Easy and hard functions for the Boolean hidden shift problem

Maris Ozols
(IBM)

Andrew Childs, Robin Kothari
(University of Waterloo & IQC)

Martin Roetteler
(NEC Labs)

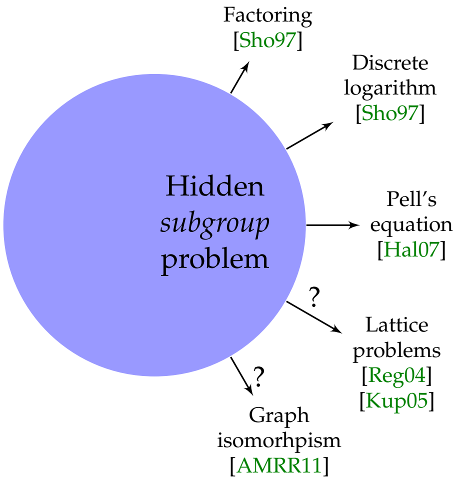
arXiv:1304.4642

May 21, 2013

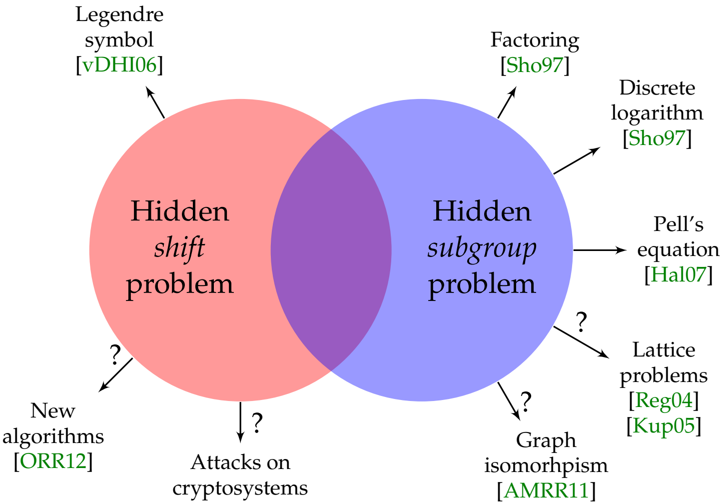
Outline

1. Motivation and problem
2. Hard instances
3. Easy instances
    - bent functions
    - random functions
4. Conclusions

Motivation


Hidden *subgroup* problem
Factoring [Sho97]
Discrete logarithm [Sho97]
Pell's equation [Hal07]
?
Lattice problems [Reg04] [Kup05]
?
Graph isomorhpism [AMRR11]

Motivation



Legendre symbol [vDHI06]
Factoring [Sho97]
Discrete logarithm [Sho97]
Hidden *shift* problem
Hidden *subgroup* problem
Pell's equation [Hal07]
?
Lattice problems [Reg04] [Kup05]
?
New algorithms [ORR12]
?
Attacks on cryptosystems
?
Graph isomorhpism [AMRR11]

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 $f_s(x) := f(x+s)$

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 $s \in \mathbb{Z}_2^n$

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:** $O_{f_s} : |x\rangle \mapsto (-1)^{f(x+s)}|x\rangle$

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 $s \in \mathbb{Z}_2^n$

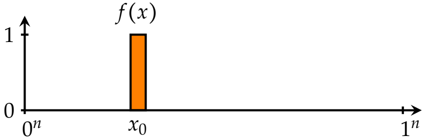
Quantum query complexity

- **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

Hard instances

Delta functions

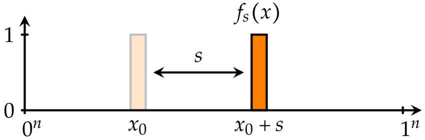
- $f(x) := \delta_{x,x_0}$ for some $x_0 \in \mathbb{Z}_2^n$



Hard instances

Delta functions

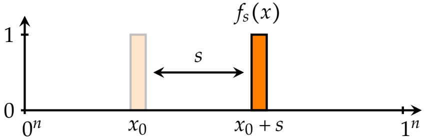
- $f(x) := \delta_{x,x_0}$ for some $x_0 \in \mathbb{Z}_2^n$



Hard instances

Delta functions

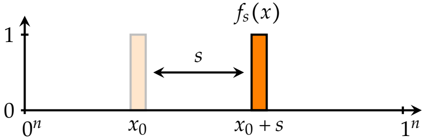
- $f(x) := \delta_{x,x_0}$ for some $x_0 \in \mathbb{Z}_2^n$
- Equivalent to Grover's search: $\Theta(\sqrt{2^n})$



Hard instances

Delta functions

- $f(x) := \delta_{x,x_0}$ for some $x_0 \in \mathbb{Z}_2^n$
- Equivalent to Grover's search: $\Theta(\sqrt{2^n})$



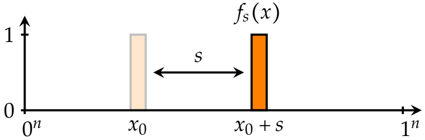
Brute force approach

- Completely extract the truth table of f_s

Hard instances

Delta functions

- $f(x) := \delta_{x,x_0}$ for some $x_0 \in \mathbb{Z}_2^n$
- Equivalent to Grover's search: $\Theta(\sqrt{2^n})$



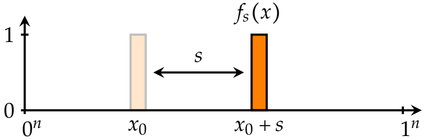
Brute force approach

- Completely extract the truth table of f_s
- Oracle identification problem [AIK+04]

Hard instances

Delta functions

- $f(x) := \delta_{x,x_0}$ for some $x_0 \in \mathbb{Z}_2^n$
- Equivalent to Grover's search: $\Theta(\sqrt{2^n})$



Brute force approach

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

Hard instances

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 $f_s(x_0) = 1$

Hard instances

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 $f_s(x_0) = 1$

Complexity

- $|f|$:= the Hamming weight of the truth table of f

Hard instances

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 $f_s(x_0) = 1$

Complexity

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

Hard instances

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 $f_s(x_0) = 1$

Complexity

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

Hard instances

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 $f_s(x_0) = 1$

Complexity

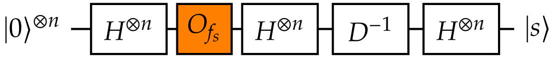
- $|f|$:= the Hamming weight of the truth table of f
- $Q(\mathrm{BHSP}_f) = \frac{\pi}{4}\sqrt{2^n/|f|} + O\left(\sqrt{|f|}\right)$
- $Q(\mathrm{BHSP}_f) = \Omega\left(\sqrt{2^n/|f|}\right)$ via adversary method

Punchline

- 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

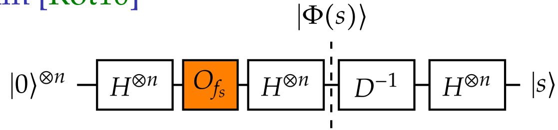
Easy instances

Algorithm [Röt10]



Easy instances

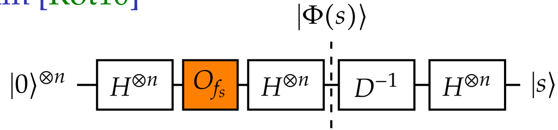
Algorithm [Röt10]



- $|\Phi(s)\rangle := \sum_{w \in \mathbb{Z}_2^n} (-1)^{s \cdot w} \hat{F}(w) |w\rangle$

Easy instances

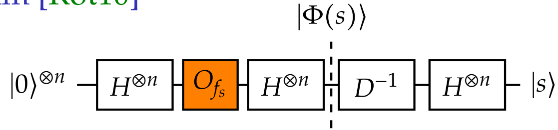
Algorithm [Röt10]



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

Easy instances

Algorithm [Röt10]



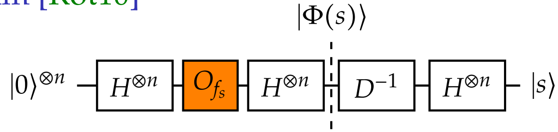
- $|\Phi(s)\rangle := \sum_{w \in \mathbb{Z}_2^n} (-1)^{s \cdot w} \hat{F}(w) |w\rangle$
- $D := \mathrm{diag}\big(\sqrt{2^n}\hat{F}(w)\big)$, may not be unitary in general

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!

Easy instances

Algorithm [Röt10]



- $|\Phi(s)\rangle := \sum_{w \in \mathbb{Z}_2^n} (-1)^{s \cdot w} \hat{F}(w) |w\rangle$
- $D := \mathrm{diag}\left(\sqrt{2^n}\hat{F}(w)\right)$, 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!

Converse

If an exact one-query algorithm exists for BHSP_f then f is bent

Easy instances

PGM algorithm

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

Easy instances

PGM algorithm

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

For $t = 1$ this agrees with [Röt10]

Easy instances

PGM algorithm

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

For $t = 1$ this agrees with [Röt10]

Random functions are easy

- f is chosen uniformly at random
- s is chosen adversarially

PGM solves BHSP_f with two queries and expected success probability exponentially close to 1

Easy instances

PGM algorithm

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

For $t = 1$ this agrees with [Röt10]

Random functions are easy

- f is chosen uniformly at random
- s is chosen adversarially

PGM solves BHSP_f with two queries and expected success probability exponentially close to 1

Proof involves: second moment method, a t-fold generalization of the Fourier transform, 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
- $\Theta\left(\sqrt{2^n/|f|}\right)$ queries when $|f|$ is small
- Exact one-query algorithm $\Leftrightarrow$ f is bent
- Two queries suffice for random f

Conclusions

Summary

- $O(\sqrt{2^n})$ queries for any f
- $\Theta\big(\sqrt{2^n/|f|}\big)$ 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

Conclusions

Summary

- $O(\sqrt{2^n})$ queries for any f
- $\Theta\big(\sqrt{2^n/|f|}\big)$ 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

Thank you!

Bibliography I

[AIK+04] Andris Ambainis, Kazuo Iwama, Akinori Kawachi, Hiroyuki Masuda, Raymond H. Putra, and Shigeru Yamashita.
Quantum identification of Boolean oracles.
In *Proceedings of the 21st Annual Symposium on Theoretical Aspects of Computer Science (STACS 2004)*, volume 2996 of *Lecture Notes in Computer Science*, pages 105–116. Springer, 2004.
arXiv:quant-ph/0403056, doi:10.1007/978-3-540-24749-4_10.

[AMRR11] Andris Ambainis, Loïck Magnin, Martin Roetteler, and Jérémie Roland.
Symmetry-assisted adversaries for quantum state generation.
In *Proceedings of the 26th Annual IEEE Conference on Computational Complexity (CCC'11)*, pages 167–177. IEEE Computer Society, 2011.
arXiv:1012.2112,doi:10.1109/CCC.2011.24.

[AS05] Alp Atıcı and Rocco A. Servedio.
Improved bounds on quantum learning algorithms.
Quantum Information Processing, 4(5):355–386, 2005.
arXiv:quant-ph/0411140,doi:10.1007/s11128-005-0001-2.

[GRR11] Dmitry Gavinsky, Martin Roetteler, and Jérémie Roland.
Quantum algorithm for the Boolean hidden shift problem.
In *Computing and Combinatorics*, volume 6842 of *Lecture Notes in Computer Science*, pages 158–167. Springer, 2011.
arXiv:1103.3017,doi:10.1007/978-3-642-22685-4_14.

Bibliography II

[Hal07] Sean Hallgren.
Polynomial-time quantum algorithms for Pell's equation and the principal ideal problem.
Journal of the ACM, 54(1):4:1–4:19, Mar 2007.
doi:10.1145/1206035.1206039.

[Kup05] Greg Kuperberg.
A subexponential-time quantum algorithm for the dihedral hidden subgroup problem.
SIAM Journal on Computing, 35(1):170–188, 2005.
arXiv:quant-ph/0302112, doi:10.1137/S0097539703436345.

[ORR12] Maris Ozols, Martin Roetteler, and Jérémie Roland.
Quantum rejection sampling.
In *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference (ITCS 2012)*, pages 290–308. ACM, 2012.
arXiv:1103.2774, doi:10.1145/2090236.2090261.

[Reg04] Oded Regev.
Quantum computation and lattice problems.
SIAM Journal on Computing, 33(3):738–760, 2004.
arXiv:cs/0304005, doi:10.1137/S0097539703440678.

Bibliography III

[Röt10] Martin Rötteler.
Quantum algorithms for highly non-linear Boolean functions.
In *Proceedings of the 21st ACM-SIAM Symposium on Discrete Algorithms (SODA 2010)*, pages 448–457. SIAM, 2010.
URL: `http://dl.acm.org/citation.cfm?id=1873601.1873638`, `arXiv:0811.3208`.

[Sho97] Peter W. Shor.
Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer.
SIAM Journal on Computing, 26(5):1484–1509, 1997.
Earlier version in FOCS 1994, pp. 124–134.
`arXiv:quant-ph/9508027`, `doi:10.1137/S0097539795293172`.

[vDHI06] Wim van Dam, Sean Hallgren, and Lawrence Ip.
Quantum algorithms for some hidden shift problems.
SIAM Journal on Computing, 36(3):763–778, 2006.
`arXiv:quant-ph/0211140`, `doi:10.1137/S009753970343141X`.