#### Fast Quantum Algorithms Lectures 1 and 2

Gábor Ivanyos MTA SZTAKI

3rd de Brún Workshop, Galway 7-10 December, 2009.

・ 同 ト ・ ヨ ト ・ ヨ ト

# Contents

- Simon's algorithm
  - 2 Basic tools
    - QFT mod powers of 2
    - Phase estimation
    - Period finding
    - QFT over abelian groups
- 3 The HSP
  - The Hidden Subgroup Problem
  - Coset states
  - Abelian Fourier sampling
  - Applications of abelian HSP
- 4 Infinite abelian HSPs
  - HSP in lattices
  - Units in number fields and hidden lattices
  - Open problems

個 と く ヨ と く ヨ と

#### Simon's problem

•  $f: \mathbb{Z}_2^n \to \mathbb{Z}_2^m \ (m \ge n)$ 

・ロン ・回 と ・ 回 と ・ 回 と

#### Simon's problem

• 
$$f: \mathbb{Z}_2^n \to \mathbb{Z}_2^m \ (m \ge n)$$

given by oracle performing  $|x
angle|0
angle\mapsto |x
angle|f(x)
angle$ 

・ロト ・回ト ・ヨト ・ヨト

#### Simon's problem

•  $f: \mathbb{Z}_2^n \to \mathbb{Z}_2^m \ (m \ge n)$ 

given by oracle performing  $|x
angle|0
angle\mapsto |x
angle|f(x)
angle$ 

Promise:

ヘロン 人間 とくほど くほとう

#### Simon's problem

•  $f: \mathbb{Z}_2^n \to \mathbb{Z}_2^m \ (m \ge n)$ 

given by oracle performing  $|x
angle|0
angle\mapsto |x
angle|f(x)
angle$ 

Promise:

• either  $\exists u \text{ s.t.}$ 

$$f(x) = f(x') \Leftrightarrow x' = x \text{ or } x' = x + u$$

イロン イヨン イヨン イヨン

#### Simon's problem

•  $f: \mathbb{Z}_2^n \to \mathbb{Z}_2^m \ (m \ge n)$ 

given by oracle performing  $|x
angle|0
angle\mapsto |x
angle|f(x)
angle$ 

Promise:

• either  $\exists u \text{ s.t.}$ 

$$f(x) = f(x') \Leftrightarrow x' = x \text{ or } x' = x + u$$

• or f injective

イロン イヨン イヨン イヨン

#### Simon's problem

• 
$$f: \mathbb{Z}_2^n \to \mathbb{Z}_2^m \ (m \ge n)$$

given by oracle performing  $|x
angle|0
angle\mapsto |x
angle|f(x)
angle$ 

• Promise:

• either  $\exists u \text{ s.t.}$ 

$$f(x) = f(x') \Leftrightarrow x' = x \text{ or } x' = x + u$$

• or f injective

• Task: decide which is the case

イロン イヨン イヨン イヨン

#### Simon's problem

•  $f: \mathbb{Z}_2^n \to \mathbb{Z}_2^m \ (m \ge n)$ 

given by oracle performing  $|x
angle|0
angle\mapsto |x
angle|f(x)
angle$ 

Promise:

• either  $\exists u \text{ s.t.}$ 

$$f(x) = f(x') \Leftrightarrow x' = x \text{ or } x' = x + u$$

- or f injective
- Task: decide which is the case
  - and find u if  $\exists$

・ロン ・回と ・ヨン ・ヨン

#### Simon's problem

•  $f: \mathbb{Z}_2^n \to \mathbb{Z}_2^m \ (m \ge n)$ 

given by oracle performing  $|x
angle|0
angle\mapsto |x
angle|f(x)
angle$ 

Promise:

• either  $\exists u \text{ s.t.}$ 

$$f(x) = f(x') \Leftrightarrow x' = x \text{ or } x' = x + u$$

- or f injective
- Task: decide which is the case
  - and find u if  $\exists$
  - Remark: reducible to the decision version

・ 御 と ・ 臣 と ・ を 臣 と

#### Simon's problem

•  $f: \mathbb{Z}_2^n \to \mathbb{Z}_2^m \ (m \ge n)$ 

given by oracle performing  $|x
angle|0
angle\mapsto |x
angle|f(x)
angle$ 

Promise:

• either  $\exists u \text{ s.t.}$ 

$$f(x) = f(x') \Leftrightarrow x' = x \text{ or } x' = x + u$$

- or f injective
- Task: decide which is the case
  - and find u if  $\exists$
  - Remark: reducible to the decision version
- Classically difficult:

▲圖▶ ★ 国▶ ★ 国▶

#### Simon's problem

•  $f: \mathbb{Z}_2^n \to \mathbb{Z}_2^m \ (m \ge n)$ 

given by oracle performing  $|x
angle|0
angle\mapsto |x
angle|f(x)
angle$ 

Promise:

• either  $\exists u \text{ s.t.}$ 

$$f(x) = f(x') \Leftrightarrow x' = x \text{ or } x' = x + u$$

- or f injective
- Task: decide which is the case
  - and find u if  $\exists$
  - Remark: reducible to the decision version
- Classically difficult:

with  $2^{\frac{n}{4}}$  queries can guess the case only with probability  $\leq \frac{1}{2} + \frac{1}{2^{n/2}}$ 

同 と く き と く き と

#### Simon's algorithm

• |0
angle|0
angle

Gábor Ivanyos MTA SZTAKI Fast Quantum Algorithms Lectures 1 and 2

・ロン ・雪 ・ ・ ヨ ・ ・ ヨ ・ ・

#### Simon's algorithm

•  $|0\rangle|0\rangle$ 

#### $\mathsf{Hadamard}^{\otimes n}$

## Simon's algorithm

•  $|0\rangle|0\rangle$   $\downarrow$ •  $\sum_{x\in\mathbb{Z}_2^n}|x\rangle|0\rangle$ 

#### $\mathsf{Hadamard}^{\otimes n}$

・ロト ・回ト ・ヨト ・ヨト

## Simon's algorithm

• 
$$|0\rangle|0\rangle$$
  
 $\downarrow$   
•  $\sum_{x\in\mathbb{Z}_{2}^{n}}|x\rangle|0\rangle$   
 $\downarrow$ 

#### $\mathsf{Hadamard}^{\otimes n}$

*f*-oracle

・ロト ・回ト ・ヨト ・ヨト

## Simon's algorithm

•  $|0\rangle|0\rangle$   $\downarrow$ •  $\sum_{x\in\mathbb{Z}_2^n}|x\rangle|0\rangle$   $\downarrow$ •  $\sum_{x\in\mathbb{Z}_2^n}|x\rangle|f(x)\rangle$ 

#### $\mathsf{Hadamard}^{\otimes n}$

*f*-oracle

・ロト ・回ト ・ヨト ・ヨト

Э

#### Simon's algorithm

•  $|0\rangle|0\rangle$ •  $\sum_{x\in\mathbb{Z}_2^n}|x\rangle|0\rangle$ •  $\sum_{x\in\mathbb{Z}_2^n}|x\rangle|f(x)\rangle$ ↓

 $\mathsf{Hadamard}^{\otimes n}$ 

f-oracle

measure f(x), drop it

・ロン ・回 と ・ ヨ と ・ ヨ と

#### Simon's algorithm

•  $|0\rangle|0\rangle$   $\downarrow$ •  $\sum_{x\in\mathbb{Z}_2^n}|x\rangle|0\rangle$   $\downarrow$ •  $\sum_{x\in\mathbb{Z}_2^n}|x\rangle|f(x)\rangle$   $\downarrow$ •  $|x\rangle + |x + u\rangle$ 

 $\mathsf{Hadamard}^{\otimes n}$ 

*f*-oracle

measure f(x), drop it

イロト イヨト イヨト イヨト

#### Simon's algorithm

•  $|0\rangle|0\rangle$   $\downarrow$ •  $\sum_{x\in\mathbb{Z}_2^n}|x\rangle|0\rangle$   $\downarrow$ •  $\sum_{x\in\mathbb{Z}_2^n}|x\rangle|f(x)\rangle$   $\downarrow$ •  $|x\rangle + |x + u\rangle$  $\downarrow$ 

 $\mathsf{Hadamard}^{\otimes n}$ 

f-oracle

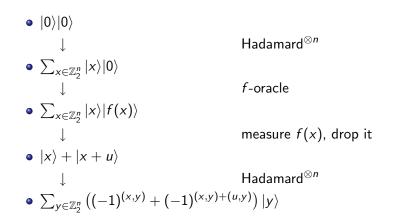
measure f(x), drop it

・ロン ・回 と ・ ヨ と ・ ヨ と

3

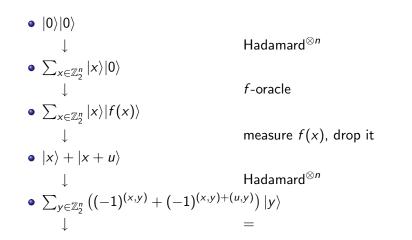
 $\mathsf{Hadamard}^{\otimes n}$ 

#### Simon's algorithm



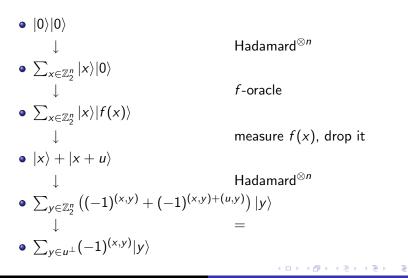
イロト イヨト イヨト イヨト

#### Simon's algorithm



▲圖▶ ▲屋▶ ▲屋▶

## Simon's algorithm



#### Simon's algorithm 2

•  $\sum_{y \in u^{\perp}} (-1)^{xy} |y\rangle$ 

・ロン ・回 と ・ ヨ と ・ ヨ と

#### Simon's algorithm 2

• 
$$\sum_{y \in u^{\perp}} (-1)^{xy} | y \rangle$$
  
 $\downarrow$  measure

Gábor Ivanyos MTA SZTAKI Fast Quantum Algorithms Lectures 1 and 2

・ロン ・雪 ・ ・ ヨ ・ ・ ヨ ・ ・

#### Simon's algorithm 2

• 
$$\sum_{y \in u^{\perp}} (-1)^{xy} | y \rangle$$
  
 $\downarrow$  measure  
• random  $y \in u^{\perp}$ 

Gábor Ivanyos MTA SZTAKI Fast Quantum Algorithms Lectures 1 and 2

< □ > < □ > < □ > < □ > < □ > < Ξ > < Ξ > □ Ξ

#### Simon's algorithm 2

• 
$$\sum_{y \in u^{\perp}} (-1)^{xy} | y \rangle$$
  
 $\downarrow$  measure

• random  $y \in u^{\perp}$ 

• 
$$\ell = O(n)$$
 iteration gives  $y_1, \ldots, y_\ell$ :

・ロン ・回 と ・ 回 と ・ 回 と

#### Simon's algorithm 2

• 
$$\sum_{y \in u^{\perp}} (-1)^{xy} | y \rangle$$
  
 $\downarrow$  measure

• random  $y \in u^{\perp}$ 

• 
$$\ell = O(n)$$
 iteration gives  $y_1, \ldots, y_\ell$ :  
 $\{y_1, \ldots, y_\ell\}^\perp = \{0, u\}$  (probably).

・ロン ・回 と ・ ヨ と ・ ヨ と

#### Simon's algorithm 2

• 
$$\sum_{y \in u^{\perp}} (-1)^{xy} | y \rangle$$
  
 $\downarrow$  measure

• random  $y \in u^{\perp}$ 

• 
$$\ell = O(n)$$
 iteration gives  $y_1, \ldots, y_\ell$ :  
 $\{y_1, \ldots, y_\ell\}^\perp = \{0, u\}$  (probably).

• Remarks:

・ロト ・回ト ・ヨト ・ヨト

#### Simon's algorithm 2

• 
$$\sum_{y \in u^{\perp}} (-1)^{xy} | y \rangle$$
  
 $\downarrow$  measure

• random  $y \in u^{\perp}$ 

• 
$$\ell = O(n)$$
 iteration gives  $y_1, \ldots, y_\ell$ :  
 $\{y_1, \ldots, y_\ell\}^\perp = \{0, u\}$  (probably).

- Remarks:
  - measurements only for simplification

・ロト ・回ト ・ヨト ・ヨト

#### Simon's algorithm 2

• 
$$\sum_{y \in u^{\perp}} (-1)^{xy} | y \rangle$$
  
 $\downarrow$  measure

• random  $y \in u^{\perp}$ 

• 
$$\ell = O(n)$$
 iteration gives  $y_1, \ldots, y_\ell$ :  
 $\{y_1, \ldots, y_\ell\}^\perp = \{0, u\}$  (probably).

- Remarks:
  - measurements only for simplification
  - $\exists$  exact method with O(n) rounds (Høyer 97)

<ロ> (日) (日) (日) (日) (日)

#### Simon's algorithm 2

• 
$$\sum_{y \in u^{\perp}} (-1)^{xy} | y \rangle$$
  
 $\downarrow$  measure

• random  $y \in u^{\perp}$ 

• 
$$\ell = O(n)$$
 iteration gives  $y_1, \ldots, y_\ell$ :  
 $\{y_1, \ldots, y_\ell\}^\perp = \{0, u\}$  (probably).

- Remarks:
  - measurements only for simplification
  - ∃ exact method with O(n) rounds (Høyer 97) uses Grover's techniques

Simon's algorithm QFT mod powers of 2 Basic tools Phase estimation The HSP Period finding Infinite abelian HSPs QFT over abelian groups

## Contents



- 2 Basic tools
  - QFT mod powers of 2
  - Phase estimation
  - Period finding
  - QFT over abelian groups
- 3 The HSP
  - The Hidden Subgroup Problem
  - Coset states
  - Abelian Fourier sampling
  - Applications of abelian HSP
- Infinite abelian HSPs
  - HSP in lattices
  - Units in number fields and hidden lattices
  - Open problems

< □ > < □ > < □ >

QFT mod powers of 2 Phase estimation Period finding QFT over abelian groups

# $\mathsf{QFT} \bmod 2^\ell$

• Fourier transform mod  $2^{\ell}$ :

$$\Phi_{2^{\ell}}: |j
angle \mapsto \sum_{k=0}^{2^{\ell}-1} \omega^{kj} |k
angle,$$

where 
$$\omega=\sqrt[2^\ell]{1}~(=e^{rac{2\pi i}{2^\ell}})$$

イロン イヨン イヨン イヨン

э.

Simon's algorithm Basic tools The HSP Infinite abelian HSPs QFT mod powers of 2 Phase estimation Period finding QFT over abelian groups

# $\mathsf{QFT} \bmod 2^\ell$

• Fourier transform mod  $2^{\ell}$ :

$$\Phi_{2^{\ell}}: |j
angle \mapsto \sum_{k=0}^{2^{\ell}-1} \omega^{kj} |k
angle, \qquad ext{ where } \omega = \sqrt[2^{\ell}]{1} \ (= e^{rac{2\pi i}{2^{\ell}}})$$

• Transformation of basis change:

・ロン ・回と ・ヨン ・ヨン

Simon's algorithm Basic tools The HSP Infinite abelian HSPs QFT mod powers of 2 Phase estimation Period finding QFT over abelian groups

# QFT mod $2^{\ell}$

• Fourier transform mod  $2^{\ell}$ :

$$\Phi_{2^{\ell}}: |j
angle \mapsto \sum_{k=0}^{2^{\ell}-1} \omega^{kj} |k
angle, \qquad ext{ where } \omega = \sqrt[2^{\ell}]{1} \ (= e^{rac{2\pi i}{2^{\ell}}})$$

• Transformation of basis change:

standard basis  $\rightarrow$  eigenvectors of shift mod  $2^n$ .

・ロン ・回と ・ヨン ・ヨン

# QFT mod $2^{\ell}$

• Fourier transform mod  $2^{\ell}$ :

$$\Phi_{2^{\ell}}: |j
angle \mapsto \sum_{k=0}^{2^{\ell}-1} \omega^{kj} |k
angle, \qquad ext{ where } \omega = \sqrt[2^{\ell}]{1} \ (= e^{rac{2\pi i}{2^{\ell}}})$$

• Transformation of basis change: standard basis  $\rightarrow$  eigenvectors of shift mod  $2^n$ .

• Spec. case  $\ell = 1$ : Hadamard-gate

# QFT mod $2^{\ell}$

• Fourier transform mod  $2^{\ell}$ :

$$\Phi_{2^{\ell}}:|j\rangle\mapsto \sum_{k=0}^{2^{\ell}-1}\omega^{kj}|k\rangle, \qquad \text{ where } \omega=\sqrt[2^{\ell}]{1} \ (=e^{\frac{2\pi i}{2^{\ell}}})$$

- Transformation of basis change: standard basis  $\rightarrow$  eigenvectors of shift mod  $2^n$ .
- $\bullet$  Spec. case  $\ell=1:$  Hadamard-gate
- qbits of *j*:

$$|j\rangle = |j_{\ell-1}\rangle |j_{\ell-2}\rangle \dots |j_1\rangle |j_0\rangle,$$

イロト イヨト イヨト イヨト

# QFT mod $2^{\ell}$

• Fourier transform mod  $2^{\ell}$ :

$$\Phi_{2^{\ell}}: |j
angle \mapsto \sum_{k=0}^{2^{\ell}-1} \omega^{kj} |k
angle, \qquad ext{ where } \omega = \sqrt[2^{\ell}]{1} \ (= e^{rac{2\pi i}{2^{\ell}}})$$

 Transformation of basis change: standard basis → eigenvectors of shift mod 2<sup>n</sup>.

- $\bullet$  Spec. case  $\ell=1:$  Hadamard-gate
- qbits of *j*:

$$|j\rangle = |j_{\ell-1}\rangle |j_{\ell-2}\rangle \dots |j_1\rangle |j_0\rangle,$$

where

$$j = j_0 + 2j_1 + \ldots + 2^{\ell-1}j_{\ell-1},$$

イロン イヨン イヨン イヨン

# QFT mod $2^{\ell}$

• Fourier transform mod  $2^{\ell}$ :

$$\Phi_{2^{\ell}}:|j\rangle\mapsto \sum_{k=0}^{2^{\ell}-1}\omega^{kj}|k\rangle, \qquad \text{ where } \omega=\sqrt[2^{\ell}]{1} \ (=e^{\frac{2\pi i}{2^{\ell}}})$$

- Transformation of basis change: standard basis → eigenvectors of shift mod 2<sup>n</sup>.
- $\bullet$  Spec. case  $\ell=1:$  Hadamard-gate
- qbits of *j*:

$$|j\rangle = |j_{\ell-1}\rangle |j_{\ell-2}\rangle \dots |j_1\rangle |j_0\rangle,$$

where

$$j = j_0 + 2j_1 + \ldots + 2^{\ell-1}j_{\ell-1},$$

induction:

$$|j\rangle = |[j/2]\rangle|j_0\rangle$$

イロン イヨン イヨン イヨン

QFT mod powers of 2 Phase estimation Period finding QFT over abelian groups

QFT mod  $2^{\ell}$ , part 2

 $\Phi_{2^{\ell}}|j\rangle = \sum_{k'=0}^{2^{\ell}-1} \omega^{k'j}|k'\rangle$ 

・ロト ・回ト ・ヨト ・ヨト

3

QFT mod powers of 2 Phase estimation Period finding QFT over abelian groups

QFT mod  $2^{\ell}$ , part 2

$$\Phi_{2^\ell}|j
angle = \sum_{k'=0}^{2^\ell-1} \omega^{k'j}|k'
angle$$

$$= \sum_{k=0}^{2^{\ell-1}-1} \omega^{2kj} |2k\rangle + \sum_{k=0}^{2^{\ell-1}-1} \omega^{(2k+1)j} |2k+1\rangle$$

・ロン ・回 と ・ヨン ・ヨン

QFT mod powers of 2 Phase estimation Period finding QFT over abelian groups

QFT mod  $2^{\ell}$ , part 2

$$\begin{split} \Phi_{2^{\ell}}|j\rangle &= \sum_{k'=0}^{2^{\ell}-1} \omega^{k'j} |k'\rangle \\ &= \sum_{k=0}^{2^{\ell-1}-1} \omega^{2kj} |2k\rangle + \sum_{k=0}^{2^{\ell-1}-1} \omega^{(2k+1)j} |2k+1\rangle \\ &= \sum_{k=0}^{2^{\ell-1}-1} \left( \omega^{2kj} |2k\rangle + \omega^{(2k+1)j} |2k+1\rangle \right) \end{split}$$

・ロン ・回 と ・ヨン ・ヨン

QFT mod powers of 2 Phase estimation Period finding QFT over abelian groups

QFT mod  $2^{\ell}$ , part 2

$$\begin{split} \Phi_{2^{\ell}}|j\rangle &= \sum_{k'=0}^{2^{\ell}-1} \omega^{k'j} |k'\rangle \\ &= \sum_{k=0}^{2^{\ell-1}-1} \omega^{2kj} |2k\rangle + \sum_{k=0}^{2^{\ell-1}-1} \omega^{(2k+1)j} |2k+1\rangle \\ &= \sum_{k=0}^{2^{\ell-1}-1} \left( \omega^{2kj} |2k\rangle + \omega^{(2k+1)j} |2k+1\rangle \right) \\ &= \sum_{k=0}^{2^{\ell-1}-1} \omega^{2kj} \left( |k\rangle |0\rangle + \omega^{j} |k\rangle |1\rangle \right) \end{split}$$

・ロト ・回 ト ・ヨト ・ヨト

QFT mod powers of 2 Phase estimation Period finding QFT over abelian groups

QFT mod  $2^{\ell}$ , part 2

$$\begin{split} \Phi_{2^{\ell}}|j\rangle &= \sum_{k'=0}^{2^{\ell}-1} \omega^{k'j} |k'\rangle \\ &= \sum_{k=0}^{2^{\ell-1}-1} \omega^{2kj} |2k\rangle + \sum_{k=0}^{2^{\ell-1}-1} \omega^{(2k+1)j} |2k+1\rangle \\ &= \sum_{k=0}^{2^{\ell-1}-1} \left( \omega^{2kj} |2k\rangle + \omega^{(2k+1)j} |2k+1\rangle \right) \\ &= \sum_{k=0}^{2^{\ell-1}-1} \omega^{2kj} \left( |k\rangle |0\rangle + \omega^{j} |k\rangle |1\rangle \right) \\ &= \left( \Phi_{2^{\ell-1}} |[j/2]\rangle \right) \otimes \left( |0\rangle + \omega^{j} |1\rangle \right) \end{split}$$

◆□ > ◆□ > ◆臣 > ◆臣 > ○

QFT mod powers of 2 Phase estimation Period finding QFT over abelian groups

### QFT mod $2^{\ell}$ - simple implementation

•  $\Phi_{2^{\ell}} = \Phi_{2^{\ell-1}}$  and cond. phase shift by  $\omega^j$ 

・ロン ・回と ・ヨン ・ヨン

# QFT mod $2^{\ell}$ - simple implementation

• 
$$\Phi_{2^{\ell}} = \Phi_{2^{\ell-1}}$$
 and cond. phase shift by  $\omega^j$   
for  $t = 0$  to  $\ell - 1$  if  $j_t = 1$  then cond phase shift by

$$\omega^{2^t} = e^{\frac{2\pi i}{2^{\ell-t}}} (t=0,\ldots,\ell-1)$$

・ロン ・回と ・ヨン・

### QFT mod $2^{\ell}$ - simple implementation

• 
$$\Phi_{2^{\ell}} = \Phi_{2^{\ell-1}}$$
 and cond. phase shift by  $\omega^j$   
for  $t = 0$  to  $\ell - 1$  if  $j_t = 1$  then cond phase shift by

$$\omega^{2^t} = e^{\frac{2\pi i}{2^{\ell-t}}} (t=0,\ldots,\ell-1)$$

#### • Procedure:

イロン 不同と 不同と 不同と

### QFT mod $2^{\ell}$ - simple implementation

• 
$$\Phi_{2^\ell} = \Phi_{2^{\ell-1}}$$
 and cond. phase shift by  $\omega^j$   
for  $t = 0$  to  $\ell - 1$  if  $j_t = 1$  then cond phase shift by

$$\omega^{2^t} = e^{\frac{2\pi i}{2^{\ell-t}}} (t=0,\ldots,\ell-1)$$

- Procedure:
  - $|j\rangle \left|0^{\ell-1}
    ight| |0\rangle$

・ロン ・回と ・ヨン・

### QFT mod $2^{\ell}$ - simple implementation

• 
$$\Phi_{2^\ell} = \Phi_{2^{\ell-1}}$$
 and cond. phase shift by  $\omega^j$   
for  $t = 0$  to  $\ell - 1$  if  $j_t = 1$  then cond phase shift by

$$\omega^{2^t} = e^{\frac{2\pi i}{2^{\ell-t}}} (t=0,\ldots,\ell-1)$$

- Procedure:
  - $|j\rangle |0^{\ell-1}\rangle |0\rangle$  $\downarrow$  QFT<sub>2</sub><sup> $\ell-1$ </sup> on  $|[j/2]\rangle$

・ロン ・回と ・ヨン ・ヨン

# QFT mod $2^{\ell}$ - simple implementation

• 
$$\Phi_{2^\ell} = \Phi_{2^{\ell-1}}$$
 and cond. phase shift by  $\omega^j$   
for  $t=0$  to  $\ell-1$  if  $j_t=1$  then cond phase shift by

$$\omega^{2^t} = e^{\frac{2\pi i}{2^{\ell-t}}} (t=0,\ldots,\ell-1)$$

• Procedure:

• 
$$|j\rangle |0^{\ell-1}\rangle |0\rangle$$
  
 $\downarrow$  QFT<sub>2</sub> <sup>$\ell-1$</sup>  on  $|[j/2]\rangle$   
•  $|j\rangle \otimes (\Phi_{2^{\ell-1}}|[j/2]\rangle) \otimes |0\rangle$ 

イロン 不同と 不同と 不同と

### QFT mod $2^{\ell}$ - simple implementation

• 
$$\Phi_{2^\ell} = \Phi_{2^{\ell-1}}$$
 and cond. phase shift by  $\omega^j$   
for  $t=0$  to  $\ell-1$  if  $j_t=1$  then cond phase shift by

$$\omega^{2^t} = e^{\frac{2\pi i}{2^{\ell-t}}} \ (t=0,\ldots,\ell-1)$$

Procedure:

• 
$$|j\rangle |0^{\ell-1}\rangle |0\rangle$$
  
 $\downarrow$   
•  $|j\rangle \otimes (\Phi_{2^{\ell-1}} |[j/2]\rangle) \otimes |0\rangle$   
 $\downarrow$ 

$$\mathsf{QFT}_2^{\ell-1} \text{ on } \ket{[j/2]}$$

・ロン ・回と ・ヨン・

æ

Hadamard

### QFT mod $2^{\ell}$ - simple implementation

• 
$$\Phi_{2^\ell}=\Phi_{2^{\ell-1}}$$
 and cond. phase shift by  $\omega^j$   
for  $t=0$  to  $\ell-1$  if  $j_t=1$  then cond phase shift by

$$\omega^{2^t} = e^{\frac{2\pi i}{2^{\ell-t}}} \ (t=0,\ldots,\ell-1)$$

Procedure:

• 
$$|j\rangle |0^{\ell-1}\rangle |0\rangle$$
  
 $\downarrow$  QFT<sub>2</sub> <sup>$\ell-1$</sup>  on  $|[j/2]\rangle$   
•  $|j\rangle \otimes (\Phi_{2^{\ell-1}} |[j/2]\rangle) \otimes |0\rangle$   
Hadamard

•  $|j\rangle \otimes (\Phi_{2^{\ell-1}}|[j/2]\rangle) \otimes (|0\rangle + |1\rangle)$ 

・ロト ・回ト ・ヨト ・ヨト

### QFT mod $2^{\ell}$ - simple implementation

• 
$$\Phi_{2^\ell} = \Phi_{2^{\ell-1}}$$
 and cond. phase shift by  $\omega^j$   
for  $t=0$  to  $\ell-1$  if  $j_t=1$  then cond phase shift by

$$\omega^{2^t} = e^{\frac{2\pi i}{2^{\ell-t}}} (t=0,\ldots,\ell-1)$$

Procedure:

• 
$$|j\rangle |0^{\ell-1}\rangle |0\rangle$$
  
 $\downarrow$  QFT<sub>2</sub> <sup>$\ell-1$</sup>  on  $|[j/2]\rangle$   
•  $|j\rangle \otimes (\Phi_{2^{\ell-1}}|[j/2]\rangle) \otimes |0\rangle$   
 $\downarrow$  Hadamard  
•  $|j\rangle \otimes (\Phi_{2^{\ell-1}}|[j/2]\rangle) \otimes (|0\rangle + |1\rangle)$   
 $\downarrow$  for( $t \in [0, l-1]$ )  
 $if(j_t \neq 0)$  then do cond. phase shift

イロン 不同と 不同と 不同と

## QFT mod $2^{\ell}$ - simple implementation

• 
$$\Phi_{2^\ell} = \Phi_{2^{\ell-1}}$$
 and cond. phase shift by  $\omega^j$   
for  $t=0$  to  $\ell-1$  if  $j_t=1$  then cond phase shift by

$$\omega^{2^t} = e^{\frac{2\pi i}{2^{\ell-t}}} (t = 0, \dots, \ell-1)$$

- Procedure:
  - $|j\rangle |0^{\ell-1}\rangle |0\rangle$   $\downarrow$  QFT<sub>2</sub><sup> $\ell-1$ </sup> on  $|[j/2]\rangle$ •  $|j\rangle \otimes (\Phi_{2^{\ell-1}}|[j/2]\rangle) \otimes |0\rangle$   $\downarrow$  Hadamard •  $|j\rangle \otimes (\Phi_{2^{\ell-1}}|[j/2]\rangle) \otimes (|0\rangle + |1\rangle)$   $\downarrow$  for $(t \in [0, l-1])$   $if(j_t \neq 0)$  then do cond. phase shift •  $|j\rangle \otimes \Phi_{2^{\ell}}(|j\rangle)$

・ロト ・回ト ・ヨト ・ヨト

2

QFT mod powers of 2 Phase estimation Period finding QFT over abelian groups

### QFT mod $2^{\ell}$ - simple implementation 2

### • So far: $P: |j\rangle \otimes |0\rangle \mapsto |j\rangle \otimes \Phi(|j\rangle)$

イロト イヨト イヨト イヨト

QFT mod powers of 2 Phase estimation Period finding QFT over abelian groups

## QFT mod $2^{\ell}$ - simple implementation 2

- So far:  $P: |j\rangle \otimes |0\rangle \mapsto |j\rangle \otimes \Phi(|j\rangle)$
- $\omega \leftrightarrow \overline{\omega}$ :  $\overline{P} : |j\rangle \otimes |0\rangle \mapsto |j\rangle \otimes \Phi^{-1}(|j\rangle)$

イロト イヨト イヨト イヨト

QFT mod powers of 2 Phase estimation Period finding QFT over abelian groups

# QFT mod $2^{\ell}$ - simple implementation 2

- So far:  $P: |j\rangle \otimes |0\rangle \mapsto |j\rangle \otimes \Phi(|j\rangle)$
- $\omega \leftrightarrow \overline{\omega}$ :  $\overline{P} : |j\rangle \otimes |0\rangle \mapsto |j\rangle \otimes \Phi^{-1}(|j\rangle)$
- Simple implementation of  $|j\rangle \mapsto \otimes \Phi(j)$  (using aux qbits):

QFT mod powers of 2 Phase estimation Period finding QFT over abelian groups

# QFT mod $2^{\ell}$ - simple implementation 2

- So far:  $P:|j\rangle\otimes |0\rangle\mapsto |j\rangle\otimes \Phi(|j\rangle)$
- $\omega \leftrightarrow \overline{\omega}$ :  $\overline{P} : |j\rangle \otimes |0\rangle \mapsto |j\rangle \otimes \Phi^{-1}(|j\rangle)$
- Simple implementation of  $|j\rangle \mapsto \otimes \Phi(j)$  (using aux qbits):

• 
$$|j
angle\otimes|0
angle$$

QFT mod powers of 2 Phase estimation Period finding QFT over abelian groups

# QFT mod $2^{\ell}$ - simple implementation 2

- So far:  $P:|j\rangle\otimes |0\rangle\mapsto |j\rangle\otimes \Phi(|j\rangle)$
- $\omega \leftrightarrow \overline{\omega}$ :  $\overline{P} : |j\rangle \otimes |0\rangle \mapsto |j\rangle \otimes \Phi^{-1}(|j\rangle)$
- Simple implementation of  $|j\rangle \mapsto \otimes \Phi(j)$  (using aux qbits):

• 
$$|j\rangle\otimes|0
angle$$
  
 $\downarrow$  P

・ロン ・回と ・ヨン ・ヨン

QFT mod powers of 2 Phase estimation Period finding QFT over abelian groups

# QFT mod $2^{\ell}$ - simple implementation 2

- So far:  $P: |j\rangle \otimes |0\rangle \mapsto |j\rangle \otimes \Phi(|j\rangle)$
- $\omega \leftrightarrow \overline{\omega}$ :  $\overline{P} : |j\rangle \otimes |0\rangle \mapsto |j\rangle \otimes \Phi^{-1}(|j\rangle)$
- Simple implementation of  $|j\rangle \mapsto \otimes \Phi(j)$  (using aux qbits):

• 
$$|j\rangle \otimes |0\rangle$$
  
 $\downarrow$   $P$   
•  $|j\rangle \otimes \Phi(|j\rangle)$ 

QFT mod powers of 2 Phase estimation Period finding QFT over abelian groups

# QFT mod $2^{\ell}$ - simple implementation 2

- So far:  $P: |j\rangle \otimes |0\rangle \mapsto |j\rangle \otimes \Phi(|j\rangle)$
- $\omega \leftrightarrow \overline{\omega}$ :  $\overline{P} : |j\rangle \otimes |0\rangle \mapsto |j\rangle \otimes \Phi^{-1}(|j\rangle)$
- Simple implementation of  $|j\rangle \mapsto \otimes \Phi(j)$  (using aux qbits):

• 
$$|j\rangle \otimes |0\rangle$$
  
 $\downarrow$   $P$   
•  $|j\rangle \otimes \Phi(|j\rangle)$   
 $\downarrow$  swap

QFT mod powers of 2 Phase estimation Period finding QFT over abelian groups

# QFT mod $2^{\ell}$ - simple implementation 2

- So far:  $P: |j\rangle \otimes |0\rangle \mapsto |j\rangle \otimes \Phi(|j\rangle)$
- $\omega \leftrightarrow \overline{\omega}$ :  $\overline{P} : |j\rangle \otimes |0\rangle \mapsto |j\rangle \otimes \Phi^{-1}(|j\rangle)$
- Simple implementation of  $|j\rangle \mapsto \otimes \Phi(j)$  (using aux qbits):

• 
$$|j\rangle \otimes |0\rangle$$
  
 $\downarrow$   $P$   
•  $|j\rangle \otimes \Phi(|j\rangle)$   
 $\downarrow$  swap  
•  $\Phi(|j\rangle) \otimes |j\rangle$ 

QFT mod powers of 2 Phase estimation Period finding QFT over abelian groups

# QFT mod $2^{\ell}$ - simple implementation 2

- So far:  $P: |j\rangle \otimes |0\rangle \mapsto |j\rangle \otimes \Phi(|j\rangle)$
- $\omega \leftrightarrow \overline{\omega}$ :  $\overline{P} : |j\rangle \otimes |0\rangle \mapsto |j\rangle \otimes \Phi^{-1}(|j\rangle)$
- Simple implementation of  $|j\rangle \mapsto \otimes \Phi(j)$  (using aux qbits):

• 
$$|j\rangle \otimes |0\rangle$$
  
 $\downarrow$   $P$   
•  $|j\rangle \otimes \Phi(|j\rangle)$   
 $\downarrow$  swap  
•  $\Phi(|j\rangle) \otimes |j\rangle$   
 $\downarrow$   $\overline{P}^{-1}$ 

QFT mod powers of 2 Phase estimation Period finding QFT over abelian groups

# QFT mod $2^{\ell}$ - simple implementation 2

- So far:  $P: |j\rangle \otimes |0\rangle \mapsto |j\rangle \otimes \Phi(|j\rangle)$
- $\omega \leftrightarrow \overline{\omega}$ :  $\overline{P} : |j\rangle \otimes |0\rangle \mapsto |j\rangle \otimes \Phi^{-1}(|j\rangle)$
- Simple implementation of  $|j\rangle \mapsto \otimes \Phi(j)$  (using aux qbits):
  - $|j\rangle \otimes |0\rangle$   $\downarrow$  P•  $|j\rangle \otimes \Phi(|j\rangle)$   $\downarrow$  swap •  $\Phi(|j\rangle) \otimes |j\rangle$   $\downarrow$   $\overline{P}^{-1}$ •  $\Phi(|j\rangle) \otimes |0\rangle$

イロト イヨト イヨト イヨト

3

QFT mod powers of 2 Phase estimation Period finding QFT over abelian groups

QFT over  $2^{\ell}$  - remark

#### Remark: QFT in the literature

・ロン ・回と ・ヨン ・ヨン

QFT mod powers of 2 Phase estimation Period finding QFT over abelian groups

QFT over  $2^{\ell}$  - remark

### Remark: QFT in the literature -reorganized in a clever way

・ロン ・回と ・ヨン・

QFT mod powers of 2 Phase estimation Period finding QFT over abelian groups

QFT over  $2^{\ell}$  - remark

### Remark: QFT in the literature -reorganized in a clever way -more "efficient"

・ロン ・回と ・ヨン ・ヨン

QFT mod powers of 2 Phase estimation Period finding QFT over abelian groups

QFT over  $2^{\ell}$  - remark

Remark: QFT in the literature -reorganized in a clever way -more "efficient" -has nice circuit description

・ロン ・回と ・ヨン・

QFT mod powers of 2 Phase estimation Period finding QFT over abelian groups

QFT over  $2^{\ell}$  - remark

Remark: QFT in the literature -reorganized in a clever way -more "efficient" -has nice circuit description -computes  $|j\rangle \mapsto \Phi(|j\rangle)$  without auxiliary qbits

・ロン ・回と ・ヨン ・ヨン

2

QFT mod powers of 2 Phase estimation Period finding QFT over abelian groups

QFT over  $2^{\ell}$  - remark

Remark: QFT in the literature -reorganized in a clever way -more "efficient" -has nice circuit description -computes  $|j\rangle \mapsto \Phi(|j\rangle)$  without auxiliary qbits Details in *Cleve, Ekert, Macchiavello, Mosca (1998)* 

・ロン ・回 と ・ ヨ と ・ ヨ と

2

QFT mod powers of 2 Phase estimation Period finding QFT over abelian groups

### Phase estimation (eigenvalue estimation)

• Given:

・ロン ・回と ・ヨン ・ヨン

Phase estimation (eigenvalue estimation)

• Given:

state (vector)  $\psi$ , an *eigenvector* 

イロト イヨト イヨト イヨト

Simon's algorithm Basic tools The HSP Infinite abelian HSPs QFT mod powers of 2 Phase estimation Period finding QFT over abelian groups

# Phase estimation (eigenvalue estimation)

• Given:

state (vector)  $\psi$ , an eigenvector of the unitary U

イロト イヨト イヨト イヨト

Simon's algorithm Basic tools The HSP Infinite abelian HSPs QFT mod powers of 2 Phase estimation Period finding QFT over abelian groups

# Phase estimation (eigenvalue estimation)

• Given:

state (vector)  $\psi$ , an *eigenvector* of the unitary Uoracles for  $U, U^2, U^4, \ldots$ 

・ロン ・回と ・ヨン・

Simon's algorithm Basic tools The HSP Infinite abelian HSPs QFT mod powers of 2 Phase estimation Period finding QFT over abelian groups

# Phase estimation (eigenvalue estimation)

• Given:

state (vector)  $\psi$ , an *eigenvector* of the unitary Uoracles for  $U, U^2, U^4, ...$ 

• Task: approximate (phase of) the eigenvalue

イロト イヨト イヨト イヨト

# Phase estimation (eigenvalue estimation)

• Given:

state (vector)  $\psi$ , an *eigenvector* of the unitary Uoracles for  $U, U^2, U^4, ...$ 

• Task: approximate (*phase* of) the eigenvalue  $U\psi = e^{\alpha \cdot 2\pi i}\psi$ 

イロト イヨト イヨト イヨト

# Phase estimation (eigenvalue estimation)

• Given:

state (vector)  $\psi$ , an *eigenvector* of the unitary Uoracles for  $U, U^2, U^4, \dots$ 

• Task: approximate (*phase* of) the eigenvalue

$$U\psi = e^{\alpha \cdot 2\pi i}\psi$$

compute the  $\ell$  most significant bits of *phase*  $\alpha$ .

イロト イポト イヨト イヨト

# Phase estimation (eigenvalue estimation)

• Given:

state (vector)  $\psi$ , an *eigenvector* of the unitary Uoracles for  $U, U^2, U^4, \ldots$ 

• Task: approximate (*phase* of) the eigenvalue  $U\psi = e^{\alpha \cdot 2\pi i}\psi$ 

compute the  $\ell$  most significant bits of *phase*  $\alpha$ .

• Operation for task:

イロト イポト イヨト イヨト

# Phase estimation (eigenvalue estimation)

• Given:

state (vector)  $\psi$ , an *eigenvector* of the unitary Uoracles for  $U, U^2, U^4, \dots$ 

• Task: approximate (*phase* of) the eigenvalue

 $U\psi = e^{\alpha \cdot 2\pi i}\psi$ 

compute the  $\ell$  most significant bits of phase  $\alpha.$ 

• Operation for task:

 $\psi\otimes\left|\mathbf{0}^{\ell}
ight
angle\mapsto\psi\otimes\left|\mathbf{k}
ight
angle$ ,

イロト イヨト イヨト イヨト

# Phase estimation (eigenvalue estimation)

• Given:

state (vector)  $\psi$ , an *eigenvector* of the unitary Uoracles for  $U, U^2, U^4, \dots$ 

• Task: approximate (*phase* of) the eigenvalue  $U\psi = e^{\alpha \cdot 2\pi i}\psi$ 

compute the  $\ell$  most significant bits of *phase*  $\alpha$ .

• Operation for task:

$$\psi\otimes\left|\mathsf{0}^{\ell}
ight
angle\mapsto\psi\otimes\left|k
ight
angle$$
,

where

$$\left|\alpha - \frac{k}{2^{\ell}}\right| \le \frac{1}{2^{\ell+1}}.$$

・ロン ・回と ・ヨン・

Simon's algorithm Basic tools The HSP Infinite abelian HSPs

QFT mod powers of 2 Phase estimation Period finding QFT over abelian groups

# Phase estimation - algorithm idea

• Assume 
$$\alpha = \frac{k}{2^{\ell}}$$

・ロト ・回ト ・ヨト ・ヨト

### Phase estimation - algorithm idea

- Assume  $\alpha = \frac{k}{2^{\ell}}$
- Then

$$\sum_{j=0}^{\ell-1} U^j \psi \otimes |j
angle = \psi \otimes \sum_{j=0}^{\ell-1} e^{lpha \cdot 2\pi i j} |j
angle$$

・ロン ・雪 ・ ・ ヨ ・ ・ ヨ ・ ・

#### Phase estimation - algorithm idea

- Assume  $\alpha = \frac{k}{2^{\ell}}$
- Then

$$\sum_{j=0}^{\ell-1} U^j \psi \otimes |j
angle = \psi \otimes \sum_{j=0}^{\ell-1} e^{lpha \cdot 2\pi i j} |j
angle$$
 $= \psi \otimes \sum_{j=0}^{\ell-1} e^{rac{2\pi i}{\ell} \cdot k j} |j
angle$ 

・ロン ・雪 ・ ・ ヨ ・ ・ ヨ ・ ・

### Phase estimation - algorithm idea

- Assume  $\alpha = \frac{k}{2^{\ell}}$
- Then

$$\sum_{j=0}^{\ell-1} U^j \psi \otimes |j
angle = \psi \otimes \sum_{j=0}^{\ell-1} e^{lpha \cdot 2\pi i j} |j
angle 
onumber \ = \psi \otimes \sum_{j=0}^{\ell-1} e^{rac{2\pi i}{\ell} \cdot k j} |j
angle 
onumber \ = \psi \otimes \Phi_{2^\ell}(|k
angle)$$

・ロン ・雪 ・ ・ ヨ ・ ・ ヨ ・ ・

### Phase estimation - algorithm idea

- Assume  $\alpha = \frac{k}{2^{\ell}}$
- Then

$$\sum_{j=0}^{\ell-1} U^j \psi \otimes \ket{j} = \psi \otimes \sum_{j=0}^{\ell-1} e^{lpha \cdot 2\pi i j} \ket{j}$$
 $= \psi \otimes \sum_{j=0}^{\ell-1} e^{rac{2\pi i}{\ell} \cdot k j} \ket{j}$  $= \psi \otimes \Phi_{2^\ell}(\ket{k})$ 

• Apply  $\Phi_{2^{\ell}}^{-1}$ , obtain

・ロン ・回と ・ヨン ・ヨン

### Phase estimation - algorithm idea

- Assume  $\alpha = \frac{k}{2^{\ell}}$
- Then

$$\sum_{j=0}^{\ell-1} U^j \psi \otimes |j
angle = \psi \otimes \sum_{j=0}^{\ell-1} e^{lpha \cdot 2\pi i j} |j
angle$$
 $= \psi \otimes \sum_{j=0}^{\ell-1} e^{rac{2\pi i}{\ell} \cdot k j} |j
angle$  $= \psi \otimes \Phi_{2^\ell}(|k
angle)$ 

• Apply  $\Phi_{2^{\ell}}^{-1}$ , obtain

 $\psi \otimes | {m k} 
angle$ 

・ロト ・回ト ・ヨト ・ヨト

Simon's algorithm Basic tools The HSP Infinite abelian HSPs

QFT mod powers of 2 Phase estimation Period finding QFT over abelian groups

## Phase estimation - the algorithm

 $r = O(\log \frac{1}{\epsilon}))$ 

・ロン ・回と ・ヨン ・ヨン

Э

Simon's algorithm Basic tools The HSP Infinite abelian HSPs QFT over

QFT mod powers of 2 Phase estimation Period finding QFT over abelian groups

## Phase estimation - the algorithm

$$egin{aligned} r &= O(\log rac{1}{\epsilon})) \ ext{Init: } \psi \otimes |0
angle &\mapsto \psi \otimes \sum_{j=0}^{\ell+r-1} |j
angle \end{aligned}$$

・ロト ・回ト ・ヨト ・ヨト

Simon's algorithm QFT mod powers of 2 Basic tools Phase estimation The HSP Infinite abelian HSPs

QFT over abelian groups

## Phase estimation - the algorithm

$$egin{aligned} r &= O(\log rac{1}{\epsilon})) \ ext{Init: } \psi \otimes |0
angle &\mapsto \psi \otimes \sum_{j=0}^{\ell+r-1} |j
angle \ ext{for } (d &= 0, d < \ell+r, d := d+1): \end{aligned}$$

・ロト ・回ト ・ヨト ・ヨト

## Phase estimation - the algorithm

$$\begin{split} r &= O(\log \frac{1}{\epsilon}))\\ \text{Init: } \psi \otimes |0\rangle &\mapsto \psi \otimes \sum_{j=0}^{\ell+r-1} |j\rangle\\ \text{for } (d &= 0, d < \ell + r, d := d + 1):\\ &\text{if } (j_d &= 1): \end{split}$$

・ロト ・回ト ・ヨト ・ヨト

## Phase estimation - the algorithm

$$\begin{split} r &= O(\log \frac{1}{\epsilon}))\\ \text{Init: } \psi \otimes |0\rangle \mapsto \psi \otimes \sum_{j=0}^{\ell+r-1} |j\rangle\\ \text{for } (d = 0, d < \ell + r, d := d + 1):\\ \text{if } (j_d = 1):\\ \text{apply } U^{2^{d-1}} \text{ to } \psi \end{split}$$

・ロト ・回ト ・ヨト ・ヨト

## Phase estimation - the algorithm

$$\begin{split} r &= O(\log \frac{1}{\epsilon}))\\ \text{Init: } \psi \otimes |0\rangle &\mapsto \psi \otimes \sum_{j=0}^{\ell+r-1} |j\rangle\\ \text{for } (d &= 0, d < \ell + r, d := d + 1):\\ &\text{ if } (j_d &= 1):\\ &\text{ apply } U^{2^{d-1}} \text{ to } \psi\\ \text{Last step: apply } \Phi_{2^{\ell+r}}^{-1} \text{ to the second part} \end{split}$$

イロン 不同と 不同と 不同と

## Phase estimation - the algorithm

$$\begin{split} r &= O(\log \frac{1}{\epsilon}))\\ \text{Init: } \psi \otimes |0\rangle \mapsto \psi \otimes \sum_{j=0}^{\ell+r-1} |j\rangle\\ \text{for } (d &= 0, d < \ell + r, d := d + 1):\\ \text{if } (j_d &= 1):\\ \text{apply } U^{2^{d-1}} \text{ to } \psi\\ \text{Last step: apply } \Phi_{2^{\ell+r}}^{-1} \text{ to the second part}\\ \text{Return the first } \ell \text{ bits} \end{split}$$

・ロン ・回と ・ヨン・

## Phase estimation - the algorithm

$$\begin{aligned} r &= O(\log \frac{1}{\epsilon}))\\ \text{Init: } \psi \otimes |0\rangle &\mapsto \psi \otimes \sum_{j=0}^{\ell+r-1} |j\rangle\\ \text{for } (d = 0, d < \ell + r, d := d + 1):\\ \text{if } (j_d = 1):\\ \text{apply } U^{2^{d-1}} \text{ to } \psi\\ \text{Last step: apply } \Phi_{2^{\ell+r}}^{-1} \text{ to the second part}\\ \text{Return the first } \ell \text{ bits} \end{aligned}$$
State before  $\Phi^{-1}$ :

$$\mathsf{State} = \sum_{j=0}^{\ell+r-1} U^j \psi \otimes |j\rangle = \psi \otimes \sum_{j=0}^{\ell+r-1} e^{\alpha \cdot 2\pi i j} |j\rangle$$

・ロン ・回と ・ヨン・

### Phase estimation - the algorithm

$$\begin{split} r &= O(\log \frac{1}{\epsilon}))\\ \text{Init: } \psi \otimes |0\rangle \mapsto \psi \otimes \sum_{j=0}^{\ell+r-1} |j\rangle\\ \text{for } (d &= 0, d < \ell + r, d := d + 1):\\ \text{ if } (j_d &= 1):\\ \text{ apply } U^{2^{d-1}} \text{ to } \psi\\ \text{Last step: apply } \Phi_{2^{\ell+r}}^{-1} \text{ to the second part}\\ \text{Return the first } \ell \text{ bits} \end{split}$$

$$\mathsf{State} = \sum_{j=0}^{\ell+r-1} U^j \psi \otimes |j\rangle = \psi \otimes \sum_{j=0}^{\ell+r-1} e^{\alpha \cdot 2\pi i j} |j
angle$$

If  $\alpha = \frac{k}{2^{\ell+r}}$ : State =  $\psi \otimes \Phi(|k\rangle)$ 

・ロト ・回ト ・ヨト ・ヨト

### Phase estimation - algorithm analysis

• Before inverse QFT (if  $\alpha = \frac{k}{2^{\ell+r}}$ )

 $\mathsf{State} = \psi \otimes \Phi(|k\rangle)$ 

・ロン ・回と ・ヨン ・ヨン

### Phase estimation - algorithm analysis

• Before inverse QFT (if  $\alpha = \frac{k}{2^{\ell+r}}$ )

 $\mathsf{State} = \psi \otimes \Phi(|k\rangle)$ 

• After inverse QFT

・ロン ・回と ・ヨン・

### Phase estimation - algorithm analysis

• Before inverse QFT (if  $\alpha = \frac{k}{2^{\ell+r}}$ )

 $\mathsf{State} = \psi \otimes \Phi(|k\rangle)$ 

After inverse QFT

if 
$$\alpha = \frac{k}{2^{\ell+r}}$$
:

 $\mathsf{State} = \psi \otimes | \textit{\textbf{k}} \rangle$ 

・ロン ・回と ・ヨン ・ヨン

### Phase estimation - algorithm analysis

• Before inverse QFT (if  $\alpha = \frac{k}{2^{\ell+r}}$ )

 $\mathsf{State} = \psi \otimes \Phi(|k\rangle)$ 

After inverse QFT

if 
$$\alpha = \frac{k}{2^{\ell+r}}$$
:

 $\mathsf{State} = \psi \otimes |\mathbf{k}\rangle$ 

if 
$$\alpha \approx \frac{k}{2^{\ell+r}}$$
:

State 
$$\approx \psi \sum_{|k'-k| < 2^r} c_{k'} |k'\rangle.$$

・ロン ・回と ・ヨン ・ヨン

### Phase estimation - algorithm analysis

• Before inverse QFT (if  $\alpha = \frac{k}{2^{\ell+r}}$ )

 $\mathsf{State} = \psi \otimes \Phi(|k\rangle)$ 

After inverse QFT

if 
$$\alpha = \frac{k}{2^{\ell+r}}$$
:

 $\mathsf{State} = \psi \otimes |k\rangle$ 

if 
$$\alpha \approx \frac{k}{2^{\ell+r}}$$
:

State 
$$\approx \psi \sum_{|\mathbf{k}'-\mathbf{k}| < 2^r} c_{\mathbf{k}'} |\mathbf{k}' \rangle.$$

• Details: In: e.g., Cleve, Ekert, Macchiavello, Mosca (1998).

・ロト ・回ト ・ヨト ・ヨト

# Period finding

• Given:  $f : \mathbb{Z} \to {\text{strings}}$ 

・ロン ・回 と ・ヨン ・ヨン

# Period finding

• Given:  $f : \mathbb{Z} \to \{\text{strings}\}$ by oracle  $U_f : |x\rangle|0\rangle \mapsto |x\rangle|f(x)\rangle$ 

・ロン ・回と ・ヨン ・ヨン

# Period finding

• Given:  $f : \mathbb{Z} \to \{\text{strings}\}$ by oracle  $U_f : |x\rangle|0\rangle \mapsto |x\rangle|f(x)\rangle$ 

spec. case:  $x \mapsto f(x)$  by classical algorithm

・ロン ・回と ・ヨン ・ヨン

# Period finding

• Given:  $f : \mathbb{Z} \to \{\text{strings}\}$ by oracle  $U_f : |x\rangle|0\rangle \mapsto |x\rangle|f(x)\rangle$ 

spec. case:  $x \mapsto f(x)$  by classical algorithm

• Promise: 
$$f(x) = f(y) \Leftrightarrow x \equiv y \pmod{r}$$

・ロン ・回と ・ヨン ・ヨン

# Period finding

• Given:  $f : \mathbb{Z} \to \{\text{strings}\}$ by oracle  $U_f : |x\rangle|0\rangle \mapsto |x\rangle|f(x)\rangle$ 

spec. case:  $x \mapsto f(x)$  by classical algorithm

- Promise:  $f(x) = f(y) \Leftrightarrow x \equiv y \pmod{r}$
- Task: find r

・ロン ・回と ・ヨン・

Simon's algorithm QFT mod powers of 2 Basic tools Phase estimation The HSP Period finding QFT mod powers of 2 Phase estimation Period finding

# Period finding

• Given:  $f : \mathbb{Z} \to \{\text{strings}\}$ 

by oracle  $U_f:|x
angle|0
angle\mapsto|x
angle|f(x)
angle$ 

spec. case:  $x \mapsto f(x)$  by classical algorithm

- Promise:  $f(x) = f(y) \Leftrightarrow x \equiv y \pmod{r}$
- Task: find r
- Gadget: quantum graph (diagram) of f:

$$|f_N\rangle = \sum_{x=0}^{N-1} |x\rangle |f(x)\rangle$$

・ロン ・回と ・ヨン ・ヨン

# Period finding 2

Computing  $|f_N\rangle$  for  $N = 2^{\ell}$ :

・ロン ・回と ・ヨン ・ヨン

ъ

# Period finding 2

Computing  $|f_N\rangle$  for  $N = 2^{\ell}$ : •  $|0\rangle|0\rangle$ 

・ロト ・回ト ・ヨト ・ヨト

# Period finding 2

# Computing $|f_N\rangle$ for $N = 2^{\ell}$ : • $|0\rangle|0\rangle$

 $\downarrow$  Hadamard<sup> $\otimes \ell$ </sup>

Gábor Ivanyos MTA SZTAKI Fast Quantum Algorithms Lectures 1 and 2

・ロン ・回 と ・ ヨ と ・ ヨ と

# Period finding 2

Computing  $|f_N\rangle$  for  $N=2^\ell$ : •  $|0\rangle|0\rangle$ 

 $\downarrow$  Hadamard<sup> $\otimes \ell$ </sup>

• 
$$\sum_{x=0}^{N-1} |x\rangle |0\rangle$$

・ロン ・回 と ・ ヨ と ・ ヨ と

# Period finding 2

Computing 
$$|f_N\rangle$$
 for  $N=2^\ell$ :  
•  $|0\rangle|0\rangle$ 

 $\downarrow$  Hadamard $^{\otimes \ell}$ 

• 
$$\sum_{x=0}^{N-1} |x\rangle |0\rangle$$

 $\downarrow U_f$ 

・ロト ・回ト ・ヨト ・ヨト

# Period finding 2

Computing 
$$|f_N\rangle$$
 for  $N=2^\ell$ :  
•  $|0\rangle|0\rangle$ 

 $\downarrow$  Hadamard $^{\otimes \ell}$ 

• 
$$\sum_{x=0}^{N-1} |x\rangle |0\rangle$$

$$\downarrow U_f$$

• 
$$\sum_{x=0}^{N-1} |x\rangle |f(x)\rangle = |f_N\rangle$$

・ロン ・回 と ・ヨン ・ヨン

#### Period finding 3

Decomposition of  $|f_N\rangle$ :

$$|f_N\rangle = \sum_{x=0}^{N-1} |x\rangle |f(x)\rangle \approx \sum_{y=0}^{r-1} \left(\sum_{z=0}^{\left\lfloor \frac{N}{r} 
ight
ceil -1} |rz+y
ight) |f(y)
angle$$

・ロト ・回ト ・ヨト ・ヨト

#### Period finding 3

Decomposition of  $|f_N\rangle$ :

$$|f_N\rangle = \sum_{x=0}^{N-1} |x\rangle|f(x)\rangle \approx \sum_{y=0}^{r-1} \left(\sum_{z=0}^{\left\lfloor\frac{N}{r}\right\rfloor-1} |rz+y\rangle\right) |f(y)\rangle$$

• Measure f(y) (i.e., take term for fixed y):

$$\sum_{z=0}^{\left[\frac{N}{r}\right]-1} |rz+y\rangle$$

・ロン ・回 と ・ヨン ・ヨン

## Period finding 3

Decomposition of  $|f_N\rangle$ :

$$|f_N\rangle = \sum_{x=0}^{N-1} |x\rangle|f(x)\rangle \approx \sum_{y=0}^{r-1} \left(\sum_{z=0}^{\left\lfloor\frac{N}{r}\right\rfloor-1} |rz+y\rangle\right) |f(y)\rangle$$

• Measure f(y) (i.e., take term for fixed y):

$$\sum_{z=0}^{\left[\frac{N}{r}\right]-1} |rz+y\rangle$$

• Decompose into eigenvectors of shift mod  $r[\frac{N}{r}]$  (QFT "in mind"):

$$\sum_{j=0}^{r[\frac{N}{r}]-1} c_{yj}u_j, \quad \text{where } u_j = \sum_{k=0}^{r[\frac{N}{r}]-1} \omega^{-kj} |k\rangle.$$

・ロト ・回ト ・ヨト ・ヨト

Simon's algorithm Basic tools The HSP Infinite abelian HSPs QFT mod powers of 2 Phase estimation Period finding QFT over abelian groups

## Period finding 4

Up to normalization:

・ロン ・回と ・ヨン・

### Period finding 4

Up to normalization:

$$c_{yj} = \sum_{z=0}^{\left[rac{N}{r}
ight]-1} \omega^{j(rz+y)} = \omega^{jy} \sum_{z=0}^{\left[rac{N}{r}
ight]-1} \omega^{jrz} =$$

・ロン ・回と ・ヨン・

## Period finding 4

Up to normalization:

$$c_{yj} = \sum_{z=0}^{\left[\frac{N}{r}\right]-1} \omega^{j(rz+y)} = \omega^{jy} \sum_{z=0}^{\left[\frac{N}{r}\right]-1} \omega^{jrz} = \omega^{jy} \left\{ \begin{array}{c} \left[\frac{N}{r}\right] & \text{if } j \equiv 0 \\ 0 & \text{otherwise} \end{array} \right. \pmod{\left[\frac{N}{r}\right]}$$

where  $\omega = \frac{r[N/r]}{\sqrt{1}}$ .

・ロト ・回ト ・ヨト ・ヨト

Э

## Period finding 5

Have state

$$\sum_{j=0}^{r[\frac{N}{r}]-1} c_{yj} u_j$$

Gábor Ivanyos MTA SZTAKI Fast Quantum Algorithms Lectures 1 and 2

・ロン ・雪 ・ ・ ヨ ・ ・ ヨ ・ ・

## Period finding 5

Have state

$$\sum_{j=0}^{r[\frac{N}{r}]-1} c_{yj} u_j$$

• 
$$c_{yj} = 0$$
 if j is not a multiple of  $\left[\frac{N}{r}\right]$ ,

・ロン ・雪 ・ ・ ヨ ・ ・ ヨ ・ ・

## Period finding 5

Have state

$$\sum_{j=0}^{r[\frac{N}{r}]-1} c_{yj} u_j$$

・ロン ・雪 ・ ・ ヨ ・ ・ ヨ ・ ・

## Period finding 5

Have state

$$\sum_{j=0}^{r[\frac{N}{r}]-1} c_{yj} u_j$$

$$\sum_{\ell=0}^{r-1} c_{y\ell[N/r]} u_{[\ell[N/r]]}$$

・ロン ・回と ・ヨン・

## Period finding 5

Have state

$$\sum_{j=0}^{r[\frac{N}{r}]-1} c_{yj} u_j$$

• 
$$c_{yj} = 0$$
 if  $j$  is not a multiple of  $[\frac{N}{r}]$ ,  
•  $|c_{yj}|$  the same for  $j = \ell[\frac{N}{r}]$ ,  $\ell = 0, \dots, r-1$ .

State:

$$\sum_{\ell=0}^{r-1} c_{y\ell[N/r]} u_{[\ell[N/r]]}$$

• comb. of eigenvectors of shift with

イロン イヨン イヨン イヨン

# Period finding 5

Have state

$$\sum_{j=0}^{r[\frac{N}{r}]-1} c_{yj} u_j$$

• 
$$c_{yj} = 0$$
 if  $j$  is not a multiple of  $[\frac{N}{r}]$ ,  
•  $|c_{yj}|$  the same for  $j = \ell[\frac{N}{r}]$ ,  $\ell = 0, \dots, r-1$ .

State:

$$\sum_{\ell=0}^{r-1} c_{y\ell[N/r]} u_{[\ell[N/r]]}$$

• comb. of eigenvectors of shift with eigenvalues

$$\omega^{\ell[N/r]} = (\sqrt[r[N/r]]{1})^{\ell[N/r]} = (\sqrt[r]{1})^{\ell}$$

Simon's algorithm Basic tools The HSP Infinite abelian HSPs QFT mod powers of 2 Phase estimation Period finding QFT rover abelian groups

#### Period finding 6

Have state

 $\sum_{\ell=0}^{r-1} c_{y\ell[N/r]} u_{[\ell[N/r]]}$ 

・ロン ・回と ・ヨン ・ヨン

## Period finding 6

Have state

$$\sum_{\ell=0}^{r-1} c_{y\ell[N/r]} u_{[\ell[N/r]]}$$

• apply phase estimation

・ロン ・回と ・ヨン・

## Period finding 6

Have state

$$\sum_{\ell=0}^{r-1} c_{y\ell[N/r]} u_{[\ell[N/r]]}$$

• apply phase estimation

$$\sum_{\ell=0}^{r-1} c_{y\ell[N/r]} u_{[\ell[N/r]]} |\ell/r\rangle$$

・ロン ・回と ・ヨン・

## Period finding 6

Have state

$$\sum_{\ell=0}^{r-1} c_{y\ell[N/r]} u_{[\ell[N/r]]}$$

• apply phase estimation

$$\sum_{\ell=0}^{r-1} c_{y\ell[N/r]} u_{[\ell[N/r]]} |\ell/r\rangle$$

• continued fraction approx. gives r

イロン 不同と 不同と 不同と

## Period finding 6

Have state

$$\sum_{\ell=0}^{r-1} c_{y\ell[N/r]} u_{[\ell[N/r]]}$$

• apply phase estimation

$$\sum_{\ell=0}^{r-1} c_{y\ell[N/r]} u_{[\ell[N/r]]} |\ell/r\rangle$$

• continued fraction approx. gives rif  $gcd(\ell, r) = 1$ .

・ロン ・回と ・ヨン・

## Period finding 6

Have state

$$\sum_{\ell=0}^{r-1} c_{y\ell[N/r]} u_{[\ell[N/r]]}$$

apply phase estimation

$$\sum_{\ell=0}^{r-1} c_{y\ell[N/r]} u_{[\ell[N/r]]} |\ell/r\rangle$$

• continued fraction approx. gives rif  $gcd(\ell, r) = 1$ .

• Details: In: Cleve, Ekert, Macchiavello, Mosca (1998).

イロン イヨン イヨン イヨン

## Period finding 6

Have state

$$\sum_{\ell=0}^{r-1} c_{y\ell[N/r]} u_{[\ell[N/r]]}$$

apply phase estimation

$$\sum_{\ell=0}^{r-1} c_{y\ell[N/r]} u_{[\ell[N/r]]} |\ell/r\rangle$$

- continued fraction approx. gives rif  $gcd(\ell, r) = 1$ .
- Details: In: Cleve, Ekert, Macchiavello, Mosca (1998).
- Original: Shor 1994

イロン イヨン イヨン イヨン

## QFT modulo m



Gábor Ivanyos MTA SZTAKI Fast Quantum Algorithms Lectures 1 and 2

< □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □

Simon's algorithm Basic tools The HSP Infinite abelian HSPs QFT over abelian groups

## QFT modulo m

•  $|j\rangle|0
angle$ 

 $\approx$  Hadamard<sup> $\otimes \log_m + \dots$ </sup>

# QFT modulo m

•  $|j\rangle|0\rangle$   $\downarrow$ •  $|j\rangle\sum_{k=0}^{m-1}|k\rangle$ 

 $\approx \mathsf{Hadamard}^{\otimes \mathsf{log}_m} + \dots$ 

# QFT modulo m

•  $|j\rangle|0\rangle$   $\downarrow$ •  $|j\rangle\sum_{k=0}^{m-1}|k\rangle$ 

 $\approx \mathsf{Hadamard}^{\otimes \mathsf{log}_m} + \dots$ 

dyadic approx of jk/m in *aux* cond. phase shifts, bitwise uncompute *aux* 

・ロト ・回ト ・ヨト ・ヨト

Simon's algorithm Basic tools The HSP Infinite abelian HSPs QFT mod powers of 2 Phase estimation Period finding QFT mod powers of 2 Phase estimation Period finding

## QFT modulo m

•  $|j\rangle|0\rangle$   $\downarrow$ •  $|j\rangle\sum_{k=0}^{m-1}|k\rangle$ 

•  $\approx |j\rangle \sum_{k=0}^{m-1} \omega^{jk} |k\rangle$ 

 $\approx \mathsf{Hadamard}^{\otimes \mathsf{log}_m} + \dots$ 

dyadic approx of jk/m in *aux* cond. phase shifts, bitwise uncompute *aux* 

・ロン ・回 と ・ ヨ と ・ ヨ と

# QFT modulo m

•  $|j\rangle|0\rangle$   $\downarrow$ •  $|j\rangle\sum_{k=0}^{m-1}|k\rangle$ 

•  $\approx |j\rangle \sum_{k=0}^{m-1} \omega^{jk} |k\rangle$ 

 $\approx \mathsf{Hadamard}^{\otimes \mathsf{log}_m} + \dots$ 

dyadic approx of jk/m in aux cond. phase shifts, bitwise uncompute aux

・ロン ・回 と ・ ヨ と ・ ヨ と

3

inverse phase estimation

# QFT modulo m

•  $|j\rangle|0\rangle$   $\downarrow$ •  $|j\rangle\sum_{k=0}^{m-1}|k\rangle$ 

•  $\approx |j\rangle \sum_{k=0}^{m-1} \omega^{jk} |k\rangle$ 

•  $|0\rangle \sum_{k=0}^{m-1} \omega^{jk} |k\rangle$ 

 $\approx \mathsf{Hadamard}^{\otimes \mathsf{log}_m} + \dots$ 

dyadic approx of jk/m in aux cond. phase shifts, bitwise uncompute aux

・ロン ・回 と ・ ヨ と ・ ヨ と

3

inverse phase estimation

# QFT modulo m

•  $|j\rangle|0\rangle$   $\downarrow$ •  $|j\rangle\sum_{k=0}^{m-1}|k\rangle$ 

•  $\approx |j\rangle \sum_{k=0}^{m-1} \omega^{jk} |k\rangle$ 

•  $|0\rangle \sum_{k=0}^{m-1} \omega^{jk} |k\rangle$ 

 $\approx \mathsf{Hadamard}^{\otimes \mathsf{log}_m} + \dots$ 

dyadic approx of jk/m in aux cond. phase shifts, bitwise uncompute aux

(ロ) (同) (E) (E) (E)

inverse phase estimation

swap

# QFT modulo m

•  $|j\rangle|0\rangle$ •  $|i\rangle \sum_{k=0}^{m-1} |k\rangle$ •  $\approx |j\rangle \sum_{k=0}^{m-1} \omega^{jk} |k\rangle$ •  $|0\rangle \sum_{k=0}^{m-1} \omega^{jk} |k\rangle$ •  $\sum_{k=0}^{m-1} \omega^{jk} |k\rangle |0\rangle$ 

 $\approx \mathsf{Hadamard}^{\otimes \mathsf{log}_m} + \dots$ 

dyadic approx of jk/m in aux cond. phase shifts, bitwise uncompute aux

(ロ) (同) (E) (E) (E)

inverse phase estimation

swap

 $\begin{array}{c} \begin{array}{c} \text{Simon's algorithm}\\ \text{Basic tools}\\ \text{The HSP}\\ \text{Infinite abelian HSPs} \end{array} \xrightarrow{\text{QFT mod powers of 2}\\ \text{Phase estimation}\\ \text{Period finding}\\ \text{QFT over abelian groups} \end{array}$ 

• Tensor product of QFT's for  $\mathbb{Z}_{m_1}, \ldots, \mathbb{Z}_{m_n}$ .

・ロット (四) (日) (日)

QFT of  $\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_n}$ 

- Tensor product of QFT's for  $\mathbb{Z}_{m_1}, \ldots, \mathbb{Z}_{m_n}$ .
- For  $\mathbb{Z}_m^n$ :

$$|u\rangle\mapsto \sum_{\mathbf{v}\in\mathbb{Z}_m^n}\omega^{(u,\mathbf{v})}|\mathbf{v}\rangle,$$

・ロット (四) (日) (日)

QFT of  $\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_n}$ 

• Tensor product of QFT's for  $\mathbb{Z}_{m_1}, \ldots, \mathbb{Z}_{m_n}$ .

• For  $\mathbb{Z}_m^n$ :

$$|u\rangle\mapsto \sum_{\mathbf{v}\in\mathbb{Z}_m^n}\omega^{(u,\mathbf{v})}|\mathbf{v}\rangle,$$

where  $\omega = \sqrt[m]{1}$ 

・ロト ・回ト ・ヨト ・ヨト

QFT of  $\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_n}$ 

• Tensor product of QFT's for  $\mathbb{Z}_{m_1}, \ldots, \mathbb{Z}_{m_n}$ .

• For  $\mathbb{Z}_m^n$ :

$$|u\rangle\mapsto \sum_{\mathbf{v}\in\mathbb{Z}_m^n}\omega^{(u,\mathbf{v})}|\mathbf{v}\rangle,$$

where  $\omega = \sqrt[m]{1}$ and  $(u, v) = \sum_{i=1}^{n} u_i v_i \pmod{m}$ .

・ロン ・回 と ・ ヨ と ・ ヨ と

QFT of  $\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_n}$ 

• Tensor product of QFT's for  $\mathbb{Z}_{m_1}, \ldots, \mathbb{Z}_{m_n}$ .

• For  $\mathbb{Z}_m^n$ :

$$|u\rangle\mapsto \sum_{\mathbf{v}\in\mathbb{Z}_m^n}\omega^{(u,\mathbf{v})}|\mathbf{v}\rangle,$$

where  $\omega = \sqrt[m]{1}$ and  $(u, v) = \sum_{i=1}^{n} u_i v_i \pmod{m}$ .

• In terms of characters:

$$|m{g}
angle\mapsto \sum_{\chi\in \widehat{m{\mathcal{G}}}}\chi(m{g})|\chi
angle,$$

・ロン ・四マ ・ヨマ ・ヨマ

QFT of  $\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_n}$ 

• Tensor product of QFT's for  $\mathbb{Z}_{m_1}, \ldots, \mathbb{Z}_{m_n}$ .

• For  $\mathbb{Z}_m^n$ :

$$|u\rangle\mapsto \sum_{\mathbf{v}\in\mathbb{Z}_m^n}\omega^{(u,\mathbf{v})}|\mathbf{v}\rangle,$$

where  $\omega = \sqrt[m]{1}$ and  $(u, v) = \sum_{i=1}^{n} u_i v_i \pmod{m}$ .

• In terms of characters:

$$|m{g}
angle\mapsto \sum_{\chi\in \widehat{m{\mathcal{G}}}}\chi(m{g})|\chi
angle,$$

G finite abelian group,  $\hat{G} = \operatorname{Hom}(G, \mathbb{C}^*)$ 

・ロン ・回と ・ヨン ・ヨン

Simon's algorithm QFT mod powers of 2 Basic tools The HSP Infinite abelian HSPs

Period finding QFT over abelian groups

# Abelian QFT – interpretations

#### Characters

Gábor Ivanyos MTA SZTAKI Fast Quantum Algorithms Lectures 1 and 2

・ロト ・回ト ・ヨト ・ヨト

3

Abelian QFT – interpretations

- Characters
  - $\hat{G} = \operatorname{Hom}(G, \mathbb{C}^*)$

$$|g
angle\mapsto \sum_{\chi\in\widehat{{\sf G}}}\chi(g)|"\chi"
angle,$$

・ロン ・回と ・ヨン・

### Abelian QFT – interpretations

• Characters

• 
$$\hat{G} = \operatorname{Hom}(G, \mathbb{C}^*)$$

$$|g
angle\mapsto \sum_{\chi\in\widehat{{\sf G}}}\chi(g)|"\chi"
angle,$$

• "
$$\chi$$
" string encoding  $\chi$ 

・ロト ・回ト ・ヨト ・ヨト

3

### Abelian QFT – interpretations

- Characters
  - $\hat{G} = \operatorname{Hom}(G, \mathbb{C}^*)$

$$|g
angle\mapsto \sum_{\chi\in\widehat{\mathcal{G}}}\chi(g)|"\chi"
angle,$$

• "
$$\chi$$
" string encoding  $\chi$ 

• in 
$$\mathbb{Z}_m^n$$
,  $v$  may encode  $\chi_v : u \mapsto \omega^{(u,v)}$ 

・ロン ・回と ・ヨン・

### Abelian QFT – interpretations

- Characters
  - $\hat{G} = \operatorname{Hom}(G, \mathbb{C}^*)$

$$|g
angle\mapsto \sum_{\chi\in\widehat{{\sf G}}}\chi(g)|"\chi"
angle,$$

• "
$$\chi$$
" string encoding  $\chi$ 

- in  $\mathbb{Z}_m^n$ , v may encode  $\chi_v : u \mapsto \omega^{(u,v)}$
- Basis change of  $\mathbb{C}G$

・ロン ・回と ・ヨン ・ヨン

### Abelian QFT – interpretations

- Characters
  - $\hat{G} = \operatorname{Hom}(G, \mathbb{C}^*)$

$$|m{g}
angle\mapsto \sum_{\chi\in\widehat{m{\mathcal{G}}}}\chi(m{g})|``\chi"
angle,$$

- " $\chi$ " string encoding  $\chi$
- in  $\mathbb{Z}_m^n$ , v may encode  $\chi_v : u \mapsto \omega^{(u,v)}$
- Basis change of  $\mathbb{C}G$ 
  - standard basis: |g
    angle,  $g\in G$

イロト イヨト イヨト イヨト

### Abelian QFT – interpretations

- Characters
  - $\hat{G} = \operatorname{Hom}(G, \mathbb{C}^*)$

$$|g
angle\mapsto \sum_{\chi\in\widehat{{\sf G}}}\chi(g)|"\chi"
angle,$$

- " $\chi$ " string encoding  $\chi$
- in  $\mathbb{Z}_m^n$ , v may encode  $\chi_v : u \mapsto \omega^{(u,v)}$
- Basis change of  $\mathbb{C}G$ 
  - standard basis: |g
    angle,  $g\in G$
  - $|\chi\rangle\in\mathbb{C}G$  common eigenvector:

$$g|\chi\rangle=\chi(g)|\chi\rangle$$

・ロト ・回ト ・ヨト ・ヨト

3

### Abelian QFT – interpretations

- Characters
  - $\hat{G} = \operatorname{Hom}(G, \mathbb{C}^*)$

$$|g
angle\mapsto \sum_{\chi\in\widehat{{\sf G}}}\chi(g)|"\chi"
angle,$$

- " $\chi$ " string encoding  $\chi$
- in  $\mathbb{Z}_m^n$ , v may encode  $\chi_v : u \mapsto \omega^{(u,v)}$
- Basis change of  $\mathbb{C}G$ 
  - standard basis: |g
    angle,  $g\in G$
  - $|\chi\rangle\in\mathbb{C}G$  common eigenvector:

$$g|\chi\rangle = \chi(g)|\chi\rangle$$

$$|\chi\rangle = \sum_{g \in G} \overline{\chi}(g) |g\rangle$$

イロン イヨン イヨン イヨン

Simon's algorithm Basic tools The HSP Infinite abelian HSP Abelian tourier sampling Applications of abelian HSP

### Contents

- **1** Simon's algorithm
- 2 Basic tools
  - QFT mod powers of 2
  - Phase estimation
  - Period finding
  - QFT over abelian groups
- 3 The HSP
  - The Hidden Subgroup Problem
  - Coset states
  - Abelian Fourier sampling
  - Applications of abelian HSP
- Infinite abelian HSPs
  - HSP in lattices
  - Units in number fields and hidden lattices
  - Open problems

< □ > < □ > < □ >

The Hidden Subgroup Problem Coset states Abelian Fourier sampling Applications of abelian HSP

### HSP - the hidden subgroup problem

• G (finite) group

・ロン ・回と ・ヨン ・ヨン

The Hidden Subgroup Problem Coset states Abelian Fourier sampling Applications of abelian HSP

# HSP - the hidden subgroup problem

- G (finite) group
- $f: G \rightarrow \{ \text{objects} \}$  hides the subgroup  $H \leq G$ , if

イロン イヨン イヨン イヨン

2

The Hidden Subgroup Problem Coset states Abelian Fourier sampling Applications of abelian HSP

# HSP - the hidden subgroup problem

- G (finite) group
- $f: G \rightarrow \{\text{objects}\}$  hides the subgroup  $H \leq G$ , if

 $f(x) = f(y) \Leftrightarrow xH = yH$ 

x and y are in the same left coset of H

<ロ> (日) (日) (日) (日) (日)

The Hidden Subgroup Problem Coset states Abelian Fourier sampling Applications of abelian HSP

### HSP - the hidden subgroup problem

- G (finite) group
- $f: G \rightarrow \{\text{objects}\}$  hides the subgroup  $H \leq G$ , if  $f(x) = f(y) \Leftrightarrow xH = yH$

x and y are in the same left coset of Hf is constant on the left cosets of Hand takes different values on different cosets

イロン イヨン イヨン イヨン

The Hidden Subgroup Problem Coset states Abelian Fourier sampling Applications of abelian HSP

### HSP - the hidden subgroup problem

- G (finite) group
- $f: G \rightarrow \{\text{objects}\}$  hides the subgroup  $H \leq G$ , if

 $f(x) = f(y) \Leftrightarrow xH = yH$ 

x and y are in the same left coset of H

f is constant on the left cosets of H

and takes different values on different cosets

• f given by an oracle (or an efficient algorithm) performing  $|x\rangle|0
angle\mapsto|x
angle|f(x)
angle$ 

- 4 同 6 4 日 6 4 日 6

The Hidden Subgroup Problem Coset states Abelian Fourier sampling Applications of abelian HSP

# HSP - the hidden subgroup problem

- G (finite) group
- $f: G \rightarrow \{\text{objects}\}$  hides the subgroup  $H \leq G$ , if

 $f(x) = f(y) \Leftrightarrow xH = yH$ 

x and y are in the same left coset of H

f is constant on the left cosets of H

and takes different values on different cosets

• f given by an oracle (or an efficient algorithm) performing  $|x
angle|0
angle\mapsto |x
angle|f(x)
angle$ 

often: classical algorithm  $x \mapsto f(x)$ 

The Hidden Subgroup Problem Coset states Abelian Fourier sampling Applications of abelian HSP

# HSP - the hidden subgroup problem

- G (finite) group
- $f: G \rightarrow \{\text{objects}\}$  hides the subgroup  $H \leq G$ , if

 $f(x) = f(y) \Leftrightarrow xH = yH$ 

x and y are in the same left coset of H

f is constant on the left cosets of H

and takes different values on different cosets

• f given by an oracle (or an efficient algorithm) performing  $|x
angle|0
angle\mapsto |x
angle|f(x)
angle$ 

often: classical algorithm  $x \mapsto f(x)$ 

• Task: find (generators for) H.

The Hidden Subgroup Problem Coset states Abelian Fourier sampling Applications of abelian HSP

# HSP - the hidden subgroup problem

- G (finite) group
- $f: G \rightarrow \{\text{objects}\}$  hides the subgroup  $H \leq G$ , if

 $f(x) = f(y) \Leftrightarrow xH = yH$ 

x and y are in the same left coset of H

f is constant on the left cosets of H

and takes different values on different cosets

• f given by an oracle (or an efficient algorithm) performing  $|x
angle|0
angle\mapsto |x
angle|f(x)
angle$ 

often: classical algorithm  $x \mapsto f(x)$ 

- Task: find (generators for) H.
- Examples:

The Hidden Subgroup Problem Coset states Abelian Fourier sampling Applications of abelian HSP

# HSP - the hidden subgroup problem

- G (finite) group
- $f: G \rightarrow \{\text{objects}\}$  hides the subgroup  $H \leq G$ , if

 $f(x) = f(y) \Leftrightarrow xH = yH$ 

x and y are in the same left coset of H

f is constant on the left cosets of H

and takes different values on different cosets

• f given by an oracle (or an efficient algorithm) performing  $|x
angle|0
angle\mapsto |x
angle|f(x)
angle$ 

often: classical algorithm  $x \mapsto f(x)$ 

- Task: find (generators for) H.
- Examples:

Period 
$$G = \mathbb{Z}$$
,  $f$  *r*-periodical,  $H = r\mathbb{Z}$ .

The Hidden Subgroup Problem Coset states Abelian Fourier sampling Applications of abelian HSP

# HSP - the hidden subgroup problem

- G (finite) group
- $f: G \rightarrow \{\text{objects}\}$  hides the subgroup  $H \leq G$ , if

 $f(x) = f(y) \Leftrightarrow xH = yH$ 

x and y are in the same left coset of H

f is constant on the left cosets of H

and takes different values on different cosets

• f given by an oracle (or an efficient algorithm) performing  $|x
angle|0
angle\mapsto |x
angle|f(x)
angle$ 

often: classical algorithm  $x \mapsto f(x)$ 

- Task: find (generators for) H.
- Examples:

Period  $G = \mathbb{Z}$ , f r-periodical,  $H = r\mathbb{Z}$ . Discrete log  $G = Z_n \times Z_n$ ,  $f(k, \ell) = u^k v^{-\ell}$ ,  $H = \{(k, \ell) | u^k = v^\ell\}.$ 

The Hidden Subgroup Problem Coset states Abelian Fourier sampling Applications of abelian HSP

### Graph automorphism

• permuted graph

・ロン ・回と ・ヨン・

The Hidden Subgroup Problem Coset states Abelian Fourier sampling Applications of abelian HSP

### Graph automorphism

- permuted graph
  - $\Gamma$  graph on  $\{1, \ldots, n\}$ ,  $\sigma \in S_n$ ,

・ロン ・回と ・ヨン ・ヨン

The Hidden Subgroup Problem Coset states Abelian Fourier sampling Applications of abelian HSP

### Graph automorphism

- permuted graph
  - $\Gamma$  graph on  $\{1, \ldots, n\}$ ,  $\sigma \in S_n$ ,
  - permuted graph  $\Gamma^{\sigma}$ , with edges:

イロン 不同と 不同と 不同と

The Hidden Subgroup Problem Coset states Abelian Fourier sampling Applications of abelian HSP

### Graph automorphism

- permuted graph
  - $\Gamma$  graph on  $\{1, \ldots, n\}$ ,  $\sigma \in S_n$ ,
  - permuted graph  $\Gamma^{\sigma}$ , with edges:  $(\sigma(i), \sigma(j))$  where (i, j) edge of  $\Gamma$ .

イロト イヨト イヨト イヨト

The Hidden Subgroup Problem Coset states Abelian Fourier sampling Applications of abelian HSP

### Graph automorphism

- permuted graph
  - $\Gamma$  graph on  $\{1, \ldots, n\}$ ,  $\sigma \in S_n$ ,
  - permuted graph  $\Gamma^{\sigma}$ , with edges:  $(\sigma(i), \sigma(j))$  where (i, j) edge of  $\Gamma$ .
- Graph automorphism as HSP

イロト イヨト イヨト イヨト

3

The Hidden Subgroup Problem Coset states Abelian Fourier sampling Applications of abelian HSP

### Graph automorphism

- permuted graph
  - $\Gamma$  graph on  $\{1, \ldots, n\}$ ,  $\sigma \in S_n$ ,
  - permuted graph Γ<sup>σ</sup>, with edges:
     (σ(i), σ(j)) where (i, j) edge of Γ.
- Graph automorphism as HSP

$$G=S_n f(\sigma)=\Gamma^{\sigma}.$$

イロト イヨト イヨト イヨト

3

The Hidden Subgroup Problem Coset states Abelian Fourier sampling Applications of abelian HSP

### Graph automorphism

- permuted graph
  - $\Gamma$  graph on  $\{1, \ldots, n\}$ ,  $\sigma \in S_n$ ,
  - permuted graph  $\Gamma^{\sigma}$ , with edges:  $(\sigma(i), \sigma(j))$  where (i, j) edge of  $\Gamma$ .
- Graph automorphism as HSP

 $G = S_n f(\sigma) = \Gamma^{\sigma}.$ hidden subgroup = Aut(G)

The Hidden Subgroup Problem Coset states Abelian Fourier sampling Applications of abelian HSP

### Graph automorphism

- permuted graph
  - $\Gamma$  graph on  $\{1, \ldots, n\}$ ,  $\sigma \in S_n$ ,
  - permuted graph  $\Gamma^{\sigma}$ , with edges:  $(\sigma(i), \sigma(j))$  where (i, j) edge of  $\Gamma$ .
- Graph automorphism as HSP

 $G=S_n f(\sigma)=\Gamma^{\sigma}.$ 

hidden subgroup = Aut(G)

In general: stabilizers in large permutation actions

The Hidden Subgroup Problem Coset states Abelian Fourier sampling Applications of abelian HSP

# Graph automorphism

- permuted graph
  - $\Gamma$  graph on  $\{1, \ldots, n\}$ ,  $\sigma \in S_n$ ,
  - permuted graph  $\Gamma^{\sigma}$ , with edges:  $(\sigma(i), \sigma(j))$  where (i, j) edge of  $\Gamma$ .
- Graph automorphism as HSP

 $G=S_n f(\sigma)=\Gamma^{\sigma}.$ 

hidden subgroup = Aut(G)

In general: stabilizers in large permutation actions

• Graph iso  $\leftarrow$  Graph auto

The Hidden Subgroup Problem Coset states Abelian Fourier sampling Applications of abelian HSP

# Graph automorphism

- permuted graph
  - $\Gamma$  graph on  $\{1, \ldots, n\}$ ,  $\sigma \in S_n$ ,
  - permuted graph  $\Gamma^{\sigma}$ , with edges:  $(\sigma(i), \sigma(j))$  where (i, j) edge of  $\Gamma$ .
- Graph automorphism as HSP

 $G=S_n f(\sigma)=\Gamma^{\sigma}.$ 

hidden subgroup = Aut(G)

In general: stabilizers in large permutation actions

• Graph iso  $\leftarrow$  Graph auto

 $\Gamma_1,\Gamma_2$  connected.

The Hidden Subgroup Problem Coset states Abelian Fourier sampling Applications of abelian HSP

# Graph automorphism

- permuted graph
  - $\Gamma$  graph on  $\{1, \ldots, n\}$ ,  $\sigma \in S_n$ ,
  - permuted graph  $\Gamma^{\sigma}$ , with edges:  $(\sigma(i), \sigma(j))$  where (i, j) edge of  $\Gamma$ .
- Graph automorphism as HSP

 $G = S_n f(\sigma) = \Gamma^{\sigma}$ . hidden subgroup = Aut(G)In general: stabilizers in large permutation actions

• Graph iso  $\leftarrow$  Graph auto

 $\begin{array}{l} \label{eq:Gamma} \Gamma_1, \Gamma_2 \text{ connected}. \\ \Gamma_1 \cong \Gamma_2 \text{ iff} \end{array}$ 

$$\left|\operatorname{Aut}(\Gamma_1 \bigcup^{\cdot} \Gamma_2)\right| = 2 \cdot |\operatorname{Aut}(\Gamma_1)| \cdot |\operatorname{Aut}(\Gamma_2)|$$

イロン 不同と 不同と 不同と

Simon's algorithm The Hidden Subgroup Problem Basic tools Coset states The HSP Abelian Fourier sampling Infinite abelian HSPs Applications of abelian HSP

#### Coset states

### • $|1_G\rangle|0 angle$

Gábor Ivanyos MTA SZTAKI Fast Quantum Algorithms Lectures 1 and 2

・ロン ・雪 ・ ・ ヨ ・ ・ ヨ ・ ・

Simon's algorithm Basic tools The HSP Infinite abelian HSP Abelian Fourier sampling Applications of abelian HSP

### Coset states

•  $|1_G\rangle|0\rangle$ 

### (usually easy)

Gábor Ivanyos MTA SZTAKI Fast Quantum Algorithms Lectures 1 and 2

◆□ > ◆□ > ◆臣 > ◆臣 > ○

Simon's algorithm Basic tools The HSP Infinite abelian HSP Abelian Fourier sampling Applications of abelian HSP

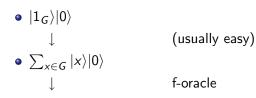
### Coset states

•  $|1_G\rangle|0\rangle$   $\downarrow$ •  $\sum_{x\in G}|x\rangle|0\rangle$ 

(usually easy)

・ロン ・回と ・ヨン ・ヨン

#### Coset states



・ロン ・回と ・ヨン ・ヨン

### Coset states

•  $|1_G\rangle|0\rangle$   $\downarrow$  (usually easy) •  $\sum_{x \in G} |x\rangle|0\rangle$   $\downarrow$  f-oracle •  $\sum_{x \in G} |x\rangle|f(x)\rangle$ 

・ロン ・回と ・ヨン ・ヨン

Simon's algorithm The Hidden Subgroup Problem Basic tools Coset states The HSP Abelian Fourier sampling Infinite abelian HSPs Applications of abelian HSP

### Coset states

•  $|1_G\rangle|0\rangle$   $\downarrow$  (usually easy) •  $\sum_{x \in G} |x\rangle|0\rangle$   $\downarrow$  f-oracle •  $\sum_{x \in G} |x\rangle|f(x)\rangle$  $\downarrow$  (equality)

・ロン ・回と ・ヨン ・ヨン

Simon's algorithm The Hidden Subgroup Problem Basic tools Coset states The HSP Abelian Fourier sampling Infinite abelian HSPs Applications of abelian HSP

#### Coset states

- $|1_G\rangle|0\rangle$   $\downarrow$  (usually easy) •  $\sum_{x \in G} |x\rangle|0\rangle$   $\downarrow$  f-oracle •  $\sum_{x \in G} |x\rangle|f(x)\rangle$  $\downarrow$  (equality)
- $\sum_{s} \sum_{f(x)=s} |x\rangle |s\rangle = \sum_{a \in T} \sum_{x \in H} |ax\rangle |f(a)\rangle$

・ロン ・回と ・ヨン ・ヨン

Simon's algorithm The Hidden Subgroup Problem Basic tools Coset states The HSP Abelian Fourier sampling Infinite abelian HSPs Applications of abelian HSP

### Coset states

•  $|1_G\rangle|0\rangle$   $\downarrow$  (usually easy) •  $\sum_{x \in G} |x\rangle|0\rangle$   $\downarrow$  f-oracle •  $\sum_{x \in G} |x\rangle|f(x)\rangle$  $\downarrow$  (equality)

• 
$$\sum_{s} \sum_{f(x)=s} |x\rangle |s\rangle = \sum_{a \in T} \sum_{x \in H} |ax\rangle |f(a)\rangle$$

*T*: left transversal of H= a set of left coset representatives by H

イロト イヨト イヨト イヨト

#### Coset states 2

 $\sum_{a \in T} \sum_{x \in H} |ax\rangle |f(a)\rangle$ 

・ロン ・回と ・ヨン・

ъ

#### Coset states 2

 $\sum_{a \in T} \sum_{x \in H} |ax\rangle |f(a)\rangle$ (equality) ↓

・ロト ・回ト ・ヨト ・ヨト

#### Coset states 2

$$\sum_{a \in T} \sum_{x \in H} |ax\rangle |f(a)\rangle$$
  
 
$$\downarrow \qquad (equality)$$
  
 
$$\sum_{a \in T} \left( \sum_{x \in H} |ax\rangle \right) |f(a)\rangle$$

< □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □

#### Coset states 2

$$\sum_{a \in T} \sum_{x \in H} |ax\rangle |f(a)\rangle$$
  

$$\downarrow \qquad (equality)$$
  

$$\sum_{a \in T} \left( \sum_{x \in H} |ax\rangle \right) |f(a)\rangle$$
  

$$\downarrow \qquad measure/ignore f(a)$$

< □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □

#### Coset states 2

$$\sum_{a \in T} \sum_{x \in H} |ax\rangle |f(a)\rangle$$
  

$$\downarrow \qquad (equality)$$
  

$$\sum_{a \in T} \left( \sum_{x \in H} |ax\rangle \right) |f(a)\rangle$$
  

$$\downarrow \qquad measure/ignore f(a)$$

coset state

$$|aH\rangle := \sum_{x\in H} |ax\rangle$$
 for random  $a\in T$ 

< 口 > < 回 > < 回 > < 回 > < 回 > <

#### Coset states 2

$$\sum_{a \in T} \sum_{x \in H} |ax\rangle |f(a)\rangle$$

$$\downarrow \qquad (equality)$$

$$\sum_{a \in T} \left( \sum_{x \in H} |ax\rangle \right) |f(a)\rangle$$

$$\downarrow \qquad measure/ignore f(a)$$

coset state

$$|aH\rangle := \sum_{x\in H} |ax\rangle$$
 for random  $a\in T$ 

 $\Leftrightarrow \text{for random } a \in G$ 

イロン イヨン イヨン イヨン

The Hidden Subgroup Problem Coset states Abelian Fourier sampling Applications of abelian HSP

#### Coset states - summary

Coset state (with random  $a \in T$  (random  $a \in G$ ))

$$|aH
angle = rac{1}{\sqrt{|H|}}\sum_{x\in H}|ax
angle$$

(normalizing factor included)

・ロン ・回と ・ヨン ・ヨン

The Hidden Subgroup Problem Coset states Abelian Fourier sampling Applications of abelian HSP

### Abelian Fourier sampling

•  $\sum_{x \in H} |ax\rangle$ 

・ロン ・回と ・ヨン ・ヨン

Э

The Hidden Subgroup Problem Coset states Abelian Fourier sampling Applications of abelian HSP

### Abelian Fourier sampling

•  $\sum_{x \in H} |ax\rangle$ <u>→</u>...\_

・ロン ・回と ・ヨン・

æ

QFT

The Hidden Subgroup Problem Coset states Abelian Fourier sampling Applications of abelian HSP

# Abelian Fourier sampling

• 
$$\sum_{x \in H} |ax\rangle$$
  
 $\downarrow$  QFT  
•  $\sum_{x \in H} \sum_{\chi \in \hat{G}} \chi(ax) |\chi\rangle$ 

・ロン ・回と ・ヨン・

Э

The Hidden Subgroup Problem Coset states Abelian Fourier sampling Applications of abelian HSP

# Abelian Fourier sampling

• 
$$\sum_{x \in H} |ax\rangle$$
  
 $\downarrow$  QFT  
•  $\sum_{x \in H} \sum_{\chi \in \hat{G}} \chi(ax) |\chi\rangle$   
 $\downarrow$  (equality)

・ロン ・回と ・ヨン・

The Hidden Subgroup Problem Coset states Abelian Fourier sampling Applications of abelian HSP

# Abelian Fourier sampling

• 
$$\sum_{x \in H} |ax\rangle$$
  
 $\downarrow$  QFT  
•  $\sum_{x \in H} \sum_{\chi \in \hat{G}} \chi(ax) |\chi\rangle$   
 $\downarrow$  (equality)  
 $\sum_{\chi \in \hat{G}} (\chi(a) \sum_{x \in H} \chi(x)) |\chi\rangle$ 

・ロト ・回ト ・ヨト ・ヨト

The Hidden Subgroup Problem Coset states Abelian Fourier sampling Applications of abelian HSP

# Abelian Fourier sampling

• 
$$\sum_{x \in H} |ax\rangle$$
  
 $\downarrow$  QFT  
•  $\sum_{x \in H} \sum_{\chi \in \hat{G}} \chi(ax) |\chi\rangle$   
 $\downarrow$  (equality)  
 $\sum_{\chi \in \hat{G}} (\chi(a) \sum_{x \in H} \chi(x)) |\chi\rangle$ 

• with normalizing factors:

$$\sum_{\chi \in \hat{G}} \left( \frac{\chi(a)}{|G|^{\frac{1}{2}} |H|^{\frac{1}{2}}} \sum_{x \in H} \chi(x) \right) |\chi\rangle$$

・ロン ・回と ・ヨン ・ヨン

The Hidden Subgroup Problem Coset states Abelian Fourier sampling Applications of abelian HSP

# Abelian Fourier sampling 2

 $\bullet$  Coefficient of  $\chi$ 

・ロン ・回と ・ヨン ・ヨン

The Hidden Subgroup Problem Coset states Abelian Fourier sampling Applications of abelian HSP

# Abelian Fourier sampling 2

 $\bullet$  Coefficient of  $\chi$ 

$$\frac{\chi(a)}{\sqrt{|G:H|}} \frac{1}{|H|} \sum_{x \in H} \chi(x) = \begin{cases} \frac{\chi(a)}{\sqrt{|G:H|}} & \text{if } \chi_H = 1, \\ 0 & \text{otherwise.} \end{cases}$$

・ロン ・回と ・ヨン ・ヨン

The Hidden Subgroup Problem Coset states Abelian Fourier sampling Applications of abelian HSP

# Abelian Fourier sampling 2

 $\bullet$  Coefficient of  $\chi$ 

$$\frac{\chi(a)}{\sqrt{|G:H|}} \frac{1}{|H|} \sum_{x \in H} \chi(x) = \begin{cases} \frac{\chi(a)}{\sqrt{|G:H|}} & \text{if } \chi_H = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Proof:

・ロン ・回と ・ヨン ・ヨン

The Hidden Subgroup Problem Coset states Abelian Fourier sampling Applications of abelian HSP

# Abelian Fourier sampling 2

 $\bullet$  Coefficient of  $\chi$ 

$$\frac{\chi(a)}{\sqrt{|G:H|}} \frac{1}{|H|} \sum_{x \in H} \chi(x) = \begin{cases} \frac{\chi(a)}{\sqrt{|G:H|}} & \text{if } \chi_H = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Proof: orthogonality of  $1_H$  and  $\chi_H$ 

・ロン ・回と ・ヨン・

The Hidden Subgroup Problem Coset states Abelian Fourier sampling Applications of abelian HSP

# Abelian Fourier sampling 2

• Coefficient of  $\chi$ 

$$\frac{\chi(a)}{\sqrt{|G:H|}} \frac{1}{|H|} \sum_{x \in H} \chi(x) = \begin{cases} \frac{\chi(a)}{\sqrt{|G:H|}} & \text{if } \chi_H = 1, \\ 0 & \text{otherwise.} \end{cases}$$

 $\begin{array}{l} \text{Proof:} \\ \text{orthogonality of } \mathbf{1}_H \text{ and } \chi_H \\ \frac{1}{|H|} \sum_{x \in H} \chi(x) = \left\{ \begin{array}{l} 1 & \text{if } \chi_H = 1, \\ 0 & \text{otherwise} \end{array} \right. \end{array}$ 

イロン 不同と 不同と 不同と

The Hidden Subgroup Problem Coset states Abelian Fourier sampling Applications of abelian HSP

# Abelian Fourier sampling 2

 $\bullet$  Coefficient of  $\chi$ 

$$\frac{\chi(a)}{\sqrt{|G:H|}} \frac{1}{|H|} \sum_{x \in H} \chi(x) = \begin{cases} \frac{\chi(a)}{\sqrt{|G:H|}} & \text{if } \chi_H = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Proof:  
orthogonality of 
$$1_H$$
 and  $\chi_H$   
 $\frac{1}{|H|} \sum_{x \in H} \chi(x) = \begin{cases} 1 & \text{if } \chi_H = 1, \\ 0 & \text{otherwise} \end{cases}$ 

 $\bullet$  Probability of observing  $\chi$ 

イロト イヨト イヨト イヨト

The Hidden Subgroup Problem Coset states Abelian Fourier sampling Applications of abelian HSP

# Abelian Fourier sampling 2

 $\bullet$  Coefficient of  $\chi$ 

$$\frac{\chi(a)}{\sqrt{|G:H|}} \frac{1}{|H|} \sum_{x \in H} \chi(x) = \begin{cases} \frac{\chi(a)}{\sqrt{|G:H|}} & \text{if } \chi_H = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Proof:  
orthogonality of 
$$1_H$$
 and  $\chi_H$   
 $\frac{1}{|H|} \sum_{x \in H} \chi(x) = \begin{cases} 1 & \text{if } \chi_H = 1, \\ 0 & \text{otherwise} \end{cases}$ 

 $\bullet$  Probability of observing  $\chi$ 

$$= \begin{array}{cc} \frac{1}{|G:H|} & \text{if } \chi \in H^{\perp}, \\ 0 & \text{otherwise} \end{array}$$

- - 4 回 ト - 4 回 ト

.

# Computing H

• 
$$\mathcal{H}^{\perp} = \{\chi \in \hat{\mathcal{G}} \mid \chi_{\mathcal{H}} = 1\}$$
 subgroup of  $\hat{\mathcal{G}}$ .

▲□→ ▲圖→ ▲厘→ ▲厘→

Э.

# Computing H

• 
$$H^{\perp} = \{\chi \in \hat{G} \mid \chi_H = 1\}$$
 subgroup of  $\hat{G}$ .

• generating set  $\Gamma$  of  $H^{\perp}$  collected in

#### expectedly $O(\log |G|)$ repetitions.

・ロン ・回と ・ヨン ・ヨン

# Computing H

• 
$$H^{\perp} = \{\chi \in \hat{G} \mid \chi_H = 1\}$$
 subgroup of  $\hat{G}$ .

• generating set  $\Gamma$  of  $H^{\perp}$  collected in

expectedly  $O(\log |G|)$  repetitions.

• 
$$H = \{x \in G \mid \chi(x) = 1 \text{ for every } \chi \in \Gamma\}.$$

・ロン ・回と ・ヨン ・ヨン

# Computing H

• 
$$H^{\perp} = \{\chi \in \hat{G} \mid \chi_H = 1\}$$
 subgroup of  $\hat{G}$ .

• generating set  $\Gamma$  of  $H^{\perp}$  collected in

expectedly  $O(\log |G|)$  repetitions.

• 
$$H = \{x \in G \mid \chi(x) = 1 \text{ for every } \chi \in \Gamma\}.$$

• computing *H*: system of linear congruences.

・ロン ・回と ・ヨン・

The Hidden Subgroup Problem Coset states Abelian Fourier sampling Applications of abelian HSP

### Remarks on Abelian Fourier Sampling

• No need of measuring the value of f

<ロ> (日) (日) (日) (日) (日)

The Hidden Subgroup Problem Coset states Abelian Fourier sampling Applications of abelian HSP

### Remarks on Abelian Fourier Sampling

- No need of measuring the value of f
- f can be quantum-state valued:

イロト イヨト イヨト イヨト

The Hidden Subgroup Problem Coset states Abelian Fourier sampling Applications of abelian HSP

### Remarks on Abelian Fourier Sampling

- No need of measuring the value of f
- f can be quantum-state valued:

 $f: G \to \mathbb{C}^X$  hides H if:

イロト イヨト イヨト イヨト

3

The Hidden Subgroup Problem Coset states Abelian Fourier sampling Applications of abelian HSP

### Remarks on Abelian Fourier Sampling

- No need of measuring the value of f
- f can be quantum-state valued:
  - $f: G \to \mathbb{C}^X$  hides H if:
  - f constant on left cosets of H

イロン イヨン イヨン イヨン

3

The Hidden Subgroup Problem Coset states Abelian Fourier sampling Applications of abelian HSP

### Remarks on Abelian Fourier Sampling

- No need of measuring the value of f
- f can be quantum-state valued:

 $f: G \to \mathbb{C}^X$  hides H if:

- f constant on left cosets of H

- 
$$f(a) \perp f(b)$$
 if  $aH \neq bH$ 

イロン イヨン イヨン イヨン

3

The Hidden Subgroup Problem Coset states Abelian Fourier sampling Applications of abelian HSP

### Remarks on Abelian Fourier Sampling

- No need of measuring the value of f
- f can be quantum-state valued:

 $f: G \to \mathbb{C}^X$  hides H if:

- f constant on left cosets of H
- $f(a) \perp f(b)$  if  $aH \neq bH$ Fourier sampling finds H efficiently if G abelian and f hides H.

イロト イポト イヨト イヨト

The Hidden Subgroup Problem Coset states Abelian Fourier sampling Applications of abelian HSP

### Remarks on Abelian Fourier Sampling

- No need of measuring the value of f
- f can be quantum-state valued:

 $f: G \to \mathbb{C}^X$  hides H if:

- f constant on left cosets of H
- $f(a) \perp f(b)$  if  $aH \neq bH$ Fourier sampling finds H efficiently if G abelian and f hides H.
- Even the function f can be different in different steps,

イロト イポト イヨト イヨト

The Hidden Subgroup Problem Coset states Abelian Fourier sampling Applications of abelian HSP

#### Remarks on Abelian Fourier Sampling

- No need of measuring the value of f
- f can be quantum-state valued:

 $f: G \to \mathbb{C}^X$  hides H if:

- f constant on left cosets of H
- $f(a) \perp f(b)$  if  $aH \neq bH$ Fourier sampling finds H efficiently if G abelian and f hides H.

#### • Even the function f can be different in different steps,

they only must hide the same H.

イロト イポト イヨト イヨト

Simon's algorithm	The Hidden Subgroup Problem
Basic tools	Coset states
The HSP	Abelian Fourier sampling
Infinite abelian HSPs	Applications of abelian HSP

• Group element order finding:  $f(k) = a^k$  (A group,  $a \in A$ )

(日) (四) (王) (王) (王)

Simon's algorithm	The Hidden Subgroup Problem
Basic tools	Coset states
The HSP	Abelian Fourier sampling
Infinite abelian HSPs	Applications of abelian HSP

- Group element order finding:  $f(k) = a^k$  (A group,  $a \in A$ )
- Discrete logarithm

Simon's algorithm	The Hidden Subgroup Problem
Basic tools	Coset states
The HSP	Abelian Fourier sampling
Infinite abelian HSPs	Applications of abelian HSP

- Group element order finding:  $f(k) = a^k$  (A group,  $a \in A$ )
- Discrete logarithm
  - $\rightarrow$  breaking many cryptosystems

・ 回 と ・ ヨ と ・ ヨ と

3

Simon's algorithm	The Hidden Subgroup Problem
Basic tools	Coset states
The HSP	Abelian Fourier sampling
Infinite abelian HSPs	Applications of abelian HSP

- Group element order finding:  $f(k) = a^k$  (A group,  $a \in A$ )
- Discrete logarithm
  - $\rightarrow$  breaking many cryptosystems
- Generalized discrete log:

(4回) (4回) (4回)

Simon's algorithm	The Hidden Subgroup Problem
Basic tools	Coset states
The HSP	Abelian Fourier sampling
Infinite abelian HSPs	Applications of abelian HSP

- Group element order finding:  $f(k) = a^k$  (A group,  $a \in A$ )
- Discrete logarithm
  - $\rightarrow$  breaking many cryptosystems
- Generalized discrete log:

a.k.a. constructive membership in abelian black box groups

(4回) (4回) (4回)

Simon's algorithm	The Hidden Subgroup Problem
Basic tools	Coset states
The HSP	Abelian Fourier sampling
Infinite abelian HSPs	Applications of abelian HSP

- Group element order finding:  $f(k) = a^k$  (A group,  $a \in A$ )
- Discrete logarithm
  - $\rightarrow$  breaking many cryptosystems
- Generalized discrete log:

a.k.a. constructive membership in abelian black box groups  $a_1, \ldots, a_n, b \in A$ , express b as:

$$b=\prod_{i=1}^n a_i^{k_i}$$

▲□→ ▲ 国 → ▲ 国 →

3

Simon's algorithm	The Hidden Subgroup Problem
Basic tools	Coset states
The HSP	Abelian Fourier sampling
Infinite abelian HSPs	Applications of abelian HSP

- Group element order finding:  $f(k) = a^k$  (A group,  $a \in A$ )
- Discrete logarithm
  - $\rightarrow$  breaking many cryptosystems
- Generalized discrete log:

a.k.a. constructive membership in abelian black box groups  $a_1, \ldots, a_n, b \in A$ , express b as:

$$b = \prod_{i=1}^n a_i^{k_i}$$

Classically difficult, even in the exponent 2 case

(日本) (日本) (日本)

The Hidden Subgroup Problem Coset states Abelian Fourier sampling Applications of abelian HSP

#### Generalized discrete log as HSP

•  $a_1,\ldots,a_n,b\in A$ ,

・ロト ・回ト ・ヨト ・ヨト

#### Generalized discrete log as HSP

- $a_1,\ldots,a_n,b\in A$ ,
- $m_i$ : order of  $a_i$ , m: order of b

・ロン ・回と ・ヨン・

#### Generalized discrete log as HSP

- $a_1,\ldots,a_n,b\in A$ ,
- $m_i$ : order of  $a_i$ , m: order of b

group

$$G = \mathbb{Z}_m \oplus \bigoplus_{i=1}^n \mathbb{Z}_{m_i}$$

・ロン ・回と ・ヨン ・ヨン

#### Generalized discrete log as HSP

- $a_1,\ldots,a_n,b\in A$ ,
- $m_i$ : order of  $a_i$ , m: order of b

group

$$G = \mathbb{Z}_m \oplus \bigoplus_{i=1}^n \mathbb{Z}_{m_i}$$

hiding function

$$f(\ell,\ell_1,\ldots,\ell_n)=b^{-\ell}\prod_{i=1}^na_i^{\ell_i}$$

・ロン ・回と ・ヨン・

#### Generalized discrete log as HSP

- $a_1,\ldots,a_n,b\in A$ ,
- $m_i$ : order of  $a_i$ , m: order of b

group

$$G = \mathbb{Z}_m \oplus \bigoplus_{i=1}^n \mathbb{Z}_{m_i}$$

hiding function

$$f(\ell,\ell_1,\ldots,\ell_n)=b^{-\ell}\prod_{i=1}^n a_i^{\ell_i}$$

hidden subgroup

$$H = \begin{cases} \langle 1, k_1, \dots, k_n \rangle & \text{if } b = \prod_{i=1}^n a_i^{k_i} \\ \{0\} & \text{otherwise.} \end{cases}$$

イロン イヨン イヨン イヨン

3

#### Applications 2

• Computing the structure of finite abelian black box groups (Cheung and Mosca 2001)

・ロン ・回と ・ヨン・

### Applications 2

• Computing the structure of finite abelian black box groups (Cheung and Mosca 2001)

classically even approximating the order is difficult

<ロ> (日) (日) (日) (日) (日)

Simon's algorithm Basic tools The HSP Infinite abelian HSPs Applications of abelian HSP

# Applications 2

- Computing the structure of finite abelian black box groups (Cheung and Mosca 2001)
  - classically even approximating the order is difficult
- Computing with solvable (and more) black box groups

イロト イポト イヨト イヨト

3

# Applications 2

• Computing the structure of finite abelian black box groups (Cheung and Mosca 2001)

classically even approximating the order is difficult

- Computing with solvable (and more) black box groups
  - Watrous (solvable)

イロン イヨン イヨン イヨン

3

# Applications 2

• Computing the structure of finite abelian black box groups (Cheung and Mosca 2001)

classically even approximating the order is difficult

- Computing with solvable (and more) black box groups
  - Watrous (solvable)

Based on uniform superposition  $|G\rangle = \sum_{g \in G} |g\rangle$ 

イロト イヨト イヨト イヨト

# Applications 2

• Computing the structure of finite abelian black box groups (Cheung and Mosca 2001)

classically even approximating the order is difficult

- Computing with solvable (and more) black box groups
  - Watrous (solvable)

Based on uniform superposition  $|G\rangle = \sum_{g \in G} |g\rangle$ 

• Beals and Babai (solvable+more)

# Applications 2

• Computing the structure of finite abelian black box groups (Cheung and Mosca 2001)

classically even approximating the order is difficult

- Computing with solvable (and more) black box groups
  - Watrous (solvable)

Based on uniform superposition  $|{\it G}\rangle = \sum_{{\it g} \in {\it G}} |{\it g}\rangle$ 

• Beals and Babai (solvable+more)

Classical, with oracles for factoring and

# Applications 2

• Computing the structure of finite abelian black box groups (Cheung and Mosca 2001)

classically even approximating the order is difficult

- Computing with solvable (and more) black box groups
  - Watrous (solvable)

Based on uniform superposition  $|G\rangle = \sum_{g \in G} |g\rangle$ 

• Beals and Babai (solvable+more)

Classical, with oracles for factoring and constructive membership in abelian subgroups

# Applications 2

• Computing the structure of finite abelian black box groups (Cheung and Mosca 2001)

classically even approximating the order is difficult

- Computing with solvable (and more) black box groups
  - Watrous (solvable)

Based on uniform superposition  $|{\it G}\rangle = \sum_{{\it g} \in {\it G}} |{\it g}\rangle$ 

• Beals and Babai (solvable+more) Classical, with oracles for factoring and

constructive membership in abelian subgroups

 $\downarrow \qquad ({\rm noticed \ in }\sim, {\rm Magniez, \ Santha \ 2001}) \\ {\rm hidden \ normal \ subgroups \ in \ such \ groups}$ 

イロト イヨト イヨト イヨト

# Applications 2

• Computing the structure of finite abelian black box groups (Cheung and Mosca 2001)

classically even approximating the order is difficult

- Computing with solvable (and more) black box groups
  - Watrous (solvable)

Based on uniform superposition  $|{\it G}\rangle = \sum_{{\it g} \in {\it G}} |{\it g}\rangle$ 

• Beals and Babai (solvable+more)

Classical, with oracles for factoring and constructive membership in abelian subgroups

- $\downarrow$  (noticed in  $\sim$ , Magniez, Santha 2001)
- hidden normal subgroups in such groups
- Probably normal HSP in other cases (Ákos)

Simon's algorithm The Hidden Subgroup Probler Basic tools Coset states The HSP Abelian Fourier sampling Infinite abelian HSPs Applications of abelian HSP

## Factoring — order finding

• Order finding in  $\mathbb{Z}_n^*$ :  $a \in \mathbb{Z}_n^*$ 

・ロト ・回ト ・ヨト ・ヨト

The Hidden Subgroup Problem Coset states Abelian Fourier sampling Applications of abelian HSP

### Factoring — order finding

• Order finding in  $\mathbb{Z}_n^*$ :  $a \in \mathbb{Z}_n^*$ o(a)=smallest r:  $a^r \equiv 1 \pmod{n}$ 

・ロン ・回と ・ヨン ・ヨン

The Hidden Subgroup Problem Coset states Abelian Fourier sampling Applications of abelian HSP

### Factoring — order finding

- Order finding in  $\mathbb{Z}_n^*$ :  $a \in \mathbb{Z}_n^*$ o(a)=smallest r:  $a^r \equiv 1 \pmod{n}$
- Assume *n* odd, not a prime power

イロン 不同と 不同と 不同と

The Hidden Subgroup Problem Coset states Abelian Fourier sampling Applications of abelian HSP

## Factoring — order finding

- Order finding in  $\mathbb{Z}_n^*$ :  $a \in \mathbb{Z}_n^*$ o(a)=smallest r:  $a^r \equiv 1 \pmod{n}$
- Assume *n* odd, not a prime power
- For random  $a \in \mathbb{Z}_n^*$ , with probability  $\geq \frac{1}{4}$

イロン 不同と 不同と 不同と

The Hidden Subgroup Problem Coset states Abelian Fourier sampling Applications of abelian HSP

## Factoring — order finding

- Order finding in  $\mathbb{Z}_n^*$ :  $a \in \mathbb{Z}_n^*$ o(a)=smallest r:  $a^r \equiv 1 \pmod{n}$
- Assume *n* odd, not a prime power
- For random  $a \in \mathbb{Z}_n^*$ , with probability  $\geq \frac{1}{4}$

- *o*(*a*) even,

・ロン ・回と ・ヨン・

3

The Hidden Subgroup Problem Coset states Abelian Fourier sampling Applications of abelian HSP

### Factoring — order finding

- Order finding in  $\mathbb{Z}_n^*$ :  $a \in \mathbb{Z}_n^*$ o(a)=smallest r:  $a^r \equiv 1 \pmod{n}$
- Assume *n* odd, not a prime power
- For random  $a \in \mathbb{Z}_n^*$ , with probability  $\geq \frac{1}{4}$ 
  - o(a) even, -  $b = a^{\frac{o(a)}{2}} \not\equiv \pm 1 \pmod{n}$ , but  $b^2 \equiv 1$ :

・ロン ・回と ・ヨン・

The Hidden Subgroup Problem Coset states Abelian Fourier sampling Applications of abelian HSP

### Factoring — order finding

∜

- Order finding in  $\mathbb{Z}_n^*$ :  $a \in \mathbb{Z}_n^*$ o(a)=smallest r:  $a^r \equiv 1 \pmod{n}$
- Assume *n* odd, not a prime power
- For random  $a \in \mathbb{Z}_n^*$ , with probability  $\geq \frac{1}{4}$ 
  - o(a) even, -  $b = a^{\frac{o(a)}{2}} \not\equiv \pm 1 \pmod{n}$ , but  $b^2 \equiv 1$ :

・ロン ・回と ・ヨン・

The Hidden Subgroup Problem Coset states Abelian Fourier sampling Applications of abelian HSP

# Factoring — order finding

∜

• Order finding in 
$$\mathbb{Z}_n^*$$
:  $a \in \mathbb{Z}_n^*$   
 $o(a)=$ smallest  $r$ :  $a^r \equiv 1 \pmod{n}$ 

- Assume *n* odd, not a prime power
- For random  $a \in \mathbb{Z}_n^*$ , with probability  $\geq \frac{1}{4}$

- 
$$o(a)$$
 even,  
-  $b = a^{\frac{o(a)}{2}} \not\equiv \pm 1 \pmod{n}$ , but  $b^2 \equiv 1$ :

$$gcd(b-1, n)$$
 a proper factor of  $n$ .

・ロト ・回ト ・ヨト ・ヨト

The Hidden Subgroup Problem Coset states Abelian Fourier sampling Applications of abelian HSP

#### Discrete log - limitations

• No efficient equality-test based discrete log

・ロン ・回と ・ヨン・

The Hidden Subgroup Problem Coset states Abelian Fourier sampling Applications of abelian HSP

#### Discrete log - limitations

• No efficient equality-test based discrete log

•  $A = \mathbb{Z}_p \times \mathbb{Z}_p$ 

・ロン ・回と ・ヨン・

The Hidden Subgroup Problem Coset states Abelian Fourier sampling Applications of abelian HSP

#### Discrete log - limitations

• No efficient equality-test based discrete log

• 
$$A = \mathbb{Z}_p \times \mathbb{Z}_p$$

• Secret:  $u \in \mathbb{Z}_p^*$ 

・ロン ・回と ・ヨン・

The Hidden Subgroup Problem Coset states Abelian Fourier sampling Applications of abelian HSP

#### Discrete log - limitations

- No efficient equality-test based discrete log
  - $A = \mathbb{Z}_p \times \mathbb{Z}_p$
  - Secret:  $u \in \mathbb{Z}_p^*$
  - Subgroup  $U = \{(x, ux) | x \in \mathbb{Z}_p\}$

イロト イヨト イヨト イヨト

The Hidden Subgroup Problem Coset states Abelian Fourier sampling Applications of abelian HSP

#### Discrete log - limitations

• No efficient equality-test based discrete log

- $A = \mathbb{Z}_p \times \mathbb{Z}_p$
- Secret:  $u \in \mathbb{Z}_p^*$
- Subgroup  $U = \{(x, ux) | x \in \mathbb{Z}_p\}$
- G = A/U: encoding and + in A;

- - 4 回 ト - 4 回 ト

The Hidden Subgroup Problem Coset states Abelian Fourier sampling Applications of abelian HSP

# Discrete log - limitations

• No efficient equality-test based discrete log

- $A = \mathbb{Z}_p \times \mathbb{Z}_p$
- Secret:  $u \in \mathbb{Z}_p^*$
- Subgroup  $U \stackrel{r}{=} \{(x, ux) | x \in \mathbb{Z}_p\}$
- G = A/U: encoding and + in A; equality test (membership in U) by black box

イロン イヨン イヨン イヨン

3

The Hidden Subgroup Problem Coset states Abelian Fourier sampling Applications of abelian HSP

# Discrete log - limitations

• No efficient equality-test based discrete log

- $A = \mathbb{Z}_p \times \mathbb{Z}_p$
- Secret:  $u \in \mathbb{Z}_p^*$
- Subgroup  $U = \{(x, ux) | x \in \mathbb{Z}_p\}$
- G = A/U: encoding and + in A; equality test (membership in U) by black box
- Property:

$$\log_{(0,1)}(-1,0) = \ell \Leftrightarrow (1,0) + \ell(0,1) \in U \Leftrightarrow \ell = u$$

イロン イヨン イヨン イヨン

The Hidden Subgroup Problem Coset states Abelian Fourier sampling Applications of abelian HSP

# Discrete log - limitations

• No efficient equality-test based discrete log

- $A = \mathbb{Z}_p \times \mathbb{Z}_p$
- Secret:  $u \in \mathbb{Z}_p^*$
- Subgroup  $U \stackrel{r}{=} \{(x, ux) | x \in \mathbb{Z}_p\}$
- G = A/U: encoding and + in A; equality test (membership in U) by black box
- Property:

 $\log_{(0,1)}(-1,0) = \ell \Leftrightarrow (1,0) + \ell(0,1) \in U \Leftrightarrow \ell = u$ 

• Gives reduction from (quantum) search

イロン イヨン イヨン イヨン

The Hidden Subgroup Problem Coset states Abelian Fourier sampling Applications of abelian HSP

# Discrete log - limitations

• No efficient equality-test based discrete log

- $A = \mathbb{Z}_p \times \mathbb{Z}_p$
- Secret:  $u \in \mathbb{Z}_p^*$
- Subgroup  $U \stackrel{r}{=} \{(x, ux) | x \in \mathbb{Z}_p\}$
- G = A/U: encoding and + in A; equality test (membership in U) by black box
- Property:

 $\log_{(0,1)}(-1,0) = \ell \Leftrightarrow (1,0) + \ell(0,1) \in U \Leftrightarrow \ell = u$ 

- Gives reduction from (quantum) search lower bound  $\Omega(\sqrt{p})$  quantum queries

イロン イヨン イヨン イヨン

The Hidden Subgroup Problem Coset states Abelian Fourier sampling Applications of abelian HSP

# Discrete log - limitations

• No efficient equality-test based discrete log

- $A = \mathbb{Z}_p \times \mathbb{Z}_p$
- Secret:  $u \in \mathbb{Z}_p^*$
- Subgroup  $U \stackrel{r}{=} \{(x, ux) | x \in \mathbb{Z}_p\}$
- G = A/U: encoding and + in A; equality test (membership in U) by black box
- Property:

 $\log_{(0,1)}(-1,0) = \ell \Leftrightarrow (1,0) + \ell(0,1) \in U \Leftrightarrow \ell = u$ 

- Gives reduction from (quantum) search lower bound  $\Omega(\sqrt{p})$  quantum queries
- Open: Complexity of equality-test-based order finding?

イロト イポト イヨト イヨト

Simon's algorithm Basic tools The HSP Infinite abelian HSPs Open problems

# Contents

- **1** Simon's algorithm
- 2 Basic tools
  - QFT mod powers of 2
  - Phase estimation
  - Period finding
  - QFT over abelian groups
- 3 The HSP
  - The Hidden Subgroup Problem
  - Coset states
  - Abelian Fourier sampling
  - Applications of abelian HSP
- Infinite abelian HSPs
  - HSP in lattices
  - Units in number fields and hidden lattices
  - Open problems

<回と < 目と < 目と

HSP in lattices Units in number fields and hidden lattices Open problems

<ロ> (四) (四) (三) (三) (三)

#### HSP in $\mathbb{Z}^n$

#### • $G = \mathbb{Z}^n$ , $f : G \to \{0, 1\}^s$

Gábor Ivanyos MTA SZTAKI Fast Quantum Algorithms Lectures 1 and 2

HSP in lattices Units in number fields and hidden lattices Open problems

◆□> ◆□> ◆注> ◆注> 二注:

• 
$$G = \mathbb{Z}^n$$
,  $f : G \to \{0, 1\}^s$   
 $f(x) = f(y) \Leftrightarrow x - y \in H$ 

HSP in lattices Units in number fields and hidden lattices Open problems

<ロ> (四) (四) (三) (三) (三)

• 
$$G = \mathbb{Z}^n$$
,  $f : G \to \{0, 1\}^s$   
 $f(x) = f(y) \Leftrightarrow x - y \in H$   
•  $|G : H| \le 2^s \Rightarrow H \ge$  rectangular lattice K,

HSP in lattices Units in number fields and hidden lattices Open problems

<ロ> (四) (四) (注) (注) (三)

HSP in lattices Units in number fields and hidden lattices Open problems

<ロ> (四) (四) (注) (注) (三)

HSP in lattices Units in number fields and hidden lattices Open problems

◆□> ◆□> ◆注> ◆注> 二注:

HSP in lattices Units in number fields and hidden lattices Open problems

◆□> ◆□> ◆注> ◆注> 二注:

HSP in lattices Units in number fields and hidden lattices Open problems

・ロト ・回 ト ・ヨト ・ヨー

## HSP in $\mathbb{Z}^n$

• Find  $H_1, H_2, \ldots, H_n$  by Shor's algorithm/phase estimation

HSP in lattices Units in number fields and hidden lattices Open problems

◆□ > ◆□ > ◆臣 > ◆臣 > ─臣 ─のへで

HSP in lattices Units in number fields and hidden lattices Open problems

<ロ> (四) (四) (三) (三) (三)

## HSP in $\mathbb{Z}^n$

• f constant on  $H \Rightarrow$  well defined on  $\mathbb{Z}^n/K$ 

HSP in lattices Units in number fields and hidden lattices Open problems

(ロ) (四) (E) (E) (E)

## HSP in $\mathbb{Z}^n$

• hides H/K in finite  $\mathbb{Z}^n/K$ 

HSP in lattices Units in number fields and hidden lattices Open problems

<ロ> (四) (四) (三) (三) (三)

## Units in number fields

• K number field

HSP in lattices Units in number fields and hidden lattices Open problems

(日) (四) (王) (王) (王)

- K number field
  - given by  $f(x) \in \mathbb{Q}[x]$  irred., deg f = m,  $K \cong \mathbb{Q}[x]/(f(x))$

HSP in lattices Units in number fields and hidden lattices Open problems

#### Units in number fields

#### • K number field

- given by  $f(x) \in \mathbb{Q}[x]$  irred., deg f = m,  $K \cong \mathbb{Q}[x]/(f(x))$
- standard repr. of elements: polynomials modulo f

・ロン ・回 と ・ 回 と ・ 回 と

3

HSP in lattices Units in number fields and hidden lattices Open problems

イロト イヨト イヨト イヨト

3

- K number field
  - given by  $f(x) \in \mathbb{Q}[x]$  irred., deg f = m,  $K \cong \mathbb{Q}[x]/(f(x))$
  - standard repr. of elements: polynomials modulo f
- $\mathcal{O}$  ring of algebraic integers in K

HSP in lattices Units in number fields and hidden lattices Open problems

## Units in number fields

- K number field
  - given by  $f(x) \in \mathbb{Q}[x]$  irred., deg f = m,  $K \cong \mathbb{Q}[x]/(f(x))$
  - standard repr. of elements: polynomials modulo f
- $\mathcal{O}$  ring of algebraic integers in K
- unit group:  $\mathcal{O}^* = \{x \in \mathcal{O} | x^{-1} \in \mathcal{O}\}$

イロト イヨト イヨト イヨト

3

HSP in lattices Units in number fields and hidden lattices Open problems

イロト イポト イヨト イヨト

3

- K number field
  - given by  $f(x) \in \mathbb{Q}[x]$  irred., deg f = m,  $K \cong \mathbb{Q}[x]/(f(x))$
  - standard repr. of elements: polynomials modulo f
- $\mathcal{O}$  ring of algebraic integers in K
- unit group:  $\mathcal{O}^* = \{x \in \mathcal{O} | x^{-1} \in \mathcal{O}\}$
- Dirichlet's unit theorem:  $\mathcal{O}^* \cong \mathbb{Z}_s \times \mathbb{Z}^r$ ,

HSP in lattices Units in number fields and hidden lattices Open problems

イロト イポト イヨト イヨト

3

- K number field
  - given by  $f(x) \in \mathbb{Q}[x]$  irred., deg f = m,  $K \cong \mathbb{Q}[x]/(f(x))$
  - standard repr. of elements: polynomials modulo f
- $\mathcal{O}$  ring of algebraic integers in K
- unit group:  $\mathcal{O}^* = \{x \in \mathcal{O} | x^{-1} \in \mathcal{O}\}$
- Dirichlet's unit theorem:  $\mathcal{O}^* \cong \mathbb{Z}_s \times \mathbb{Z}^r$ ,
  - s largest s.t.  $\sqrt[s]{1} \in K$ ,

HSP in lattices Units in number fields and hidden lattices Open problems

イロト イポト イヨト イヨト

3

- K number field
  - given by  $f(x) \in \mathbb{Q}[x]$  irred., deg f = m,  $K \cong \mathbb{Q}[x]/(f(x))$
  - standard repr. of elements: polynomials modulo f
- $\mathcal{O}$  ring of algebraic integers in K
- unit group:  $\mathcal{O}^* = \{x \in \mathcal{O} | x^{-1} \in \mathcal{O}\}$
- Dirichlet's unit theorem:  $\mathcal{O}^* \cong \mathbb{Z}_s \times \mathbb{Z}^r$ ,
  - s largest s.t.  $\sqrt[s]{1} \in K$ ,
  - f(x) has  $r_1$  real,  $2r_2$  imaginary roots

HSP in lattices Units in number fields and hidden lattices Open problems

イロト イポト イヨト イヨト

3

- K number field
  - given by  $f(x) \in \mathbb{Q}[x]$  irred., deg f = m,  $K \cong \mathbb{Q}[x]/(f(x))$
  - standard repr. of elements: polynomials modulo f
- $\mathcal{O}$  ring of algebraic integers in K
- unit group:  $\mathcal{O}^* = \{x \in \mathcal{O} | x^{-1} \in \mathcal{O}\}$
- Dirichlet's unit theorem:  $\mathcal{O}^* \cong \mathbb{Z}_s \times \mathbb{Z}^r$ ,
  - s largest s.t.  $\sqrt[s]{1} \in K$ ,
  - f(x) has  $r_1$  real,  $2r_2$  imaginary roots

• 
$$r = r_1 + r_2 - 1$$

HSP in lattices Units in number fields and hidden lattices Open problems

イロト イポト イヨト イヨト

## Units in number fields

- K number field
  - given by  $f(x) \in \mathbb{Q}[x]$  irred., deg f = m,  $K \cong \mathbb{Q}[x]/(f(x))$
  - standard repr. of elements: polynomials modulo f
- $\mathcal{O}$  ring of algebraic integers in K
- unit group:  $\mathcal{O}^* = \{x \in \mathcal{O} | x^{-1} \in \mathcal{O}\}$
- Dirichlet's unit theorem:  $\mathcal{O}^* \cong \mathbb{Z}_s \times \mathbb{Z}^r$ ,
  - s largest s.t.  $\sqrt[s]{1} \in K$ ,
  - f(x) has  $r_1$  real,  $2r_2$  imaginary roots

• 
$$r = r_1 + r_2 - 1$$

• Task find basis for (free part of)  $\mathcal{O}^*$ 

HSP in lattices Units in number fields and hidden lattices Open problems

イロト イポト イヨト イヨト

- K number field
  - given by  $f(x) \in \mathbb{Q}[x]$  irred., deg f = m,  $K \cong \mathbb{Q}[x]/(f(x))$
  - standard repr. of elements: polynomials modulo f
- $\mathcal{O}$  ring of algebraic integers in K
- unit group:  $\mathcal{O}^* = \{x \in \mathcal{O} | x^{-1} \in \mathcal{O}\}$
- Dirichlet's unit theorem:  $\mathcal{O}^* \cong \mathbb{Z}_s \times \mathbb{Z}^r$ ,
  - s largest s.t.  $\sqrt[s]{1} \in K$ ,
  - f(x) has  $r_1$  real,  $2r_2$  imaginary roots

• 
$$r = r_1 + r_2 - 1$$

- Task find basis for (free part of)  $\mathcal{O}^*$
- finding  $\sqrt[s]{1} \in K$  easy (deterministic poly time)

HSP in lattices Units in number fields and hidden lattices Open problems

(日) (四) (王) (王) (王)

# Unit groups - naive HSP approach

•  $G = K^*$ ;  $F(x) = xO = \{xy | y \in O\}$  principal fractional ideal

HSP in lattices Units in number fields and hidden lattices Open problems

3

- $G = K^*$ ;  $F(x) = xO = \{xy | y \in O\}$  principal fractional ideal
- hidden subgroup is  $\mathcal{O}^*$ :  $F(x) = F(y) \Leftrightarrow x^{-1}y \in \mathcal{O}^*$ .

HSP in lattices Units in number fields and hidden lattices Open problems

3

- $G = K^*$ ;  $F(x) = xO = \{xy | y \in O\}$  principal fractional ideal
- hidden subgroup is  $\mathcal{O}^*$ :  $F(x) = F(y) \Leftrightarrow x^{-1}y \in \mathcal{O}^*$ .
- Difficulties:

HSP in lattices Units in number fields and hidden lattices Open problems

イロト イポト イヨト イヨト

3

- $G = K^*$ ;  $F(x) = xO = \{xy | y \in O\}$  principal fractional ideal
- hidden subgroup is  $\mathcal{O}^*$ :  $F(x) = F(y) \Leftrightarrow x^{-1}y \in \mathcal{O}^*$ .
- Difficulties:
  - encoding of fractional ideals

HSP in lattices Units in number fields and hidden lattices Open problems

イロト イポト イヨト イヨト

3

# Unit groups - naive HSP approach

- $G = K^*$ ;  $F(x) = xO = \{xy | y \in O\}$  principal fractional ideal
- hidden subgroup is  $\mathcal{O}^*$ :  $F(x) = F(y) \Leftrightarrow x^{-1}y \in \mathcal{O}^*$ .
- Difficulties:
  - encoding of fractional ideals

-factorization into powers of prime ideals

HSP in lattices Units in number fields and hidden lattices Open problems

・ロト ・回ト ・ヨト ・ヨト

3

- $G = K^*$ ;  $F(x) = xO = \{xy | y \in O\}$  principal fractional ideal
- hidden subgroup is  $\mathcal{O}^*$ :  $F(x) = F(y) \Leftrightarrow x^{-1}y \in \mathcal{O}^*$ .
- Difficulties:
  - encoding of fractional ideals
    - -factorization into powers of prime ideals
    - -Hermite normal form (HNF): special basis, can be large

HSP in lattices Units in number fields and hidden lattices Open problems

・ロン ・回と ・ヨン ・ヨン

3

- $G = K^*$ ;  $F(x) = xO = \{xy | y \in O\}$  principal fractional ideal
- hidden subgroup is  $\mathcal{O}^*$ :  $F(x) = F(y) \Leftrightarrow x^{-1}y \in \mathcal{O}^*$ .
- Difficulties:
  - encoding of fractional ideals
    - -factorization into powers of prime ideals
    - -Hermite normal form (HNF): special basis, can be large
  - K\* infinitely generated

HSP in lattices Units in number fields and hidden lattices Open problems

イロト イポト イヨト イヨト

3

- $G = K^*$ ;  $F(x) = xO = \{xy | y \in O\}$  principal fractional ideal
- hidden subgroup is  $\mathcal{O}^*$ :  $F(x) = F(y) \Leftrightarrow x^{-1}y \in \mathcal{O}^*$ .
- Difficulties:
  - encoding of fractional ideals
    - -factorization into powers of prime ideals
    - -Hermite normal form (HNF): special basis, can be large
  - K\* infinitely generated
    - not known how to find a "small" piece containing the units

HSP in lattices Units in number fields and hidden lattices Open problems

イロト イポト イヨト イヨト

3

- $G = K^*$ ;  $F(x) = xO = \{xy | y \in O\}$  principal fractional ideal
- hidden subgroup is  $\mathcal{O}^*$ :  $F(x) = F(y) \Leftrightarrow x^{-1}y \in \mathcal{O}^*$ .
- Difficulties:
  - encoding of fractional ideals
    - -factorization into powers of prime ideals
    - -Hermite normal form (HNF): special basis, can be large
  - K\* infinitely generated
    - not known how to find a "small" piece containing the units
  - generators may have exponential size

HSP in lattices Units in number fields and hidden lattices Open problems

・ロト ・回ト ・ヨト ・ヨト

3

- $G = K^*$ ;  $F(x) = xO = \{xy | y \in O\}$  principal fractional ideal
- hidden subgroup is  $\mathcal{O}^*$ :  $F(x) = F(y) \Leftrightarrow x^{-1}y \in \mathcal{O}^*$ .
- Difficulties:
  - encoding of fractional ideals
    - -factorization into powers of prime ideals
    - -Hermite normal form (HNF): special basis, can be large
  - K\* infinitely generated
    - not known how to find a "small" piece containing the units
  - generators may have exponential size using usual representations

HSP in lattices Units in number fields and hidden lattices Open problems

イロト イポト イヨト イヨト

- $G = K^*$ ;  $F(x) = xO = \{xy | y \in O\}$  principal fractional ideal
- hidden subgroup is  $\mathcal{O}^*$ :  $F(x) = F(y) \Leftrightarrow x^{-1}y \in \mathcal{O}^*$ .
- Difficulties:
  - encoding of fractional ideals
    - -factorization into powers of prime ideals
    - -Hermite normal form (HNF): special basis, can be large
  - K\* infinitely generated
    - not known how to find a "small" piece containing the units
  - generators may have exponential size using usual representations
  - Solution: "compact representations" (Thiel 95)

HSP in lattices Units in number fields and hidden lattices Open problems

イロト イポト イヨト イヨト

- $G = K^*$ ;  $F(x) = xO = \{xy | y \in O\}$  principal fractional ideal
- hidden subgroup is  $\mathcal{O}^*$ :  $F(x) = F(y) \Leftrightarrow x^{-1}y \in \mathcal{O}^*$ .
- Difficulties:
  - encoding of fractional ideals
    - -factorization into powers of prime ideals
    - -Hermite normal form (HNF): special basis, can be large
  - K\* infinitely generated
    - not known how to find a "small" piece containing the units
  - generators may have exponential size using usual representations
  - Solution: "compact representations" (Thiel 95) special straight-line programs

HSP in lattices Units in number fields and hidden lattices Open problems

・ロン ・回 と ・ 回 と ・ 回 と

æ

## Unit groups - the Log map

•  $K = \mathbb{Q}[\alpha] = \mathbb{Q}[x]/(f(x))$ 

Gábor Ivanyos MTA SZTAKI Fast Quantum Algorithms Lectures 1 and 2

HSP in lattices Units in number fields and hidden lattices Open problems

・ロン ・回 と ・ ヨ と ・ ヨ と

3

# Unit groups - the Log map

- $K = \mathbb{Q}[\alpha] = \mathbb{Q}[x]/(f(x))$
- Roots of  $f(x) \alpha_1, \ldots, \alpha_{r_1}$  (real)

HSP in lattices Units in number fields and hidden lattices Open problems

◆□▶ ◆□▶ ◆目▶ ◆目▶ ●目 - のへで

## Unit groups - the Log map

- $K = \mathbb{Q}[\alpha] = \mathbb{Q}[x]/(f(x))$
- Roots of  $f(x) \alpha_1, \ldots, \alpha_{r_1}$  (real)
  - $\alpha_{r_1+1}, \overline{\alpha_{r_1+1}}, \dots, \alpha_{r_1+r_2}, \overline{\alpha_{r_1+r_2}}$  (imaginary)

HSP in lattices Units in number fields and hidden lattices Open problems

# Unit groups - the Log map

• 
$$K = \mathbb{Q}[\alpha] = \mathbb{Q}[x]/(f(x))$$

• Roots of 
$$f(x) \alpha_1, \dots, \alpha_{r_1}$$
 (real)  
 $\alpha_{r_1+1}, \overline{\alpha_{r_1+1}}, \dots, \alpha_{r_1+r_2}, \overline{\alpha_{r_1+r_2}}$  (imaginary)

• absolute values  $y = g(\alpha) \in K$ ,  $|y|_i = |g(\alpha_i)|$ 

HSP in lattices Units in number fields and hidden lattices Open problems

・ロン ・回 と ・ ヨ と ・ ヨ と

3

## Unit groups - the Log map

• 
$$K = \mathbb{Q}[\alpha] = \mathbb{Q}[x]/(f(x))$$

 $r_1 + r_2$  achimedean absolute values

HSP in lattices Units in number fields and hidden lattices Open problems

(日) (四) (王) (王) (王)

# Unit groups - the Log map

• 
$$K = \mathbb{Q}[\alpha] = \mathbb{Q}[x]/(f(x))$$
  
• Roots of  $f(x) \alpha_1, \dots, \alpha_{r_1}$  (real)  
 $\alpha_{r_1+1}, \overline{\alpha_{r_1+1}}, \dots, \alpha_{r_1+r_2}, \overline{\alpha_{r_1+r_2}}$  (imaginary)  
• absolute values  $y = g(\alpha) \in K$ ,  $|y|_i = |g(\alpha_i)|$   
 $r_1 + r_2$  achimedean absolute values  
 $\text{Log} : K^* \to \mathbb{R}^r \ y \mapsto \log |y|_1, \dots, \log |y|_r$   $(r = r_1 + r_2 - 1)$ 

HSP in lattices Units in number fields and hidden lattices Open problems

< □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □

# Unit groups - the Log map

• 
$$K = \mathbb{Q}[\alpha] = \mathbb{Q}[x]/(f(x))$$
  
• Roots of  $f(x) \alpha_1, \dots, \alpha_{r_1}$  (real)  
 $\alpha_{r_1+1}, \overline{\alpha_{r_1+1}}, \dots, \alpha_{r_1+r_2}, \overline{\alpha_{r_1+r_2}}$  (imaginary)  
• absolute values  $y = g(\alpha) \in K$ ,  $|y|_i = |g(\alpha_i)|$   
 $r_1 + r_2$  achimedean absolute values  
 $\text{Log} : K^* \to \mathbb{R}^r \ y \mapsto \log |y|_1, \dots, \log |y|_r$   $(r = r_1 + r_2 - 1)$   
• Dirichlet:  $\text{Log}(\mathcal{O}^*)$  full lattice in  $\mathbb{R}^r$ .

HSP in lattices Units in number fields and hidden lattices Open problems

æ

# Unit groups - the Log map

• 
$$\mathcal{K} = \mathbb{Q}[\alpha] = \mathbb{Q}[x]/(f(x))$$
  
• Roots of  $f(x) \alpha_1, \dots, \alpha_{r_1}$  (real)  
 $\alpha_{r_1+1}, \overline{\alpha_{r_1+1}}, \dots, \alpha_{r_1+r_2}, \overline{\alpha_{r_1+r_2}}$  (imaginary)  
• absolute values  $y = g(\alpha) \in \mathcal{K}$ ,  $|y|_i = |g(\alpha_i)|$   
 $r_1 + r_2$  achimedean absolute values  
 $\text{Log} : \mathcal{K}^* \to \mathbb{R}^r \ y \mapsto \log |y|_1, \dots, \log |y|_r$   $(r = r_1 + r_2 - 1)$   
• Dirichlet:  $\text{Log}(\mathcal{O}^*)$  full lattice in  $\mathbb{R}^r$ .

• Remarks: for  $y \in \mathcal{O}^*$ :

$$\prod_{i=1}^{r_1} |y|_i \prod_{j=r_1+1}^{r_1+r_2} |y|_j^2 = \operatorname{Norm}(y) = 1.$$

 $\mathcal{O} \cap \ker \mathsf{Log} = \langle \sqrt[s]{1} \rangle$  (Kronecker)

HSP in lattices Units in number fields and hidden lattices Open problems

(日) (四) (王) (王) (王)

## Unit groups - minima

• partial order on  $K^*$ /some subgroup  $a \le b$  iff  $|a|_i \le |b_i|$  $(i = 1, ..., r_1 + r_2)$ 

HSP in lattices Units in number fields and hidden lattices Open problems

(日) (四) (王) (王) (王)

## Unit groups - minima

- partial order on  $K^*$ /some subgroup  $a \le b$  iff  $|a|_i \le |b_i|$  $(i = 1, ..., r_1 + r_2)$
- Minimal element of a fractional ideal I:

HSP in lattices Units in number fields and hidden lattices Open problems

・ロン ・ 日 ・ ・ 日 ・ ・ 日 ・ ・ 日 ・

## Unit groups - minima

- partial order on K<sup>\*</sup>/some subgroup a ≤ b iff |a|<sub>i</sub> ≤ |b<sub>i</sub>| (i = 1,..., r<sub>1</sub> + r<sub>2</sub>)
- Minimal element of a fractional ideal I:
  - minimal element of I w.r.t  $\leq$  above

Simon's algorithm Basic tools The HSP Infinite abelian HSPs Infinite abelian HSPs

### Unit groups - minima

- partial order on K<sup>\*</sup>/some subgroup a ≤ b iff |a|<sub>i</sub> ≤ |b<sub>i</sub>| (i = 1,..., r<sub>1</sub> + r<sub>2</sub>)
- Minimal element of a fractional ideal *I*:
  - minimal element of I w.r.t  $\leq$  above

• 
$$a \in I \setminus \{0\}$$
, s.t.  $\exists a' \in I \setminus \{0\}$ :  
 $|a'|_i \leq |a|_i \text{ for } i = 1, \dots, r+1 \text{ and } \exists i: |a'|_i < |a|_i$ 

・ロン ・ 日 ・ ・ 日 ・ ・ 日 ・ ・ 日 ・

#### Unit groups - minima

- partial order on K<sup>\*</sup>/some subgroup a ≤ b iff |a|<sub>i</sub> ≤ |b<sub>i</sub>| (i = 1,..., r<sub>1</sub> + r<sub>2</sub>)
- Minimal element of a fractional ideal I:
  - minimal element of I w.r.t  $\leq$  above

• 
$$a \in I \setminus \{0\}$$
, s.t.  $\exists a' \in I \setminus \{0\}$ :  
 $|a'|_i \leq |a|_i$  for  $i = 1, \dots, r+1$  and  $\exists i: |a'|_i < |a|_i$ 

• Examples in  $\mathcal{O}$ : units + usually  $\exists$  others

・ロン ・回 と ・ 回 と ・ 回 と

#### Unit groups - minima

- partial order on K<sup>\*</sup>/some subgroup a ≤ b iff |a|<sub>i</sub> ≤ |b<sub>i</sub>| (i = 1,..., r<sub>1</sub> + r<sub>2</sub>)
- Minimal element of a fractional ideal I:
  - minimal element of I w.r.t  $\leq$  above

• 
$$a \in I \setminus \{0\}$$
, s.t.  $\exists a' \in I \setminus \{0\}$ :  
 $|a'|_i \leq |a|_i \text{ for } i = 1, \dots, r+1 \text{ and } \exists i: |a'|_i < |a|_i$ 

- Examples in  $\mathcal{O}$ : units + usually  $\exists$  others
- Minkowksi's convex body thm  $\Rightarrow$

・ロン ・回 と ・ ヨ と ・ ヨ と

#### Unit groups - minima

- partial order on K<sup>\*</sup>/some subgroup a ≤ b iff |a|<sub>i</sub> ≤ |b<sub>i</sub>| (i = 1,..., r<sub>1</sub> + r<sub>2</sub>)
- Minimal element of a fractional ideal I:
  - minimal element of I w.r.t  $\leq$  above

• 
$$a \in I \setminus \{0\}$$
, s.t.  $\exists a' \in I \setminus \{0\}$ :  
 $|a'|_i \leq |a|_i \text{ for } i = 1, \dots, r+1 \text{ and } \exists i: |a'|_i < |a|_i$ 

- Examples in  $\mathcal{O}$ : units + usually  $\exists$  others
- Minkowksi's convex body thm ⇒
   Bound on log of norms of minima: poly in

・ロン ・回 と ・ ヨ と ・ ヨ と

#### Unit groups - minima

- partial order on K<sup>\*</sup>/some subgroup a ≤ b iff |a|<sub>i</sub> ≤ |b<sub>i</sub>| (i = 1,..., r<sub>1</sub> + r<sub>2</sub>)
- Minimal element of a fractional ideal I:
  - minimal element of I w.r.t  $\leq$  above

• 
$$a \in I \setminus \{0\}$$
, s.t.  $\exists a' \in I \setminus \{0\}$ :  
 $|a'|_i \leq |a|_i \text{ for } i = 1, \dots, r+1 \text{ and } \exists i: |a'|_i < |a|_i$ 

- Examples in  $\mathcal{O}$ : units + usually  $\exists$  others
- Minkowksi's convex body thm ⇒
   Bound on log of norms of minima: poly in
  - #bits of input (f(x))

・ロン ・回 と ・ ヨ と ・ ヨ と

#### Unit groups - minima

- partial order on K<sup>\*</sup>/some subgroup a ≤ b iff |a|<sub>i</sub> ≤ |b<sub>i</sub>| (i = 1,..., r<sub>1</sub> + r<sub>2</sub>)
- Minimal element of a fractional ideal I:
  - minimal element of I w.r.t  $\leq$  above

• 
$$a \in I \setminus \{0\}$$
, s.t.  $\exists a' \in I \setminus \{0\}$ :  
 $|a'|_i \leq |a|_i \text{ for } i = 1, \dots, r+1 \text{ and } \exists i: |a'|_i < |a|_i$ 

- Examples in  $\mathcal{O}$ : units + usually  $\exists$  others
- Minkowksi's convex body thm ⇒
   Bound on log of norms of minima: poly in
  - #bits of input (f(x))
  - log of norm of I

イロト イヨト イヨト イヨト

#### Unit groups - minima

- partial order on K<sup>\*</sup>/some subgroup a ≤ b iff |a|<sub>i</sub> ≤ |b<sub>i</sub>| (i = 1,..., r<sub>1</sub> + r<sub>2</sub>)
- Minimal element of a fractional ideal I:
  - minimal element of I w.r.t  $\leq$  above

• 
$$a \in I \setminus \{0\}$$
, s.t.  $\exists a' \in I \setminus \{0\}$ :  
 $|a'|_i \leq |a|_i \text{ for } i = 1, \dots, r+1 \text{ and } \exists i: |a'|_i < |a|_i$ 

- Examples in  $\mathcal{O}$ : units + usually  $\exists$  others
- Minkowksi's convex body thm ⇒
   Bound on log of norms of minima: poly in
  - #bits of input (f(x))
  - log of norm of I

∜

(1日) (三) (三)

## Unit groups - minima

- partial order on K<sup>\*</sup>/some subgroup a ≤ b iff |a|<sub>i</sub> ≤ |b<sub>i</sub>| (i = 1,..., r<sub>1</sub> + r<sub>2</sub>)
- Minimal element of a fractional ideal I:
  - minimal element of I w.r.t  $\leq$  above

• 
$$a \in I \setminus \{0\}$$
, s.t.  $\exists a' \in I \setminus \{0\}$ :  
 $|a'|_i \leq |a|_i \text{ for } i = 1, \dots, r+1 \text{ and } \exists i: |a'|_i < |a|_i$ 

- Examples in  $\mathcal{O}$ : units + usually  $\exists$  others
- Minkowksi's convex body thm ⇒
   Bound on log of norms of minima: poly in
  - #bits of input (f(x))
  - log of norm of I

 $\Downarrow$ 

• finitely ( $\leq$  exponentially) many minima in I

· < @ > < 문 > < 문 > \_ 문

HSP in lattices Units in number fields and hidden lattices Open problems

### Unit groups - reduced ideals

• *I* reduced if 1 is a minimum of *I* 

HSP in lattices Units in number fields and hidden lattices Open problems

・ロン ・回 と ・ ヨ と ・ ヨ と

3

### Unit groups - reduced ideals

- / reduced if 1 is a minimum of /
- If I reduced fractional ideal then

HSP in lattices Units in number fields and hidden lattices Open problems

・ロン ・回 と ・ ヨ と ・ ヨ と

3

### Unit groups - reduced ideals

- / reduced if 1 is a minimum of /
- If I reduced fractional ideal then

• 
$$I^{-1} = \{x \in K^* | xI \in \mathcal{O}\}$$
 ideal of  $\mathcal{O}$ 

HSP in lattices Units in number fields and hidden lattices Open problems

イロン イヨン イヨン イヨン

2

## Unit groups - reduced ideals

- I reduced if 1 is a minimum of I
- If I reduced fractional ideal then
  - $I^{-1} = \{x \in K^* | xI \in \mathcal{O}\}$  ideal of  $\mathcal{O}$
  - I has poly size HNF

HSP in lattices Units in number fields and hidden lattices Open problems

## Unit groups - reduced ideals

- / reduced if 1 is a minimum of /
- If I reduced fractional ideal then
  - $I^{-1} = \{x \in K^* | xI \in \mathcal{O}\}$  ideal of  $\mathcal{O}$
  - I has poly size HNF

(by Minkowski's convex body thm)

・ロン ・回と ・ヨン・

HSP in lattices Units in number fields and hidden lattices Open problems

## Unit groups - reduced ideals

- / reduced if 1 is a minimum of /
- If I reduced fractional ideal then
  - $I^{-1} = \{x \in K^* | xI \in \mathcal{O}\}$  ideal of  $\mathcal{O}$
  - I has poly size HNF

∜

(by Minkowski's convex body thm)

<ロ> (日) (日) (日) (日) (日)

HSP in lattices Units in number fields and hidden lattices Open problems

## Unit groups - reduced ideals

- / reduced if 1 is a minimum of /
- If I reduced fractional ideal then
  - $I^{-1} = \{x \in K^* | xI \in \mathcal{O}\}$  ideal of  $\mathcal{O}$
  - I has poly size HNF

(by Minkowski's convex body thm)

・ 同 ト ・ ヨ ト ・ ヨ ト

- $\Downarrow$
- finitely (at most exponentially) many reduced ideals

HSP in lattices Units in number fields and hidden lattices Open problems

## Unit groups - reduced ideals

- / reduced if 1 is a minimum of /
- If I reduced fractional ideal then
  - $I^{-1} = \{x \in K^* | xI \in \mathcal{O}\}$  ideal of  $\mathcal{O}$
  - I has poly size HNF

(by Minkowski's convex body thm)

- 4 同 6 4 日 6 4 日 6

- $\Downarrow$
- finitely (at most exponentially) many reduced ideals
- reduced principal ideals:  $\frac{1}{a}O$ , where *a* minimum of O.

HSP in lattices Units in number fields and hidden lattices Open problems

・ロン ・回 と ・ ヨ と ・ ヨ と

3

Unit groups - neighboring minima

• Buchmann's algorithm

HSP in lattices Units in number fields and hidden lattices Open problems

・ロン ・回 と ・ ヨ と ・ ヨ と

3

# Unit groups - neighboring minima

- Buchmann's algorithm
  - Given  $x \in \mathbb{R}^r$ ,

HSP in lattices Units in number fields and hidden lattices Open problems

・ロン ・回 と ・ ヨ と ・ ヨ と

3

# Unit groups - neighboring minima

- Buchmann's algorithm
  - Given  $x \in \mathbb{R}^r$ ,
  - List:

HSP in lattices Units in number fields and hidden lattices Open problems

・ロン ・回 と ・ ヨ と ・ ヨ と

3

## Unit groups - neighboring minima

- Buchmann's algorithm
  - Given  $x \in \mathbb{R}^r$ ,
  - List:

(compact representations for)

HSP in lattices Units in number fields and hidden lattices Open problems

・ロン ・回 と ・ ヨ と ・ ヨ と

3

## Unit groups - neighboring minima

- Buchmann's algorithm
  - Given  $x \in \mathbb{R}^r$ ,
  - List:

(compact representations for)

minima y s.t.

HSP in lattices Units in number fields and hidden lattices Open problems

・ロン ・回 と ・ 回 と ・ 回 と

3

# Unit groups - neighboring minima

- Buchmann's algorithm
  - Given  $x \in \mathbb{R}^r$ ,
  - List:

(compact representations for)

minima y s.t. Log(y) close to x.

HSP in lattices Units in number fields and hidden lattices Open problems

イロン イヨン イヨン イヨン

3

# Unit groups - neighboring minima

#### • Buchmann's algorithm

- Given  $x \in \mathbb{R}^r$ ,
- List:

(compact representations for)

minima y s.t. Log(y) close to x.

• in polynomial time for constant degree

HSP in lattices Units in number fields and hidden lattices Open problems

イロン イヨン イヨン イヨン

æ

# Unit groups - neighboring minima

#### • Buchmann's algorithm

- Given  $x \in \mathbb{R}^r$ ,
- List:

(compact representations for)

minima y s.t. Log(y) close to x.
in polynomial time for constant degree (polynomially many such y)

HSP in lattices Units in number fields and hidden lattices Open problems

ヘロン 人間 とくほど くほとう

2

# Unit groups - neighboring minima

#### • Buchmann's algorithm

- Given  $x \in \mathbb{R}^r$ ,
- List:

(compact representations for)

```
minima y s.t.
```

```
Log(y) close to x.
```

• in polynomial time for constant degree

(polynomially many such y)

• Hiding function  $F : \mathbb{R}^r \ni x \mapsto (I_x, \delta_x)$  hides  $Log(\mathcal{O}^*)$ , where

HSP in lattices Units in number fields and hidden lattices Open problems

ヘロン 人間 とくほど くほとう

3

# Unit groups - neighboring minima

#### • Buchmann's algorithm

- Given  $x \in \mathbb{R}^r$ ,
- List:

(compact representations for)

- minima y s.t.
  - Log(y) close to x.
- in polynomial time for constant degree (polynomially many such y)
- Hiding function  $F : \mathbb{R}^r \ni x \mapsto (I_x, \delta_x)$  hides  $Log(\mathcal{O}^*)$ , where
  - y minimum with Log(y) "downwards closest" to x

HSP in lattices Units in number fields and hidden lattices Open problems

・ロト ・回ト ・ヨト ・ヨト

3

# Unit groups - neighboring minima

#### • Buchmann's algorithm

- Given  $x \in \mathbb{R}^r$ ,
- List:

(compact representations for)

minima y s.t.

Log(y) close to x.

 in polynomial time for constant degree (polynomially many such y)

• Hiding function  $F : \mathbb{R}^r \ni x \mapsto (I_x, \delta_x)$  hides  $Log(\mathcal{O}^*)$ , where

 y minimum with Log(y) "downwards closest" to x (appropriate choice if more)

HSP in lattices Units in number fields and hidden lattices Open problems

イロン イヨン イヨン イヨン

3

# Unit groups - neighboring minima

#### • Buchmann's algorithm

- Given  $x \in \mathbb{R}^r$ ,
- List:

(compact representations for)

minima y s.t.

Log(y) close to x.

 in polynomial time for constant degree (polynomially many such y)

• Hiding function  $F : \mathbb{R}^r \ni x \mapsto (I_x, \delta_x)$  hides  $Log(\mathcal{O}^*)$ , where

• y minimum with Log(y) "downwards closest" to x

(appropriate choice if more)

•  $I_x = y^{-1}O$  reduced ideal (by HNF)

HSP in lattices Units in number fields and hidden lattices Open problems

・ロト ・回ト ・ヨト ・ヨト

3

# Unit groups - neighboring minima

#### • Buchmann's algorithm

- Given  $x \in \mathbb{R}^r$ ,
- List:

(compact representations for)

minima y s.t.

Log(y) close to x.

 in polynomial time for constant degree (polynomially many such y)

• Hiding function  $F : \mathbb{R}^r \ni x \mapsto (I_x, \delta_x)$  hides  $Log(\mathcal{O}^*)$ , where

• y minimum with Log(y) "downwards closest" to x

(appropriate choice if more)

• 
$$I_x = y^{-1}\mathcal{O}$$
 reduced ideal (by HNF)

• 
$$\delta_x = x - \operatorname{Log}(y)$$

### Hidden lattice in $\mathbb{R}^r$

• function  $f : \mathbb{R}^r \to *$ 

Simon's algorithm Basic tools The HSP Infinite abelian HSPs Basic tools Units in number fields and hidden lattices Open problems

### Hidden lattice in $\mathbb{R}^r$

- function  $f : \mathbb{R}^r \to *$
- hides full lattice L:

### Hidden lattice in $\mathbb{R}^r$

- function  $f : \mathbb{R}^r \to *$
- hides full lattice L:

$$f(x) = f(y) \Leftrightarrow x - y \in L$$

### Hidden lattice in $\mathbb{R}^r$

- function  $f : \mathbb{R}^r \to *$
- hides full lattice L:

$$f(x) = f(y) \Leftrightarrow x - y \in L$$
  
need good discretized version on  $\frac{1}{N}\mathbb{Z}$ 

#### Hidden lattice in $\mathbb{R}^r$

- function  $f : \mathbb{R}^r \to *$
- hides full lattice L:

$$f(x) = f(y) \Leftrightarrow x - y \in L$$

need good discretized version on  $\frac{1}{N}\mathbb{Z}$ 

• Task: Find approx. basis of L

### Hidden lattice in $\mathbb{R}^r$

- function  $f : \mathbb{R}^r \to *$
- hides full lattice L:

$$f(x) = f(y) \Leftrightarrow x - y \in L$$

need good discretized version on  $\frac{1}{N}\mathbb{Z}$ 

- Task: Find approx. basis of L
- Fourier sampling finds (dual) basis in in poly time if

ヘロン 人間 とくほど くほとう

### Hidden lattice in $\mathbb{R}^r$

- function  $f : \mathbb{R}^r \to *$
- hides full lattice L:

$$f(x) = f(y) \Leftrightarrow x - y \in L$$

need good discretized version on  $\frac{1}{N}\mathbb{Z}$ 

- Task: Find approx. basis of L
- Fourier sampling finds (dual) basis in in poly time if
  - r is constant

・ロン ・回 と ・ 回 と ・ 回 と

### Hidden lattice in $\mathbb{R}^r$

- function  $f : \mathbb{R}^r \to *$
- hides full lattice L:

$$f(x) = f(y) \Leftrightarrow x - y \in L$$

need good discretized version on  $\frac{1}{N}\mathbb{Z}$ 

- Task: Find approx. basis of L
- Fourier sampling finds (dual) basis in in poly time if
  - r is constant
  - *L* is not very "ill-positioned"

ヘロン 人間 とくほど くほとう

### Hidden lattice in $\mathbb{R}^r$

- function  $f : \mathbb{R}^r \to *$
- hides full lattice L:

$$f(x) = f(y) \Leftrightarrow x - y \in L$$

need good discretized version on  $\frac{1}{N}\mathbb{Z}$ 

- Task: Find approx. basis of L
- Fourier sampling finds (dual) basis in in poly time if
  - r is constant
  - *L* is not very "ill-positioned"
- Details: Hallgren, Vollmer–Schmidt, STOC 2005.

### Hidden lattice in $\mathbb{R}^r$

- function  $f : \mathbb{R}^r \to *$
- hides full lattice L:

$$f(x) = f(y) \Leftrightarrow x - y \in L$$

need good discretized version on  $\frac{1}{N}\mathbb{Z}$ 

- Task: Find approx. basis of L
- Fourier sampling finds (dual) basis in in poly time if
  - r is constant
  - *L* is not very "ill-positioned"
- Details: Hallgren, Vollmer–Schmidt, STOC 2005. Real quadratic case: Jozsa 2003.

イロト イポト イヨト イヨト

## Hidden lattice in $\mathbb{R}^r$

- function  $f : \mathbb{R}^r \to *$
- hides full lattice L:

$$f(x) = f(y) \Leftrightarrow x - y \in L$$

need good discretized version on  $\frac{1}{N}\mathbb{Z}$ 

- Task: Find approx. basis of L
- Fourier sampling finds (dual) basis in in poly time if
  - r is constant
  - *L* is not very "ill-positioned"
- Details: Hallgren, Vollmer–Schmidt, STOC 2005. Real quadratic case: Jozsa 2003.
- approx. basis of  $\mathsf{Log}(\mathcal{O}^*) \to$

・ロン ・回と ・ヨン ・ヨン

## Hidden lattice in $\mathbb{R}^r$

- function  $f : \mathbb{R}^r \to *$
- hides full lattice L:

$$f(x) = f(y) \Leftrightarrow x - y \in L$$

need good discretized version on  $\frac{1}{N}\mathbb{Z}$ 

- Task: Find approx. basis of L
- Fourier sampling finds (dual) basis in in poly time if
  - r is constant
  - *L* is not very "ill-positioned"
- Details: Hallgren, Vollmer–Schmidt, STOC 2005. Real quadratic case: Jozsa 2003.
- approx. basis of  $\mathsf{Log}(\mathcal{O}^*) \to$

compact repr. of generators for  $\mathcal{O}^*$  (Thiel).

ロト (部) (注) (注) (注)

HSP in lattices Units in number fields and hidden lattices Open problems

# Principal ideal

- *I* principal, if I = aO for some  $a \in K^*$ *a* must be a minimum of *I*
- Task: given *I* (by HNF), find *a* s.t. *I* = *a*O (or "not principal")
- Discrete log-like hiding function:
  - $F_I: \mathbb{Z} \times \mathbb{R}^r$
  - assume I = aO,  $I = I_{\zeta}$  with  $\zeta = Log(a)$
  - want:  $F_I(k,x) = F(I_{k\zeta-x}) = (I_{k\zeta-x}, \delta_{k\zeta-x})$
  - $k\zeta x = Log(minimum of I^k)$  "downwards closest" to -x
  - this computes  $F_I$  without knowing  $\zeta$
- Hidden subgroup  $\ni$  (1,  $\zeta'$ )  $\zeta' = Log(a')$ , I = aO.

HSP in lattices Units in number fields and hidden lattices Open problems

3

# Class group under GRH

- Thiel (94): "small" prime ideals  $P_1, \ldots, P_\ell$  generate class group
- $G = \mathbb{Z}^{\ell}$ , (quantum-valued) hiding function:

$$(k_1,\ldots,k_\ell)\mapsto |R(J)
angle = \sum_{I\in R(J)}|I
angle,$$
 where

• 
$$J = P_1^{k_1} \cdots P_{\ell}^{k_{\ell}}$$
,  
•  $R(J) = \{ \text{reduced ideals} \sim J \}$   
• computing  $|J\rangle|0\rangle \mapsto |J\rangle|R(J)\rangle$ :  
•  $M(J) := \{ \text{minima of } J \}$   
• "easy":  $|J\rangle \sum_{\mu \in M(J)} |\mu\rangle |\mu^{-1}J\rangle$   
•  $|J\rangle \sum_{I \in R(J)} (\sum_{\mu \in M(J): I = \mu^{-1}J} |\mu\rangle |J\rangle) |I\rangle$   
• term in middle term computable from  $I$  and  $J$   
(principal ideal algorithm)

## Open problems

• Sketched algorithms: Unit group, etc. constant degree

ヘロン 人間 とくほど くほとう

## Open problems

- Sketched algorithms: Unit group, etc. constant degree
- Unit group, etc for non-constant degree

イロン イヨン イヨン イヨン

# Open problems

- Sketched algorithms: Unit group, etc. constant degree
- Unit group, etc for non-constant degree
- Other approaches?

イロン イヨン イヨン イヨン

# Open problems

- Sketched algorithms: Unit group, etc. constant degree
- Unit group, etc for non-constant degree
- Other approaches?
- Dispensing of GRH?

イロン イヨン イヨン イヨン

# Open problems

- Sketched algorithms: Unit group, etc. constant degree
- Unit group, etc for non-constant degree
- Other approaches?
- Dispensing of GRH?
- Solving norm equations from  $L^*$  to  $K^*$ , where  $Q \leq K < L$

イロン イヨン イヨン イヨン

# Open problems

- Sketched algorithms: Unit group, etc. constant degree
- Unit group, etc for non-constant degree
- Other approaches?
- Dispensing of GRH?
- Solving norm equations from  $L^*$  to  $K^*$ , where  $Q \leq K < L$ 
  - Hasse's local-global principle

イロト イポト イヨト イヨト

## Open problems

- Sketched algorithms: Unit group, etc. constant degree
- Unit group, etc for non-constant degree
- Other approaches?
- Dispensing of GRH?
- Solving norm equations from  $L^*$  to  $K^*$ , where  $Q \leq K < L$ 
  - Hasse's local-global principle
    - First glance: gives "probably" identity test modulo  $N(L^*)$

イロト イポト イヨト イヨト

# Open problems

- Sketched algorithms: Unit group, etc. constant degree
- Unit group, etc for non-constant degree
- Other approaches?
- Dispensing of GRH?
- Solving norm equations from  $L^*$  to  $K^*$ , where  $Q \leq K < L$ 
  - Hasse's local-global principle
    - First glance: gives "probably" identity test modulo  $N(L^*)$
    - $\exists$  "correct" non-constructive identity test

イロト イポト イヨト イヨト

## Open problems

- Sketched algorithms: Unit group, etc. constant degree
- Unit group, etc for non-constant degree
- Other approaches?
- Dispensing of GRH?
- Solving norm equations from  $L^*$  to  $K^*$ , where  $Q \leq K < L$ 
  - Hasse's local-global principle
    - First glance: gives "probably" identity test modulo  $N(L^*)$
    - $\exists$  "correct" non-constructive identity test
  - good "small" subgroup of L\* (S-units)?

・ロト ・回ト ・ヨト ・ヨト

## Open problems

- Sketched algorithms: Unit group, etc. constant degree
- Unit group, etc for non-constant degree
- Other approaches?
- Dispensing of GRH?
- Solving norm equations from  $L^*$  to  $K^*$ , where  $Q \leq K < L$ 
  - Hasse's local-global principle
    - First glance: gives "probably" identity test modulo  $N(L^*)$
    - $\exists$  "correct" non-constructive identity test
  - good "small" subgroup of L\* (S-units)?
- Further HSP-like problems in algebraic number theory?

イロト イポト イヨト イヨト

## Open problems

- Sketched algorithms: Unit group, etc. constant degree
- Unit group, etc for non-constant degree
- Other approaches?
- Dispensing of GRH?
- Solving norm equations from  $L^*$  to  $K^*$ , where  $Q \leq K < L$ 
  - Hasse's local-global principle
    - First glance: gives "probably" identity test modulo  $N(L^*)$
    - $\exists$  "correct" non-constructive identity test
  - good "small" subgroup of L\* (S-units)?
- Further HSP-like problems in algebraic number theory?
- Your favorite number theory problem?

イロト イポト イヨト イヨト