Lattice Problems

Phong Nguyễn

INVENTORS FOR THE DIGITAL WORLD

ÉCOLE NORMALE SUPÉRIEURE

Lattice Algorithms

- Input = integer matrix, whose rows span the lattice. Parameters:
  - Size of basis coefficients
  - Lattice dimension
- Asymptotically:
  - dim increases
  - coeff-size polynomial in dim.

Euclid with Vectors

- If $b_1,\ldots,b_n \in \mathbf{Z}^m$, $L(b_1,\ldots,b_n)$ is a lattice: can you efficiently find a lattice basis?
- This would be our first non-trivial lattice algorithm.
  - If n=2 and m=1, this is exactly the gcd problem, so we are trying to generalize Euclid's algorithm.

Hard Lattice Problems

- Since 1996, lattices are very trendy in classical and quantum complexity theory.
- Depending on the dimension d:

	approx. factor	
NP-hardness	$O(1)$	1
non NP-hardness (NP∩co-NP)	$\sqrt{d}$	
worst-case/average-case reduction	$d \log d$	
cryptography	$d^{O(1)}$	
subexp-time algorithms	$2^{\sqrt{d}}$	
poly-time algorithms	$2^{\frac{d \log \log d}{\log d}}$	∞

Hard Lattice Problems

- Input: a lattice L and an n-dim ball C.
- Output: decide if $L \cap C$ is non-trivial, and find a point when applicable. Easy if $L = \mathbf{Z}^n$.
- Two settings
  - Approx: $L \cap C$ has many points. Ex: SIS and ISIS.
  - Unique: only one non-trivial point. Ex: BDD.

The Shortest Vector Problem (SVP)

- Input: a basis of a d-dim lattice L
- Output: nonzero $v \in L$ minimizing $||v||$ i.e. $||v|| = \lambda_1(L)$

2	0	0	0	0
0	2	0	0	0
0	0	2	0	0
0	0	0	2	0
1	1	1	1	1

Relaxing SVP

- Input: a basis of a d-dim lattice L.
- Output: nonzero $v \in L$ such that
- Approximate-SVP: $\|v\| \leq f(d) \; \lambda_1(L)$ [relative]
- Hermite-SVP: $\|v\| \leq g(d) \; vol(L)^{1/d}$ [absolute]

Lattice Challenges

WILMINGTON, MA (PRWEB) FEBRUARY 05, 2015

Security Innovation is pleased to launch the NTRU Challenge today, February 5th, 2015. The NTRU Challenge will increase the understanding of the shortest vector problem in NTRU lattices while encouraging and stimulating further research into the security analysis of NTRU-based cryptosystems. The NTRU Challenge has been designed to provide additional information to users of NTRU public key cryptosystems to aid in their selection of suitable key lengths for a desired level of security.

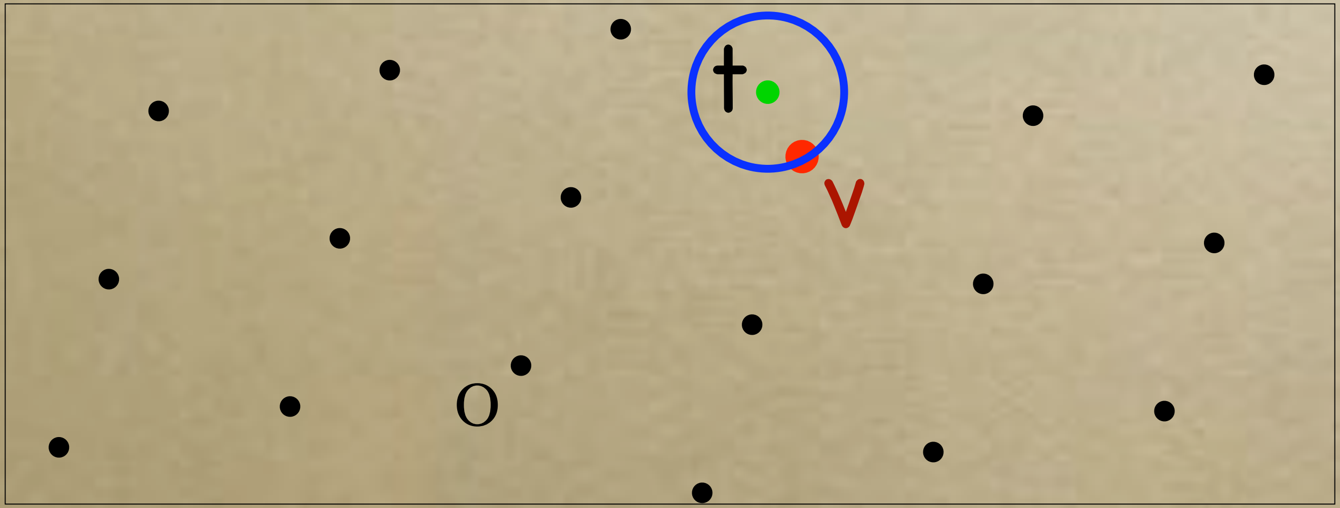
Access the challenge here: http://www.SecurityInnovation.com/NTRUChallenge

The Challenge asks participants to compute the NTRU private keys from the given list of public keys and associated system parameters. This is the type of problem faced by hackers who wish to defeat an NTRU-based cryptosystem. The Challenge consists of several individual NTRU challenges, targeted at different security levels, some of which can be solved in a day, some in a few months and some which are considered to be computationally intractable.

The prize for the first correct solution for the 11 lower security level challenges will be $1,000 each, with $5,000 being awarded per solution for the 16 higher security level challenges. Additionally, participants who arrive at innovative and unique solutions may be chosen for induction into the NTRU Hall of Fame, an award which includes an all-expenses paid trip to a major cryptographic conference.

The Closest Vector Problem (CVP)

- Input: a basis of a lattice L of dim d, and a target vector t.
- Output: v∈L minimizing ||v-t||.



- BDD (bounded distance decoding): special case when t is very close to L.

Intuition

- SVP is not harder than CVP: if one can solve exact CVP, one can solve exact SVP.

Random Instances

- Which distributions of integer lattices (SVP and CVP) and target (CVP/BDD)?
- A full-rank integer lattice $L \subseteq \mathbf{Z}^m$ defines a finite Abelian group $\mathbf{Z}^m/L$. Two different lattices can define the same quotient.
- Can we fix a quotient, then generate a random lattice with that quotient?

The SIS Problem (1996): Small Integer Solutions

- Let (G,+) be a finite Abelian group: $G=(\mathbf{Z}/q\mathbf{Z})^n$ in [Ajtai96]. View G as a $\mathbf{Z}$-module.
- Pick $g_1,\ldots,g_m$ uniformly at random from G.
- Goal: Find short $(x_1,\ldots,x_m)\in\mathbf{Z}^m$ s.t. $\sum_i x_i g_i = 0$, e.g. $||x|| \le m\ (\#G)^{1/m}$.
- This is essentially finding a short vector in a (uniform) random lattice of $L_m(G) = \{$ lattices $L\subseteq\mathbf{Z}^m$ s.t. $\mathbf{Z}^m/L \sim G$ $\}$.

Ex: Cyclic G

- Let $G = \mathbf{Z}/q\mathbf{Z}$
- Pick $g_1,\ldots,g_m$ uniformly at random mod q.
- Goal: Find short $x=(x_1,\ldots,x_m)\in\mathbf{Z}^m$ 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 $\mathbf{Z}^m/L \sim \mathbf{Z}/q\mathbf{Z}$.

Worst-case to Average-case Reduction

- [Ajtai96]: If one can efficiently solve SIS for $G=(\mathbf{Z}/q_n\mathbf{Z})^n$ 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 $\geq n^{\Omega(\max(n,\mathrm{rank}(G)))}$ and m too. Ex: $(\mathbf{Z}/2\mathbf{Z})^n$ is not.

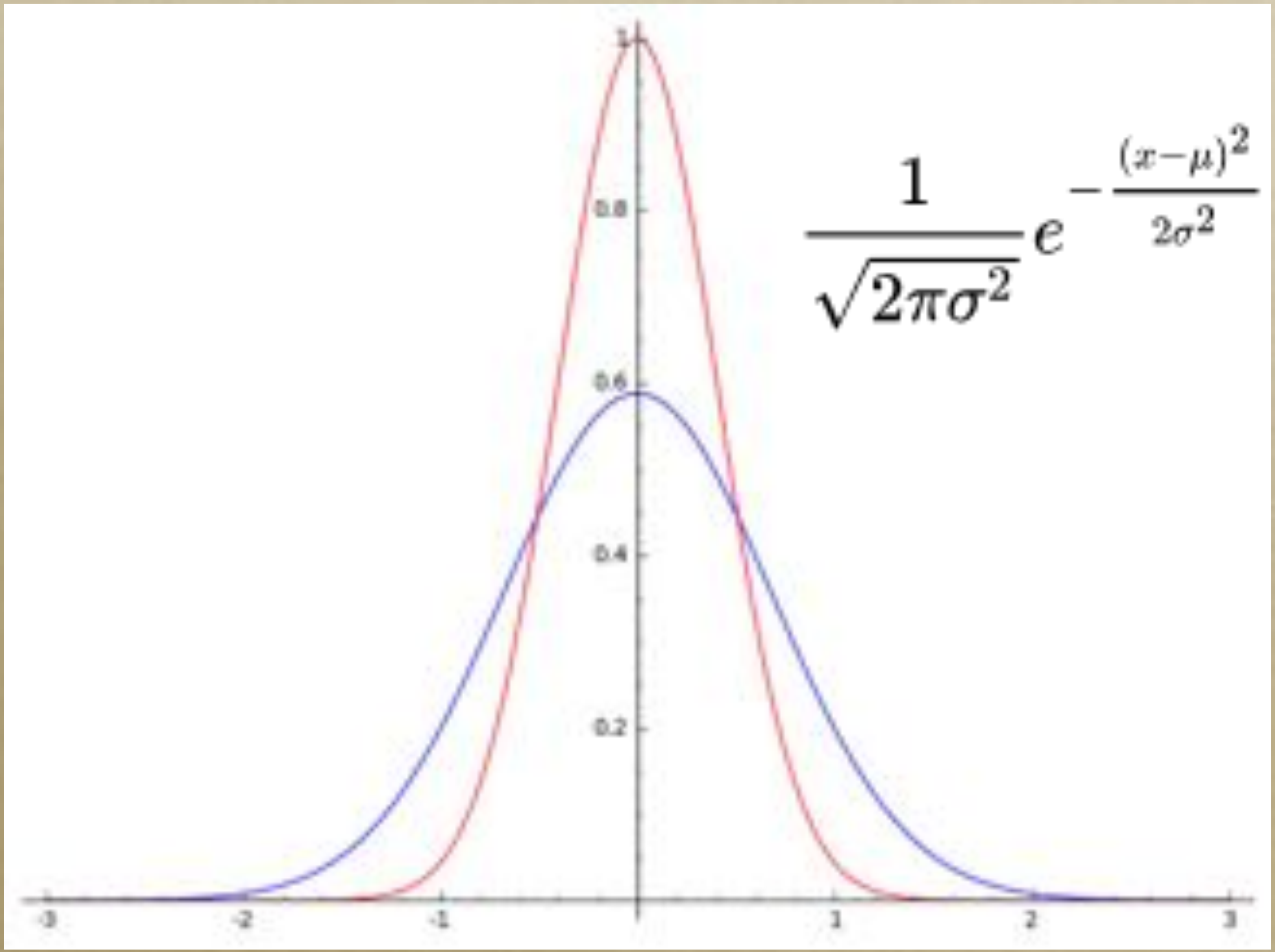
Duality

- Remember the SIS lattice:
  - $g_1,\dots,g_m$ in some finite Abelian group $(G,+)$
  - $L=\{x=(x_1,\dots,x_m)\in\mathbf{Z}^m$ s.t. $\sum_i x_i g_i = 0\}$
- The dual lattice of L is related to the dual group $G^\vee$ of (additive) characters of G: morphisms from G to **T=R/Z**
  - $L^\vee=\{(y_1,\dots,y_m)\in\mathbf{R}^m$ s.t. for some $s\in G^\vee$, for all i $y_i \equiv s(g_i) \pmod 1\}$

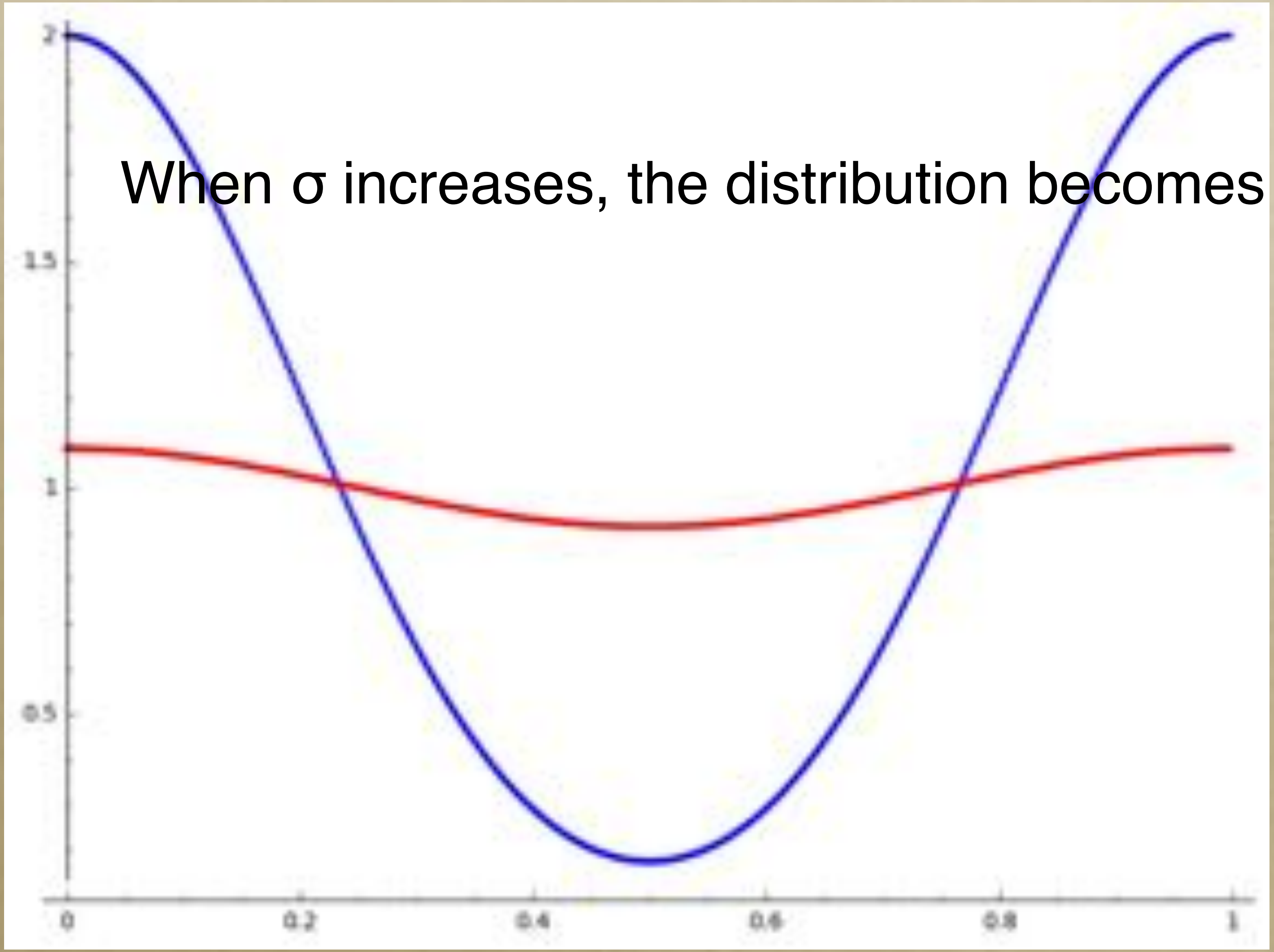
The LWE Problem: Learning (a Character) with Errors

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

Gaussian Noise over **R**



Gaussian Noise over **R/Z**



When σ increases, the distribution becomes uniform

Ex: Cyclic G

- Let $G = \mathbf{Z}/q\mathbf{Z}$
- Pick $g_1,\ldots,g_m$ uniformly at random mod q.
- Goal: recover $s \in \mathbf{Z}$ given $g_1,\ldots,g_m$ and randomized approximations of sg_1 mod q,..., sg_m mod 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.

A Glimpse of Worst-case to Average-case Reductions

Short Lattice Vectors: Minkowski's Inequality

- [Minkowski]: Any d-dim lattice L has at least one non-zero vector of norm ≤

$$2\frac{\Gamma(1+d/2)^{1/d}}{\sqrt{\pi}}\mathrm{covol}(\mathrm{L})^{1/d} \leq \sqrt{d}\ \mathrm{covol}(\mathrm{L})^{1/d}$$

- This is Minkowski's inequality on Hermite's constant:

$$\sqrt{\gamma_d} \leq \frac{2}{v_d^{1/d}} = 2\frac{\Gamma(1+\frac{d}{2})^{1/d}}{\sqrt{\pi}} \leq \sqrt{d}$$

Four Proofs of Minkowski's Inequality

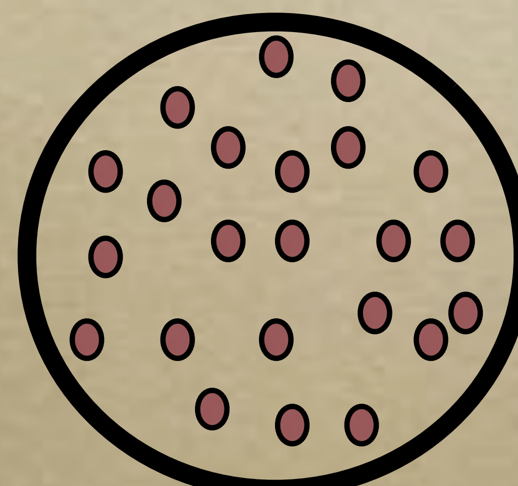
- Blichfeldt's proof: «continuous» pigeon-hole principle.

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

Mordell's Proof (1933)

Mordell's Proof (1933)

- For $q \in \mathbf{N}$, let $\bar{L} = q^{-1}L$ then $[\bar{L}:L] = q^d$.
  Among $> q^d$ points $v_1, \ldots, v_m$ 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: 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.
  - Let distinct $v_1,\ldots,v_m \in \bar{L}=q^{-1}L$.
  - Consider the integer lattice L' formed by all $(x_1,\ldots,x_m)\in\mathbf{Z}^m$ 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 $\underset{\cdot}{\bar{L}}$.
  - Among these exponentially many lattice points, find a difference in L, possibly by exhaustive search.
  - Both steps are expensive.

Wishful Thinking

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

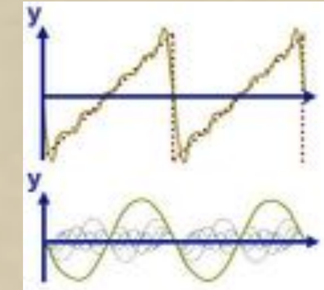
Overlattices and Groups

- 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 an exact sequence:

$$0 \to L \xrightarrow{1} \bar{L} \xrightarrow{\varphi} G \to 0$$

- $L=\mathrm{Ker}\,\phi$ where ϕ is efficiently computable.
- Let $v_1,\ldots,v_m \in \bar{L}$ and define $g_1,\ldots,g_m \in G$ by $g_i=\phi(v_i)$.
- If $\sum_i x_i g_i = 0$ for $(x_1,\ldots,x_m) \in \mathbf{Z}^m$ then $\sum_i x_i v_i \in L$.

Fourier Analysis



- Fourier analysis shows that if $v_1,\ldots,v_m \in \bar{L}$ are chosen from a suitable (short) distribution, $g_i = \phi(v_i)$ has uniform distribution over G.
  - Any probability mass function f over $\bar{L}$ s.t. for any $x \in \bar{L}$, $\sum_{y \in L} f(x+y) \approx 1/\#G$. Ex: discrete Gaussian distribution.
- This is a key step: transforming a worst-case into an average-case.

Remember SIS

- Let $(G,+)$ be a finite Abelian group: $G=(\mathbf{Z}/q\mathbf{Z})^n$ in [Ajtai96]. View G as a $\mathbf{Z}$-module.
- Pick $g_1,\ldots,g_m$ uniformly at random from G.
- Goal: Find short $(x_1,\ldots,x_m)\in\mathbf{Z}^m$ s.t. $\sum_i x_i g_i = 0$, e.g. $\|x\| \le m\,(\#G)^{1/m}$.
- This is essentially finding a short vector in a (uniform) random lattice of $L_m(G) = \{$ lattices $L\subseteq\mathbf{Z}^m$ s.t. $\mathbf{Z}^m/L \sim G$ $\}$.

Worst-to-average Reduction from Mordell's Proof

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

Generalized SIS Reduction

- The SIS reduction is based on this crucial fact: If B is a reduced basis of a lattice L, then $q^{-1}B$ is a reduced basis of the overlattice $\bar{L}=q^{-1}L$.
- If G is an arbitrary finite Abelian group, [GINX16] finds a reduced basis of some overlattice $\bar{L} \supseteq L$ s.t. $\bar{L}/L \simeq G$, so that we can sample short vectors in $\bar{L}$.