}$
 - $L^\times = \{(\mathbf{y}_1, \dots, \mathbf{y}_m) \in \mathbb{R}^m \text{ s.t. for some } s \in G^\times, \text{ for all } i \mathbf{y}_i \equiv s(g_i) \pmod{1}\}$

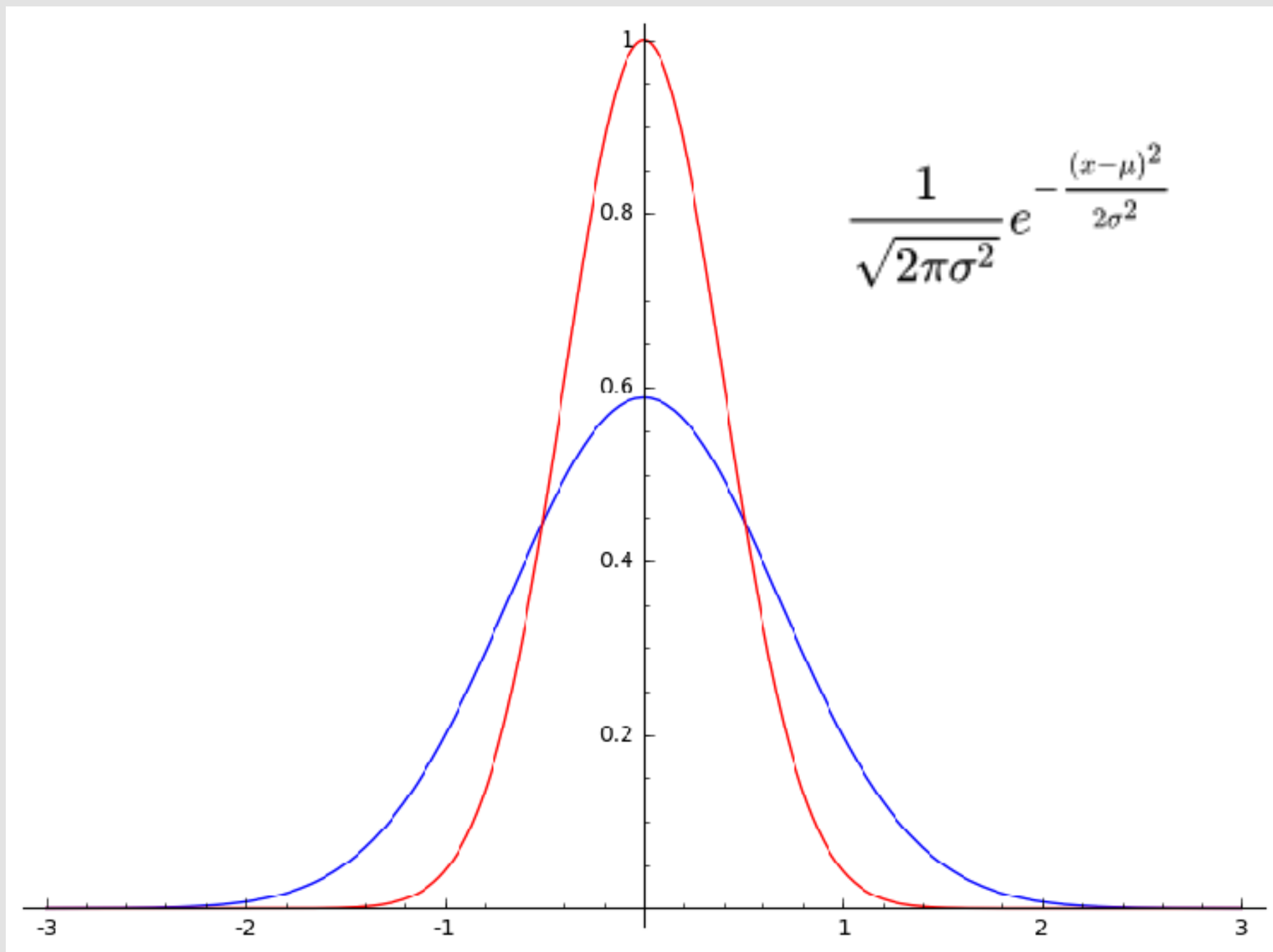
WHY?

- Let $\mathbf{x} \in L$: $\mathbf{x} = (\mathbf{x}_1, \dots, \mathbf{x}_m) \in \mathbb{Z}^m$ s.t. $\sum_i \mathbf{x}_i g_i = 0$
- For any character s in $G^\times$, we have $s(\sum_i \mathbf{x}_i g_i) = 0$ in $\mathbf{T} = \mathbf{R} / \mathbf{Z}$ so $\sum_i \mathbf{x}_i s(g_i) = 0$
- Hence, for any $(\mathbf{y}_1, \dots, \mathbf{y}_m) \in \mathbf{R}^m$ s.t. for all i $\mathbf{y}_i \equiv s(g_i) \pmod{1}$, we have
$$\sum_{i=1}^m x_i y_i \in \mathbb{Z} \text{ so } (\mathbf{y}_1, \dots, \mathbf{y}_m) \in L^\times$$
- Reciprocally if $\sum_{i=1}^m x_i y_i \in \mathbb{Z}$ whenever $\sum_i \mathbf{x}_i g_i = 0$, there is s in $G^\times$ s.t. for all i $\mathbf{y}_i \equiv s(g_i) \pmod{1}$. This defines s over the subgroup generated by the g_i 's:
if $\sum_{i=1}^m a_i g_i = \sum_{i=1}^m b_i g_i$ then $s(\sum_{i=1}^m a_i g_i) = s(\sum_{i=1}^m b_i g_i)$ because
$$\sum_{i=1}^m (a_i - b_i) g_i = 0 \text{ implies that } \sum_{i=1}^m (a_i - b_i) y_i \in \mathbb{Z}$$

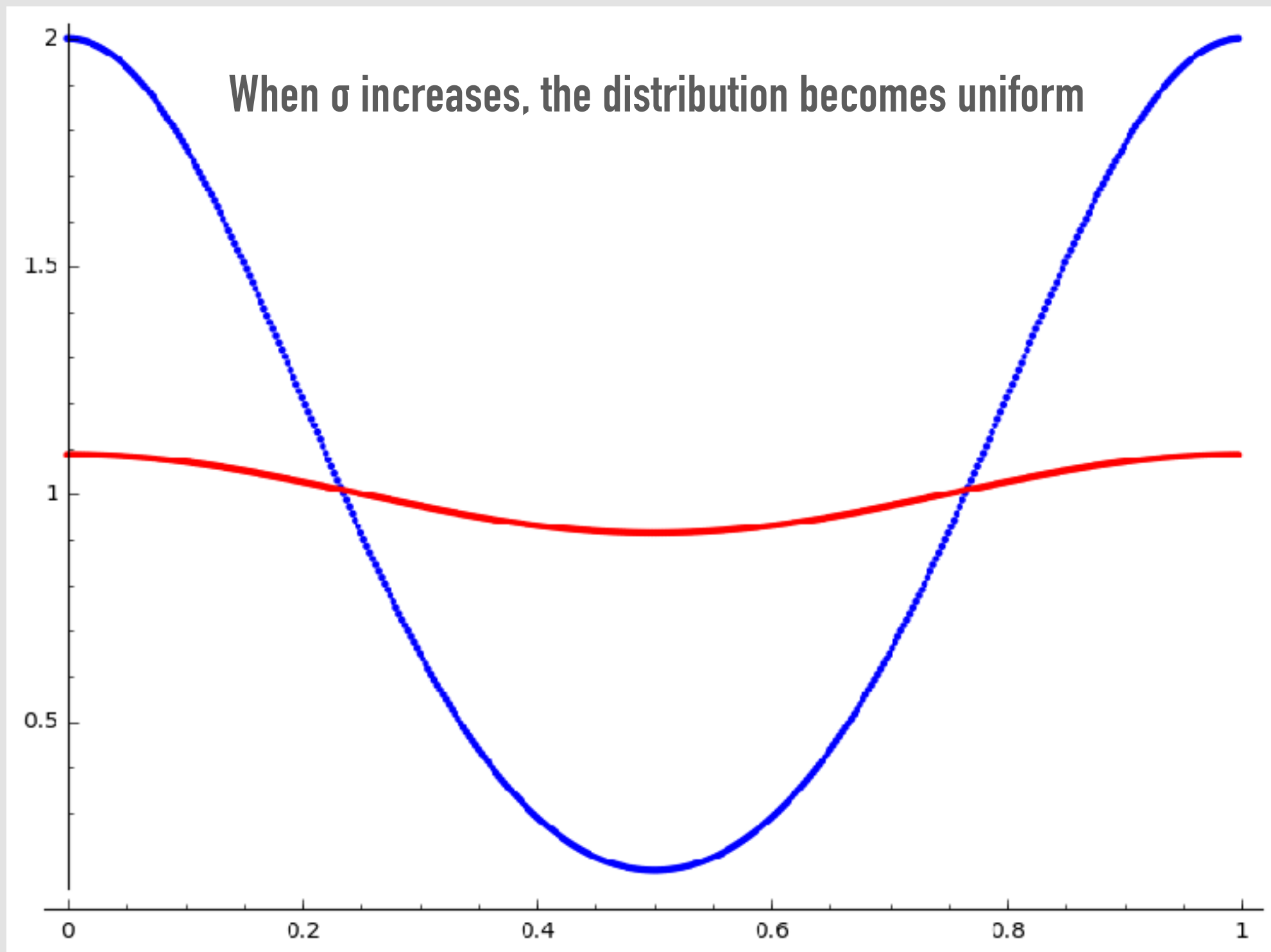
THE LWE PROBLEM: LEARNING (A CHARACTER) WITH ERRORS

- Let $(G, +)$ be any finite Abelian group.
 - e.g. $G = (\mathbb{Z} / q\mathbb{Z})^n$ in [Re05]
- Pick $g_1, \dots, g_m$ uniformly at random from G .
- Pick a random **character** s in $G^\times$.
- Goal: recover **s** given $g_1, \dots, g_m$ and **noisy** approximations of $s(g_1), \dots, s(g_m)$.
 - Ex: Gaussian noise

GAUSSIAN NOISE OVER R



GAUSSIAN NOISE OVER THE TORUS R/Z



EX: CYCLIC G

- Let $G = \mathbb{Z} / q\mathbb{Z}$. Then the dual group is $G^\times = \left\{ x \mapsto \frac{ax}{q} \bmod 1 \right\}_{a \in \mathbb{Z}/q}$
 - Pick $g_1, \dots, g_m$ uniformly at random mod q .
 - Goal: recover $s \in \mathbb{Z}$ given $g_1, \dots, g_m$ and randomized approximations of $sg_1 \bmod q, \dots, sg_m \bmod q$.
- This is exactly a randomized variant of Boneh-Venkatesan's **Hidden Number Problem** from CRYPTO '96.

HARDNESS OF LWE

- [Regev05]: If one can efficiently solve LWE for $G=(\mathbf{Z} / q_n\mathbf{Z})^n$ on the average, then one can **quantum**-efficiently find short vectors in **every** **n-dim** lattice.
- [GINX16]: This can be generalized to any sequence (G_n) of finite abelian groups, provided that **$\#G_n$ is sufficiently large**.

INTERPRETATION

- If you believe that finding short vectors in lattices is hard in the worst case, even for quantum computers, then SIS and LWE are hard on the average.
- However, is that true?
 - New AI-assisted preprints claim subexponential algorithms solving LWE.
 - But when plugged into the worst-case to average-case reduction, it does not seem to give better lattice algorithms.

DECISIONAL-LWE

- Let $(G, +)$ be any finite Abelian group.
 - e.g. $G = (\mathbf{Z} / q\mathbf{Z})^n$ in [Re05]
- Pick $g_1, \dots, g_m$ uniformly at random from G .
- Pick a random **character** s in $G^\vee$.
- Goal: Distinguish $(g_1, \dots, g_m, \text{noisy approximations of } s(g_1), \dots, s(g_m))$ and uniform samples of $G^m \times (\mathbf{R} / \mathbf{Z})^m$

SIS AND DECISIONAL-LWE

- Suppose that one finds a short $(\mathbf{x}_1, \dots, \mathbf{x}_m) \in \mathbb{Z}^m$ s.t. $\sum_i \mathbf{x}_i \mathbf{g}_i = 0$.
- What can you say about $\sum_i \mathbf{x}_i \mathbf{y}_i$
 - If $y_1, \dots, y_m$ are random in $\mathbb{R}/\mathbb{Z}$.
 - If $y_1, \dots, y_m$ are approximations of $\mathbf{s}(\mathbf{g}_1), \dots, \mathbf{s}(\mathbf{g}_m)$ with a small Gaussian noise

VARIANTS OF SIS AND LWE



VARIANTS OF SIS AND LWE

- Replace the $\mathbf{Z}$ -module by an $\mathbf{R}$ -module, to make the problems more efficient.
- Change the distribution of:
 - the LWE noise
 - the secret character

RING TRADEOFFS

- NTRU [HPS98] proposed to use **special** lattices: better efficiency, yet stronger hardness assumption.
- Starting with [Mi02], one can obtain ‘**restricted**’ worst-case to average-case reductions:
 - The worst-case now refers to a special class of lattices, e.g. **ideal lattices** or **module lattices**.

M-SIS: SIS OVER MODULES

- Let M be a finite R -module for some ring R : $R=\mathbb{Z}$ in SIS.
- Pick $g_1, \dots, g_m \in M$ uniformly at random.
- Goal: find short $(\mathbf{x}_1, \dots, \mathbf{x}_m) \in R^m$ s.t. $\sum_i \mathbf{x}_i g_i = 0$.
- If R^m is a lattice, this is finding a short vector in some **random (module) sublattice** of R^m .
- Ex: NTRU used $m=2$, $R=\mathbb{Z}[X]/(X^N-1)$ and $M=\mathbb{Z}[X]/(q, X^N-1)$ but g_1 =public key, $g_2=-1$.

M-LWE: LWE OVER MODULES

- This is used in Kyber and Dilithium.
- Kyber uses the ring $R = (\mathbb{Z}/q\mathbb{Z})[X] / (X^N + 1)$ with $N=256$ and $q=3329$
- A is a small random square matrix in R : 2×2 , 3×3 , or 4×4 .
- Secret key: small vector $\mathbf{s}$ with coefficients in R .
- Public key: $\mathbf{t} = A\mathbf{s} + \mathbf{e}$ in R where $\mathbf{e}$ is a small noise.
- Distribution of noise $\mathbf{e}$ and secret $\mathbf{s}$:
- Each coefficient mod q is a binomial over $\{-2, -1, 0, 1, 2\}$:
 - Add 2 random bits and subtract 2 random bits

Sampling from a binomial distribution. Noise in KYBER is sampled from a centered binomial distribution B_η for $\eta = 2$ or $\eta = 3$. We define B_η as follows:

Sample $(a_1, \dots, a_\eta, b_1, \dots, b_\eta) \leftarrow \{0, 1\}^{2\eta}$

and output $\sum_{i=1}^{\eta} (a_i - b_i)$.

WORST-CASE TO AVERAGE-CASE REDUCTIONS FOR MODULES

- [LaSt14]: If one can efficiently solve M-SIS for $M=(R/qR)^d$ where R is the ring of integers of a cyclotomic field, then one can efficiently find short vectors in **every module lattice of R^d** .
- This generalizes previous ideal-lattice reductions for $d=1$ [Mi02,LyMi06].
- Similar results for M-LWE [LaSt14] generalizing Ring-LWE hardness [LPR10].

THE SIS WORST-CASE TO AVERAGE-CASE REDUCTION



PROVING THAT SHORT VECTORS EXIST

SHORT LATTICE VECTORS: MINKOWSKI'S INEQUALITY

- [Minkowski]: Any d -dim lattice L has at least one non-zero vector of norm $\leq 2 \frac{\Gamma(1 + d/2)^{1/d}}{\sqrt{\pi}} \text{covol}(L)^{1/d} \leq \sqrt{d} \text{covol}(L)^{1/d}$
- This is **Minkowski's inequality**.



Hermann Minkowski

FOUR PROOFS OF MINKOWSKI'S INEQUALITY

- Blichfeldt's proof: «continuous» pigeon-hole principle.
- Minkowski's original proof: sphere packings.
- Siegel's proof: Poisson summation.
- Mordell's proof: pigeon-hole principle.



MORDELL'S PROOF (1933)

REMEMBER BLICHFELDT'S PROOF

- The short lattice vector is some $u-v$ where $u,v \in F$ for a well-chosen convex (**infinite**) set F .

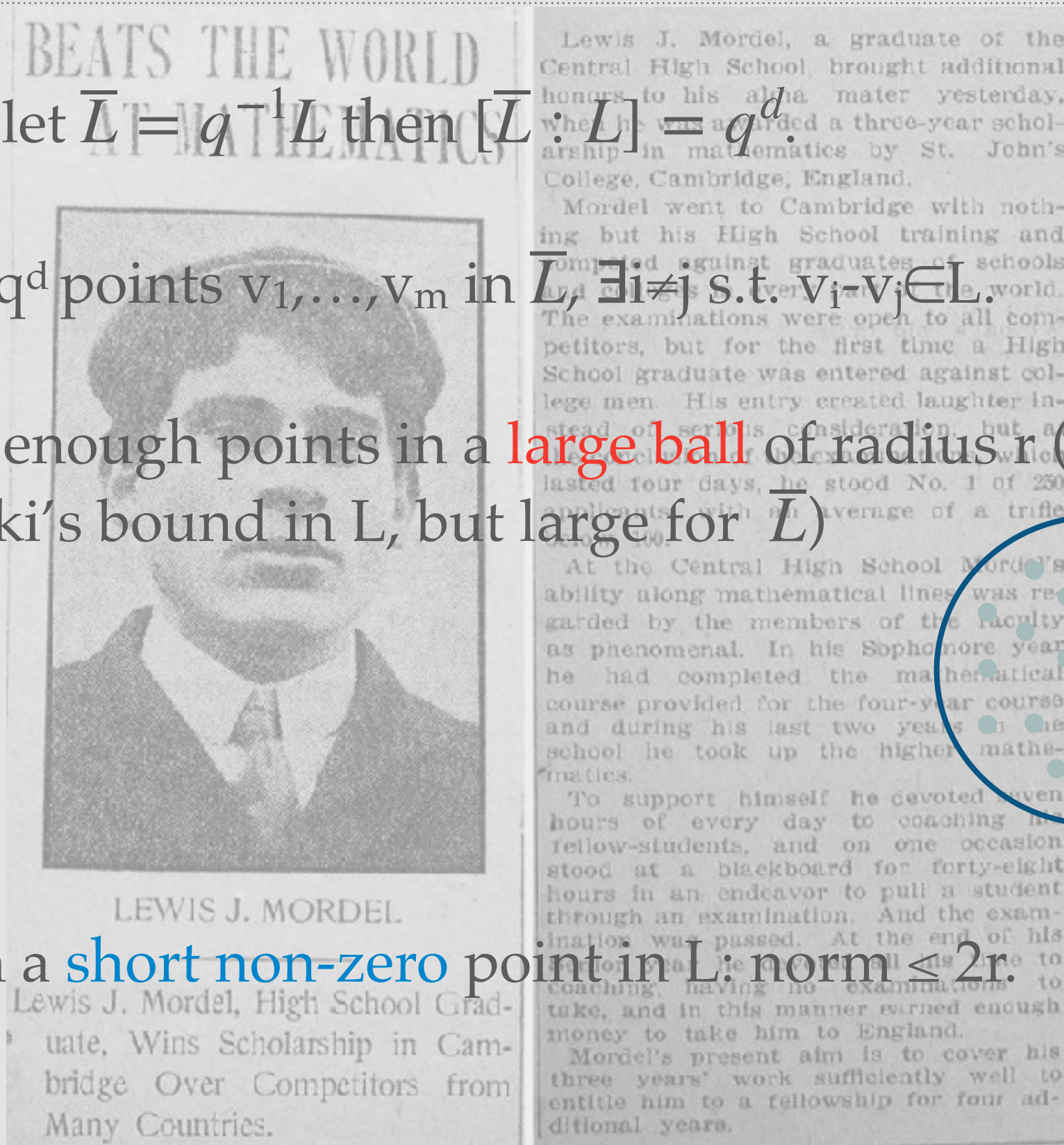


Hans Frederick Blichfeldt

- Mordell's proof uses a **finite** F .

MORDELL'S PROOF (1933)

- For $q \in \mathbb{N}$, let $\bar{L} = q^{-1}L$ then $[\bar{L} : L] = q^d$.
- Among $> q^d$ points $v_1, \dots, v_m$ in $\bar{L}$, $\exists i \neq j$ s.t. $v_i - v_j \in L$.
- There are enough points in a **large ball** of radius r (r is close to Minkowski's bound in L , but large for $\bar{L}$)



- We obtain a **short non-zero** point in L : $\text{norm} \leq 2r$.

KEY POINT

- Mordell proved the existence of short lattice vectors by using the existence of short vectors in a **special** class of **higher-dimensional integer** lattices.



Louis Joel Mordell

- Let distinct $v_1, \dots, v_m \in \bar{L} = q^{-1}L$.
- Consider the integer lattice L' formed by all $(x_1, \dots, x_m) \in \mathbb{Z}^m$ s.t. $\sum_i x_i v_i \in L$.
 - If $m > q^d$, $\lambda_1(L') \leq \sqrt{2}$.

AN ALGORITHM FROM MORDELL'S PROOF

- Mordell's proof gives an (**inefficient**) algorithm:
 - Need to generate $>q^d$ lattice points in $\bar{L}$.
 - Among these exponentially many lattice points, find a difference in L , possibly by **exhaustive search**.
 - Both steps are expensive.
- [BGJ14] and [ADRS15] are more efficient randomized variants of Mordell's algorithm: sampling over $\bar{L}$ may allow to sample over L .

WISHFUL THINKING

- To apply the pigeon-hole principle, we need an exponential number m of lattice vectors in $\bar{L}$.
- Can we get away with a **small polynomial number m** and make the algorithm efficient? (unlike [BGJ14] and [ADRS15])
- Maybe if we could find short vectors in certain higher-dimensional random lattices.

THE SIS REDUCTION

REMEMBER SIS

- Let $(G, +)$ be a finite Abelian group: $G = (\mathbb{Z} / q\mathbb{Z})^n$ in [Ajtai96]. View G as a $\mathbb{Z}$ -module.
- Pick $g_1, \dots, g_m$ uniformly at random from G .
- Goal: Find short $(\mathbf{x}_1, \dots, \mathbf{x}_m) \in \mathbb{Z}^m$ s.t. $\sum_i \mathbf{x}_i g_i = 0$,
e.g. $\|\mathbf{x}\| \leq m (\#G)^{1/m}$.
- This is essentially finding a short vector in a (uniform) **random lattice** of $L_m(G) = \{ \text{lattices } L \subseteq \mathbb{Z}^m \text{ s.t. } \mathbb{Z}^m / L \sim G \}$.

OVERLATTICES AND GROUPS

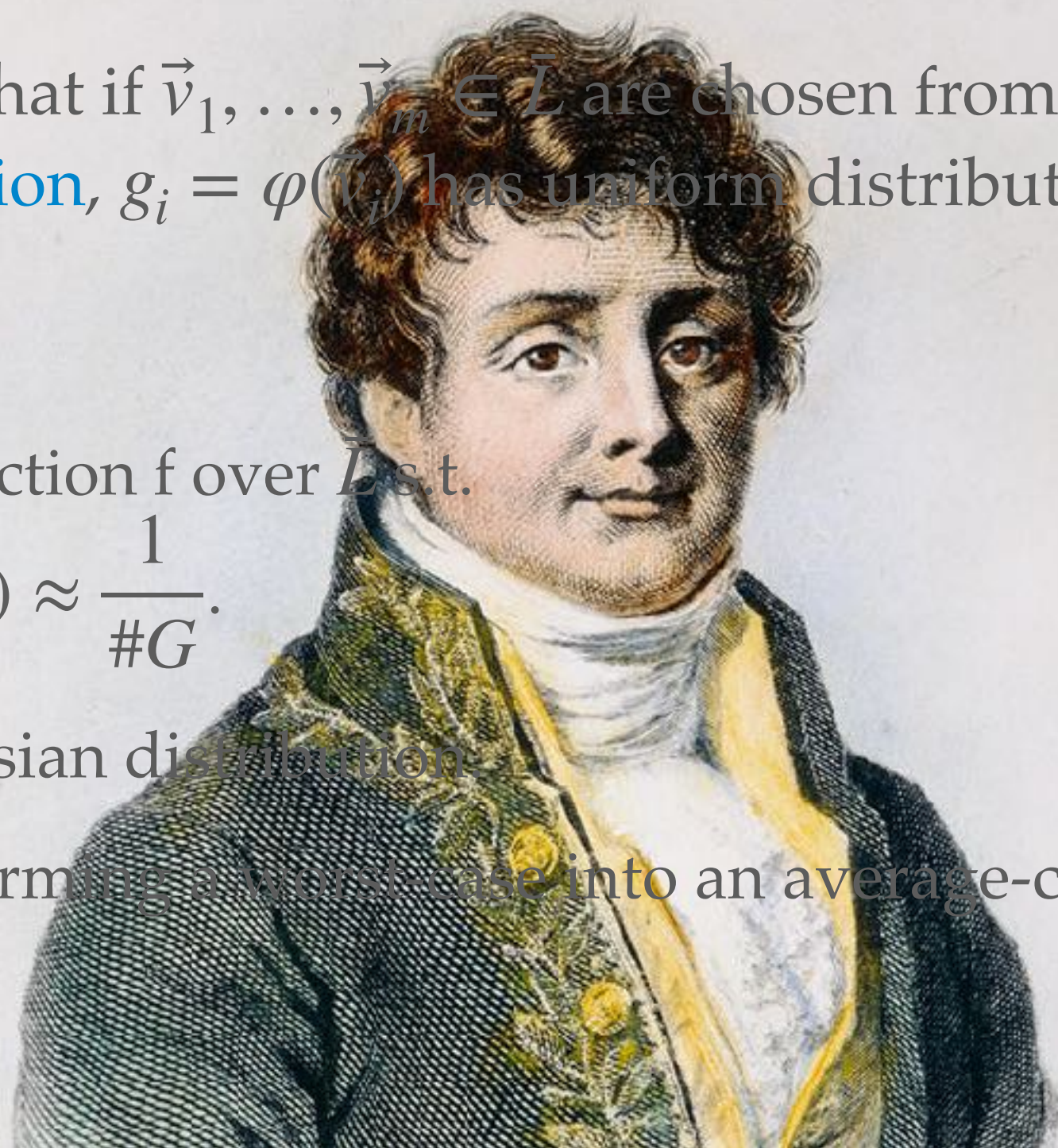
- If L is n -dim, $\bar{L} = q^{-1}L$ and $G = (\mathbf{Z} / q\mathbf{Z})^n$ then $\bar{L}/L \simeq G$.
- There is a surjective morphism $\phi : \bar{L} \rightarrow G$ such that $L = \text{Ker}(\phi)$
- ϕ is efficiently computable: which ϕ ?
- Let $v_1, \dots, v_m \in \bar{L}$ and define $g_1, \dots, g_m \in G$ by $g_i = \phi(v_i)$.
- Then $\sum_i \mathbf{x}_i g_i = 0$ for $(\mathbf{x}_1, \dots, \mathbf{x}_m) \in \mathbf{Z}^m$ iff $\sum_i \mathbf{x}_i v_i \in L$.

WORST-TO-AVERAGE REDUCTION FROM MORDELL'S PROOF

- Sample short $v_1, \dots, v_m \in \bar{L}$ from a suitable distribution, so that $g_i = \phi(v_i)$ has uniform distribution over $G = (\mathbf{Z} / q\mathbf{Z})^n$
- Call the SIS-oracle on $(g_1, \dots, g_m)$ to find a short $\mathbf{x} = (x_1, \dots, x_m) \in \mathbf{Z}^m$ s.t. $\sum_i x_i g_i = 0$ in G , i.e. $\sum_i x_i v_i \in L$.
- Return $\sum_i x_i v_i \in L$.

KEYPOINT: FOURIER ANALYSIS

- Fourier analysis shows that if $\vec{v}_1, \dots, \vec{v}_m \in \bar{L}$ are chosen from a **suitable (short) distribution**, $g_i = \varphi(\vec{v}_i)$ has uniform distribution over G .
- Any probability mass function f over $\bar{L}$ s.t.
for any $\vec{x} \in \bar{L}$, $\sum_{\vec{y} \in L} f(\vec{x} + \vec{y}) \approx \frac{1}{\#G}$.
 - Ex: discrete Gaussian distribution.
- This is a **key step**: transforming a worst-case into an average-case.



Joseph Fourier

WHY FOURIER ANALYSIS?

- Recall Poisson's summation: if $f : \mathbb{R} \rightarrow \mathbb{C}$ is a "nice" function, then

$$\sum_{n \in \mathbb{Z}} f(n) = \sum_{n \in \mathbb{Z}} \hat{f}(n) \text{ where } \hat{f}(n) = \int_{-\infty}^{+\infty} f(t) e^{-2i\pi n t} dt \text{ and more}$$

$$\text{generally } \forall x \in \mathbb{R} \quad \sum_{n \in \mathbb{Z}} f(x + n) = \sum_{n \in \mathbb{Z}} \hat{f}(n) e^{2i\pi n x}$$

- In arbitrary dimension, if $f : \mathbb{R}^n \rightarrow \mathbb{C}$ is a "nice" function and L is a

$$\text{full-rank lattice in } \mathbb{R}^n, \text{ then } \sum_{\vec{x} \in L} f(\vec{x}) = \frac{1}{\text{covol}(L)} \sum_{\vec{y} \in L^\times} \hat{f}(\vec{y}) \text{ and more}$$

$$\text{generally } \forall \vec{x} \in \mathbb{R}^n \quad \sum_{\vec{y} \in L} f(\vec{x} + \vec{y}) = \sum_{\vec{y} \in L^\times} \hat{f}(\vec{y}) e^{2i\pi \langle \vec{x}, \vec{y} \rangle}$$

WHY FOURIER ANALYSIS?

- We'd like $\forall \vec{x} \in \mathbb{R}^n \quad \sum_{\vec{y} \in L} f(\vec{x} + \vec{y}) = \sum_{\vec{y} \in L^\times} \hat{f}(\vec{y}) e^{2i\pi \langle \vec{x}, \vec{y} \rangle}$ to be nearly constant over $\vec{x}$.
- $\sum_{\vec{y} \in L^\times} \hat{f}(\vec{y}) e^{2i\pi \langle \vec{x}, \vec{y} \rangle} = \hat{f}(0) + \sum_{\vec{y} \in L^\times \setminus \{0\}} \hat{f}(\vec{y}) e^{2i\pi \langle \vec{x}, \vec{y} \rangle}$ so we want $\sum_{\vec{y} \in L^\times \setminus \{0\}} \hat{f}(\vec{y}) e^{2i\pi \langle \vec{x}, \vec{y} \rangle}$ to be uniformly small.
 - $\lambda_1(L^\times)$ is related to $1/\lambda_n(L)$
 - The Fourier transform of a Gaussian function is Gaussian with inverse parameter: if $f(\vec{x}) = e^{-\pi \|\vec{x}\|^2 / s^2}$ then $\hat{f}(\vec{x}) = e^{-\pi s^2 \|\vec{x}\|^2}$
 - If s is big enough, then $\hat{f}(\vec{y})$ will be very small.
 - $\|\vec{y}\| \geq \lambda_1(L^\times) \geq 1/\lambda_n(L)$ so we need s somewhat larger than $\lambda_n(L)$.

SAMPLING LATTICE VECTORS

GAUSSIAN MEASURE

- Though lattices are **infinite**, there is a **natural probability distribution** over lattice points, introduced by [Ba1993] for **transference**.
- This **Gaussian measure** was implicitly used in [Klein00]'s **randomized variant** of Babai's nearest-plane algorithm to solve BDD.
- [Regev2005] noted that the Gaussian measure could **sometimes** be sampled.
- [GPV2008] rediscovered [Klein00] and showed that it samples from the Gaussian measure.



Philip N. Klein



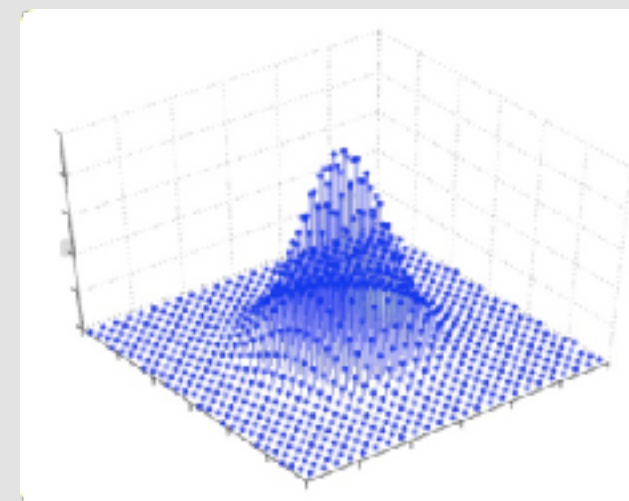
Oded Regev

GAUSSIAN MEASURE

- Center c , parameter s
- Mass of $x \in L$ proportional to

$$\rho_{s,\vec{c}}(\vec{x}) = e^{-\pi \left\| \frac{\vec{x} - \vec{c}}{s} \right\|^2}$$

- The distribution is **independent** of a basis.



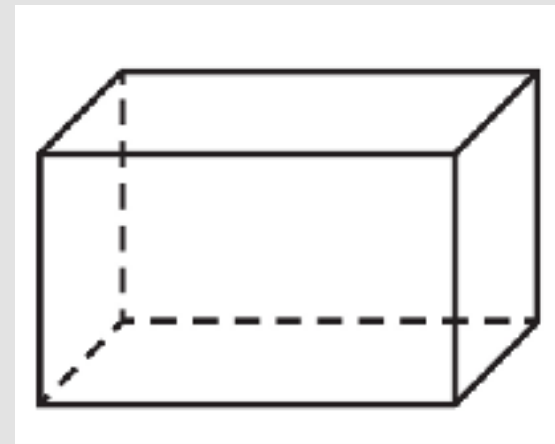
- Introduced in [Ba93], then used in cryptography in [Cai99,Regev03,MiRe04,...]

INTUITION

- Beyond a so-called smoothing parameter, the discrete Gaussian distribution behaves like a continuous Gaussian.
- This smoothing parameter is a bit larger than $\lambda_n(L)$.
- If X is a real Gaussian with standard deviation beyond the smoothing parameter, then $X \bmod 1$ is uniform over $\mathbb{R}/\mathbb{Z}$.
- If X is a multivariate Gaussian of $\mathbb{R}^n$ with standard deviation beyond the smoothing parameter, then $X \bmod L$ is uniform over $\mathbb{R}^n/L$.

BABAI'S NEAREST PLANE ALGORITHM

- Input: a basis $(\vec{b}_1, \dots, \vec{b}_n)$ of a lattice L and a target $\vec{t}$ in $\text{span}(L)$.
- Output: a lattice point $\vec{u}$ such that $\vec{t} - \vec{u} \in \left\{ \sum_{i=1}^n x_i \vec{b}_i^*, -1/2 \leq x_i < 1/2 \right\}$ where the $\vec{b}_i^*$'s are the Gram-Schmidt orthogonalization.



- For $i=n$ downto 1

- Compute $\mu_i = \frac{\langle \vec{t}, \vec{b}_i^* \rangle}{\|\vec{b}_i^*\|^2}$

- $\vec{t} \leftarrow \vec{t} - \lfloor \mu_i \rfloor \vec{b}_i$

- Return

$$\vec{u} = \sum_{i=1}^n \lfloor \mu_i \rfloor \vec{b}_i$$

RANDOMIZING BABAI'S NEAREST PLANE ALGORITHM

- Input: a basis $(\vec{b}_1, \dots, \vec{b}_n)$ of a lattice L and a target $\vec{t}$ in $\text{span}(L)$.
- Output: a "random" lattice point $\vec{u}$ "close" to $\vec{t}$.
- For $i=n$ downto 1
 - Compute $\mu_i = \frac{\langle \vec{t}, \vec{b}_i^\star \rangle}{\|\vec{b}_i^\star\|^2}$ and
 - $x_i = \text{RandomizedRounding}(\mu_i) = \text{ShortElement}(\mu_i + \mathbb{Z})$
 - $\vec{t} \leftarrow \vec{t} - x_i \vec{b}_i$
- Return
 - $\vec{u} = \sum_{i=1}^n x_i \vec{b}_i$

GOAL

- We want to output $\vec{u} \in L$ with probability proportional to $\rho_{s,\vec{t}}(\vec{u}) = e^{-\pi\|\vec{u}-\vec{t}\|^2/s^2}$
- Here, $\vec{t} - \vec{u} = \sum_{i=1}^n (\mu_i - x_i) \vec{b}_i^\star$
- The sample is close to the discrete Gaussian distribution if s is a bit larger than the smoothing parameter of $\mathbb{Z}^n$ multiplied by $\max_{1 \leq i \leq n} \|\vec{b}_i^\star\|$
 - The better the basis, the smaller s can be
 - This is the Klein / GPV discrete gaussian sampler.