Efficient quantum algorithms for the principal ideal problem and class group problem in \textit{arbitrary-degree} number fields

Fang Song
Institute for Quantum Computing
University of Waterloo

Joint work with
Jean-François Biasse (U. South Florida)
Which problems have faster quantum algorithms than classical algorithms?

Existence of Poly-time quantum algorithms for:

- Factoring and discrete logarithm [Shor’94]
- Basic problems in computational algebraic number theory
  - Unit group in number fields
  - Principal Ideal Problem (PIP) & Class group problem
  - Constant degree [Hallgren’02’05, SchmidtVollmer’05]
  - Arbitrary degree [EHKS’14]
  - Constant degree number fields [H’02’05, SV’05]
  - This work: arbitrary degree!

Best known classical algorithms need (at least) sub-exponential time
Results and Implications

- Efficient quantum algorithms for several basic problems in number fields of arbitrary-degree
- Examples of quantum exponential speedup
- Minor: converting solutions into compact representation

Application: PIP algorithm can be used to break classical crypto

- Smart-V Fully Homomorphic Encryption, GargGH multilinear mapping scheme, ... [CGS14,CDPR15,BS15]
- Previously considered quantum-safe (based on ideal lattice problems instead of factoring/DL)
Outline of our quantum algorithms

**INPUT:** a degree n number field K

- Principal ideal problem
- Class group problem
- Norm eqns, ...

**Computing** *S*-units in K

* S = \{prime ideals\} may differ for each problem

**Main contribution**

Quantum reduction

**Continuous HSP**

Hidden Subgroup Problem

**OUTPUT**

S-units of K

Invoke quantum HSP alg. in [EHKS’14]
Hidden subgroup problem (HSP) framework

**Input**
- Problem $\Pi$

**Reduction**
- HSP on a group $G$

**Quantum Algorithm**
- Solution to $\Pi$

- Captures most quantum exponential speedup

- **Standard Def.**: HSP on finite group $G$
  - **Given**: oracle function $f: G \rightarrow S$, 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) $H$.

- **Uncountable group $\mathbb{R}^m$**: tricky due to discretization!
  - Some earlier defs. only suitable for small dimension $m$ [Ho2, Ho5, SVo5]
  - A “right” def. in high dimensions: continuous HSP [EHKS14]
Continuous HSP on $\mathbb{R}^m$

Given $f: \mathbb{R}^m \rightarrow \{\text{quantum states}\}$, s.t.: $\exists$ discrete $H \leq \mathbb{R}^m$,

1. (Periodic) $x - y \in H \Rightarrow |f(x)\rangle = |f(y)\rangle$.
2. (Pseudo-injective) $x - y$ far from $H \Rightarrow |f(x)\rangle \perp |f(y)\rangle$.
3. (Lipschitz continuity) $x - y$ close to $H \Rightarrow |f(x)\rangle \approx |f(y)\rangle$.

Goal: Find (hidden subgroup) $H$.

Theorem [EHKS14] $\exists$ efficient quantum algorithm solving continuous HSP on $\mathbb{R}^m$.

N.B.: $H$ is a Lattice
$L(B) = \{a_1v_1 + \cdots + a_mv_m : a_i \in \mathbb{Z}\} \subseteq \mathbb{R}^m$
- Basis $B: \{v_i \in \mathbb{R}^n : i = 1, \ldots, m\}$
- $L$ has (infinitely) many bases
### Interesting HSP instances

<table>
<thead>
<tr>
<th>Computational Problems</th>
<th>HSP on G</th>
</tr>
</thead>
<tbody>
<tr>
<td>Factoring</td>
<td>$\mathbb{Z}$</td>
</tr>
<tr>
<td>Discrete logarithm</td>
<td>$\mathbb{Z}_N \times \mathbb{Z}_N$</td>
</tr>
<tr>
<td>Unit group, PIP, class group, constant-degree fields</td>
<td>$\mathbb{R}^{\text{const}}$</td>
</tr>
<tr>
<td>Unit group, arbitrary degree $n$</td>
<td>Continuous $\mathbb{R}^{O(n)}$</td>
</tr>
<tr>
<td>[This work] PIP, class group, arbitrary degree $n$</td>
<td>Continuous $\mathbb{R}^{O(n)}$</td>
</tr>
<tr>
<td>Graph isomorphism</td>
<td>Symmetric group</td>
</tr>
<tr>
<td>Unique shortest vector problem</td>
<td>Dihedral group</td>
</tr>
</tbody>
</table>

- **Abelian groups**
  - $\exists$ efficient quantum alg.
- **Non-abelian groups**
  - Open question: $\exists$ efficient quantum alg.
Outline of our quantum algorithms

INPUT: a degree n number field K

Principal ideal problem
Class group problem
Norm eqns, ...

Computing* S-units in K

Quantum reduction

Continuous HSP

OUTPUT

S-units of K
Number Field Basics

- **Number Field** $K \subseteq \mathbb{C}$: Finite extension of $\mathbb{Q}$.
  - Degree $n$: dimension of $K$ as vector space over $\mathbb{Q}$

- **Ring of Integers** $\mathcal{O}$: $K \cap$ Roots of monic irreducible poly $\mathbb{Z}[X]$. (e.g. $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$)
  
  **Ex (Cyclotomic field).** $\mathbb{Q}(\omega) = \{a_0 + a_1 \omega + \cdots + a_{p-2} \omega^{p-2} : a_i \in \mathbb{Q}\}. \omega = e^{2\pi i/p}, p$ prime.
  - $\mathcal{O} = \mathbb{Z}[\omega], n = p - 1$

- **Group of S-units** $U_S$:
  - $S = \{p_1, \ldots, p_k\}$ a set of prime ideals
  - $U_{\emptyset} = \{\alpha \in \mathcal{O} : \alpha \mathcal{O} = p_1^{v_1} \cdots p_k^{v_k} \text{ for some } v_i \in \mathbb{Z}\}$

- **Special case: Unit group** $U$
  - $S = \emptyset \Rightarrow U_{\emptyset} = U = \{\text{invertible elements in } \mathcal{O}\}$

<table>
<thead>
<tr>
<th>Principal Ideal Problem</th>
</tr>
</thead>
<tbody>
<tr>
<td>Given ideal $I \subseteq \mathcal{O}$ decide if $I = \alpha \mathcal{O}$ and find $\alpha$ if so.</td>
</tr>
</tbody>
</table>

- **Classical alg’s:** $\exp(n) \exp(|\mathcal{O}|)$
- **Quantum alg’s:** $\exp(n) \text{ poly } (|\mathcal{O}|)$
- **This work:** $\text{poly}(n) \text{ poly } (|\mathcal{O}|)$
Outline of our quantum algorithms

INPUT: a degree n number field \( K \)

Principal ideal problem
Class group problem
Norm eqns, ...

Computing* S-units in \( K \)

Quantum reduction

Continuous HSP

\( \surd_2 \)

\( \surd_1 \)

3

OUTPUT

S-units of \( K \)
Reducing $S$-units to Continuous HSP

[HSP instance] $f = f_q \circ f_c$

- Units $U$
  $\phi$
  $m = O(n)$
  $\Lambda \subseteq \mathbb{R}^m$

- {lattices in $\mathbb{R}^n$}

- $f_c$
  $\{\text{lattices in } \mathbb{R}^n\}$

- $f_q$
  $\{\text{quantum states}\}$

[EHKS14] $\{q\text{-units}\} \leq \mathbb{R}^m$

- This work $S = \{p_1, \ldots, p_k\}$

- $S$-Units $U_S$
  $\phi_S$
  $\Lambda_S \subseteq \mathbb{R}^m \times \mathbb{Z}^k$

- $\{\text{lattices in } \mathbb{R}^n\}$

- $g_c$
  $\{\text{lattices in } \mathbb{R}^n\}$

- $f_q$
  $\{\text{quantum states}\}$

[HSP instance*] $f_S = f_q \circ g_c$

* $f_S$ can further be turned into an $f'_S$ on $\mathbb{R}^{m+k}$
Identifying $S$-units as a subgroup

$\alpha \in U_S \iff \alpha \mathcal{O} \cdot \Pi_{i=1}^k p_i^{-v_i} = \mathcal{O}, v_i \in \mathbb{Z}$

- Canonical embedding 
  $\alpha \in K \mapsto \underline{\alpha} := (\alpha_1, ..., \alpha_n) \in \mathbb{R}^n$
- Fact: $\mathcal{O} \mapsto \underline{\mathcal{O}} \subseteq \mathbb{R}^n$, a lattice!

$\phi_S : \alpha \in U_S \mapsto (x, v) \in \mathbb{R}^{m \times \mathbb{Z}^k}$

$\Lambda_S := \phi_S(U_S) \subseteq \mathbb{R}^{m \times \mathbb{Z}^k}$ is a full-rank lattice!

Characterization of $S$-units

- $L_x := e^x \underline{\mathcal{O}} = \begin{bmatrix} e^{x_1} \\ \vdots \\ e^{x_m} \end{bmatrix} \cdot \underline{\mathcal{O}}$
- $L_v := \Pi_{i=1}^k p_i^{-v_i} \subseteq \mathcal{O}$

$\Rightarrow (x, v) \in \Lambda_S \iff L_x \cdot L_v = \mathcal{O}$
Defining hiding function: classical part

\[(x, v) \in \Lambda_S \iff L_x \cdot L_v = \varnothing\]

\[g_c(x, v) = L_x \cdot L_v\]

1. (\(\Lambda_S\)-periodic)
   \[(x, v) \in \Lambda_S \Rightarrow (x, v) \in \Lambda_S\]

2. (Lipschitz)
   “Small” shift in inputs
   \(\Rightarrow\) “Similar” output lattices

3. (Pseudo-inj)
   “Big” shift in inputs
   \(\Rightarrow\) Small-overlap lattices
Completing the HSP reduction

S-Units $U_S$

$\phi_S \downarrow$

$\Lambda_S \leq \mathbb{R}^m \times \mathbb{Z}^k$

$g_c \downarrow$

{lattices in $\mathbb{R}^n$}

$f_q \downarrow$

{quantum states}

**Issue:** no unique representation for lattices in $\mathbb{R}^n$
- $L_{x,v} = L_{x',v'}$ same lattice, but $g_c(x,v)$ and $g_c(x',v')$ output different bases.

**Fix:** encode lattices in quantum states [EHKS14]
- $f_q: L \mapsto |L\rangle = $ superposition over “all” lattice points

$\Rightarrow \langle L'|L \rangle \propto L \cap L'$

**Theorem.** $f_S = f_q \circ g_c$ is a continuous HSP instance w. period $\Lambda_S$.
- (Lipschitz) $(x,v) - (x',v')$ close to $\Lambda_S \xrightarrow{g_c} L \approx L' \xrightarrow{f_q} \langle L'|L \rangle \approx 1$
- (P-Inj.) $(x,v) - (x',v')$ far from $\Lambda_S \xrightarrow{g_c} L \& L'$ small overlap $\xrightarrow{f_q} \langle L'|L \rangle$ small

**What's missing:** efficiently implement $f_S$
- ! Computing $g_c$ delicate: $e^x$ doubly-exp. large & precision loss

$\Rightarrow$ Invoke quantum HSP algorithm [EHKS14], we find $\Lambda_S$ efficiently!
Summary

Number field $K$ of arbitrary degree $n$

- PIP, class group, ...

Future Directions

- Solving more problems in the continuous HSP framework
- Quantum attacks on other (ideal) lattice cryptosystems
- Better quantum algorithms for Non-abelian HSP?

Thank you!