A Quantum Algorithm for Computing the Unit Group of an Arbitrary-Degree Number Field

Fang Song

IQC, University of Waterloo

Joint Work with:

Kirsten Eisentraeger (Penn State)

Sean Hallgren (Penn State)

Alexei Kitaev (Caltech & KITP)

exponentially

*Which problems have faster |**quantum**⟩ algorithms than classical algorithms?*

(Number theory problems are a good source)

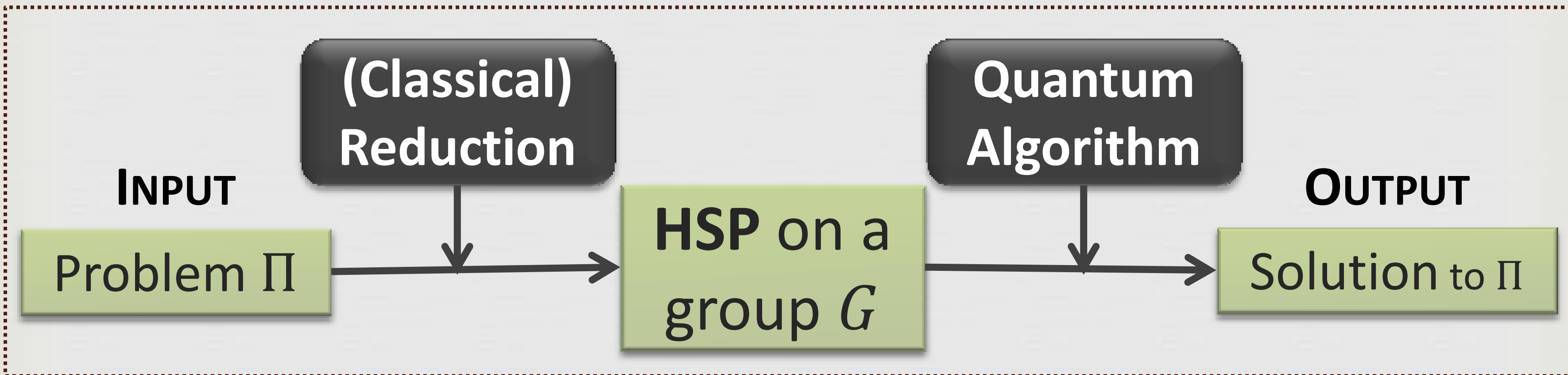
∃ Poly-time quantum algorithms for:

- Factoring and discrete logarithm [Shor'94]
- Unit group in number fields **THIS WORK:** arbitrary-degree
  - Degree two fields (Pell's equation as a special case) [Hallgren'02]
  - Constant-degree [Hallgren'05,SchmidtVollmer'05]
- Principal Ideal Problem (PIP) and class group computation
  - Constant degree number fields [H'02'05,SV'05]

Best known classical algorithms need super-polynomial time

All these quantum alg's fall into the framework of

Hidden Subgroup Problem (HSP)



✓ Reduction & Algorithm for HSP both need to be efficient.

Existing algorithms for **constant**-degree unit finding

[H'02'05,SV05]

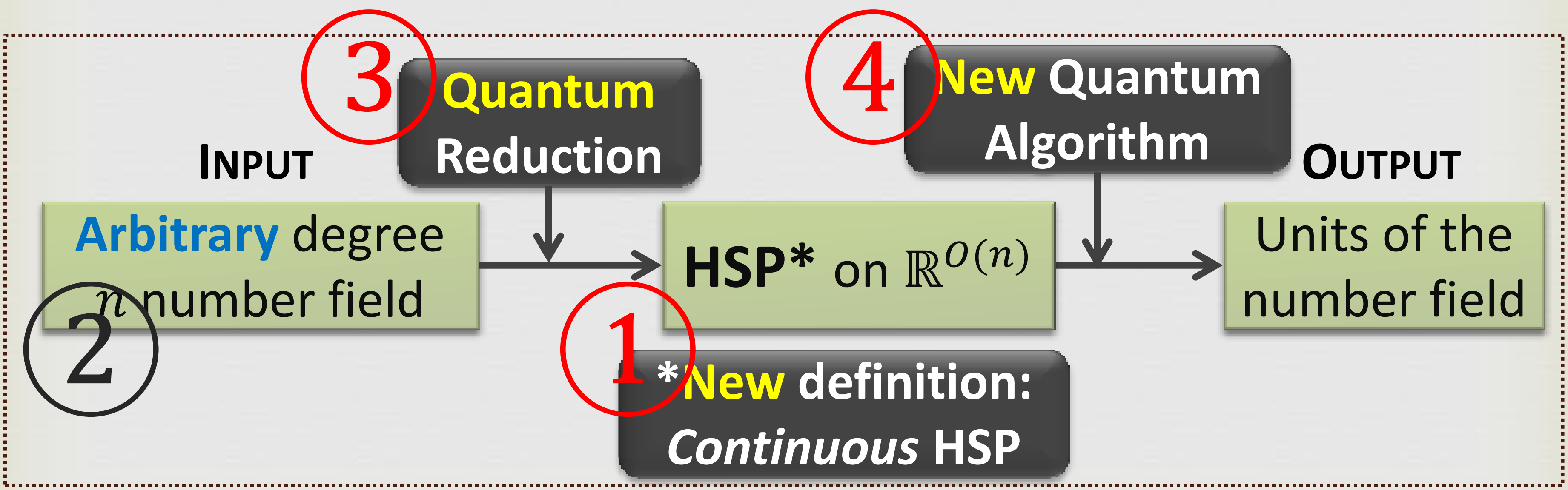
Difficulty of extending to high degrees

- Reduction takes exponential time in degree.
- HSP instance in high dimension hard to solve.

Existing algorithms for **constant**-degree unit finding

[H'02'05,SV05]

Our algorithm for **arbitrary**-degree unit finding



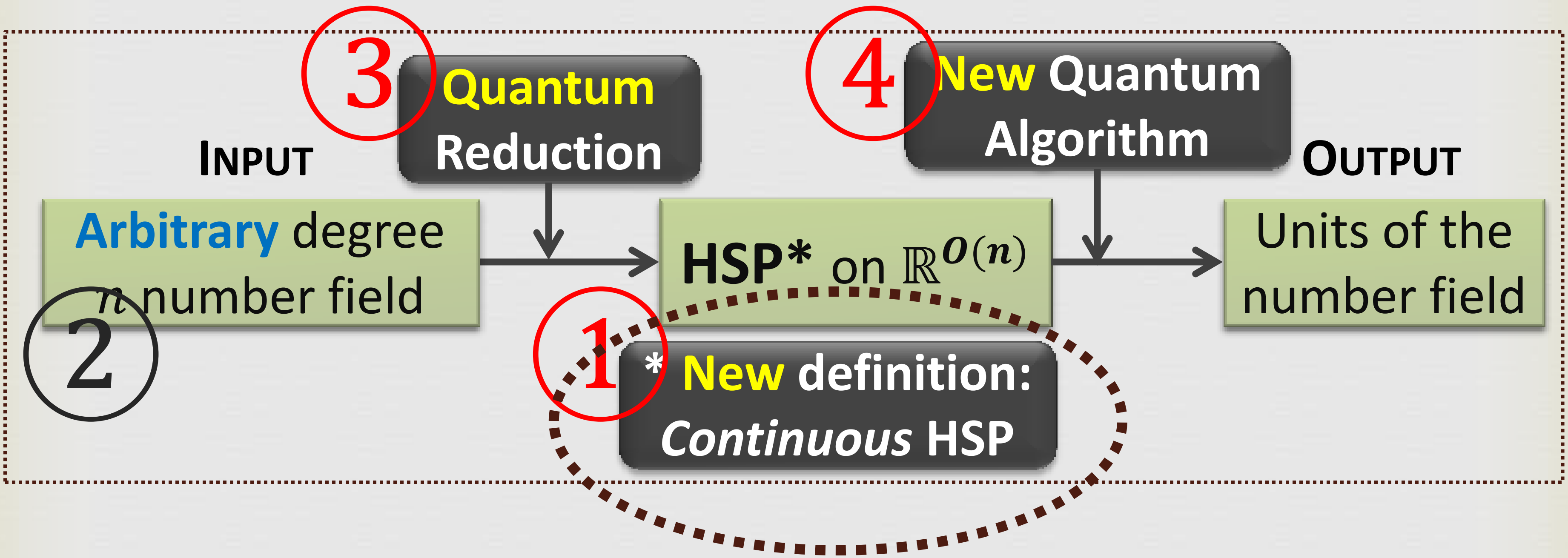
Quantum Attacks on Classical Cryptography

- Quantum algorithms can break classical crypto-systems
  - Anything based on factoring/D-Log [Shor94]: e.g. RSA encryption…
  - Buchmann-Williams key exchange (based on degree-two PIP) [H'02]

- **OPEN QUESTION**: quantum attacks on (*ideal*) lattice based crypto
  - Fully homomorphic encryption, code obfuscation, and more [Gentry09,SmartV'10,GGH+13…]
  - Our alg. deals with similar objects: ideal lattices in number fields
  - A classical approach [Dan Bernstein Blog 2014]
    - A key component: computing units in classical *sub-exp.* time

    ➔ This part becomes (quantum) *poly-time* by our alg.

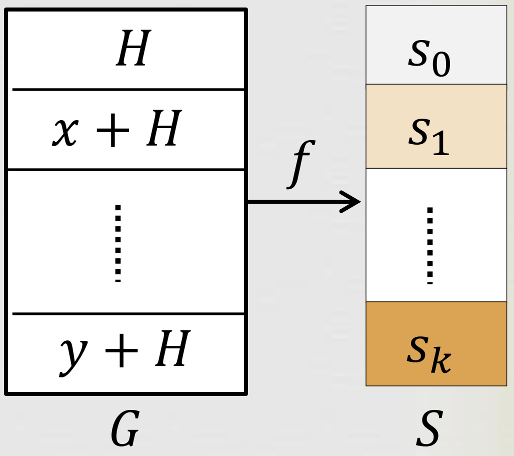
Roadmap of Our Algorithm



Review: Hidden Subgroup Problem (HSP)

- Finite Group G
  Given: oracle function $f: G \to S$, s.t. $\exists\, H \leq G$,
  1. (Periodic on H)
     $$x - y \in H \Rightarrow f(x) = f(y)$$
  2. (Injective on G/H)
     $$x - y \notin H \Rightarrow f(x) \neq f(y)$$

  Goal: Find (hidden subgroup) H.



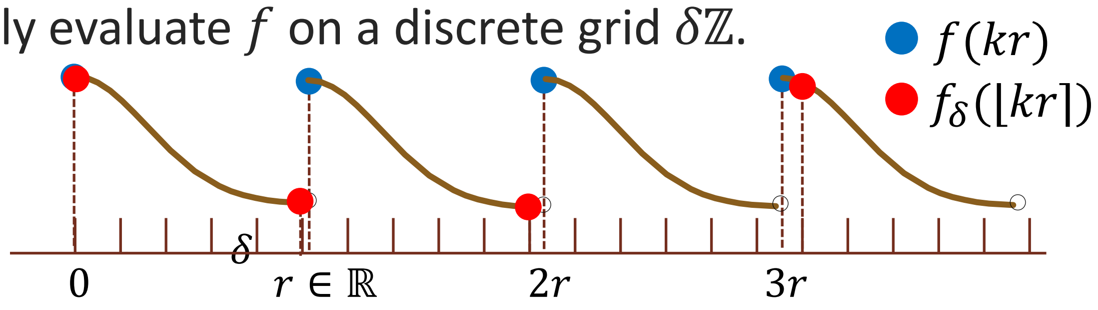
- Extend the definition to infinite group $\mathbb{Z}^m$ ✓
- Extend to *uncountable* group $\mathbb{R}^m$: **non-trivial!**

An issue with discretization

- Assume $f: \mathbb{R} \to S$ periodic with period $r \in \mathbb{R}$.
- Digital computers can only evaluate f on a discrete grid $\delta\mathbb{Z}$.

$$f_\delta \triangleq f|_{\delta\mathbb{Z}}: \delta\mathbb{Z} \to S$$

may lose HSP properties (e.g. periodic)!



Define Continuous HSP on $\mathbb{R}^m$

- Previous definition: extra constraint on **discrete** f_δ
  - E.g. pseudo-periodic [H'02]: $f_\delta(\lfloor kr \rceil + x) = f_\delta(x)$ for most x.
  - Not suitable in high dimensions $\mathbb{R}^m$.
- Our definition **(HSP on $\mathbb{R}^m$)**: make f **continuous**

Given $f : \mathbb{R}^m \to \mathcal{H}$ (quantum states), s.t.: $\exists\, H \le \mathbb{R}^m$,

1. (Periodic) $x - y \in H \Rightarrow |f(x)\rangle = |f(y)\rangle$.
2. (Pseudo-injective)

$$\min_{v \in H} ||x - y - v|| \ge r \Rightarrow \langle f(x)|f(y)\rangle \le \epsilon.$$

"$x - y$ **far** from $H \Rightarrow \langle f(x)|f(y)\rangle$ **small**"

3. (Lipschitz) $|||f(x)\rangle - |f(y)\rangle|| \le a \cdot ||x - y||$.

"$x - y$ **close** to $H \Rightarrow \langle f(x)|f(y)\rangle$ **big**"

Goal: Find (hidden subgroup) H.

Interesting HSP Instances

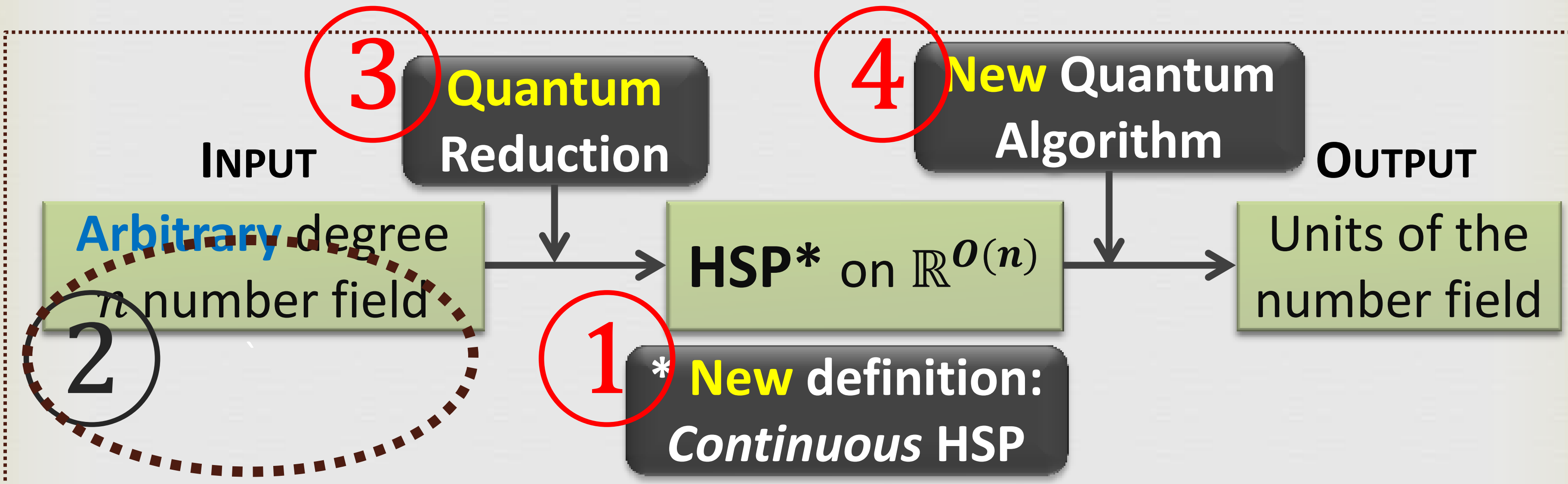
Computational Problems		Abelian HSP on G
Discrete log	$\rightarrow$	$\mathbb{Z}_N \times \mathbb{Z}_N$
Factoring	$\rightarrow$	$\mathbb{Z}$
Unit group, PIP, class group, constant degree	$\rightarrow$	$\mathbb{R}^{const}$
[**This Work**] Unit group, **arbitrary** degree n	$\rightarrow$	$\mathbb{R}^{O(n)}$ [New Definition]

∃ efficient quantum algorithms

Computational Problems		Non-abelian HSP on G
Graph isomorphism	$\rightarrow$	Symmetric group S_n
Unique shortest vector	$\rightarrow$	Dihedral group D_n

? efficient alg. (open question)

Roadmap of Our Algorithm



Number Field Basics

- Number Field $K \subseteq \mathbb{C}$: Finite field extension of $\mathbb{Q}$.
  - Ex. 1 (Quadratic field). Take $d \in \mathbb{Z}$, $\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} : a, b \in \mathbb{Q}\}$.
  - Ex. 2 (Cyclotomic field). Take $\omega = e^{2\pi i/p}$, p prime.
    $$\mathbb{Q}(\omega) = \{a_0 + a_1\omega + \cdots + a_{p-2}\omega^{p-2} : a_i \in \mathbb{Q}\}.$$
- Ring of Integers $\mathcal{O}$: K $\cap$ Roots of monic irreducible poly $\mathbb{Z}[X]$.
- Group of Units $\mathcal{O}^*$: **invertible** elements in $\mathcal{O}$.

Field	K	$\mathbb{Q}$	$\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} : a, b \in \mathbb{Q}\}$
	$\vert$	$\vert$	$\vert$
Ring of integers	$\mathcal{O}$	$\mathbb{Z}$	$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}$
	$\vert$	$\vert$	$\vert$
Unit group	$\mathcal{O}^*$	$\{\pm 1\}$	$\mathcal{O}^* = \{\pm u^k : k \in \mathbb{Z}\}$

$d = 109$, $\quad u = 158070671986249 + 15140424455100\sqrt{109}$

Exercise. Verify $uu^{-1} = 1$.

Complexity of Computing Unit Group

- Two parameters for measuring computational complexity
  - Degree n: dimension of K as vector space over $\mathbb{Q}$.
  - Discriminant Δ: "size" of ring of integers. [more to come]

$$\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} : a, b \in \mathbb{Q}\}, \qquad \boldsymbol{n = 2, \Delta \approx d}$$
$$\mathbb{Q}(\omega) = \{a_0 + a_1\omega + \cdots + a_{p-2}\omega^{p-2} : a_i \in \mathbb{Q}\}, \boldsymbol{n = p - 1, \Delta \approx p^p}$$

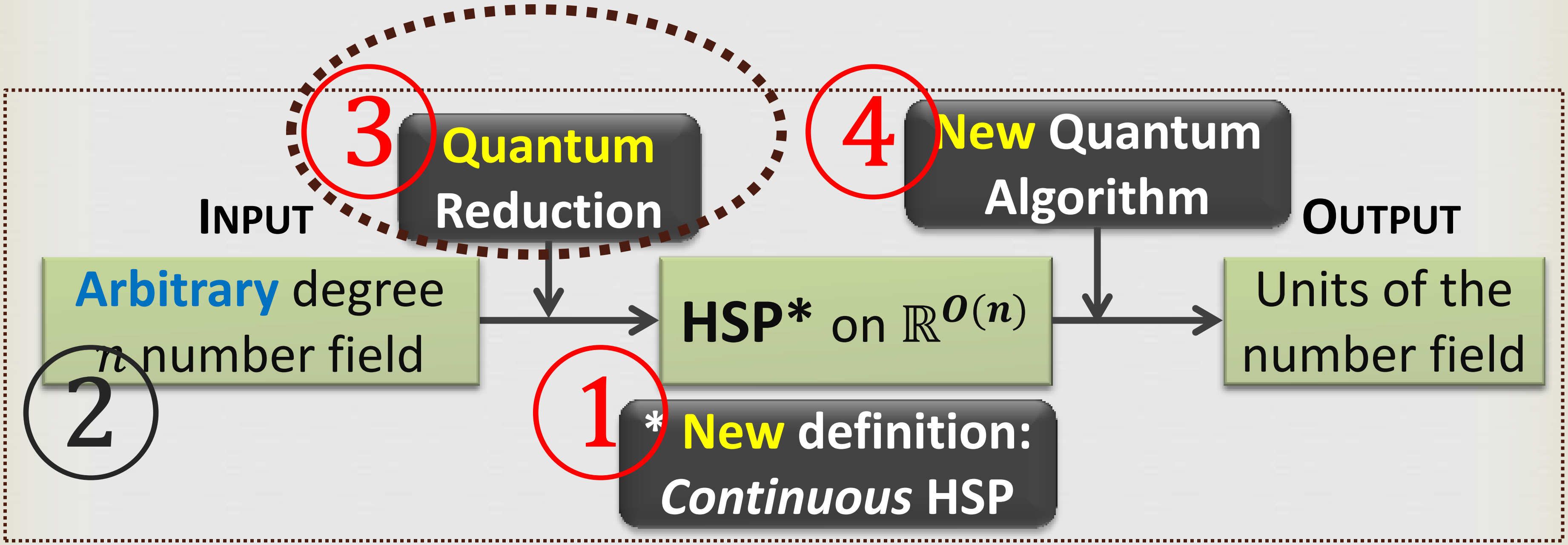
Goal: computation in time $\mathrm{poly}(n, \log \Delta)$.

- Previous algorithms for computing units

	Classical	**Quantum**
(Factoring) [reduces to $\mathbb{Q}(\sqrt{d})$ case]	$\exp((\log \Delta)^{1/3})$	$\mathrm{poly}(\log \Delta)$
$\mathbb{Q}(\sqrt{d})$	$\exp((\log \Delta)^{1/2})$	$\mathrm{poly}(\log \Delta)$
$\mathbb{Q}(\omega_p)$	$\exp(n, \log \Delta)$	$\exp(n)\mathrm{poly}(\log \Delta)$

This work
$\mathrm{poly}(n, \log \Delta)$

Roadmap of Our Algorithm



Outline of Quantum Reduction

1. Identify $\mathcal{O}^*$ as a subgroup in $\mathbb{R}^m, m = O(n)$.

2. Define $f: \mathbb{R}^m \to \mathcal{H}$ satisfying HSP properties.
   - (Periodic) $x - y \in \mathcal{O}^* \Rightarrow |f(x)\rangle = |f(y)\rangle$
   - (Pseudo-injective) $x - y$ far from $\mathcal{O}^* \Rightarrow \langle f(x)|f(y)\rangle$ small
   - (Lipschitz) $x - y$ close to $\mathcal{O}^* \Rightarrow \langle f(x)|f(y)\rangle$ big

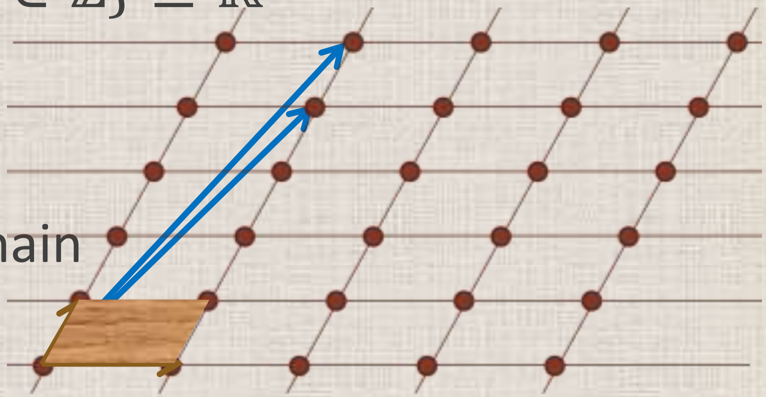
3. Compute f by an efficient **quantum** algorithm. (omitted)

Set Up Units as a Subgroup

- $\mathcal{O}$ is identified with a lattice $\underline{\mathcal{O}}$ in $\mathbb{R}^n$.
  - $z \in \mathcal{O} \mapsto \underline{z} := (z_1, \dots, z_n) \in \mathbb{R}^n$ (conjugate vector representation)

Lattice $L(B) = \{a_1 v_1 + \cdots + a_n v_n : a_i \in \mathbb{Z}\} \subseteq \mathbb{R}^n$

- Basis $B : \{v_i \in \mathbb{R}^n : i = 1, \dots, n\}$
- L has (infinitely) many bases
- $\det(L)$: volume of fundamental domain



- Discriminant of $\mathcal{O}$: $\Delta = \det^2(\underline{\mathcal{O}})$

- Log coordinates of units: $z \in \mathcal{O}^* \to z_i \neq 0 \to$ write $u_i \coloneqq \log|z_i|$
- **Fact**: units have algebraic norm 1

$$z \in \mathcal{O}^* \to |\mathcal{N}(z)| = \Pi|z_i| = 1 \to \sum u_i = 0.$$

➔ $\mathcal{O}^* \leq \mathbb{R}^{n-1} = \{(u_1, \dots, u_n) \in \mathbb{R}^n : \sum u_i = 0\}$

N.B.: Not precise; sign/phase info. missing!

Define Hiding Function: Classical Part

$$f: \boxed{\mathbb{R}^{n-1}} \xrightarrow{f_c} \boxed{\{\text{lattices in } \mathbb{R}^n\}} \xrightarrow{f_q} \boxed{\{\text{quantum states}\}}$$

Input: $\vec{x} = (x_1, \dots, x_n)^T, \sum x_i = 0 \overset{f_c}{\mapsto}$ **Output:** $L_x = e^{\vec{x}}\underline{\mathcal{O}}$

- Example. $K = \mathbb{Q}(\sqrt{d}), d \in \mathbb{Z}^+, n = 2, \underline{\mathcal{O}} \subseteq \mathbb{R}^2$.

$$f_c: (x, -x) \mapsto e^{\vec{x}}\underline{\mathcal{O}}$$

$$\forall\, v = (v_1, v_2)^T \in \underline{\mathcal{O}}$$
$$e^{\vec{x}}v := (e^{x}v_1, e^{-x}v_2)^T$$

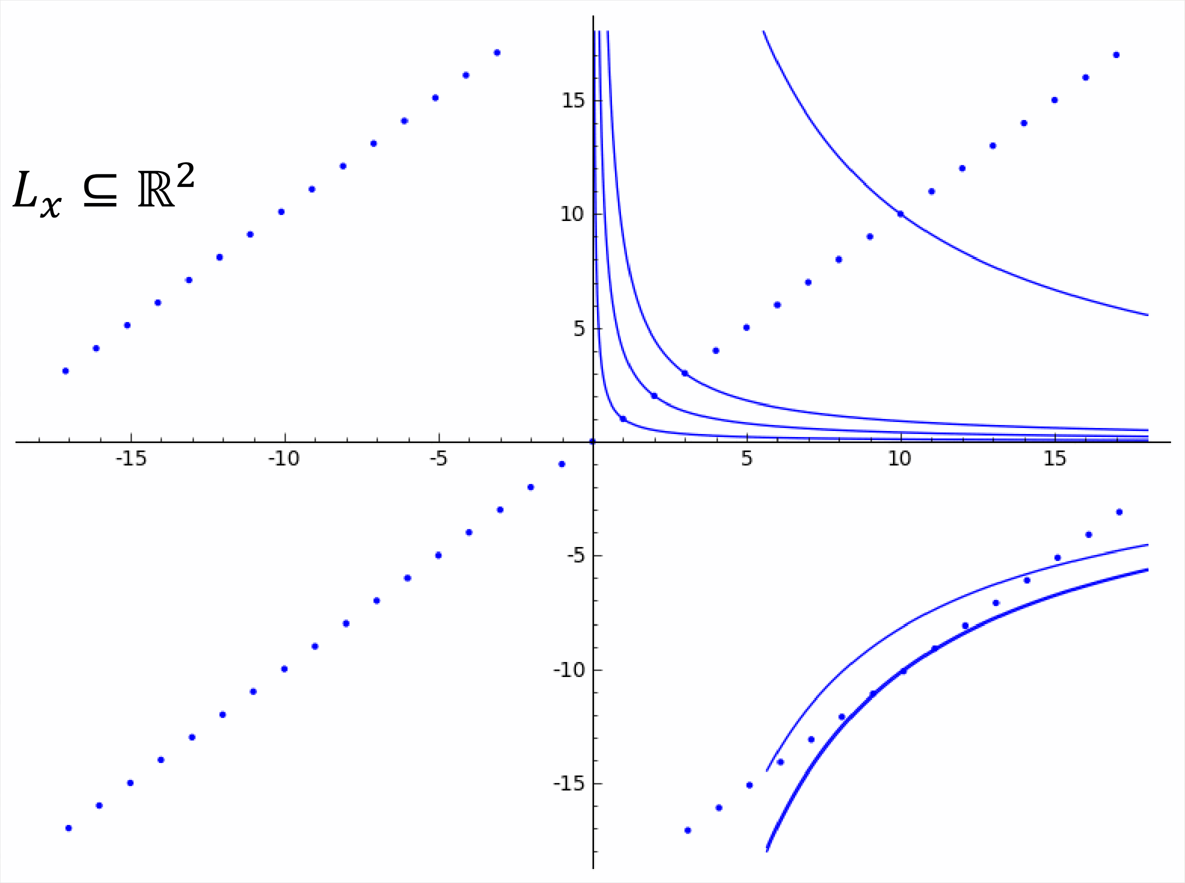
- Stretch/Squeeze each coordinate

- **Obs**. f_c preserves algebraic norm $\mathcal{N}(z) = \Pi z_k$.

Real Quadratic Example

- $\mathbb{Q}(\sqrt{102}), n = 2, f_c\colon \mathbb{R} \to \{\text{lattices in } \mathbb{R}^2\}$

$x \in \mathbb{R} \overset{f_c}{\mapsto} L_x \subseteq \mathbb{R}^2$



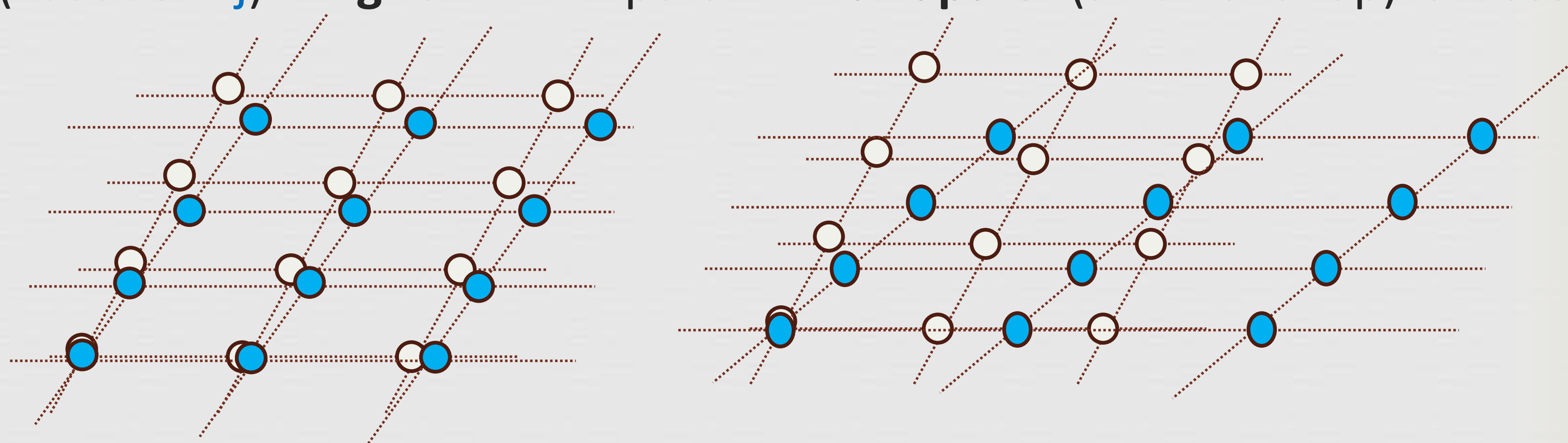
Courtesy of Hallgren.

Properties of f_c

$$f: \mathbb{R}^{n-1} \xrightarrow{f_c} \{\text{lattices in } \mathbb{R}^n\} \xrightarrow{f_q} \{\text{quantum states}\}$$

$$f_c: x \mapsto L = e^x \underline{\mathcal{O}}$$

- $\mathcal{O}^*$-Periodic. (**Fact**: $u \in \mathcal{O}^* \Rightarrow u\underline{\mathcal{O}} = \underline{\mathcal{O}}$)
  - →If $e^{\vec{y}} \in \mathcal{O}^*$, then $e^{\vec{x}+\vec{y}}\underline{\mathcal{O}} = e^{\vec{x}}\underline{\mathcal{O}}$.
- (Lipschitz) "**Small**" shift in inputs → "**Similar**" lattices in outputs
- (Pseudo-inj) "**Big**" shift in inputs → "**Far-apart**" (small overlap) lattices



! Computing f_c delicate: e^x doubly-exp. large & precision loss.

Define Hiding Function: Quantum Encoding

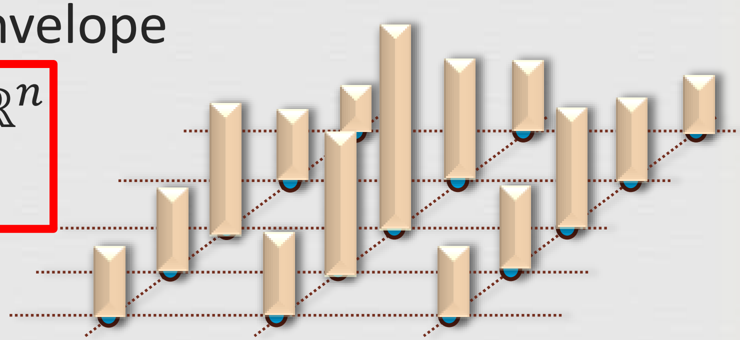
$f: \mathbb{R}^{n-1} \xrightarrow{f_c} \{\text{lattices in } \mathbb{R}^n\} \xrightarrow{f_q} \{\text{quantum states}\}$

needed for Quantum HSP alg.

- **Issue**: no unique representation for lattices in $\mathbb{R}^n$
  - $e^{\vec{x}}\underline{\mathcal{O}} = e^{\vec{y}}\underline{\mathcal{O}}$ same lattice, but $f_c(\vec{x})$ and $f_c(\vec{y})$ different bases.
- **Fix**: encode lattices in quantum states!
  - Superposition over all lattice points

$$f_q: L \mapsto |L\rangle = \gamma \sum_{v \in L} \rho_s(v) |\mathrm{str}_\delta(v)\rangle$$

- $\rho_s(\cdot) = e^{-\pi||\cdot||^2/s^2}$: wide Gaussian envelope
- $|\mathrm{str}_\delta(v)\rangle$: straddle encoding of $v \in \mathbb{R}^n$
  - **Goal**: $|\mathrm{str}_\delta(v)\rangle \approx |\mathrm{str}_\delta(v')\rangle$ iff. $v \approx v'$
  - Naïve approach fails: $\langle .0001 | .0002 \rangle = 0$

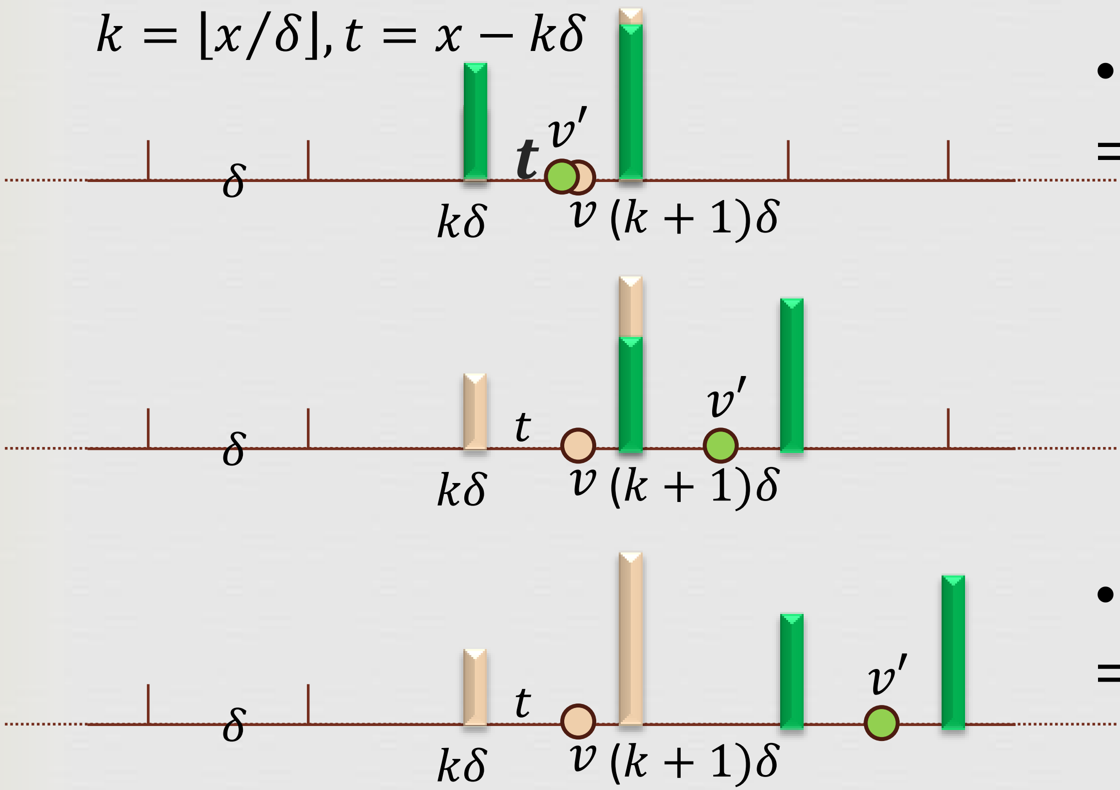


Quantum Straddle Encoding

- Straddle encoding a real number in a quantum state.

$$|\mathrm{str}_\delta(v)\rangle = \cos(t)|k\rangle + \sin(t)|k+1\rangle$$

$k = \lfloor x/\delta \rfloor, t = x - k\delta$

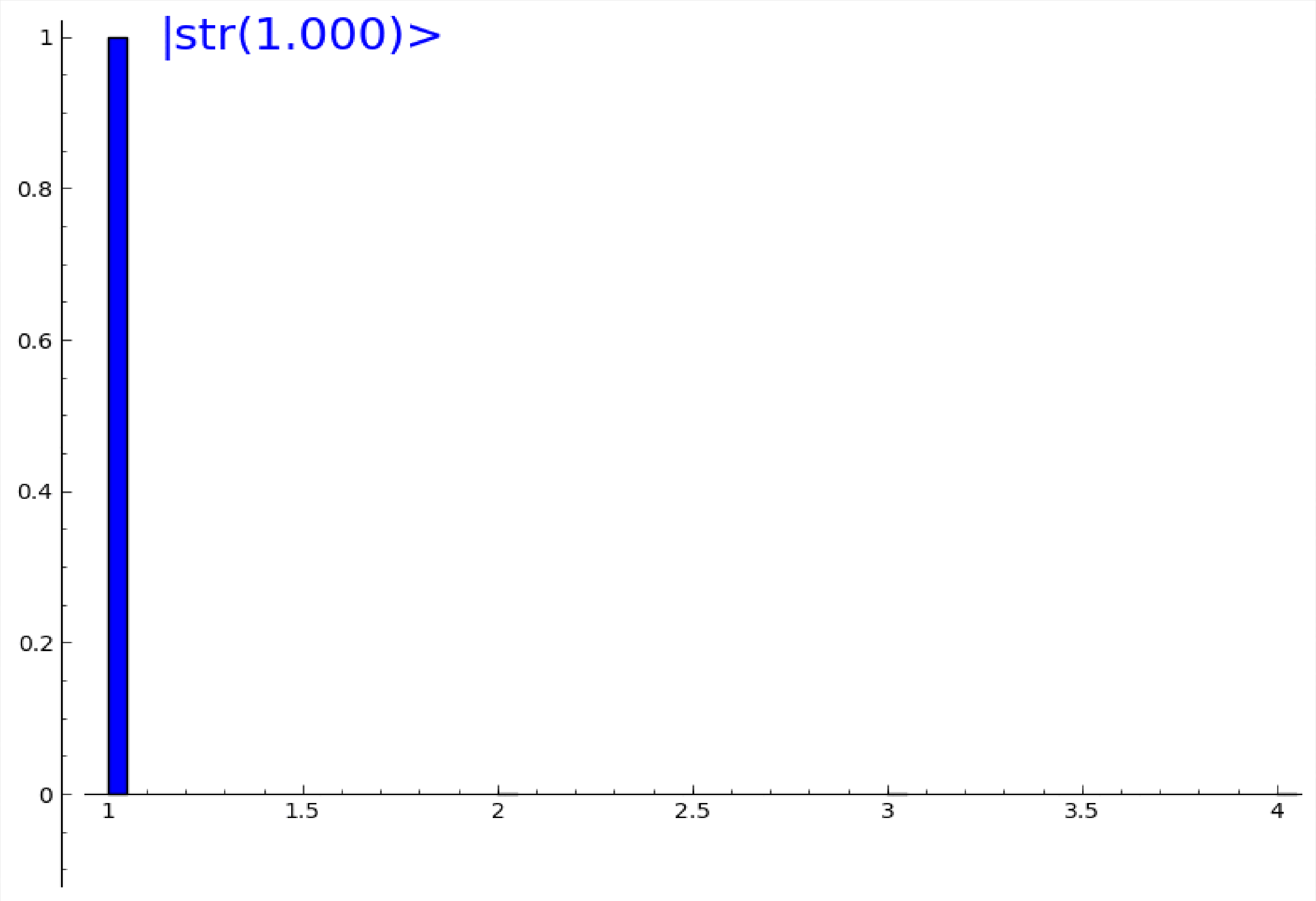


- $|v - v'|$ small
$\Rightarrow \langle \mathrm{str}_\delta(v') | \mathrm{str}_\delta(v) \rangle \approx 1$

- $|v - v'| \geq 2\delta$
$\Rightarrow \langle \mathrm{str}_\delta(v') | \mathrm{str}_\delta(v) \rangle = 0$

- Encode a vector in $\mathbb{R}^n$: coordinate-wise straddle encoding

Quantum Straddle Encoding: An Animation

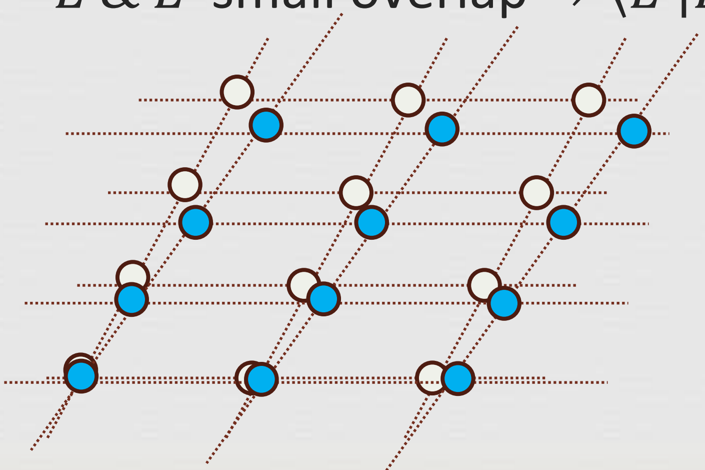


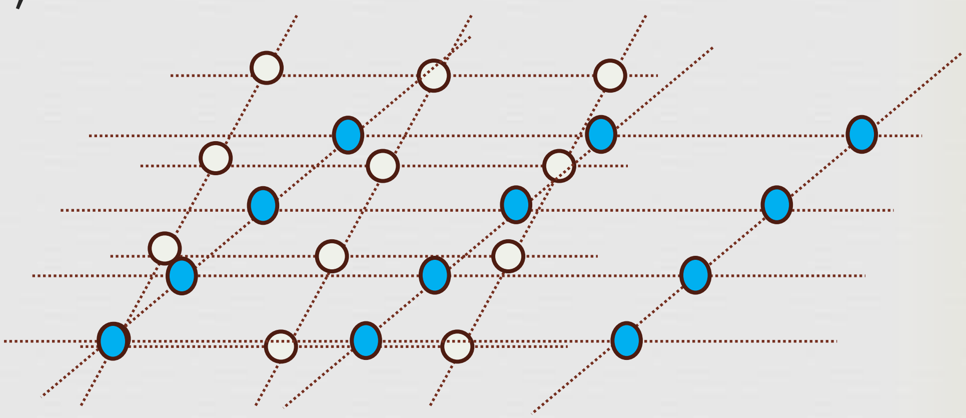
Properties of f_q

$$f: \boxed{\mathbb{R}^{n-1}} \xrightarrow{f_c} \boxed{\{\text{lattices in } \mathbb{R}^n\}} \xrightarrow{f_q} \boxed{\{\text{quantum states}\}}$$

$$\boxed{f_q: L \mapsto |L\rangle = \gamma \sum \rho_s(v)|\mathrm{str}_\delta(v)\rangle}$$

- $\langle L'|L\rangle \propto \sum_{v \in L, v' \in L'} \langle \mathrm{str}_\delta(v')|\mathrm{str}_\delta(v)\rangle$
  - $||v - v'||$ small $\Rightarrow \langle \mathrm{str}_\delta(v')|\mathrm{str}_\delta(v)\rangle \approx 1$
  - $||v - v'|| \geq 2\delta \Rightarrow \langle \mathrm{str}_\delta(v')|\mathrm{str}_\delta(v)\rangle = 0$
  - $L \approx L' \Rightarrow \langle L'|L\rangle \approx 1$
  - L & L' small overlap $\Rightarrow \langle L'|L\rangle$ small





Establish HSP Properties

$f: \boxed{\mathbb{R}^{n-1}} \xrightarrow{f_c} \boxed{\{\text{lattices in } \mathbb{R}^n\}} \xrightarrow{f_q} \boxed{\{\text{quantum states}\}}$

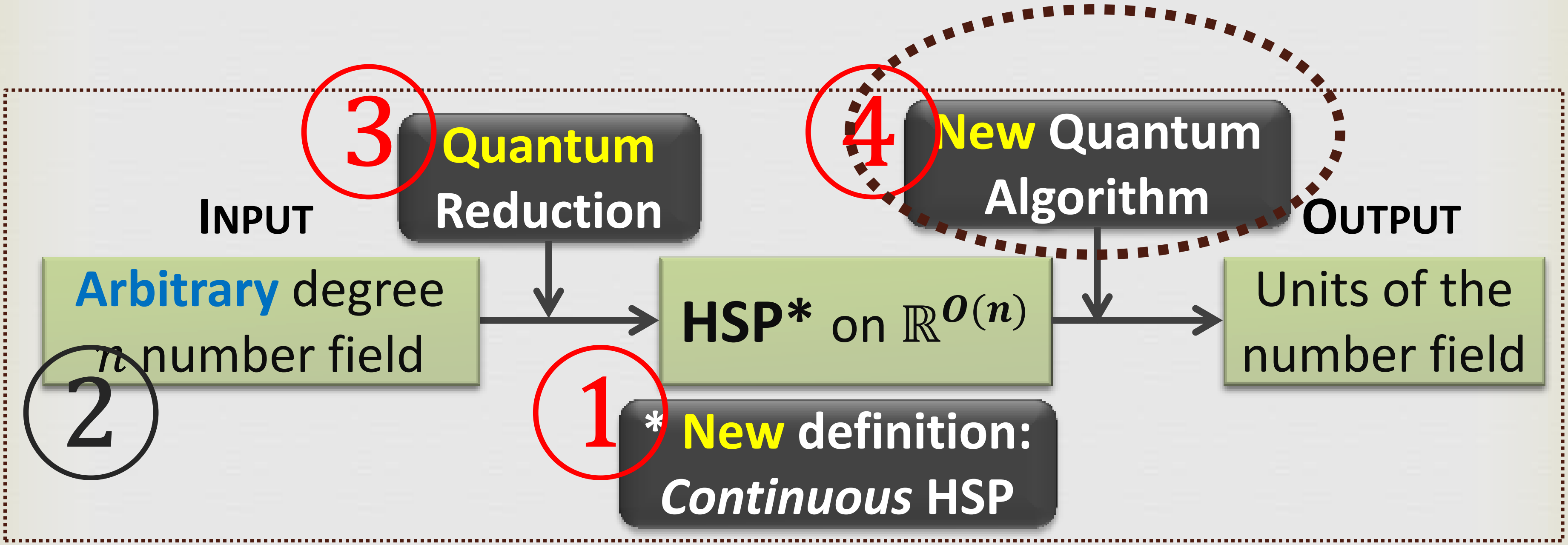
Theorem. $f = f_q \circ f_c$ is periodic over $\mathcal{O}^*$ with HSP properties.

- (Lipschitz) $x - x'$ close to $\mathcal{O}^* \overset{f_c}{\rightarrow} L \approx L' \overset{f_q}{\rightarrow} \langle L' | L \rangle \approx 1$
- (P-Inj.) $x - x'$ far from $\mathcal{O}^* \overset{f_c}{\rightarrow} L$ & L' small overlap $\overset{f_q}{\rightarrow} \langle L' | L \rangle$ small

➔ Invoke quantum HSP algorithm (next), we find $\mathcal{O}^*$ efficiently!

- Applications of quantum straddle encoding
  - A canonical representation for real-valued lattices.
  - Can reduce existing (abelian) HSP to our HSP on $\mathbb{R}^m$.

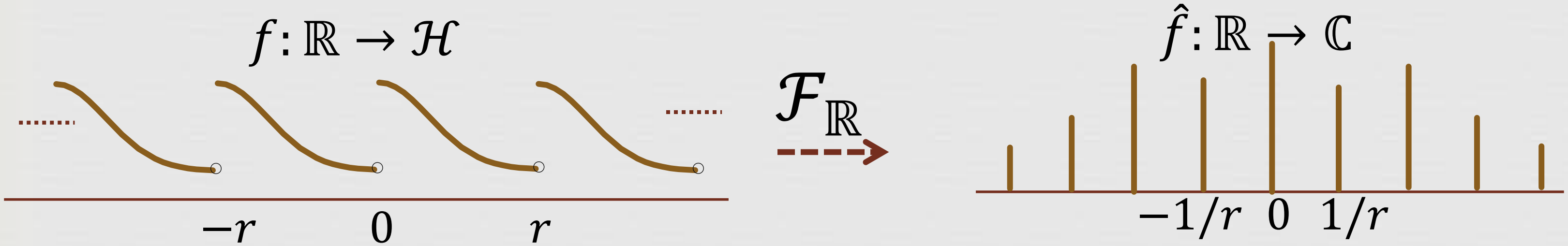
Roadmap of Our Algorithm



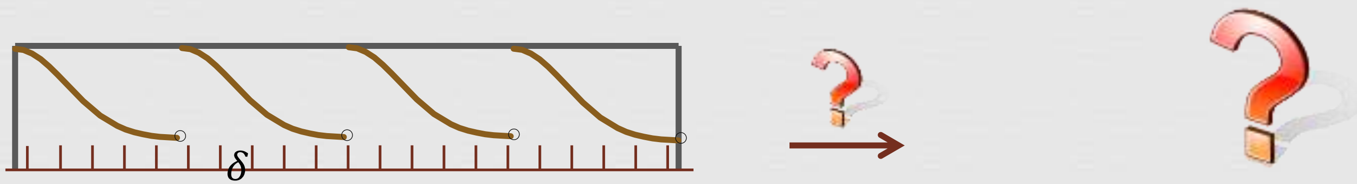
Solving HSP on $\mathbb{R}^m$: Main Idea

Input: oracle function f that hides $H \subseteq \mathbb{R}^m$

Real Domain | Fourier Spectrum



- **Ideal world**: $\hat{f}$ peaked at dual of H, i.e. k/r.
- **Reality**: need to truncate and discretize f.

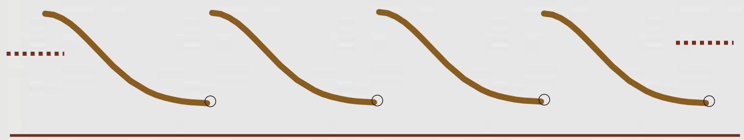


- **Goal:** get samples that approximate the **ideal** Fourier spectrum

Output: (Generators of) H?

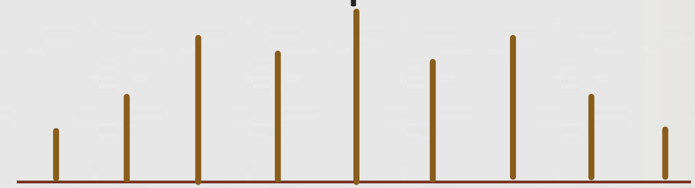
Effect of Truncation

Real Domain

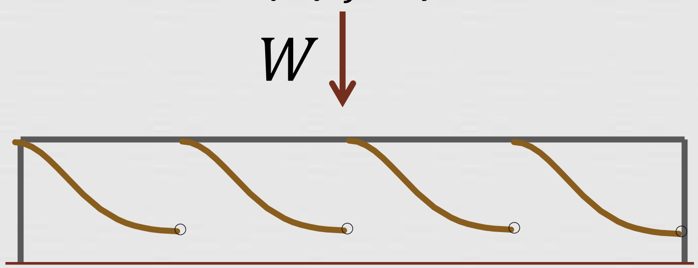


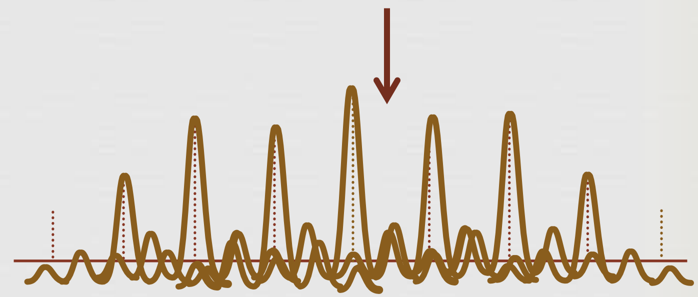
$\mathcal{F}_{\mathbb{R}}$

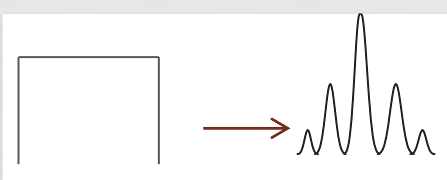
Fourier Spectrum



Truncation: multiply f by window function W.



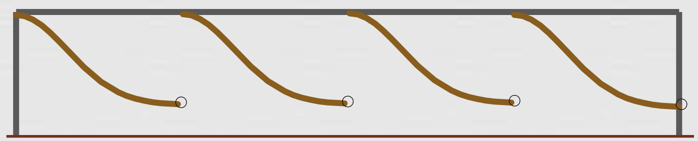


- Mult./Convolution Duality: $\mathcal{F}(fg) = \hat{f} * \hat{g}$
- 

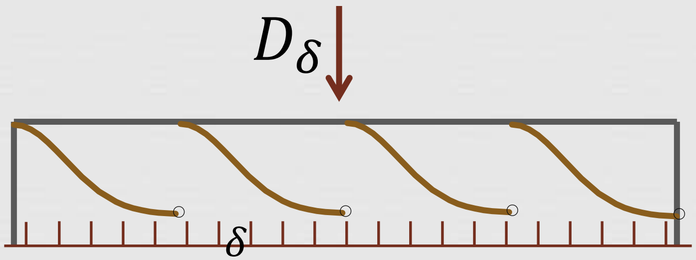
Need a smooth window: $w(x) = \begin{cases} \frac{1}{\sqrt{W/2}} \sin(\pi x/W), x \in [0, W] \\ 0, \text{otherwise} \end{cases}$

Effect of Discretization

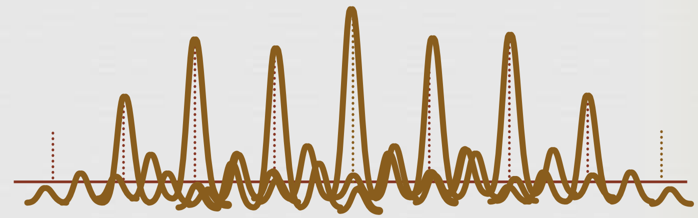
Real Domain

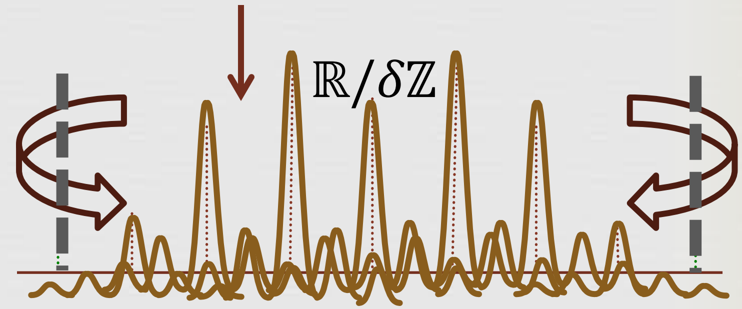


Discretization: restrict f on grid $\delta\mathbb{Z}$, $f_\delta \triangleq f|_{\delta\mathbb{Z}}$.



Fourier Spectrum





- **Poisson Summation Formula** $\Rightarrow$

$$\widehat{f_\delta}(z) = \sum_{k\in\mathbb{Z}} \hat{f}(z + k\delta^{-1})$$

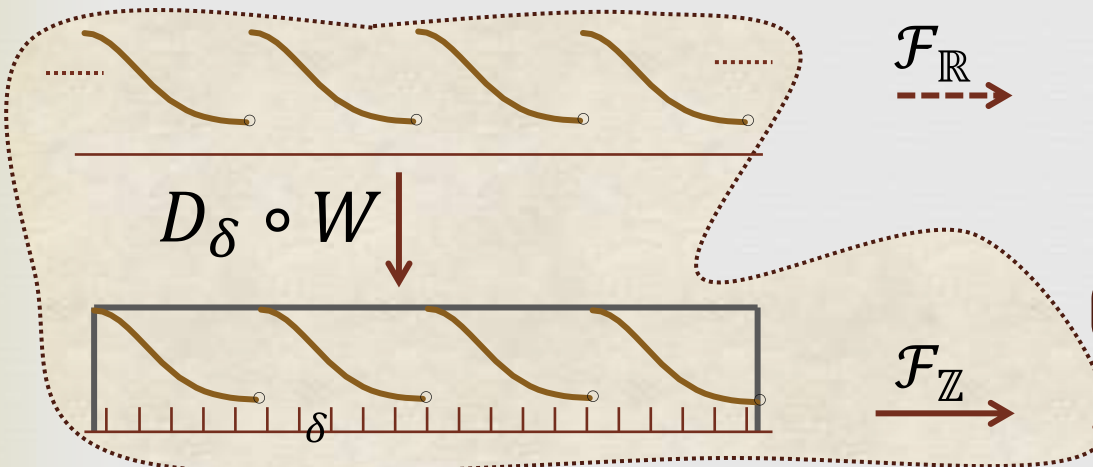
- f **Lipschitz** ➔ $\hat{f}$ small tail

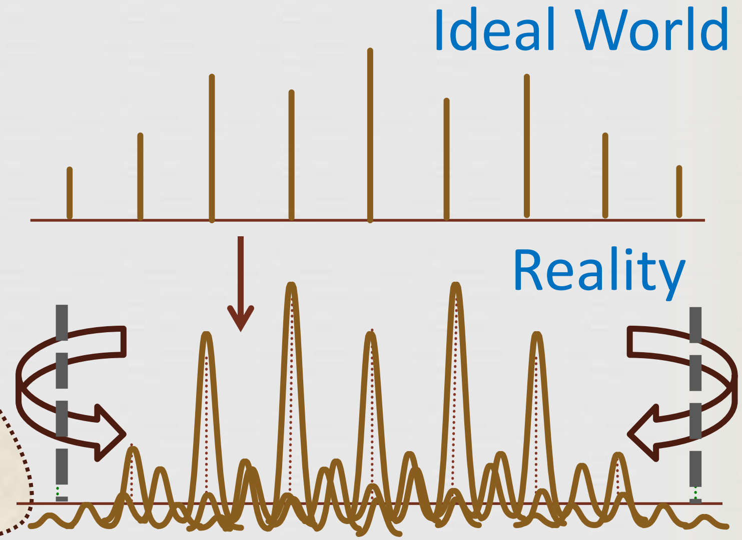
$f = 1 \rightarrow \hat{f} = \delta(x)$

$\Rightarrow$ Wrapping only causes small disturbance

Quantum Algorithm for HSP on $\mathbb{R}^m$

- Our Algorithm



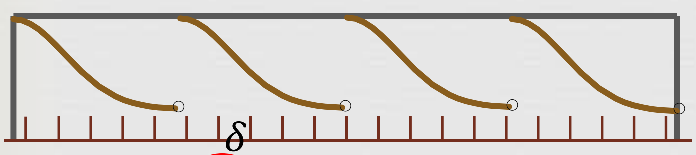


$Wf_\delta : \mathbb{Z} \to \mathcal{H}$

i.e. view it as an **infinite** sequence

✓ Our alg. samples from this spectrum (by **phase estimation**).

- Previous Algorithms



$Wf_\delta : \mathbb{Z}_N \to \mathcal{H}, N = W\delta^{-1}$

(Quantum Fourier transform)

☹ Get “clean” sample w.p. $\mathcal{O}(\frac{1}{2^m})$.

Quantum Algorithm for HSP on $\mathbb{R}^m$

Input: oracle function f that hides $H \subseteq \mathbb{R}^m$

- **Our Algorithm**:
  - Create $\sum_{x\in\mathbb{Z}} |x\rangle \otimes \sin(\frac{\delta x}{W}) |f(\delta x)\rangle$, $N = W\delta^{-1}$
  - $\mathcal{F}_{\mathbb{Z}}: |x\rangle \mapsto \int_{y\in\mathbb{R}} e^{2\pi \mathrm{i} xy} |y\rangle$ and measure.

    ✓ Implement by **Phase Estimation.**
  - Classical post-processing.

Output: (Generators of) H.

- Existing Algorithm:
  - $\mathcal{F}_{\mathbb{Z}_N}: |x\rangle \mapsto \sum_{y\in\mathbb{Z}_N} e^{2\pi i \frac{x\cdot y}{N}} |y\rangle$ and measure.

Discussion

New definition:
Continuous HSP

Arbitrary degree n number field	**Quantum Reduction** →	**HSP*** on $\mathbb{R}^{O(n)}$	**New Algorithm** →	Units of the number field

- Future Directions
  - Other problems in number fields, function fields…
  - Harness the power the continuous (abelian) HSP framework
  - Solve (ideal) lattice problems
  - ➔ Breaking lattice-based crypto?
- Update: PIP and class group in arb. degree solved [BiasseSong'14]

Thank you!