

Quantum boolean functions

Ashley Montanaro¹ and Tobias Osborne²

¹Department of Computer Science
University of Bristol
Bristol, UK

²Department of Mathematics
Royal Holloway, University of London
London, UK

12 January 2009



Introduction

Perhaps the most fundamental object in computer science is the **boolean function**:

$$f : \{0, 1\}^n \rightarrow \{0, 1\}$$

Introduction

Perhaps the most fundamental object in computer science is the **boolean function**:

$$f : \{0, 1\}^n \rightarrow \{0, 1\}$$

Many interpretations:

- Truth table
- Subset of $[2^n] = \{1, \dots, 2^n\}$
- Family of subsets of $[n]$
- Colouring of the n -cube
- Voting system
- Decision tree
- ...

x_1	x_2	$f(x_1, x_2)$
0	0	0
0	1	1
1	0	1
1	1	0

$$\mathcal{F} = \{\{1\}, \{2\}\}$$



Fourier analysis of boolean functions

The field of [analysis of boolean functions](#) aims to derive information about boolean functions by looking at their [Fourier expansion](#).

Fourier analysis of boolean functions

The field of [analysis of boolean functions](#) aims to derive information about boolean functions by looking at their [Fourier expansion](#).

This involves expanding functions

$$f : \{0, 1\}^n \rightarrow \mathbb{R}$$

in terms of the characters of \mathbb{Z}_2^n . These characters are the parity functions

$$\chi_S(x) = (-1)^{\sum_{i \in S} x_i}.$$

Fourier analysis of boolean functions

The field of **analysis of boolean functions** aims to derive information about boolean functions by looking at their **Fourier expansion**.

This involves expanding functions

$$f : \{0, 1\}^n \rightarrow \mathbb{R}$$

in terms of the characters of \mathbb{Z}_2^n . These characters are the parity functions

$$\chi_S(x) = (-1)^{\sum_{i \in S} x_i}.$$

Any $f : \{0, 1\}^n \rightarrow \mathbb{R}$ has the expansion

$$f = \sum_{S \subseteq [n]} \hat{f}_S \chi_S$$

for some real $\{\hat{f}_S\}$ – the **Fourier coefficients** of f .

Applications of analysis of boolean functions

This approach has led to new results in a number of areas, including:

Applications of analysis of boolean functions

This approach has led to new results in a number of areas, including:

- **Property testing.** Given a constant number of uses of f , determine whether f has some property, or is far from having that property.

Applications of analysis of boolean functions

This approach has led to new results in a number of areas, including:

- **Property testing.** Given a constant number of uses of f , determine whether f has some property, or is far from having that property.
- **Structural properties.** If we know that f is boolean, what can we say about its Fourier expansion?

Applications of analysis of boolean functions

This approach has led to new results in a number of areas, including:

- **Property testing.** Given a constant number of uses of f , determine whether f has some property, or is far from having that property.
- **Structural properties.** If we know that f is boolean, what can we say about its Fourier expansion?
- **Computational learning.** Output an approximation to f , given $\text{poly}(n)$ uses of f and the promise that f is picked from a specific class of functions.

Applications of analysis of boolean functions

This approach has led to new results in a number of areas, including:

- **Property testing.** Given a constant number of uses of f , determine whether f has some property, or is far from having that property.
- **Structural properties.** If we know that f is boolean, what can we say about its Fourier expansion?
- **Computational learning.** Output an approximation to f , given $\text{poly}(n)$ uses of f and the promise that f is picked from a specific class of functions.

This talk: quantum generalisations of these results.

Quantum boolean functions

First step: to define the concept of a [quantum boolean function](#).

Quantum boolean functions

First step: to define the concept of a **quantum boolean function**.

Definition

A quantum boolean function (QBF) of n qubits is a unitary operator f on n qubits whose eigenvalues are all ± 1 .

Quantum boolean functions

First step: to define the concept of a **quantum boolean function**.

Definition

A quantum boolean function (QBF) of n qubits is a unitary operator f on n qubits whose eigenvalues are all ± 1 .

Is this a generalisation of the concept of a boolean function?

Quantum boolean functions

First step: to define the concept of a [quantum boolean function](#).

Definition

A quantum boolean function (QBF) of n qubits is a unitary operator f on n qubits whose eigenvalues are all ± 1 .

Is this a generalisation of the concept of a boolean function?

Yes: given any boolean function f , there are two natural ways of implementing f on a quantum computer:

Quantum boolean functions

First step: to define the concept of a **quantum boolean function**.

Definition

A quantum boolean function (QBF) of n qubits is a unitary operator f on n qubits whose eigenvalues are all ± 1 .

Is this a generalisation of the concept of a boolean function?

Yes: given any boolean function f , there are two natural ways of implementing f on a quantum computer:

- The *bit oracle* $|x\rangle|y\rangle \mapsto |x\rangle|y + f(x)\rangle$,

Quantum boolean functions

First step: to define the concept of a **quantum boolean function**.

Definition

A quantum boolean function (QBF) of n qubits is a unitary operator f on n qubits whose eigenvalues are all ± 1 .

Is this a generalisation of the concept of a boolean function?

Yes: given any boolean function f , there are two natural ways of implementing f on a quantum computer:

- The *bit oracle* $|x\rangle|y\rangle \mapsto |x\rangle|y + f(x)\rangle$,
- The *phase oracle* $|x\rangle \mapsto (-1)^{f(x)}|x\rangle$

...and both of these give QBFs.

Other examples of QBFs

A projector P onto any subspace gives rise to a QBF: take $f = \mathbb{I} - 2P$. Thus:

- Any quantum algorithm solving a decision problem gives rise to a QBF (consider it as a projector onto the “yes” inputs)
- Any quantum error correcting code gives rise to a QBF (via the projector onto the code space).

Other examples of QBFs

A projector P onto any subspace gives rise to a QBF: take $f = \mathbb{I} - 2P$. Thus:

- Any quantum algorithm solving a decision problem gives rise to a QBF (consider it as a projector onto the “yes” inputs)
- Any quantum error correcting code gives rise to a QBF (via the projector onto the code space).

There are uncountably many QBFs, even on one qubit: for any real θ , consider

$$f = \begin{pmatrix} \cos \theta & \sin \theta \\ \sin \theta & -\cos \theta \end{pmatrix}$$

“Fourier analysis” for QBFs

It turns out that a natural analogue of the characters of \mathbb{Z}_2 are the **Pauli matrices**:

$$\sigma^0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma^1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma^2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \text{and} \quad \sigma^3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

The Pauli matrices are all QBFs.

“Fourier analysis” for QBFs

It turns out that a natural analogue of the characters of \mathbb{Z}_2 are the **Pauli matrices**:

$$\sigma^0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma^1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma^2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \text{and} \quad \sigma^3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

The Pauli matrices are all QBFs.

We write a tensor product of Paulis (a **stabiliser operator**) as $\chi_{\mathbf{s}} \equiv \sigma^{s_1} \otimes \sigma^{s_2} \otimes \cdots \otimes \sigma^{s_n}$, where $s_j \in \{0, 1, 2, 3\}$.

“Fourier analysis” for QBFs

It turns out that a natural analogue of the characters of \mathbb{Z}_2 are the **Pauli matrices**:

$$\sigma^0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma^1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma^2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \text{and} \quad \sigma^3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

The Pauli matrices are all QBFs.

We write a tensor product of Paulis (a **stabiliser operator**) as $\chi_{\mathbf{s}} \equiv \sigma^{s_1} \otimes \sigma^{s_2} \otimes \cdots \otimes \sigma^{s_n}$, where $s_j \in \{0, 1, 2, 3\}$.

It's well known that any n qubit Hermitian operator f has an expansion

$$f = \sum_{\mathbf{s} \in \{0,1,2,3\}^n} \hat{f}_{\mathbf{s}} \chi_{\mathbf{s}},$$

with all the $\hat{f}_{\mathbf{s}}$ real. This is our analogue of the Fourier expansion of a function $f : \{0, 1\}^n \rightarrow \mathbb{R}$.

Norms and closeness

Some definitions we'll need later:

- The (normalised) Schatten p -norm: for any d -dimensional operator f ,

$$\|f\|_p \equiv \left(\frac{1}{d} \sum_{j=1}^d \sigma_j^p \right)^{\frac{1}{p}},$$

where $\{\sigma_j\}$ are the singular values of f .

Norms and closeness

Some definitions we'll need later:

- The (normalised) Schatten p -norm: for any d -dimensional operator f ,

$$\|f\|_p \equiv \left(\frac{1}{d} \sum_{j=1}^d \sigma_j^p \right)^{\frac{1}{p}},$$

where $\{\sigma_j\}$ are the singular values of f .

- Note the non-standard normalisation, and that, if f is a QBF, $\|f\|_p = 1$ for all p .

Norms and closeness

Some definitions we'll need later:

- The (normalised) Schatten p -norm: for any d -dimensional operator f ,

$$\|f\|_p \equiv \left(\frac{1}{d} \sum_{j=1}^d \sigma_j^p \right)^{\frac{1}{p}},$$

where $\{\sigma_j\}$ are the singular values of f .

- Note the non-standard normalisation, and that, if f is a QBF, $\|f\|_p = 1$ for all p .
- **Closeness:** Let f and g be two QBFs. Then we say that f and g are ϵ -close if $\|f - g\|_2^2 \leq 4\epsilon$.

Quantum property testing

Consider the following representative example:

Stabiliser testing

Given oracle access to an unknown QBF f on n qubits, determine whether f is a stabiliser operator χ_s for some s .

This problem is a generalisation of classical [linearity](#) testing.

Quantum property testing

Consider the following representative example:

Stabiliser testing

Given oracle access to an unknown QBF f on n qubits, determine whether f is a stabiliser operator χ_s for some s .

This problem is a generalisation of classical [linearity](#) testing.

We give a test (the [quantum stabiliser test](#)) that has the following property.

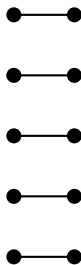
Proposition

Suppose that a QBF f passes the quantum stabiliser test with probability $1 - \epsilon$. Then f is ϵ -close to a stabiliser operator χ_s .

The test uses 2 queries (best known classical test uses 3).

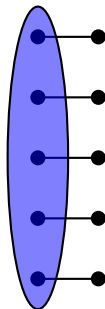
Quantum stabiliser testing algorithm (sketch)

- 1 Apply f to the halves of n maximally entangled states $|\Phi\rangle^{\otimes n}$ resulting in a quantum state $|f\rangle = f \otimes \mathbb{I}|\Phi\rangle^{\otimes n}$.



Quantum stabiliser testing algorithm (sketch)

- 1 Apply f to the halves of n maximally entangled states $|\Phi\rangle^{\otimes n}$ resulting in a quantum state $|f\rangle = f \otimes \mathbb{I}|\Phi\rangle^{\otimes n}$.



Quantum stabiliser testing algorithm (sketch)

- 1 Apply f to the halves of n maximally entangled states $|\Phi\rangle^{\otimes n}$ resulting in a quantum state $|f\rangle = f \otimes \mathbb{I}|\Phi\rangle^{\otimes n}$.
- 2 If f is a stabiliser then $|f\rangle$ should be an n -fold product of one of four possible states (corresponding to Paulis).

$$\sigma^1$$

$$\sigma^3$$

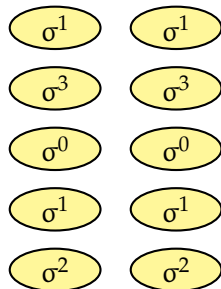
$$\sigma^0$$

$$\sigma^1$$

$$\sigma^2$$

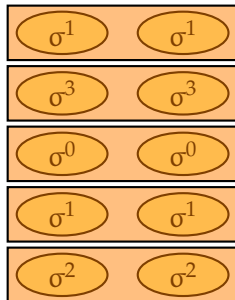
Quantum stabiliser testing algorithm (sketch)

- 1 Apply f to the halves of n maximally entangled states $|\Phi\rangle^{\otimes n}$ resulting in a quantum state $|f\rangle = f \otimes \mathbb{I}|\Phi\rangle^{\otimes n}$.
- 2 If f is a stabiliser then $|f\rangle$ should be an n -fold product of one of four possible states (corresponding to Paulis).
- 3 Create two copies of $|f\rangle$.



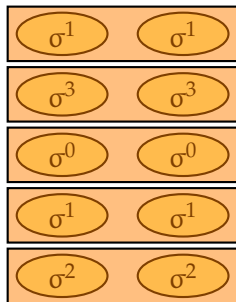
Quantum stabiliser testing algorithm (sketch)

- 1 Apply f to the halves of n maximally entangled states $|\Phi\rangle^{\otimes n}$ resulting in a quantum state $|f\rangle = f \otimes \mathbb{I}|\Phi\rangle^{\otimes n}$.
- 2 If f is a stabiliser then $|f\rangle$ should be an n -fold product of one of four possible states (corresponding to Paulis).
- 3 Create two copies of $|f\rangle$.
- 4 Perform a joint measurement on the two copies for each of the n qubits to see if they're both produced by the same Pauli operator.



Quantum stabiliser testing algorithm (sketch)

- 1 Apply f to the halves of n maximally entangled states $|\Phi\rangle^{\otimes n}$ resulting in a quantum state $|f\rangle = f \otimes \mathbb{I}|\Phi\rangle^{\otimes n}$.
- 2 If f is a stabiliser then $|f\rangle$ should be an n -fold product of one of four possible states (corresponding to Paulis).
- 3 Create two copies of $|f\rangle$.
- 4 Perform a joint measurement on the two copies for each of the n qubits to see if they're both produced by the same Pauli operator.
- 5 Accept if all measurements say "yes".



It turns out that for the stabiliser test $\Pr[\text{test accepts}] = \sum_s \hat{f}_s^4$, which implies the proposition.

Hypercontractivity and noise

- An essential component in many results in classical analysis of boolean functions is the **hypercontractive** inequality of Bonami, Gross and Beckner for functions $f : \{0, 1\}^n \rightarrow \mathbb{R}$.

Hypercontractivity and noise

- An essential component in many results in classical analysis of boolean functions is the **hypercontractive** inequality of Bonami, Gross and Beckner for functions $f : \{0, 1\}^n \rightarrow \mathbb{R}$.
- Informally, this result states that **local noise** applied to a function has a strong **global smoothing** effect.

Hypercontractivity and noise

- An essential component in many results in classical analysis of boolean functions is the **hypercontractive inequality** of Bonami, Gross and Beckner for functions $f : \{0, 1\}^n \rightarrow \mathbb{R}$.
- Informally, this result states that **local noise** applied to a function has a strong **global smoothing** effect.
- One possible generalisation of this result to **matrix-valued functions** $f : \{0, 1\}^n \rightarrow M_d$ was given by Ben-Aroya, Regev and de Wolf and used to prove bounds on generalised quantum random access codes.

Hypercontractivity and noise

- An essential component in many results in classical analysis of boolean functions is the **hypercontractive inequality** of Bonami, Gross and Beckner for functions $f : \{0, 1\}^n \rightarrow \mathbb{R}$.
- Informally, this result states that **local noise** applied to a function has a strong **global smoothing** effect.
- One possible generalisation of this result to **matrix-valued functions** $f : \{0, 1\}^n \rightarrow M_d$ was given by Ben-Aroya, Regev and de Wolf and used to prove bounds on generalised quantum random access codes.
- We state and prove a different generalisation, to **Hermitian operators** on n qubits, which has an interpretation in terms of the qubit depolarising channel.

Quantum hypercontractivity

- Let \mathcal{D}_ϵ be the qubit depolarising channel with noise rate $1 - \epsilon$, i.e. $\mathcal{D}_\epsilon(f) = \frac{(1-\epsilon)}{2} \text{tr}(f)\mathbb{I} + \epsilon f$.

Quantum hypercontractivity

- Let \mathcal{D}_ϵ be the qubit depolarising channel with noise rate $1 - \epsilon$, i.e. $\mathcal{D}_\epsilon(f) = \frac{(1-\epsilon)}{2} \text{tr}(f)\mathbb{I} + \epsilon f$.
- Let f be a Hermitian operator on n qubits and assume that $1 \leq p \leq 2 \leq q \leq \infty$. Then, provided that $\epsilon \leq \sqrt{\frac{p-1}{q-1}}$, we have

$$\|\mathcal{D}_\epsilon^{\otimes n}(f)\|_q \leq \|f\|_p.$$

Quantum hypercontractivity

- Let \mathcal{D}_ϵ be the qubit depolarising channel with noise rate $1 - \epsilon$, i.e. $\mathcal{D}_\epsilon(f) = \frac{(1-\epsilon)}{2} \text{tr}(f)\mathbb{I} + \epsilon f$.
- Let f be a Hermitian operator on n qubits and assume that $1 \leq p \leq 2 \leq q \leq \infty$. Then, provided that $\epsilon \leq \sqrt{\frac{p-1}{q-1}}$, we have

$$\|\mathcal{D}_\epsilon^{\otimes n}(f)\|_q \leq \|f\|_p.$$

Notes on the proof:

- Not a simple generalisation of the classical proof, but would be if the maximum output $p \rightarrow q$ norm were multiplicative!
- Proof is by induction on n and relies on a non-commutative generalisation of Hanner's inequality by King.

Application: A quantum FKN theorem

- The classical FKN (Friedgut-Kalai-Naor) theorem: Let f be a boolean function. Then, if $\sum_{|S|>1} \hat{f}_S^2 < \epsilon$, f is $O(\epsilon)$ -close to depending on 1 variable (being a dictator).

Application: A quantum FKN theorem

- The classical FKN (Friedgut-Kalai-Naor) theorem: Let f be a boolean function. Then, if $\sum_{|S|>1} \hat{f}_S^2 < \epsilon$, f is $O(\epsilon)$ -close to depending on 1 variable (being a dictator).
- Proof uses hypercontractivity, and generalises to the quantum case (fairly) straightforwardly, giving:

Application: A quantum FKN theorem

- The classical FKN (Friedgut-Kalai-Naor) theorem: Let f be a boolean function. Then, if $\sum_{|S|>1} \hat{f}_S^2 < \epsilon$, f is $O(\epsilon)$ -close to depending on 1 variable (being a dictator).
- Proof uses hypercontractivity, and generalises to the quantum case (fairly) straightforwardly, giving:

Quantum FKN theorem

Let f be a QBF. If

$$\sum_{|S|>1} \hat{f}_S^2 < \epsilon,$$

then there is a constant K such that f is $K\epsilon$ -close to being a dictator (acting non-trivially on only 1 qubit) or constant.

Application: A quantum FKN theorem

- The classical **FKN** (Friedgut-Kalai-Naor) theorem: Let f be a boolean function. Then, if $\sum_{|S|>1} \hat{f}_S^2 < \epsilon$, f is $O(\epsilon)$ -close to depending on 1 variable (being a **dictator**).
- Proof uses hypercontractivity, and generalises to the quantum case (fairly) straightforwardly, giving:

Quantum FKN theorem

Let f be a QBF. If

$$\sum_{|S|>1} \hat{f}_S^2 < \epsilon,$$

then there is a constant K such that f is $K\epsilon$ -close to being a dictator (acting non-trivially on only 1 qubit) or constant.

- This result is the first stab at understanding the structure of the Fourier expansion of QBFs.
- Applications? “Quantum voting”?

Computational learning of QBFs

What does it mean to **approximately learn** a quantum boolean function f ?

- Given some number of uses of f ...
- ...output (a classical description of) an approximation \tilde{f} ...
- ...such that \tilde{f} is ϵ -close to f .

Computational learning of QBFs

What does it mean to **approximately learn** a quantum boolean function f ?

- Given some number of uses of f ...
- ...output (a classical description of) an approximation \tilde{f} ...
- ...such that \tilde{f} is ϵ -close to f .

A natural dynamical counterpart of recent work by Aaronson on “pretty good” state tomography.

Computational learning of QBFs

What does it mean to **approximately learn** a quantum boolean function f ?

- Given some number of uses of f ...
- ...output (a classical description of) an approximation \tilde{f} ...
- ...such that \tilde{f} is ϵ -close to f .

A natural dynamical counterpart of recent work by Aaronson on “pretty good” state tomography.

We give a quantum algorithm that outputs the **large Fourier coefficients** of f . If f is almost completely determined by these, this is sufficient to approximately learn f .

Computational learning of QBFs

Quantum Goldreich-Levin algorithm

Given oracle access to a quantum boolean function f , and given $\gamma, \delta > 0$, there is a poly $\left(n, \frac{1}{\gamma}\right) \log\left(\frac{1}{\delta}\right)$ -time algorithm which outputs a list $L = \{\mathbf{s}_1, \mathbf{s}_2, \dots, \mathbf{s}_m\}$ such that with prob. $1 - \delta$: (1) if $|\hat{f}_{\mathbf{s}}| \geq \gamma$, then $\mathbf{s} \in L$; and (2) if $\mathbf{s} \in L$, $|\hat{f}_{\mathbf{s}}| \geq \gamma/2$.

Computational learning of QBFs

Quantum Goldreich-Levin algorithm

Given oracle access to a quantum boolean function f , and given $\gamma, \delta > 0$, there is a poly $\left(n, \frac{1}{\gamma}\right) \log\left(\frac{1}{\delta}\right)$ -time algorithm which outputs a list $L = \{\mathbf{s}_1, \mathbf{s}_2, \dots, \mathbf{s}_m\}$ such that with prob. $1 - \delta$: (1) if $|\hat{f}_{\mathbf{s}}| \geq \gamma$, then $\mathbf{s} \in L$; and (2) if $\mathbf{s} \in L$, $|\hat{f}_{\mathbf{s}}| \geq \gamma/2$.

Example: learning dynamics of a 1D spin chain. Informally:

Theorem

Let H be a Hamiltonian corresponding to an n -site spin chain, and let $t = O(\log n)$. Then we can approximately learn the QBFs $\sigma_j^s(t) \equiv e^{-itH} \sigma_j^s e^{itH}$ with poly(n) uses of e^{itH} .

Computational learning of QBFs

Quantum Goldreich-Levin algorithm

Given oracle access to a quantum boolean function f , and given $\gamma, \delta > 0$, there is a poly $\left(n, \frac{1}{\gamma}\right) \log\left(\frac{1}{\delta}\right)$ -time algorithm which outputs a list $L = \{\mathbf{s}_1, \mathbf{s}_2, \dots, \mathbf{s}_m\}$ such that with prob. $1 - \delta$: (1) if $|\hat{f}_{\mathbf{s}}| \geq \gamma$, then $\mathbf{s} \in L$; and (2) if $\mathbf{s} \in L$, $|\hat{f}_{\mathbf{s}}| \geq \gamma/2$.

Example: learning dynamics of a 1D spin chain. Informally:

Theorem

Let H be a Hamiltonian corresponding to an n -site spin chain, and let $t = O(\log n)$. Then we can approximately learn the QBFs $\sigma_j^s(t) \equiv e^{-itH} \sigma_j^s e^{itH}$ with poly(n) uses of e^{itH} .

So we can predict the outcome of measuring σ^s on site j after a short time, **on average** over all input states.

Conclusions

Summary:

- We've defined a quantum generalisation of the concept of a boolean function.
- Many classical results from the theory of boolean functions have natural quantum analogues.

Conclusions

Summary:

- We've defined a quantum generalisation of the concept of a boolean function.
- Many classical results from the theory of boolean functions have natural quantum analogues.

We still have many open conjectures... such as:

- **Conjecture:** There exists an efficient quantum property tester for dictators.
- **Conjecture:** Every traceless quantum boolean function has an influential qubit: there is a j such that $\| \text{tr}_j f \otimes \mathbb{I}/2 - f \|_2^2 = \Omega((\log n)/n)$.
- ...

The end

Further reading:

- Our paper: [arXiv:0810.2435](https://arxiv.org/abs/0810.2435).
- Survey paper by Ronald de Wolf:
<http://theoryofcomputing.org/articles/gs001/gs001.pdf>
- Lecture course by Ryan O'Donnell:
<http://www.cs.cmu.edu/~odonnell/boolean-analysis/>

The end

Further reading:

- Our paper: [arXiv:0810.2435](https://arxiv.org/abs/0810.2435).
- Survey paper by Ronald de Wolf:
<http://theoryofcomputing.org/articles/gs001/gs001.pdf>
- Lecture course by Ryan O'Donnell:
<http://www.cs.cmu.edu/~odonnell/boolean-analysis/>

Thanks for your time!