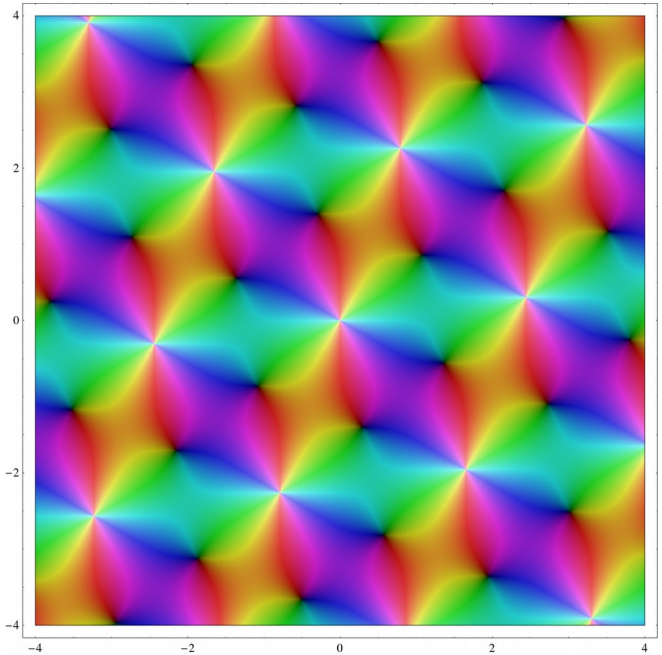
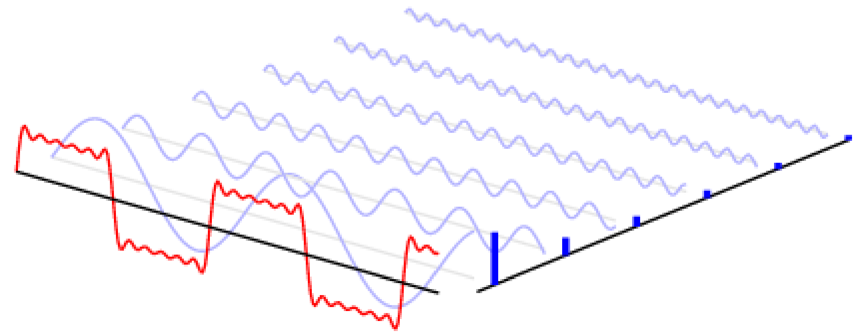




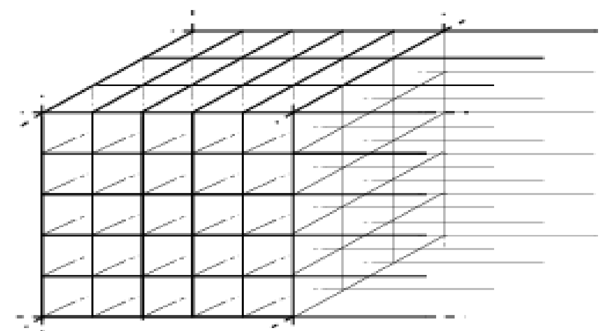
On the quantum complexity of the continuous hidden subgroup problem

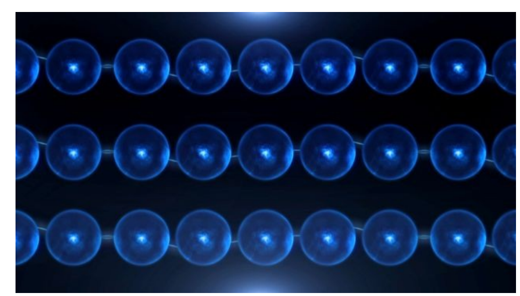
Koen de Boer, Léo Ducas, Serge Fehr

Paper: https://eprint.iacr.org/2019/716.pdf

Overview

- Introduction
- Problem statement
- Quantum algorithm
- Error analysis





Introduction

A quantum algorithm for computing the unit group of an arbitrary degree number field (2014)

Kirsten Eisenträger[*]
Department of Mathematics
The Pennsylvania State University
eisentra@math.psu.edu
and Harvard University

Sean Hallgren[†]
Dept. of Computer Science and Engineering
The Pennsylvania State University
hallgren@cse.psu.edu

Alexei Kitaev
Kavli Institute for Theoretical Physics
University of California, Santa Barbara
kitaev@kitp.ucsb.edu
and California Institute of Technology

Fang Song
Department of Combinatorics & Optimization
and Institute for Quantum Computing
University of Waterloo
fang.song@uwaterloo.ca

- Generalizes the Hidden Subgroup Problem to $\mathbb{R}^m$
- Computes unit groups of number fields
- Used to prove a (quantum) hardness-gap between Ideal-SVP and SVP [CGS14,CDPR16,BS16]
- Possible conseq. in crypto based on lattices with algebraic structure [CDW17]

Introduction

A quantum algorithm for computing the unit group of an arbitrary degree number field

Kirsten Eisenträger*
Department of Mathematics
The Pennsylvania State University
eisentra@math.psu.edu
and Harvard University

Sean Hallgren†
Dept. of Computer Science and Engineering
The Pennsylvania State University
hallgren@cse.psu.edu

Alexei Kitaev
Kavli Institute for Theoretical Physics
University of California, Santa Barbara
kitaev@kitp.ucsb.edu
and California Institute of Technology

Fang Song
Department of Combinatorics & Optimization
and Institute for Quantum Computing
University of Waterloo
j.song@uwaterloo.ca

Extended abstract (2014)

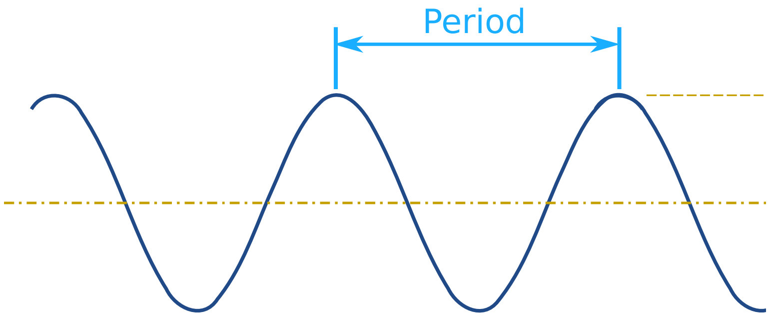
Shortcomings

THEOREM 6.1. *There is a polynomial time quantum algorithm for solving the HSP over* $\mathbb{R}^m$.

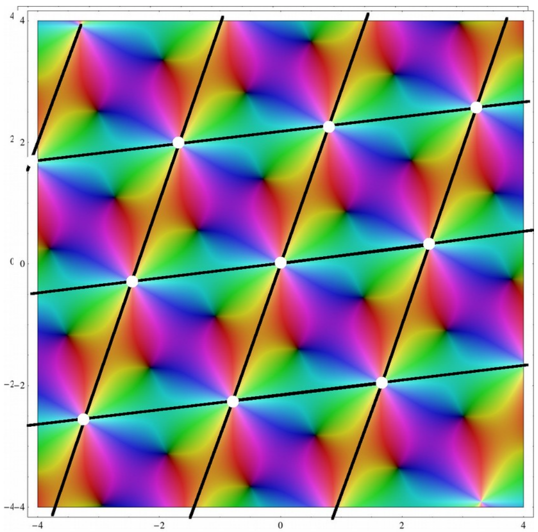
- No exclusion of intractable instances
- Polynomial in which variable?
- Only high-level reasoning in the ext. abstract
- Up to now, 5 years later, no full version published

Problem statement (informal)

- Given a 'nice' periodic function, find its period.



- More psychedelic example in 2d:



- Insight: In higher dimensions the period is encoded by a ***lattice***

Problem statement (formal)

- Given black-box access to a function $f : \mathbb{R}^m \to \mathcal{S} \subseteq \mathbb{C}^n$ that satisfies the following:

  (i) f is *periodic* w.r.t. some lattice Λ

  $$f(x+\ell) = f(x) \text{ for all } x \in \mathbb{R}^m \text{ and } \ell \in \Lambda$$

  (ii) f is *Lipschitz-continuous*

  $$|f(x) - f(y)| \leq a \cdot |x - y|$$

  (iii) f is *seperable*, i.e., not too constant.

$$\text{If } \mathrm{d}_{\mathbb{R}^m/\Lambda}(x,y) \geq r, \text{ then } |\langle f(x), f(y)\rangle| \leq \epsilon, \text{ for all } x, y \in \mathbb{R}^m$$

- **Find:** A τ-approximate basis of the lattice Λ

Our contributions

- Statement with all dependencies on parameters

Theorem 1. *There exists a quantum algorithm that, given access to an (a, r, ϵ)-HSP oracle with period lattice Λ, $r < \lambda_1(\Lambda)/6$ and $\epsilon < 1/4$, computes, with constant success probability, an approximate basis $\tilde{B} = B + \Delta_B$ of this lattice Λ, satisfying $\|\Delta_B\| < \tau$.*

This algorithm makes k quantum oracle calls to the (a, r, ϵ)-HSP oracle, and uses $mQ + n$ qubits, $O(km^2Q^2)$ quantum gates and $poly(m, \log \frac{a}{\lambda_1^* \tau})$ classical bit operations, where

$$Q = O(m \log(m \log k)) + O(mk) + O\left(\log \frac{a}{\lambda_1^* \tau}\right), \quad (1)$$

$$k = O(m) + O(\log m + m \log a + \log \det \Lambda). \quad (2)$$

- Rigorous proof of this statement
- Simplifying the quantum algorithm of Eisenträger et al.

High level approach

This talk

- Sample approx. dual lattice points $\tilde{\ell}^*$ with $\ell^* \in \Lambda^*$ using a quantum algorithm

- From enough of such $\tilde{\ell}^*$, recover an approx. dual basis $\tilde{D}$ of Λ^*

- From $\tilde{D}$ recover an approx. primal basis $\tilde{B}$ of Λ

Some important thoughts

- The notion of the *dual lattice*

$$\Lambda^* = \{\ell^* \in \operatorname{span}(\Lambda) \mid \langle \ell^*, \ell\rangle \in \mathbb{Z} \text{ for all } \ell \in \Lambda\}$$

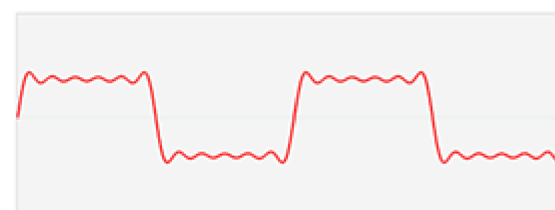
- Define

$$\chi_{\ell^*} : x \mapsto e^{2\pi i\langle x, \ell^*\rangle}$$

- Every nice Λ-periodic function f can be written

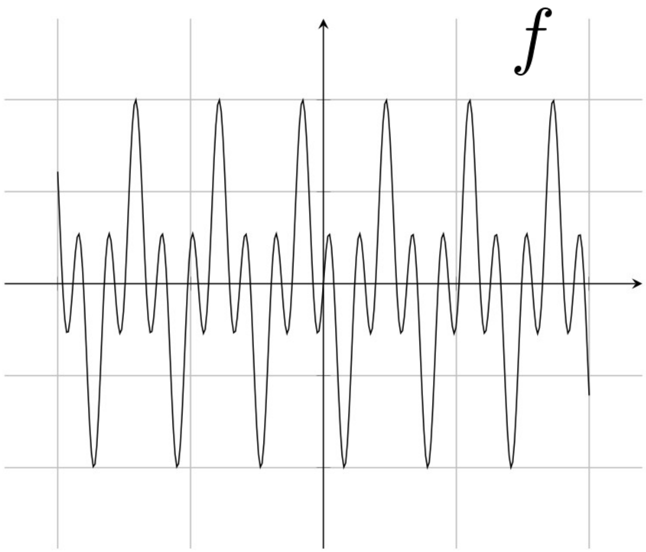
$$f = \sum_{\ell^* \in \Lambda^*} c_{\ell^*}\chi_{\ell^*} \quad \text{with} \quad c_{\ell^*} \in \mathbb{C}^n$$

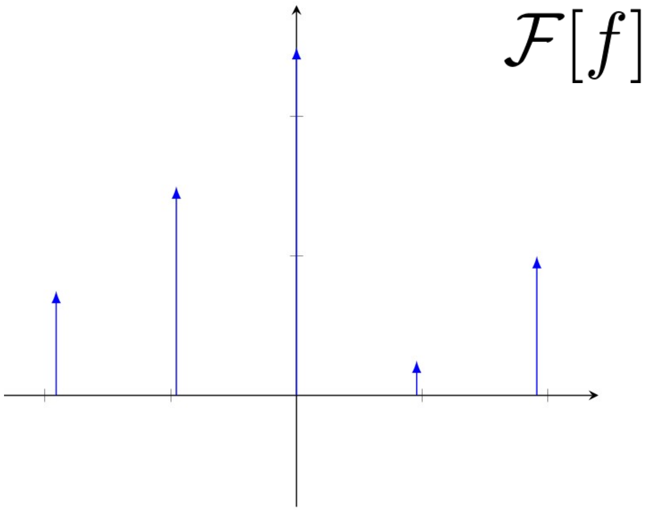
the *Fourier decomposition of* f

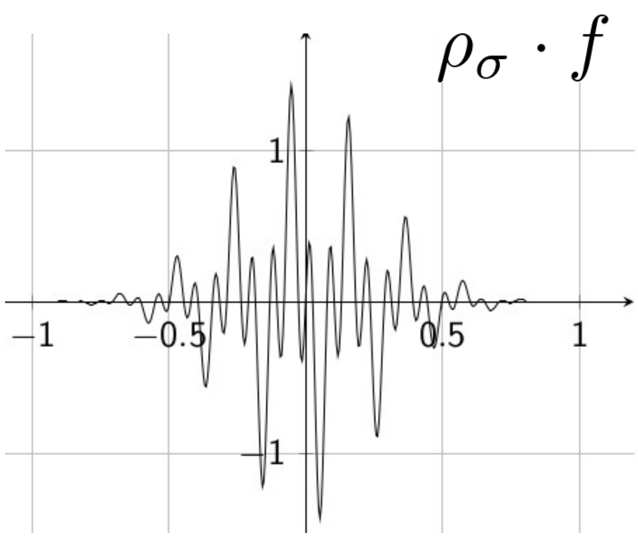


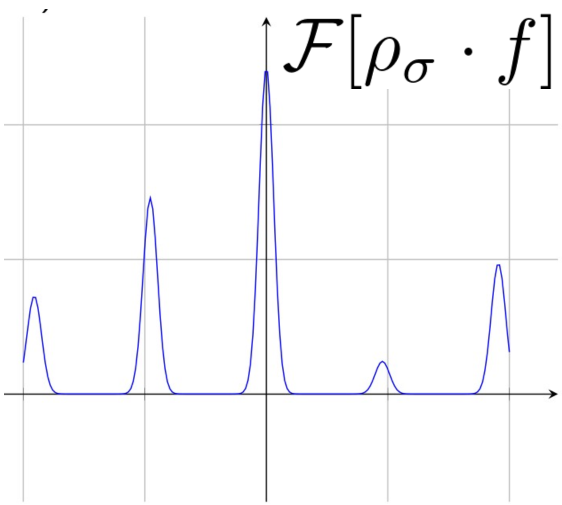
One more important thought

- The convolution theorem $\mathcal{F}[f \cdot g] = \mathcal{F}[f] \star \mathcal{F}[g]$



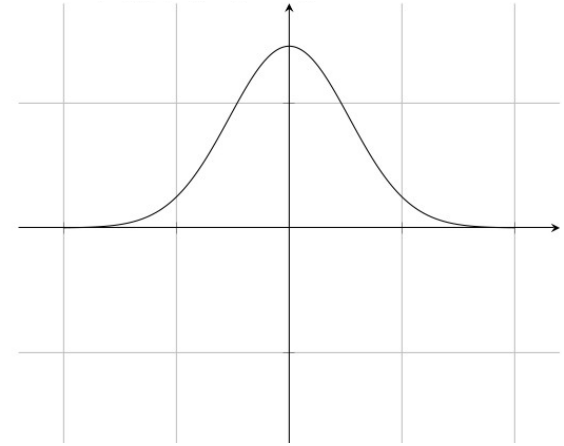






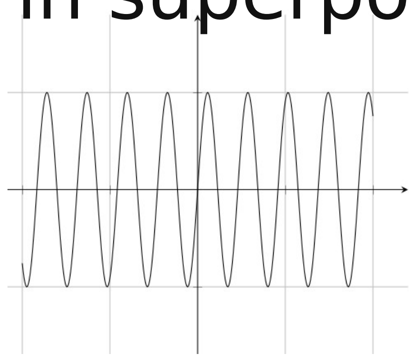
Global idea

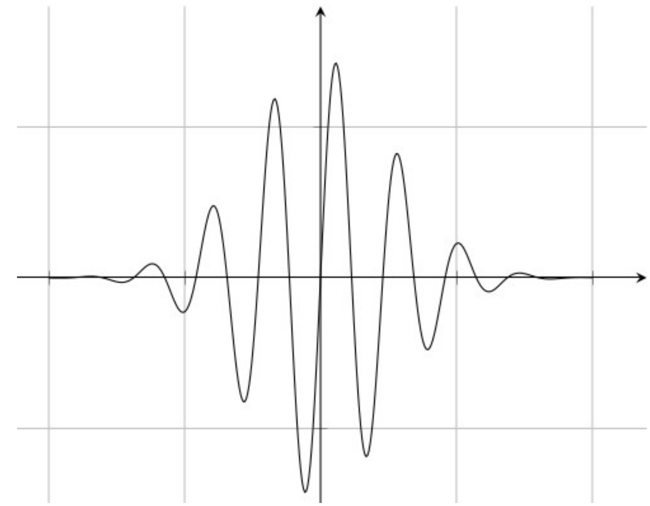
- Create the Gaussian superposition



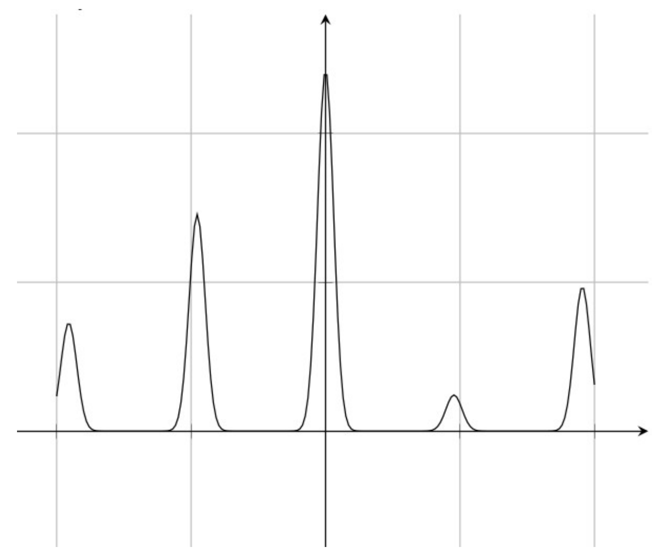
- Query f in superposition

$$f =$$





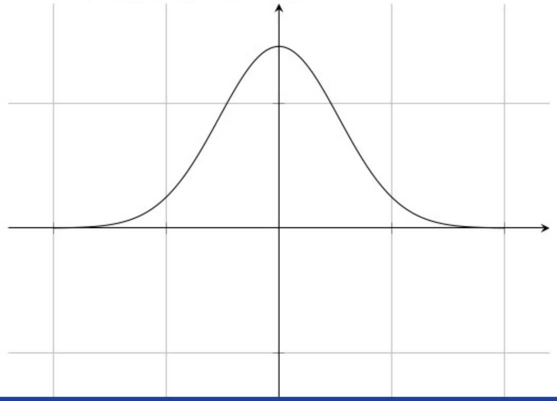
- Apply the Fourier Transform



- Measure

Global idea

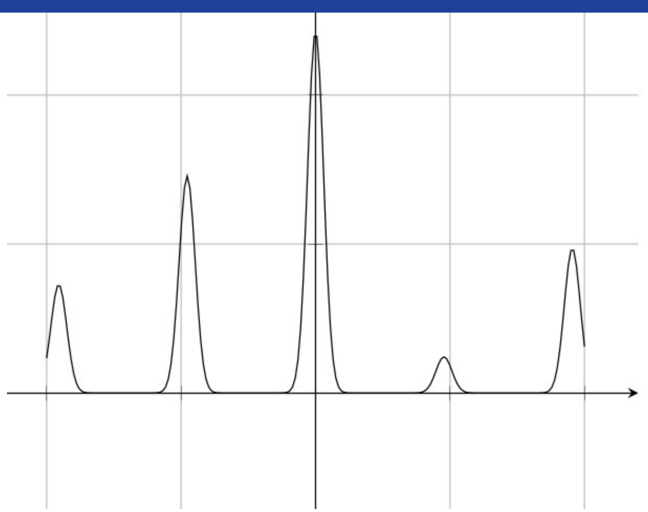
- Create the Gaussian superposition



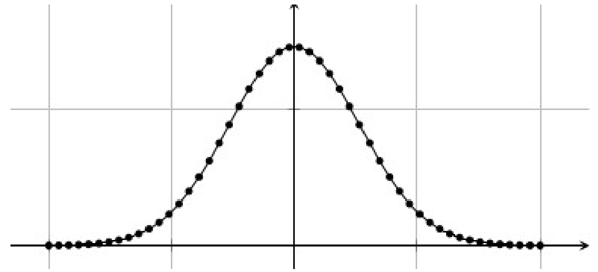
- Q computers only have finitely many qubits
- We need to discretize and ‘window’ the wave
- Fourier transf. becomes Finite Fourier Transf.

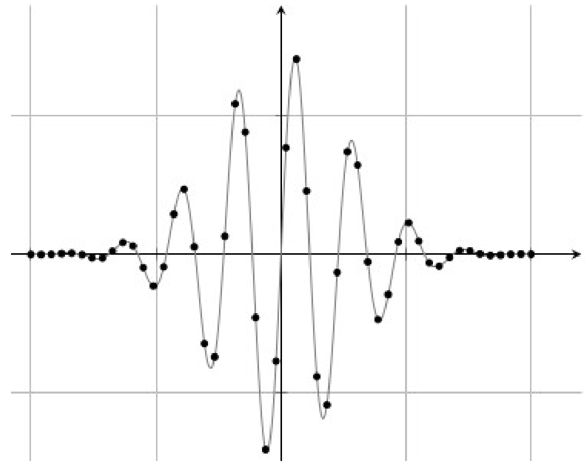
- Apply the Fourier Transform

- Measure



Quantum algorithm



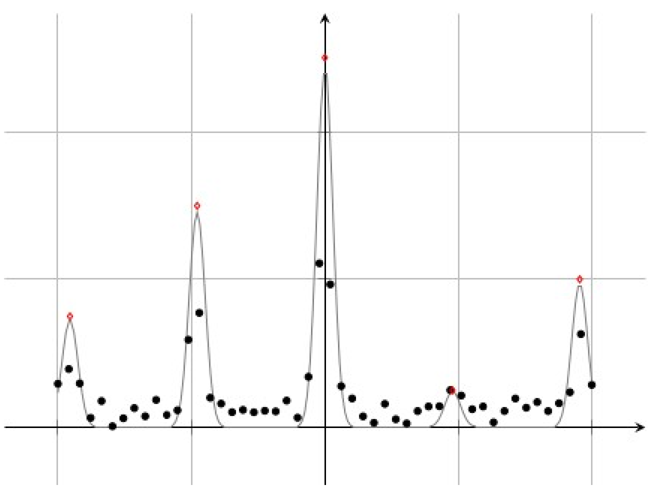


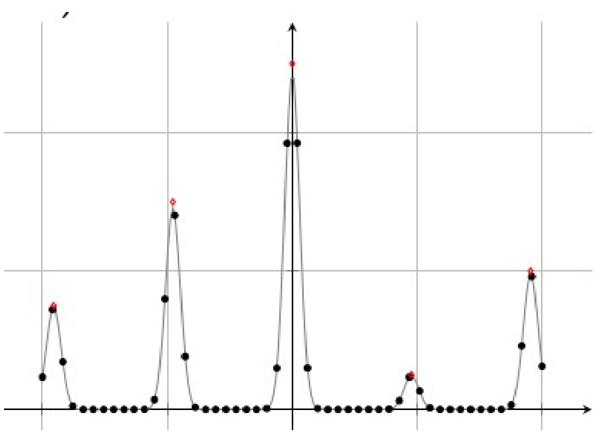
Actual case:
<u>Finite</u> Fourier transform

Ideal case:
Fourier transform restricted to grid

?

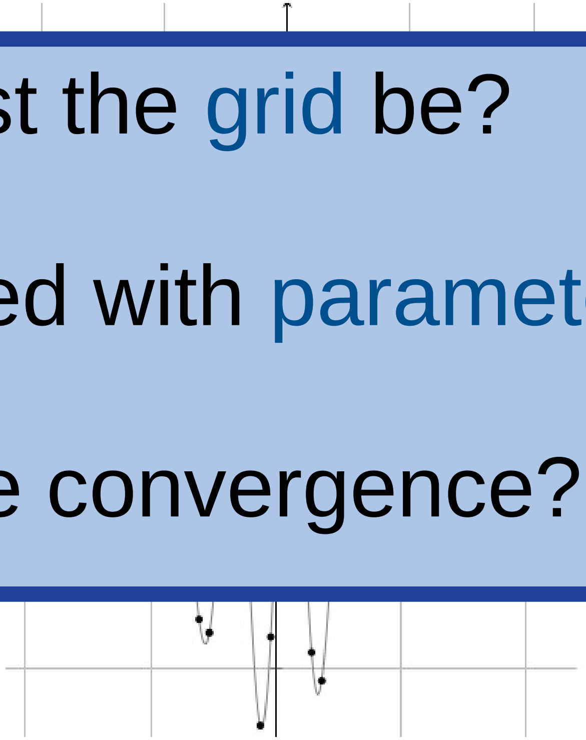
≈





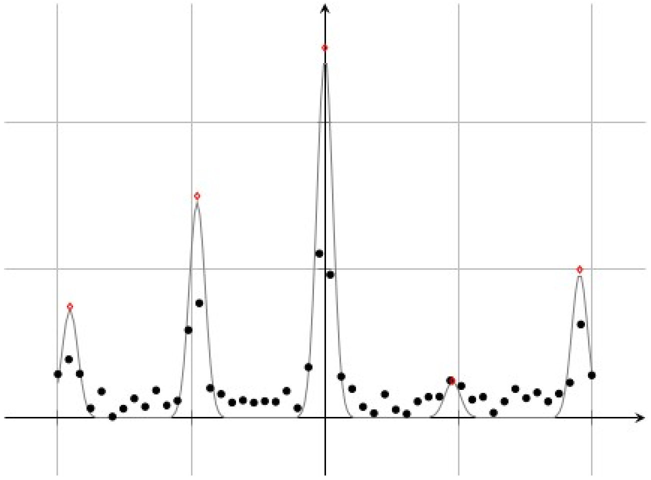
Quantum algorithm

- How ‘fine’ must the grid be?
- How is it related with parameters a, r, ε, τ ?
- How fast is the convergence?



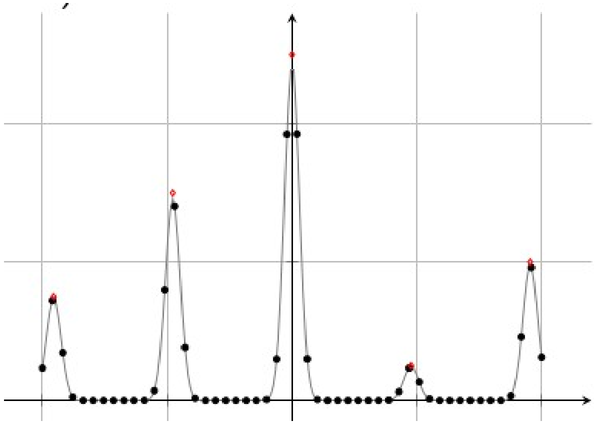
Actual case:
Finite Fourier transform

Ideal case:
Fourier transform restricted to grid



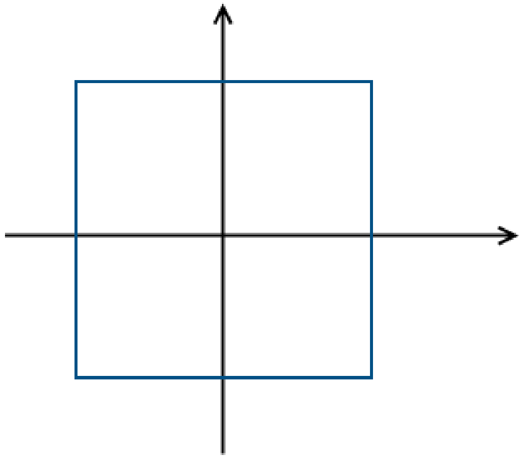
?

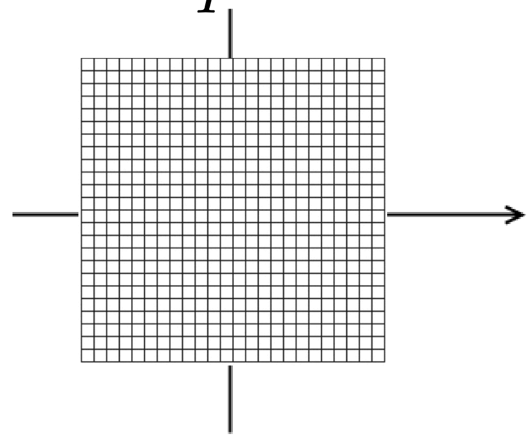
≈



Fourier transforms

$$\mathbb{T} = [-1/2, 1/2]^m \qquad \mathbb{G} = \frac{1}{q} \cdot \mathbb{Z}^m \cap \mathbb{T}$$





$$\mathcal{F}_{\mathbb{G}}\{f \cdot \rho_\sigma\}(y) = \frac{1}{|\mathbb{G}|} \sum_{x \in \mathbb{G}} e^{-2\pi i \langle x, y \rangle} \cdot f(x) \rho_\sigma(x)$$

$$\text{error } \approx \frac{a}{q}$$

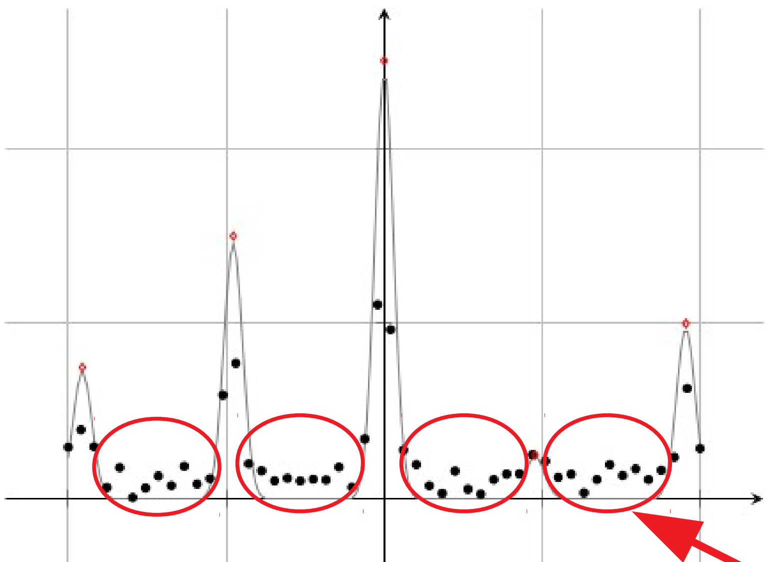
$$\mathcal{F}_{\mathbb{T}}\{f \cdot \rho_\sigma\}(y) = \int_{x \in \mathbb{T}} e^{-2\pi i \langle x, y \rangle} \cdot f(x) \rho_\sigma(x) dx$$

$$\text{error } \approx e^{-\sigma^2}$$

$$\mathcal{F}_{\mathbb{R}^m}\{f \cdot \rho_\sigma\}(y) = \int_{x \in \mathbb{R}^m} e^{-2\pi i \langle x, y \rangle} \cdot f(x) \rho_\sigma(x) dx$$

Fourier transforms

- These are pointwise errors
- We want the error in the L_2-distance



We want the sum of those to be small

Actual Analysis

- Grid $\to$ Unit cube: the Yudin-Jackson theorem

$$\mathcal{F}_{\mathbb{G}}\{f \cdot \rho_\sigma\} \approx \mathcal{F}_{\mathbb{T}}\{f \cdot \rho_\sigma\}$$

About optimal trigonometric approximations

- Unit cube $\to$ real space: the Poisson Summation Formula

$$\mathcal{F}_{\mathbb{T}}\{f \cdot \rho_\sigma\} \approx \mathcal{F}_{\mathbb{R}^m}\{f \cdot \rho_\sigma\}\big|_{\mathbb{Z}^m}$$

About the interplay between Fourier transforms the operations ‘restriction’ and ‘periodization’ on functions

Main theorem

Theorem 1. *There exists a quantum algorithm that, given access to an (a, r, ϵ)-HSP oracle with period lattice Λ, $r < \lambda_1(\Lambda)/6$ and $\epsilon < 1/4$, computes, with constant success probability, an approximate basis $\tilde{B} = B + \Delta_B$ of this lattice Λ, satisfying $\|\Delta_B\| < \tau$.*

This algorithm makes k quantum oracle calls to the (a, r, ϵ)-HSP oracle, and uses $mQ + n$ qubits, $O(km^2Q^2)$ quantum gates and poly$(m, \log \frac{a}{\lambda_1^* \tau})$ classical bit operations, where

$$Q = O(m \log(m \log k)) + O(mk) + O\left(\log \frac{a}{\lambda_1^* \tau}\right), \quad (1)$$

$$k = O(m) + O(\log m + m \log a + \log \det \Lambda). \quad (2)$$

Taking $k = O(m)$ we need $\tilde{O}(m^3)$ qubits and $\tilde{O}(m^7)$ quantum gates

This high complexity is mostly due to numerical instability of generating a dual basis and inverting this basis to obtain a primal basis.

Open questions

- Complexity unit group or class group computation?
- Complexity of Principal Ideal Problem?
- Are there assumptions on the oracle function making the complexity better?
- Using BKZ to improve the numerical stability of recovering the primal basis?
- Using sublattices or symmetries of lattices to improve complexity

Questions?

Me: **finishes an academic presentation with some immature meme**
The scientific community: