Easy and hard functions for the Boolean hidden shift problem

arXiv:1304.4642

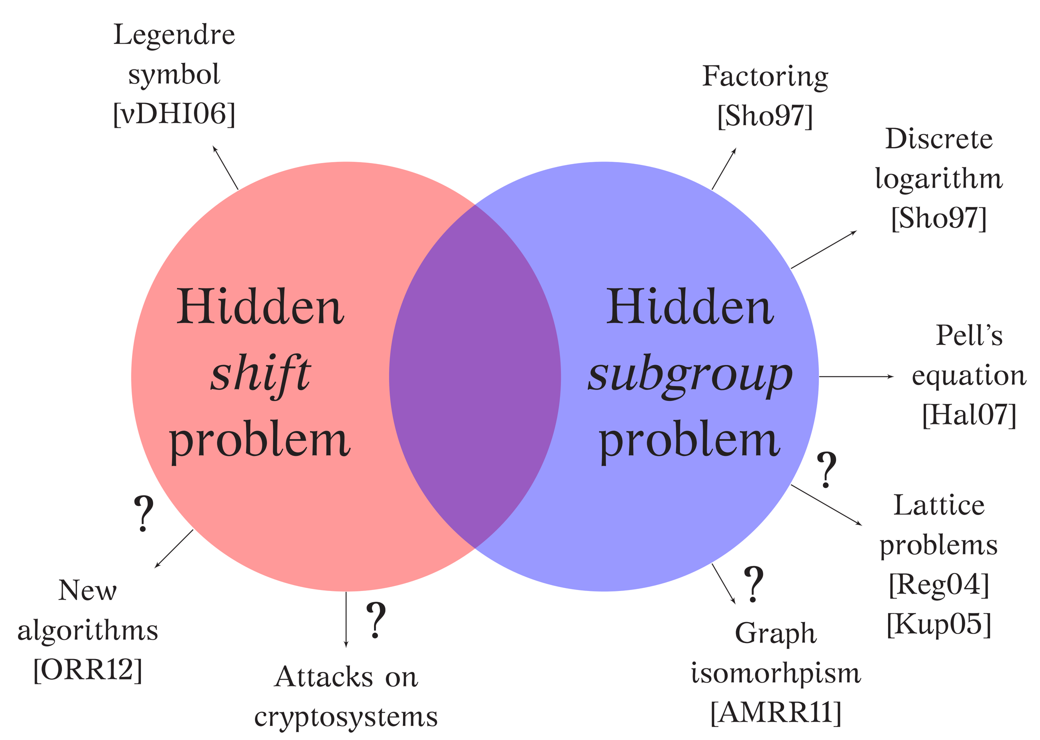
Andrew M. Childs[1], Robin Kothari[1], Maris Ozols[2], Martin Roetteler[3]

[1]University of Waterloo & Institute for Quantum Computing

[2]University of Cambridge

[3]Microsoft Research

Motivation



Problem

Boolean hidden shift problem

- **Given:** complete description of $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ and access to a black-box oracle for $f_s(x) := f(x + s)$
- **Determine:** hidden shift $s \in \mathbb{Z}_2^n$

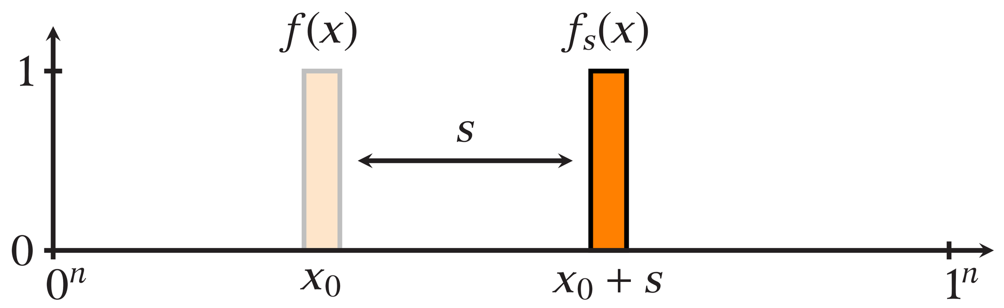
Quantum query complexity

- **Oracle:** $O_{f_s} : |x\rangle \mapsto (-1)^{f(x+s)}|x\rangle$
- $Q(\mathrm{BHSP}_f)$:= bounded error quantum query complexity of the Boolean hidden shift problem for function f

Hardest instances

Delta functions

- $f(x) := \delta_{x,x_0}$ for some $x_0 \in \mathbb{Z}_2^n$
- BHSP_f is equivalent to Grover's search: $Q(\mathrm{BHSP}_f) = \Theta(\sqrt{2^n})$



Hard instances

Quantum "brute force" approach

- Completely extract the truth table of f_s
- Oracle identification problem [AIK+04]
- $Q(\mathrm{BHSP}_f) = O(\sqrt{2^n})$

Algorithm

1. Use Grover's algorithm to find some x_0 with $f_s(x_0) = 1$
2. Brute force through all s that give $f_s(x_0) = 1$

Theorem

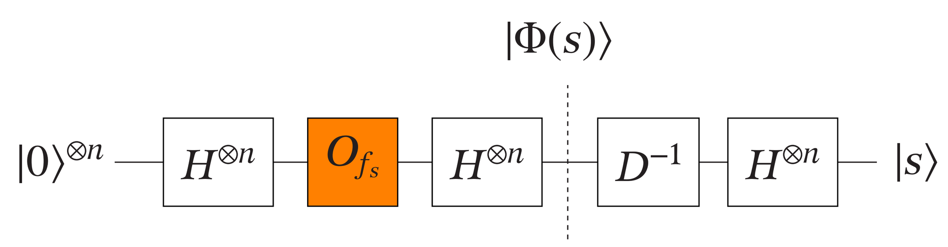
- $Q(\mathrm{BHSP}_f) = \frac{\pi}{4}\sqrt{2^n/|f|} + O(\sqrt{|f|})$
- $Q(\mathrm{BHSP}_f) = \Omega(\sqrt{2^n/|f|})$ via adversary method
- $|f|$:= the Hamming weight of the truth table of f

Observations

- For f to be hard, it is necessary that $|f|$ is $O(1)$ or $\Theta(2^n)$
- Delta functions are the hardest instances
- Hamming weight alone does not determine hardness

Easy instances

Algorithm [Röt10]



- $|\Phi(s)\rangle := \sum_{w \in \mathbb{Z}_2^n} (-1)^{s \cdot w} \hat{F}(w)|w\rangle$
- $D := \mathrm{diag}(\sqrt{2^n}\hat{F}(w))$, may not be unitary in general

Bent functions

- $|\hat{F}(w)| = 1/\sqrt{2^n}$ for all $w \in \mathbb{Z}_2^n$
- D is unitary
- Exact algorithm with one query!

Theorem

An exact one-query algorithm exists for BHSP_f iff f is bent

Random functions are easy

Algorithm PGM(t)

1. Prepare $|\Phi^t(s)\rangle := \left(O_{f_s}|+\rangle^{\otimes n}\right)^{\otimes t}$
2. Perform Pretty Good Measurement for $\left\{|\Phi^t(s)\rangle : s \in \mathbb{Z}_2^n\right\}$

Note: for $t = 1$ this agrees with [Röt10]

Theorem

If f is chosen uniformly at random and s is chosen adversarially, then PGM(2) solves BHSP_f with two queries and expected success probability exponentially close to 1.

Proof. Second moment method, a t-fold generalization of the Fourier transform, and combinatorics of pairings.

Comparison

Approach	Functions		
	delta	bent	random
PGM	$O(2^n)$	1	2
[ORR12]	$O(\sqrt{2^n})$	1	?
[GRR11]	$O(n\sqrt{2^n})$	$O(n)$	$O(n)$
[AS05]	$O(n \log n \sqrt{2^n})$	$O(n \log n)$	$O(n \log n)$
Lower bounds:	$\Omega(\sqrt{2^n})$	1	1

Conclusions

Summary

- $O(\sqrt{2^n})$ queries for any f
- $\Theta(\sqrt{2^n/|f|})$ queries when $|f|$ is small
- Exact one-query algorithm $\Leftrightarrow$ f is bent
- Two queries suffice for random f

Open questions

- Query-optimal quantum algorithm for all f
- Time-efficient algorithm for some f
- Applications in cryptography