Quantum algorithms for shifted subset problems

Ashley Montanaro[1]

[1]Department of Computer Science
University of Bristol
Bristol, UK

21st August 2008

Introduction

The abelian hidden subgroup problem is a major success of quantum computation.

Introduction

The abelian hidden subgroup problem is a major success of quantum computation.

Abelian Hidden Subgroup Problem

Input:

- A known abelian group G

Introduction

The abelian hidden subgroup problem is a major success of quantum computation.

Abelian Hidden Subgroup Problem

Input:

- A known abelian group G
- An unknown subgroup $H \leqslant G$

Introduction

The abelian hidden subgroup problem is a major success of quantum computation.

Abelian Hidden Subgroup Problem

Input:

- A known abelian group G
- An unknown subgroup $H \leqslant G$
- An oracle function $f : G \to S$.

Promise:

- f is constant on cosets of H in G
- f is distinct on each coset.

Introduction

The abelian hidden subgroup problem is a major success of quantum computation.

Abelian Hidden Subgroup Problem

Input:

- A known abelian group G
- An unknown subgroup $H \leqslant G$
- An oracle function $f : G \to S$.

Promise:

- f is constant on cosets of H in G
- f is distinct on each coset.

Task: Determine H.

Introduction

The abelian hidden subgroup problem is a major success of quantum computation.

Abelian Hidden Subgroup Problem

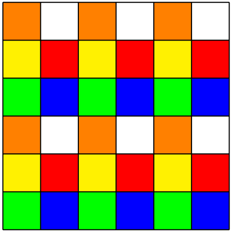
Input:

- A known abelian group G
- An unknown subgroup $H \leqslant G$
- An oracle function $f : G \to S$.

Promise:

- f is constant on cosets of H in G
- f is distinct on each coset.

Task: Determine H.

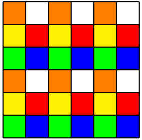


$G = \mathbb{Z}_6 \times \mathbb{Z}_6$,
$H = \mathbb{Z}_2 \times \mathbb{Z}_3$.

Generalising the abelian HSP

The first steps of the quantum algorithm for the abelian HSP are:

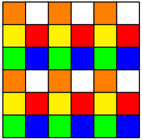
1. Query f on a superposition of all elements in G, giving $\sum_{g \in G} |g\rangle|f(g)\rangle$.



Generalising the abelian HSP

The first steps of the quantum algorithm for the abelian HSP are:

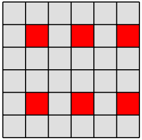
1. Query f on a superposition of all elements in G, giving $\sum_{g \in G} |g\rangle|f(g)\rangle$.



2. Measure the second register, leaving

$$|\psi\rangle = \sum_{g \in G, f(g) = f_0} |g\rangle = \sum_{g \in H} |g + x\rangle$$

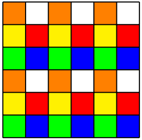
for some random x.



Generalising the abelian HSP

The first steps of the quantum algorithm for the abelian HSP are:

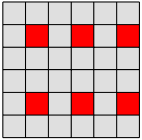
1. Query f on a superposition of all elements in G, giving $\sum_{g \in G} |g\rangle|f(g)\rangle$.



2. Measure the second register, leaving

$$|\psi\rangle = \sum_{g \in G, f(g) = f_0} |g\rangle = \sum_{g \in H} |g + x\rangle$$

for some random x.



The algorithm then identifies H by applying the QFT to $|\psi\rangle$ and measuring.

The shifted subset problem

This can be generalised to the following [Childs et al. ’07]:

The shifted subset problem

This can be generalised to the following [Childs et al. ’07]:

Shifted Subset Problem

Input:

- A known abelian group G

The shifted subset problem

This can be generalised to the following [Childs et al. '07]:

Shifted Subset Problem

Input:

- A known abelian group G
- An unknown subset $S \subseteq G$ picked from some known family of subsets

The shifted subset problem

This can be generalised to the following [Childs et al. '07]:

Shifted Subset Problem

Input:

- A known abelian group G
- An unknown subset $S \subseteq G$ picked from some known family of subsets
- An oracle producing quantum states of the form

$$|S + x\rangle = \sum_{s \in S} |s + x\rangle,$$

for some arbitrary shift x.

Task: Determine S.

The shifted subset problem

This can be generalised to the following [Childs et al. '07]:

Shifted Subset Problem

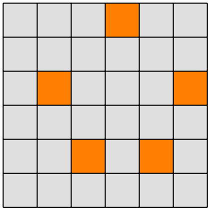
Input:

- A known abelian group G
- An unknown subset $S \subseteq G$ picked from some known family of subsets
- An oracle producing quantum states of the form

$$|S + x\rangle = \sum_{s \in S} |s + x\rangle,$$

for some arbitrary shift x.

Task: Determine S.



The shifted subset problem

This can be generalised to the following [Childs et al. '07]:

Shifted Subset Problem

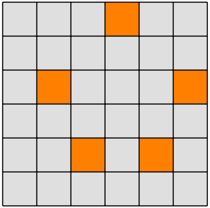
Input:

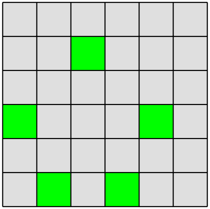
- A known abelian group G
- An unknown subset $S \subseteq G$ picked from some known family of subsets
- An oracle producing quantum states of the form

$$|S + x\rangle = \sum_{s \in S} |s + x\rangle,$$

for some arbitrary shift x.

Task: Determine S.





The shifted subset problem

Childs et al considered subsets of the additive group of $\mathbb{F}_q^n$ for constant n.

- In particular, hidden spheres in $\mathbb{F}_q^n$ ($x = (x_1, \ldots, x_n)$ is on the sphere in $\mathbb{F}_q^n$ with radius $r \in \mathbb{F}_q$ centred at the origin if $\sum_i x_i^2 = r$).
- Found a $\text{poly}(\log q)$ quantum algorithm to determine the quadratic character of the radius of a hidden sphere when n is odd.

The shifted subset problem

Childs et al considered subsets of the additive group of $\mathbb{F}_q^n$ for constant n.

- In particular, hidden spheres in $\mathbb{F}_q^n$ ($x = (x_1, \ldots, x_n)$ is on the sphere in $\mathbb{F}_q^n$ with radius $r \in \mathbb{F}_q$ centred at the origin if $\sum_i x_i^2 = r$).
- Found a $\mathrm{poly}(\log q)$ quantum algorithm to determine the quadratic character of the radius of a hidden sphere when n is odd.

Here, we consider the boolean cube $\mathbb{Z}_2^n$.

Goal: quantum algorithms to find subsets of $\mathbb{Z}_2^n$ in time $\mathrm{poly}(n)$.

This is a natural generalisation of Simon's problem.

The shifted sphere problem

Definition. Let $|x|$ be the Hamming weight of the bit-string x. The sphere of radius r in the cube $\mathbb{Z}_2^n$ is the set $S_r = \{x : |x| = r\}$.

The shifted sphere problem

Definition. Let $|x|$ be the Hamming weight of the bit-string x. The sphere of radius r in the cube $\mathbb{Z}_2^n$ is the set $S_r = \{x : |x| = r\}$.

Shifted Sphere Problem

Input:

- An unknown radius r, $0 \leqslant r \leqslant n/2$

The shifted sphere problem

Definition. Let $|x|$ be the Hamming weight of the bit-string x. The sphere of radius r in the cube $\mathbb{Z}_2^n$ is the set $S_r = \{x : |x| = r\}$.

Shifted Sphere Problem

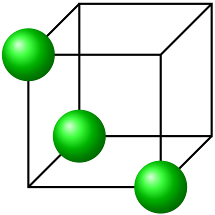
Input:

- An unknown radius r, $0 \leqslant r \leqslant n/2$
- An oracle producing quantum states of the form

$$|S_r + x\rangle = \frac{1}{\sqrt{\binom{n}{r}}} \sum_{s \in S_r} |s + x\rangle,$$

for some arbitrary shift x.

Task: Determine r.



$S_1 \subset \mathbb{Z}_2^3$

Main results

1. A polynomial-time quantum algorithm for the hidden sphere problem.

Main results

1. A polynomial-time quantum algorithm for the hidden sphere problem.
2. Polynomial-time quantum algorithms for some other classes of subsets.

Main results

1. A polynomial-time quantum algorithm for the hidden sphere problem.
2. Polynomial-time quantum algorithms for some other classes of subsets.
3. An exponential black-box separation from classical computation for any shifted subset problem that has a polynomial-time quantum algorithm.

Algorithm outline

Quantum component is the same for any subset $S \subseteq \mathbb{Z}_2^n$.

Algorithm outline

Quantum component is the same for any subset $S \subseteq \mathbb{Z}_2^n$.

1. Given $\frac{1}{\sqrt{|S|}} \sum_{s \in S} |s + x\rangle$, remove unknown shift by applying Hadamards on each qubit:

Algorithm outline

Quantum component is the same for any subset $S \subseteq \mathbb{Z}_2^n$.

1. Given $\frac{1}{\sqrt{|S|}} \sum_{s \in S} |s + x\rangle$, remove unknown shift by applying Hadamards on each qubit:

$$H^{\otimes n}|S + x\rangle = \frac{1}{\sqrt{|S|2^n}} \sum_{y \in S} \sum_{z \in \{0,1\}^n} (-1)^{z \cdot (y+x)} |z\rangle$$

Algorithm outline

Quantum component is the same for any subset $S \subseteq \mathbb{Z}_2^n$.

1. Given $\frac{1}{\sqrt{|S|}} \sum_{s \in S} |s + x\rangle$, remove unknown shift by applying Hadamards on each qubit:

$$\begin{aligned} H^{\otimes n}|S + x\rangle &= \frac{1}{\sqrt{|S|2^n}} \sum_{y \in S} \sum_{z \in \{0,1\}^n} (-1)^{z \cdot (y+x)} |z\rangle \\ &= \frac{1}{\sqrt{|S|2^n}} \sum_{z \in \{0,1\}^n} (-1)^{x \cdot z} \sum_{y \in S} (-1)^{y \cdot z} |z\rangle. \end{aligned}$$

Algorithm outline (2)

2. Measure this state, giving rise to the following probability distribution.

$$\pi_S(z) = \frac{1}{|S|2^n} \left(\sum_{y \in S} (-1)^{y \cdot z} \right)^2$$

3. Use samples from this distribution to infer S.

Algorithm outline (2)

2. Measure this state, giving rise to the following probability distribution.

$$\pi_S(z) = \frac{1}{|S|2^n} \left(\sum_{y \in S} (-1)^{y \cdot z} \right)^2$$

3. Use samples from this distribution to infer S.

What does this distribution look like for the shifted sphere problem?

Shifted spheres

We have

$$\pi_{S_r}(z) = \frac{1}{\binom{n}{r} 2^n} \left(\sum_{|y|=r} (-1)^{y \cdot z} \right)^2$$

which only depends on r, $|z|$.

Shifted spheres

We have

$$\pi_{S_r}(z) = \frac{1}{\binom{n}{r} 2^n} \left(\sum_{|y|=r} (-1)^{y \cdot z} \right)^2$$

which only depends on r, $|z|$.

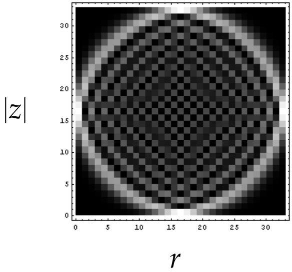
The sum in red is an example of a Krawtchouk polynomial, which have been much studied in coding theory. What do these probability distributions look like?

Shifted spheres

We have

$$\pi_{S_r}(z) = \frac{1}{\binom{n}{r}2^n} \left(\sum_{|y|=r} (-1)^{y \cdot z} \right)^2$$

which only depends on r, $|z|$.
The sum in red is an example of a Krawtchouk polynomial, which have been much studied in coding theory. What do these probability distributions look like?



Shifted spheres (2)

It turns out that:

- For any r, this probability distribution has a lot of weight at $|z| \approx n/2$.

Shifted spheres (2)

It turns out that:

- For any r, this probability distribution has a lot of weight at $|z| \approx n/2$.
- We can calculate an exact expression for the Krawtchouk polynomial at $|z| = n/2$ (n even) and $|z| = (n-1)/2$ (n odd).

Shifted spheres (2)

It turns out that:

- For any r, this probability distribution has a lot of weight at $|z| \approx n/2$.
- We can calculate an exact expression for the Krawtchouk polynomial at $|z| = n/2$ (n even) and $|z| = (n-1)/2$ (n odd).

Algorithm sketch:

- Sample from π_{S_r} some number of times. Count the number of occurrences of outcomes z with $|z| = n/2$ (or $(n-1)/2$).

Shifted spheres (2)

It turns out that:

- For any r, this probability distribution has a lot of weight at $|z| \approx n/2$.
- We can calculate an exact expression for the Krawtchouk polynomial at $|z| = n/2$ (n even) and $|z| = (n-1)/2$ (n odd).

Algorithm sketch:

- Sample from π_{S_r} some number of times. Count the number of occurrences of outcomes z with $|z| = n/2$ (or $(n-1)/2$).
- Use this count to estimate r.

Shifted spheres (3)

Set $\pi_r(x) = \sum_{|z|=x} \pi_{S_r}(z)$. For even n, one can show that:

- If r is odd, $\pi_r(n/2) = 0$. If r is even, $\pi_r(n/2) = \Omega(1/n)$.

Shifted spheres (3)

Set $\pi_r(x) = \sum_{|z|=x} \pi_{S_r}(z)$. For even n, one can show that:

- If r is odd, $\pi_r(n/2) = 0$. If r is even, $\pi_r(n/2) = \Omega(1/n)$.
- For r even and $r \neq s$, $|\pi_r(n/2) - \pi_s(n/2)| = \Omega(n^{-3})$.

Shifted spheres (3)

Set $\pi_r(x) = \sum_{|z|=x} \pi_{S_r}(z)$. For even n, one can show that:

- If r is odd, $\pi_r(n/2) = 0$. If r is even, $\pi_r(n/2) = \Omega(1/n)$.
- For r even and $r \neq s$, $|\pi_r(n/2) - \pi_s(n/2)| = \Omega(n^{-3})$.
- For r odd and $r \neq s$, $|\pi_r(n/2-1) - \pi_s(n/2-1)| = \Omega(n^{-3})$.

Shifted spheres (3)

Set $\pi_r(x) = \sum_{|z|=x} \pi_{S_r}(z)$. For even n, one can show that:

- If r is odd, $\pi_r(n/2) = 0$. If r is even, $\pi_r(n/2) = \Omega(1/n)$.
- For r even and $r \neq s$, $|\pi_r(n/2) - \pi_s(n/2)| = \Omega(n^{-3})$.
- For r odd and $r \neq s$, $|\pi_r(n/2-1) - \pi_s(n/2-1)| = \Omega(n^{-3})$.

Implies that $O(n^6)$ samples are sufficient to estimate r with a bounded probability of error.

Bonus: $O(n)$ samples are enough to identify whether r is odd or even.

n odd: $O(n^4)$ samples are sufficient to estimate r.

Summary

- We've introduced shifted subset problems on the cube $\mathbb{Z}_2^n$ – a natural generalisation of the abelian hidden subgroup problem.
- We've seen a polynomial-time quantum algorithm for the shifted sphere problem.
- This gives an exponential separation from classical computation.

Summary

- We've introduced shifted subset problems on the cube $\mathbb{Z}_2^n$ – a natural generalisation of the abelian hidden subgroup problem.
- We've seen a polynomial-time quantum algorithm for the shifted sphere problem.
- This gives an exponential separation from classical computation.

Possible extensions:

- Improve the time complexity of the algorithm to something reasonable.
- Find other interesting families of subsets to distinguish.
- Consider the group $\mathbb{Z}_k^n$, where k is constant.

Summary

- We've introduced shifted subset problems on the cube $\mathbb{Z}_2^n$ – a natural generalisation of the abelian hidden subgroup problem.
- We've seen a polynomial-time quantum algorithm for the shifted sphere problem.
- This gives an exponential separation from classical computation.

Possible extensions:

- Improve the time complexity of the algorithm to something reasonable.
- Find other interesting families of subsets to distinguish.
- Consider the group $\mathbb{Z}_k^n$, where k is constant.

Applications?

The end

Further reading: arXiv:0806.3362.

Thanks for your time!

Other shifted subsets

We can also give polynomial-time quantum algorithms for some other classes of subsets:

Other shifted subsets

We can also give polynomial-time quantum algorithms for some other classes of subsets:

- **Hamming balls,** i.e. sets $\{x : |x| \leqslant r\}$. Reduces to the shifted sphere problem.

Other shifted subsets

We can also give polynomial-time quantum algorithms for some other classes of subsets:

- **Hamming balls,** i.e. sets $\{x : |x| \leqslant r\}$. Reduces to the shifted sphere problem.
- **Subsets whose sizes are very different.** Follows from the fact that the probability of getting outcome 0 is proportional to the size of the subset.

Other shifted subsets

We can also give polynomial-time quantum algorithms for some other classes of subsets:

- **Hamming balls,** i.e. sets $\{x : |x| \leqslant r\}$. Reduces to the shifted sphere problem.
- **Subsets whose sizes are very different.** Follows from the fact that the probability of getting outcome 0 is proportional to the size of the subset.
- **Juntas.** Sets whose characteristic functions each depend on a constant number of variables.

Other shifted subsets

We can also give polynomial-time quantum algorithms for some other classes of subsets:

- **Hamming balls,** i.e. sets $\{x : |x| \leqslant r\}$. Reduces to the shifted sphere problem.
- **Subsets whose sizes are very different.** Follows from the fact that the probability of getting outcome 0 is proportional to the size of the subset.
- **Juntas.** Sets whose characteristic functions each depend on a constant number of variables.
- **Parity functions.** Sets whose characteristic functions are parity functions.

Exponential separation from classical computation

We define a black-box (oracular) problem to show a separation from classical computation. It uses three oracle functions:

- A **colouring** operator $c : \{0,1\}^{2n} \longrightarrow [2^{2n}]$.
  [gives each point a colour; $|S|$ points have each colour]

Exponential separation from classical computation

We define a black-box (oracular) problem to show a separation from classical computation. It uses three oracle functions:

- A **colouring** operator $c : \{0,1\}^{2n} \to [2^{2n}]$.
  [gives each point a colour; $|S|$ points have each colour]

- A **shifting** operator $s : \{0,1\}^{2n} \times [2^{2n}] \to \{0,1\}^{n}$.
  [converts (point, colour) to (shifted point); depends on S]

Exponential separation from classical computation

We define a black-box (oracular) problem to show a separation from classical computation. It uses three oracle functions:

- A **colouring** operator $c : \{0,1\}^{2n} \longrightarrow [2^{2n}]$.
  [gives each point a colour; $|S|$ points have each colour]

- A **shifting** operator $s : \{0,1\}^{2n} \times [2^{2n}] \longrightarrow \{0,1\}^{n}$.
  [converts (point, colour) to (shifted point); depends on S]

- An **uncolouring** operator $c^{-1} : [2^{2n}] \times \{0,1\}^{n} \longrightarrow \{0,1\}^{2n}$.
  [uncomputes the colour]

Exponential separation from classical computation

We define a black-box (oracular) problem to show a separation from classical computation. It uses three oracle functions:

- A **colouring** operator $c : \{0,1\}^{2n} \to [2^{2n}]$.
  [gives each point a colour; $|S|$ points have each colour]
- A **shifting** operator $s : \{0,1\}^{2n} \times [2^{2n}] \to \{0,1\}^{n}$.
  [converts (point, colour) to (shifted point); depends on S]
- An **uncolouring** operator $c^{-1} : [2^{2n}] \times \{0,1\}^{n} \to \{0,1\}^{2n}$.
  [uncomputes the colour]

Goal: use these operators to find S. Can show that any classical algorithm must make $\Omega(2^{n/2})$ queries to c to get *any* information about S.