Quantum algorithms for the hidden shift problem of Boolean functions

NEC Laboratories America
Relentless passion for innovation

Maris Ozols[1,2], Martin Roetteler[1], and Jérémie Roland[1]

[1]*NEC Laboratories America, Inc.*

[2]*University of Waterloo & Institute for Quantum Computing*

University of Waterloo

IQC Institute for Quantum Computing

Hidden shift problem for Boolean functions

The **hidden shift problem** for Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is the following problem: given an oracle access to *shifted function*

$$f_{\vec{s}}(\vec{x}) := f(\vec{x} + \vec{s})$$

for some unknown value of $\vec{s} \in \mathbb{F}_2^n$, determine the value of $\vec{s}$ by querying the oracle on different inputs. The number of queries needed to determine the value of $\vec{s}$ is called the *query complexity* of the hidden shift problem for f.

Fourier analysis on the Boolean cube

The **Fourier transform of a Boolean function** $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is the function $\hat{f} : \mathbb{F}_2^n \to \mathbb{R}$ defined as

$$\hat{f}(\vec{w}) := \frac{1}{2^n} \sum_{\vec{x} \in \mathbb{F}_2^n} (-1)^{\vec{w}\cdot\vec{x} + f(\vec{x})}$$

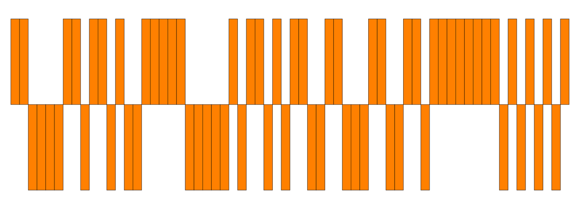
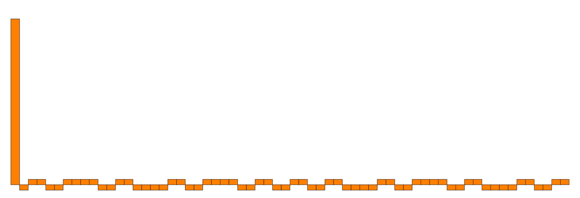
where the arithmetic in the exponent is modulo 2.

Bent and delta functions

Boolean function f is

- a **bent function** if it has a flat Fourier spectrum:
$$|\widehat{f}(\vec{w})| = 2^{-n/2} \quad \forall \vec{w} \in \mathbb{F}_2^n$$
- a **delta function** if $\exists \vec{x}_0 \in \mathbb{F}_2^n$ such that
$$f(x) = \begin{cases} 1 & \text{if } x = x_0 \\ 0 & \text{otherwise} \end{cases}$$

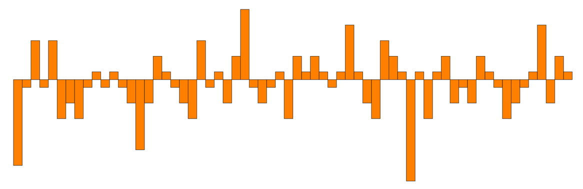
Query complexity of bent and delta functions

	Bent functions	*Delta functions*
Classical:	$\Omega(n)$	$\Theta(2^n)$
Quantum:	1	$\Theta(\sqrt{2^n})$
Spectrum:		

Main idea behind the algorithm

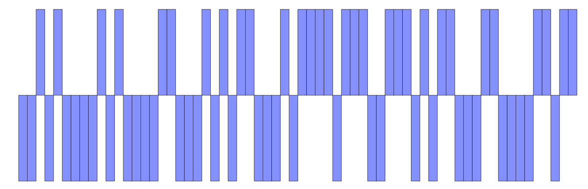
Spiky state (Fourier spectrum)

$$\left|\psi_{\hat{f}}(\vec{s})\right\rangle := \textstyle\sum_{\vec{w}\in\mathbb{F}_2^n} (-1)^{\vec{w}\cdot\vec{s}} \hat{f}(\vec{w}) \left|\vec{w}\right\rangle$$



Flat state

$$\left|\psi(\vec{s})\right\rangle := \tfrac{1}{\sqrt{2^n}} \textstyle\sum_{\vec{w}\in\mathbb{F}_2^n} (-1)^{\vec{w}\cdot\vec{s}} \left|\vec{w}\right\rangle$$



The algorithm relies on the following:

1. Using one oracle call to $O_{f_{\vec{s}}}$, we can construct $\left|\psi_{\hat{f}}(\vec{s})\right\rangle$
$$|0\rangle^{\otimes n} \;/\; \boxed{H^{\otimes n}} \;/\; \boxed{O_{f_{\vec{s}}}} \;/\; \boxed{H^{\otimes n}} \;/\; \quad \left|\psi_{\hat{f}}(\vec{s})\right\rangle$$
2. From $\left|\psi(\vec{s})\right\rangle$, we can easily obtain the hidden shift $\vec{s}$
$$\left|\psi(\vec{s})\right\rangle \;/\; \boxed{H^{\otimes n}} \;/\; \quad \left|\vec{s}\right\rangle$$

Therefore, the goal is to prepare $\left|\psi(\vec{s})\right\rangle$ from $\left|\psi_{\hat{f}}(\vec{s})\right\rangle$, i.e., we would like to implement the operation

$$\hat{f}(\vec{w}) \left|\vec{w}\right\rangle \mapsto \frac{1}{\sqrt{2^n}} \left|\vec{w}\right\rangle.$$

For bent functions, the Fourier spectrum is flat ($|\hat{f}(\vec{w})| = \frac{1}{\sqrt{2^n}}$), and this operation may immediately be implemented [1].
In general, this operation is not unitary and the solution is to entangle this state with an ancillary qubit to create a state

$$\left|\Psi_{\vec{\varepsilon}}(\vec{s})\right\rangle = \sum_{\vec{w}} (-1)^{\vec{w}\cdot\vec{s}} \left|\vec{w}\right\rangle \left(\sqrt{|\hat{f}(\vec{w})|^2 - \varepsilon_{\vec{w}}^2}\, |0\rangle + \varepsilon_{\vec{w}} |1\rangle \right),$$

where $0 \le \varepsilon_{\vec{w}} \le |\hat{f}(\vec{w})|$. By using amplitude amplification on the ancilla being in state $|1\rangle$, we can in turn prepare a state

$$\left|\psi_{\vec{\varepsilon}}(\vec{s})\right\rangle := \frac{1}{\sqrt{q_{\vec{\varepsilon}}}} \sum_{\vec{w}} (-1)^{\vec{w}\cdot\vec{s}} \varepsilon_{\vec{w}} \left|\vec{w}\right\rangle,$$

which has large overlap over $\left|\psi(\vec{s})\right\rangle$ if $\vec{\varepsilon}$ is rather flat.

Amplitude amplification

The amplitude amplification part of our algorithm is

$$\mathcal{A} := \left(\mathrm{ref}_{|\psi_{\vec{\varepsilon}}(\vec{s})\rangle} \cdot (I_n \otimes \mathrm{ref}_{|1\rangle})\right)^k,$$

where $\mathrm{ref}_{|\psi_{\vec{\varepsilon}}(\vec{s})\rangle}$ and $\mathrm{ref}_{|1\rangle}$ are reflections through these states.
It remains to optimize the vector $\vec{\varepsilon}$ to minimize $k = O(1/\sqrt{q_{\vec{\varepsilon}}})$ while keeping a large success probability $p_{\vec{\varepsilon}}$, where

$$q_{\vec{\varepsilon}} = \left\| (I_n \otimes |1\rangle\langle 1|) \left|\Psi_{\vec{\varepsilon}}(\vec{s})\right\rangle \right\|^2 = \left\|\vec{\varepsilon}\right\|_2^2,$$

$$p_{\vec{\varepsilon}} = \left| \langle \psi(\vec{s}) | \psi_{\vec{\varepsilon}}(\vec{s}) \rangle \right|^2 = \frac{1}{2^n} \frac{\left\|\vec{\varepsilon}\right\|_1^2}{\left\|\vec{\varepsilon}\right\|_2^2}.$$

Description via SDP

The optimal choice of $\vec{\varepsilon}$ and the query complexity of the corresponding algorithm can be found by solving the following semidefinite optimization problem:

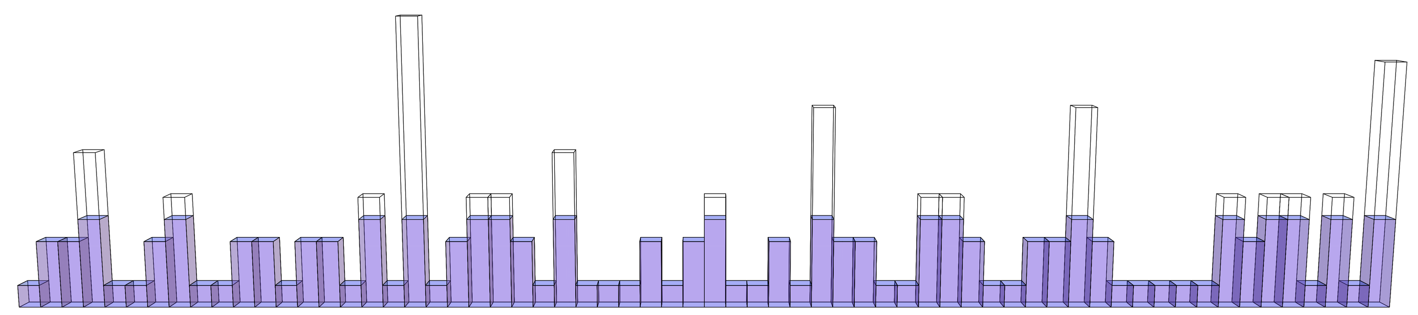
$$\max_{M \ge 0} \operatorname{Tr} M \quad \text{s.t. } \forall \vec{w} \in \mathbb{F}_2^n : \hat{f}(\vec{w})^2 \ge M_{\vec{w},\vec{w}} \qquad \text{(SDP)}$$
$$\operatorname{Tr}((J - c2^n I)M) \ge 0$$

where c is the desired success probability and I, J are the identity and all-ones matrices, respectively.

Optimal solution

The optimal solution of SDP corresponds to a rank-1 matrix $M = \vec{\varepsilon} \cdot \vec{\varepsilon}^{\mathsf{T}}$, where $\vec{\varepsilon} \in \mathbb{R}^{2^n}$ is the "water filling" vector of the Fourier spectrum of f given by

$$\varepsilon_{\vec{w}} = \begin{cases} \hat{f}(\vec{w}) & \text{if } |\hat{f}(\vec{w})| \le \delta \\ \delta & \text{otherwise} \end{cases}$$



Main result

Theorem. If $c \le 1 - N_0/2^n$, where N_0 is the number of zero Fourier coefficients, then SDP achieves its maximum at $M = \vec{\varepsilon} \cdot \vec{\varepsilon}^{\mathsf{T}}$ with objective value equal to $\left\|\vec{\varepsilon}\right\|_2^2$, where $\vec{\varepsilon}$ is the "water-filling" vector of $\hat{f}$ for δ such that

$$\frac{1}{2^n} \frac{\left\|\vec{\varepsilon}\right\|_1^2}{\left\|\vec{\varepsilon}\right\|_2^2} = c$$

If $c > 1 - N_0/2^n$, then SDP has no feasible point.

References

[1] M. Roetteler. Quantum algorithms for highly non-linear Boolean functions. *Proc. SODA'10*, 448–457, 2010.