Quantum boolean functions

Ashley Montanaro[1] and Tobias Osborne[2]

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

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

3 December 2008

Introduction

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

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

Introduction

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

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

Many interpretations:

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

Analysis of boolean functions

Questions we might want to ask about boolean functions:

- Which functions are extremal in some sense?
  - e.g. least noise-sensitive, “fairest”, ...

Analysis of boolean functions

Questions we might want to ask about boolean functions:

- Which functions are extremal in some sense?
  - e.g. least noise-sensitive, "fairest", ...
- How complex is some specific (class of) function?
  - e.g. circuit complexity, decision tree complexity, learning complexity, ...

Analysis of boolean functions

Questions we might want to ask about boolean functions:

- Which functions are extremal in some sense?
  - e.g. least noise-sensitive, "fairest", ...
- How complex is some specific (class of) function?
  - e.g. circuit complexity, decision tree complexity, learning complexity, ...

The field of analysis of boolean functions aims to answer such questions.

Analysis of boolean functions

Questions we might want to ask about boolean functions:

- Which functions are extremal in some sense?
  - e.g. least noise-sensitive, "fairest", ...
- How complex is some specific (class of) function?
  - e.g. circuit complexity, decision tree complexity, learning complexity, ...

The field of analysis of boolean functions aims to answer such questions.

Ryan O'Donnell:

"By analysis of boolean functions, roughly speaking we mean deriving information about boolean functions by looking at their 'Fourier expansion'."

(See http://www.cs.cmu.edu/~odonnell/boolean-analysis/ for an entire course on the subject.)

Fourier analysis of boolean functions

For an n-bit boolean function, we need to do Fourier analysis over the group $\mathbb{Z}_2^n$. This involves expanding functions

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

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

For an n-bit boolean function, we need to do Fourier analysis over the group $\mathbb{Z}_2^n$. This involves expanding functions

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

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

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

One can show that any f has the expansion

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

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

Fourier analysis of boolean functions

For an n-bit boolean function, we need to do Fourier analysis over the group $\mathbb{Z}_2^n$. This involves expanding functions

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

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

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

One can show that any f has the expansion

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

for some $\{\hat{f}_S\}$ – the Fourier coefficients of f. How do we find them? By carrying out the Fourier transform over $\mathbb{Z}_2^n$ – i.e. a (renormalised) Hadamard transform!

Fourier analysis of boolean functions (2)

Think of f and $\hat{f}$ as 2^n-dimensional vectors; then

$$\hat{f} = \frac{1}{2^n} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}^{\otimes n} f.$$

Fourier analysis of boolean functions (2)

Think of f and $\hat{f}$ as 2^n-dimensional vectors; then

$$\hat{f} = \frac{1}{2^n} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}^{\otimes n} f.$$

The Fourier expansion gives us a notion of complexity of functions. The degree of a function f is defined as

$$\deg(f) = \max_{S, \hat{f}_S \neq 0} |S|.$$

Intuition: f has high degree $\Leftrightarrow$ f is complex.

Fourier analysis of boolean functions (2)

Think of f and $\hat{f}$ as 2^n-dimensional vectors; then

$$\hat{f} = \frac{1}{2^n} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}^{\otimes n} f.$$

The Fourier expansion gives us a notion of complexity of functions. The degree of a function f is defined as

$$\deg(f) = \max_{S, \hat{f}_S \neq 0} |S|.$$

Intuition: f has high degree $\Leftrightarrow$ f is complex.

So what can we do with Fourier analysis?

Property testing of boolean functions

Say two boolean functions f, g are ϵ-close if $\Pr_x[f(x) \neq g(x)] = \epsilon$.

Property testing of boolean functions

Say two boolean functions f, g are ϵ-close if $\Pr_x[f(x) \neq g(x)] = \epsilon$.

Problem

Given oracle access to a boolean function f, find a test T that:

Property testing of boolean functions

Say two boolean functions f, g are ϵ-close if $\Pr_x[f(x) \neq g(x)] = \epsilon$.

Problem

Given oracle access to a boolean function f, find a test T that:

1. uses f a constant number of times

Property testing of boolean functions

Say two boolean functions f, g are ϵ-close if $\Pr_x[f(x) \neq g(x)] = \epsilon$.

Problem

Given oracle access to a boolean function f, find a test T that:

1. uses f a constant number of times
2. outputs TRUE with certainty if f has property P

Property testing of boolean functions

Say two boolean functions f, g are ϵ-close if $\Pr_x[f(x) \neq g(x)] = \epsilon$.

Problem

Given oracle access to a boolean function f, find a test T that:

1. uses f a constant number of times
2. outputs True with certainty if f has property P
3. outputs False with probability at least δ if f is δ-close to having property P.

Property testing of boolean functions

Say two boolean functions f, g are ϵ-close if $\Pr_x[f(x) \neq g(x)] = \epsilon$.

Problem

Given oracle access to a boolean function f, find a test T that:

1. uses f a constant number of times
2. outputs TRUE with certainty if f has property P
3. outputs FALSE with probability at least δ if f is δ-close to having property P.

Example properties we might consider:

- Linearity ($f(x+y) = f(x) + f(y)$ for all x, y)
- Dictatorship ($f(x) = x_i$ for some i)

Structural/analytic properties of boolean functions

Problem

What can we say about the Fourier coefficients (or other "structural" property) of a boolean function?

Structural/analytic properties of boolean functions

Problem

What can we say about the Fourier coefficients (or other "structural" property) of a boolean function?

One principle: "Boolean functions have heavy tails": e.g.

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

Structural/analytic properties of boolean functions

Problem

What can we say about the Fourier coefficients (or other "structural" property) of a boolean function?

One principle: "Boolean functions have heavy tails": e.g.

1. The FKN (Friedgut-Kalai-Naor) theorem: If $\sum_{|S|>1} \hat{f}_S^2 < \epsilon$, then f is $O(\epsilon)$-close to depending on 1 variable (being a dictator).
2. Bourgain's theorem: If $\sum_{|S|>k} \hat{f}_S^2 < k^{-1/2-o(1)}$, then f is close to depending on k variables (being a k-junta).

Structural/analytic properties of boolean functions

Problem

What can we say about the Fourier coefficients (or other "structural" property) of a boolean function?

One principle: "Boolean functions have heavy tails": e.g.

1. The FKN (Friedgut-Kalai-Naor) theorem: If $\sum_{|S|>1} \hat{f}_S^2 < \epsilon$, then f is $O(\epsilon)$-close to depending on 1 variable (being a dictator).
2. Bourgain's theorem: If $\sum_{|S|>k} \hat{f}_S^2 < k^{-1/2-o(1)}$, then f is close to depending on k variables (being a k-junta).

These results have been useful in social choice theory and hardness of approximation.

Learning boolean functions

Problem

Given oracle access to a boolean function f promised to be in some class (e.g. low degree, "sparse",...), output a function $\tilde{f}$ such that $\tilde{f} \approx f$.

Learning boolean functions

Problem

Given oracle access to a boolean function f promised to be in some class (e.g. low degree, "sparse",...), output a function $\tilde{f}$ such that $\tilde{f} \approx f$.

Would usually expect that this would need $\sim 2^n$ queries to f.

Learning boolean functions

Problem

Given oracle access to a boolean function f promised to be in some class (e.g. low degree, "sparse",...), output a function $\tilde{f}$ such that $\tilde{f} \approx f$.

Would usually expect that this would need $\sim 2^n$ queries to f.

- Idea: If we can approximate $\hat{f}$, then we can approximate f.

Learning boolean functions

Problem

Given oracle access to a boolean function f promised to be in some class (e.g. low degree, "sparse",...), output a function $\tilde{f}$ such that $\tilde{f} \approx f$.

Would usually expect that this would need $\sim 2^n$ queries to f.

- Idea: If we can approximate $\hat{f}$, then we can approximate f.
- We can estimate an *individual* Fourier coefficient efficiently...

Learning boolean functions

Problem

Given oracle access to a boolean function f promised to be in some class (e.g. low degree, "sparse",...), output a function $\tilde{f}$ such that $\tilde{f} \approx f$.

Would usually expect that this would need $\sim 2^n$ queries to f.

- Idea: If we can approximate $\hat{f}$, then we can approximate f.
- We can estimate an *individual* Fourier coefficient efficiently...
- ...so if there aren't too many we can estimate f efficiently!

Learning boolean functions

Problem

Given oracle access to a boolean function f promised to be in some class (e.g. low degree, "sparse",...), output a function $\tilde{f}$ such that $\tilde{f} \approx f$.

Would usually expect that this would need $\sim 2^n$ queries to f.

- Idea: If we can approximate $\hat{f}$, then we can approximate f.
- We can estimate an *individual* Fourier coefficient efficiently...
- ...so if there aren't too many we can estimate f efficiently!

Important extension: the Goldreich-Levin algorithm, which outputs a list of the "large" Fourier coefficients of f "efficiently".

Quantum boolean functions

We'd like to generalise this body of work to the quantum regime. So we need to define the concept of a quantum boolean function.

Quantum boolean functions

We'd like to generalise this body of work to the quantum regime. So we need to define the concept of a quantum boolean function.

Definition

A quantum boolean function (QBF) of n qubits is an operator f on n qubits such that $f^2 = \mathbb{I}$.

Quantum boolean functions

We'd like to generalise this body of work to the quantum regime. So we need to define the concept of a quantum boolean function.

Definition

A quantum boolean function (QBF) of n qubits is an operator f on n qubits such that $f^2 = \mathbb{I}$.

The remainder of this talk:

- Basic consequences of this definition (why it's the *right* definition)
- Generalisations of classical results to QBFs (why it's an *interesting* definition)

Sanity checks of this definition

Sanity check 1: Can any QBF f be expressed as a quantum circuit?

Sanity checks of this definition

Sanity check 1: Can any QBF f be expressed as a quantum circuit?
Yes: f is a unitary operator.
(In fact, f's eigenvalues are all ± 1, so f is also Hermitian).

Sanity checks of this definition

Sanity check 1: Can any QBF f be expressed as a quantum circuit?
Yes: f is a unitary operator.
(In fact, f's eigenvalues are all ± 1, so f is also Hermitian).

Sanity check 2: Is the concept of QBF a generalisation of classical boolean functions?

Sanity checks of this definition

Sanity check 1: Can any QBF f be expressed as a quantum circuit?
Yes: f is a unitary operator.
(In fact, f's eigenvalues are all ± 1, so f is also Hermitian).

Sanity check 2: Is the concept of QBF a generalisation of classical boolean functions?
Yes: Given any classical boolean function $f : \{0,1\}^n \to \{0,1\}$, there are two natural ways of implementing f on a quantum computer:

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

Sanity checks of this definition

Sanity check 1: Can any QBF f be expressed as a quantum circuit?
Yes: f is a unitary operator.
(In fact, f's eigenvalues are all ± 1, so f is also Hermitian).

Sanity check 2: Is the concept of QBF a generalisation of classical boolean functions?
Yes: Given any classical boolean function $f : \{0,1\}^n \to \{0,1\}$, 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.
- Any quantum error correcting code gives rise to a QBF.

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.
- Any quantum error correcting code gives rise to a QBF.

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

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

Norms and inner products

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 inner products

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.
- If f is quantum boolean, then $\|f\|_p = 1$ for all p.

Norms and inner products

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.
- If f is quantum boolean, then $\|f\|_p = 1$ for all p.
- Note that $\|f\|_p$ is not a submultiplicative matrix norm (except at $p = \infty$), and that $p \geqslant q \Rightarrow \|f\|_p \geqslant \|f\|_q$.

Norms and inner products

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.
- If f is quantum boolean, then $\|f\|_p = 1$ for all p.
- Note that $\|f\|_p$ is not a submultiplicative matrix norm (except at $p = \infty$), and that $p \geqslant q \Rightarrow \|f\|_p \geqslant \|f\|_q$.
- We'll also use a (normalised) inner product on d-dimensional operators: $\langle f, g \rangle = \frac{1}{d}\operatorname{tr}(f^\dagger g)$.

Norms and inner products

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.
- If f is quantum boolean, then $\|f\|_p = 1$ for all p.
- Note that $\|f\|_p$ is not a submultiplicative matrix norm (except at $p = \infty$), and that $p \geqslant q \Rightarrow \|f\|_p \geqslant \|f\|_q$.
- We'll also use a (normalised) inner product on d-dimensional operators: $\langle f, g \rangle = \frac{1}{d}\operatorname{tr}(f^\dagger g)$.
- Note Hölder's inequality: for $1/p + 1/q = 1$, $|\langle f, g \rangle| \leqslant \|f\|_p \|g\|_q$.

“Fourier analysis” for QBFs

We want to find an analogue of Fourier analysis over $\mathbb{Z}_2^n$ for QBFs.

"Fourier analysis" for QBFs

We want to find an analogue of Fourier analysis over $\mathbb{Z}_2^n$ for QBFs.

The natural analogue of the characters of $\mathbb{Z}_2$ are the Pauli matrices:

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

The Pauli matrices are all QBFs.

"Fourier analysis" for QBFs

We want to find an analogue of Fourier analysis over $\mathbb{Z}_2^n$ for QBFs.

The natural analogue of the characters of $\mathbb{Z}_2$ are the Pauli matrices:

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

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

We want to find an analogue of Fourier analysis over $\mathbb{Z}_2^n$ for QBFs.

The natural analogue of the characters of $\mathbb{Z}_2$ are the Pauli matrices:

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

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 $s_j \in \{0, 1, 2, 3\}$.

We use the notation σ_i^j for the dictator which acts as σ^j at the i'th position, and trivially elsewhere.

"Fourier analysis" for QBFs (2)

The $\{\chi_{\mathbf{s}}\}$ operators form an orthonormal basis for the space of operators on n qubits, implying

- any n qubit Hermitian operator f has an expansion

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

  where $\hat{f}_{\mathbf{s}} = \langle f, \chi_{\mathbf{s}} \rangle \in \mathbb{R}$. This is our analogue of the Fourier expansion of a function $f : \{0,1\}^n \to \mathbb{R}$.

"Fourier analysis" for QBFs (2)

The $\{\chi_{\mathbf{s}}\}$ operators form an orthonormal basis for the space of operators on n qubits, implying

- any n qubit Hermitian operator f has an expansion

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

  where $\hat{f}_{\mathbf{s}} = \langle f, \chi_{\mathbf{s}} \rangle \in \mathbb{R}$. This is our analogue of the Fourier expansion of a function $f : \{0,1\}^n \to \mathbb{R}$.

- Plancherel's theorem and Parseval's equality:

“Fourier analysis” for QBFs (2)

The $\{\chi_{\mathbf{s}}\}$ operators form an orthonormal basis for the space of operators on n qubits, implying

- any n qubit Hermitian operator f has an expansion

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

  where $\hat{f}_{\mathbf{s}} = \langle f, \chi_{\mathbf{s}} \rangle \in \mathbb{R}$. This is our analogue of the Fourier expansion of a function $f : \{0,1\}^n \to \mathbb{R}$.

- Plancherel’s theorem and Parseval’s equality: If f and g are Hermitian operators on n qubits, $\langle f, g \rangle = \sum_{\mathbf{s}} \hat{f}_{\mathbf{s}} \hat{g}_{\mathbf{s}}$.

“Fourier analysis” for QBFs (2)

The $\{\chi_{\mathbf{s}}\}$ operators form an orthonormal basis for the space of operators on n qubits, implying

- any n qubit Hermitian operator f has an expansion

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

  where $\hat{f}_{\mathbf{s}} = \langle f, \chi_{\mathbf{s}} \rangle \in \mathbb{R}$. This is our analogue of the Fourier expansion of a function $f : \{0,1\}^n \to \mathbb{R}$.

- Plancherel’s theorem and Parseval’s equality: If f and g are Hermitian operators on n qubits, $\langle f, g \rangle = \sum_{\mathbf{s}} \hat{f}_{\mathbf{s}} \hat{g}_{\mathbf{s}}$. Moreover, $\|f\|_2^2 = \sum_{\mathbf{s}} \hat{f}_{\mathbf{s}}^2$.

"Fourier analysis" for QBFs (2)

The $\{\chi_\mathbf{s}\}$ operators form an orthonormal basis for the space of operators on n qubits, implying

- any n qubit Hermitian operator f has an expansion

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

  where $\hat{f}_\mathbf{s} = \langle f, \chi_\mathbf{s} \rangle \in \mathbb{R}$. This is our analogue of the Fourier expansion of a function $f : \{0,1\}^n \to \mathbb{R}$.

- Plancherel's theorem and Parseval's equality: If f and g are Hermitian operators on n qubits, $\langle f, g \rangle = \sum_\mathbf{s} \hat{f}_\mathbf{s} \hat{g}_\mathbf{s}$. Moreover, $\|f\|_2^2 = \sum_\mathbf{s} \hat{f}_\mathbf{s}^2$.

- Thus, if f is quantum boolean, $\sum_\mathbf{s} \hat{f}_\mathbf{s}^2 = 1$.

Generalising classical results to QBFs

Now we have our quantum analogue of a Fourier expansion, we can try to generalise classical results that depend on Fourier analysis. We find:

Generalising classical results to QBFs

Now we have our quantum analogue of a Fourier expansion, we can try to generalise classical results that depend on Fourier analysis. We find:

- Quantum property testers that determine with a small number of uses of an unknown QBF whether it is close to having some property.

Generalising classical results to QBFs

Now we have our quantum analogue of a Fourier expansion, we can try to generalise classical results that depend on Fourier analysis. We find:

- Quantum property testers that determine with a small number of uses of an unknown QBF whether it is close to having some property.
- Quantum analogues of computational learning results: an algorithm that outputs the large Fourier coefficients of an unknown QBF, accessed as an oracle.

Generalising classical results to QBFs

Now we have our quantum analogue of a Fourier expansion, we can try to generalise classical results that depend on Fourier analysis. We find:

- Quantum property testers that determine with a small number of uses of an unknown QBF whether it is close to having some property.
- Quantum analogues of computational learning results: an algorithm that outputs the large Fourier coefficients of an unknown QBF, accessed as an oracle.
- A quantum analogue of the FKN theorem regarding Fourier expansion of QBFs.

Generalising classical results to QBFs

Now we have our quantum analogue of a Fourier expansion, we can try to generalise classical results that depend on Fourier analysis. We find:

- Quantum property testers that determine with a small number of uses of an unknown QBF whether it is close to having some property.
- Quantum analogues of computational learning results: an algorithm that outputs the large Fourier coefficients of an unknown QBF, accessed as an oracle.
- A quantum analogue of the FKN theorem regarding Fourier expansion of QBFs.

In order to get this last result, we prove a quantum hypercontractive inequality which may be of independent interest.

Quantum property testing

We want to solve problems of the following kind.

Quantum property testing

Given access to a QBF f that is promised to either have some property, or to be "far" from having some property, determine which is the case, using a small number of uses of f.

Quantum property testing

We want to solve problems of the following kind.

Quantum property testing

Given access to a QBF f that is promised to either have some property, or to be "far" from having some property, determine which is the case, using a small number of uses of f.

We first need to define a notion of closeness for QBFs.

Closeness

Let f and g be two QBFs. Then we say that f and g are ϵ-close if $\langle f, g \rangle \geqslant 1 - 2\epsilon$ (equivalently, $\|f - g\|_2^2 \leqslant 4\epsilon$).

Note that the use of the 2-norm gives an average-case, rather than worst-case, notion of closeness.

Quantum property testing

Consider the following representative example:

Stabiliser testing

Given oracle access to an unknown operator f on n qubits, determine whether f is a stabiliser operator $\chi_{\mathbf{s}}$ for some $\mathbf{s}$.

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 operator f on n qubits, determine whether f is a stabiliser operator $\chi_{\mathbf{s}}$ for some $\mathbf{s}$.

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 $\chi_{\mathbf{s}}$.

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 $|f\rangle = f \otimes \mathbb{I}|\Phi\rangle^{\otimes n}$.
2. If f is a stabiliser then $|f\rangle$ should be an n-fold product of one of four possible states (corresponding to Paulis).

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".

Quantum stabiliser testing: proof of correctness

We can calculate the probability of saying "yes" using Fourier analysis. It turns out that for the stabiliser test

$$\Pr[\text{test accepts}] = \sum_{\mathbf{s}} \hat{f}_{\mathbf{s}}^4.$$

Quantum stabiliser testing: proof of correctness

We can calculate the probability of saying "yes" using Fourier analysis. It turns out that for the stabiliser test

$$\Pr[\text{test accepts}] = \sum_{\mathbf{s}} \hat{f}_{\mathbf{s}}^4.$$

Now, thanks to Parseval's relation, we have $\sum_{\mathbf{s}} \hat{f}_{\mathbf{s}}^2 = 1$, and, given that the test passes with probability $1 - \epsilon$, we thus have

$$1 - \epsilon \leqslant \sum_{\mathbf{s}} \hat{f}_{\mathbf{s}}^4$$

Quantum stabiliser testing: proof of correctness

We can calculate the probability of saying "yes" using Fourier analysis. It turns out that for the stabiliser test

$$\Pr[\text{test accepts}] = \sum_{\mathbf{s}} \hat{f}_{\mathbf{s}}^4.$$

Now, thanks to Parseval's relation, we have $\sum_{\mathbf{s}} \hat{f}_{\mathbf{s}}^2 = 1$, and, given that the test passes with probability $1 - \epsilon$, we thus have

$$1 - \epsilon \leqslant \sum_{\mathbf{s}} \hat{f}_{\mathbf{s}}^4 \leqslant \left(\max_{\mathbf{s}} \hat{f}_{\mathbf{s}}^2 \right) \sum_{\mathbf{s}} \hat{f}_{\mathbf{s}}^2$$

Quantum stabiliser testing: proof of correctness

We can calculate the probability of saying “yes” using Fourier analysis. It turns out that for the stabiliser test

$$\Pr[\text{test accepts}] = \sum_{\mathbf{s}} \hat{f}_{\mathbf{s}}^4.$$

Now, thanks to Parseval’s relation, we have $\sum_{\mathbf{s}} \hat{f}_{\mathbf{s}}^2 = 1$, and, given that the test passes with probability $1 - \epsilon$, we thus have

$$1 - \epsilon \leqslant \sum_{\mathbf{s}} \hat{f}_{\mathbf{s}}^4 \leqslant \left(\max_{\mathbf{s}} \hat{f}_{\mathbf{s}}^2\right) \sum_{\mathbf{s}} \hat{f}_{\mathbf{s}}^2 = \max_{\mathbf{s}} \hat{f}_{\mathbf{s}}^2.$$

Quantum stabiliser testing: proof of correctness

We can calculate the probability of saying "yes" using Fourier analysis. It turns out that for the stabiliser test

$$\Pr[\text{test accepts}] = \sum_{\mathbf{s}} \hat{f}_{\mathbf{s}}^4.$$

Now, thanks to Parseval's relation, we have $\sum_{\mathbf{s}} \hat{f}_{\mathbf{s}}^2 = 1$, and, given that the test passes with probability $1 - \epsilon$, we thus have

$$1 - \epsilon \leqslant \sum_{\mathbf{s}} \hat{f}_{\mathbf{s}}^4 \leqslant \left(\max_{\mathbf{s}} \hat{f}_{\mathbf{s}}^2\right) \sum_{\mathbf{s}} \hat{f}_{\mathbf{s}}^2 = \max_{\mathbf{s}} \hat{f}_{\mathbf{s}}^2.$$

So there is exactly one term $\hat{f}_{\mathbf{s}}^2$ which is greater than $1 - \epsilon$, and the rest are each smaller than ϵ.

Quantum stabiliser testing: proof of correctness

We can calculate the probability of saying "yes" using Fourier analysis. It turns out that for the stabiliser test

$$\Pr[\text{test accepts}] = \sum_{\mathbf{s}} \hat{f}_{\mathbf{s}}^4.$$

Now, thanks to Parseval's relation, we have $\sum_{\mathbf{s}} \hat{f}_{\mathbf{s}}^2 = 1$, and, given that the test passes with probability $1 - \epsilon$, we thus have

$$1 - \epsilon \leqslant \sum_{\mathbf{s}} \hat{f}_{\mathbf{s}}^4 \leqslant \left(\max_{\mathbf{s}} \hat{f}_{\mathbf{s}}^2\right) \sum_{\mathbf{s}} \hat{f}_{\mathbf{s}}^2 = \max_{\mathbf{s}} \hat{f}_{\mathbf{s}}^2.$$

So there is exactly one term $\hat{f}_{\mathbf{s}}^2$ which is greater than $1 - \epsilon$, and the rest are each smaller than ϵ. Thus f is ϵ-close to a stabiliser operator ($\langle f, \chi_{\mathbf{s}} \rangle > \sqrt{1 - \epsilon}$).

Other quantum property testers

Another obvious property we might want to test: locality.

Locality testing

Given oracle access to an unknown operator f on n qubits, determine whether f is a local operator $U_1 \otimes U_2 \otimes \cdots \otimes U_n$.

Other quantum property testers

Another obvious property we might want to test: locality.

Locality testing

Given oracle access to an unknown operator f on n qubits, determine whether f is a local operator $U_1 \otimes U_2 \otimes \cdots \otimes U_n$.

We have a test conjectured to solve this problem, but haven't been able to analyse its probability of success.

Other quantum property testers

Another obvious property we might want to test: locality.

Locality testing

Given oracle access to an unknown operator f on n qubits, determine whether f is a local operator $U_1 \otimes U_2 \otimes \cdots \otimes U_n$.

We have a test conjectured to solve this problem, but haven't been able to analyse its probability of success.

Conjecture

Let ρ be a quantum state on n qubits such that $\frac{1}{2^n} \sum_{S \subseteq [n]} \operatorname{tr} \rho_S^2$ is "high". Then ρ is "close" to a product state.

Other quantum property testers

Another obvious property we might want to test: locality.

Locality testing

Given oracle access to an unknown operator f on n qubits, determine whether f is a local operator $U_1 \otimes U_2 \otimes \cdots \otimes U_n$.

We have a test conjectured to solve this problem, but haven't been able to analyse its probability of success.

Conjecture

Let ρ be a quantum state on n qubits such that $\frac{1}{2^n} \sum_{S \subseteq [n]} \operatorname{tr} \rho_S^2$ is "high". Then ρ is "close" to a product state.

Can also define two versions of classical dictator testing: we have a test for one variant (stabiliser dictator testing), but not the other.

Hypercontractivity and noise

An essential component in many results in classical analysis of boolean functions is the hypercontractive inequality of Bonami, Gross and Beckner[1].

[1] See Lecture 16 of Ryan O'Donnell's notes (qv.) for bibliographic info.

Hypercontractivity and noise

An essential component in many results in classical analysis of boolean functions is the hypercontractive inequality of Bonami, Gross and Beckner[1].

For example, the inequality allows us to prove:

- Every balanced boolean function has an influential variable.
- Boolean functions that are not juntas have heavy "Fourier tails".

[1] See Lecture 16 of Ryan O'Donnell's notes (qv.) for bibliographic info.

Hypercontractivity and noise

An essential component in many results in classical analysis of boolean functions is the hypercontractive inequality of Bonami, Gross and Beckner[1].

For example, the inequality allows us to prove:

- Every balanced boolean function has an influential variable.
- Boolean functions that are not juntas have heavy "Fourier tails".

This inequality is most easily defined in terms of a noise operator which performs local smoothing.

[1] See Lecture 16 of Ryan O'Donnell's notes (qv.) for bibliographic info.

Hypercontractivity and noise

For a bit-string $x \in \{0,1\}^n$, define the distribution $y \sim_\epsilon x$:

- $y_i = x_i$ with probability $1/2 + \epsilon/2$
- $y_i = 1 - x_i$ with probability $1/2 - \epsilon/2$

Hypercontractivity and noise

For a bit-string $x \in \{0,1\}^n$, define the distribution $y \sim_\epsilon x$:

- $y_i = x_i$ with probability $1/2 + \epsilon/2$
- $y_i = 1 - x_i$ with probability $1/2 - \epsilon/2$

Then the noise operator with rate $-1 \leqslant \epsilon \leqslant 1$, written T_ϵ, is defined via

$$(T_\epsilon f)(x) = \mathbb{E}_{y \sim_\epsilon x}[f(y)].$$

Hypercontractivity and noise

For a bit-string $x \in \{0,1\}^n$, define the distribution $y \sim_\epsilon x$:

- $y_i = x_i$ with probability $1/2 + \epsilon/2$
- $y_i = 1 - x_i$ with probability $1/2 - \epsilon/2$

Then the noise operator with rate $-1 \leqslant \epsilon \leqslant 1$, written T_ϵ, is defined via

$$(T_\epsilon f)(x) = \mathbb{E}_{y \sim_\epsilon x}[f(y)].$$

Equivalently, T_ϵ may be defined by its action on Fourier coefficients, as

$$T_\epsilon f = \sum_{S \subseteq [n]} \epsilon^{|S|} \hat{f}_S \chi_S.$$

Hypercontractivity

Bonami-Gross-Beckner inequality

Let f be a function $f : \{0,1\}^n \to \mathbb{R}$ and assume that $1 \leqslant p \leqslant q \leqslant \infty$. Then, provided that

$$\epsilon \leqslant \sqrt{\frac{p-1}{q-1}},$$

we have

$$\|T_\epsilon f\|_q \leqslant \|f\|_p.$$

Hypercontractivity

Bonami-Gross-Beckner inequality

Let f be a function $f : \{0,1\}^n \to \mathbb{R}$ and assume that $1 \leqslant p \leqslant q \leqslant \infty$. Then, provided that

$$\epsilon \leqslant \sqrt{\frac{p-1}{q-1}},$$

we have

$$\|T_\epsilon f\|_q \leqslant \|f\|_p.$$

Intuition behind this inequality:

- For $p \leqslant q$, it always holds that $\|f\|_p \leqslant \|f\|_q$.
- This inequality says that, if we smooth f enough, then the inequality holds in the other direction too.

A quantum noise operator

We can immediately find a quantum version of the Fourier-theoretic definition of the noise operator.

Noise superoperator

The noise superoperator with rate $-1/3 \leqslant \epsilon \leqslant 1$, written T_ϵ, is defined as

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

A quantum noise operator

We can immediately find a quantum version of the Fourier-theoretic definition of the noise operator.

Noise superoperator

The noise superoperator with rate $-1/3 \leqslant \epsilon \leqslant 1$, written T_ϵ, is defined as

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

Turns out that this has an equivalent definition in terms of the qubit depolarising channel!

Noise superoperator (2)

$T_\epsilon f = \mathcal{D}_\epsilon^{\otimes n} f$, where $\mathcal{D}_\epsilon$ is the qubit depolarising channel with noise rate ϵ, i.e. $\mathcal{D}_\epsilon(f) = \frac{(1-\epsilon)}{2} \operatorname{tr}(f) \mathbb{I} + \epsilon f$.

(This connection is well-known, see e.g. [Kempe et al '08].)

Quantum hypercontractivity

It turns out that the naive generalisation of the classical hypercontractive inequality to a quantum hypercontractive inequality works!

Quantum hypercontractivity

It turns out that the naive generalisation of the classical hypercontractive inequality to a quantum hypercontractive inequality works!

Quantum hypercontractive inequality

Let f be a Hermitian operator on n qubits and assume that $1 \leqslant p \leqslant 2 \leqslant q \leqslant \infty$. Then, provided that

$$\epsilon \leqslant \sqrt{\frac{p-1}{q-1}},$$

we have

$$\|T_\epsilon f\|_q \leqslant \|f\|_p.$$

Proof sketch

- The proof is by induction on n. The case $n = 1$ follows immediately from the classical proof.

[2] C. King, "Inequalities for trace norms of 2x2 block matrices", 2003

Proof sketch

- The proof is by induction on n. The case $n = 1$ follows immediately from the classical proof.
- For $n > 1$, expand f as $f = \mathbb{I} \otimes a + \sigma^1 \otimes b + \sigma^2 \otimes c + \sigma^3 \otimes d$, and write it as a block matrix.

[2] C. King, "Inequalities for trace norms of 2x2 block matrices", 2003

Proof sketch

- The proof is by induction on n. The case $n = 1$ follows immediately from the classical proof.
- For $n > 1$, expand f as $f = \mathbb{I} \otimes a + \sigma^1 \otimes b + \sigma^2 \otimes c + \sigma^3 \otimes d$, and write it as a block matrix.
- Using a non-commutative Hanner's inequality for block matrices[2], can bound $\|T_\epsilon f\|_q$ in terms of the norm of a 2×2 matrix whose entries are the norms of the blocks of $T_\epsilon f$.

[2] C. King, "Inequalities for trace norms of 2x2 block matrices", 2003

Proof sketch

- The proof is by induction on n. The case $n = 1$ follows immediately from the classical proof.
- For $n > 1$, expand f as $f = \mathbb{I} \otimes a + \sigma^1 \otimes b + \sigma^2 \otimes c + \sigma^3 \otimes d$, and write it as a block matrix.
- Using a non-commutative Hanner's inequality for block matrices[2], can bound $\|T_\epsilon f\|_q$ in terms of the norm of a 2×2 matrix whose entries are the norms of the blocks of $T_\epsilon f$.
- Bound the norms of these blocks using the inductive hypothesis.

---

[2]C. King, "Inequalities for trace norms of 2x2 block matrices", 2003

Proof sketch

- The proof is by induction on n. The case $n = 1$ follows immediately from the classical proof.
- For $n > 1$, expand f as $f = \mathbb{I} \otimes a + \sigma^1 \otimes b + \sigma^2 \otimes c + \sigma^3 \otimes d$, and write it as a block matrix.
- Using a non-commutative Hanner's inequality for block matrices[2], can bound $\|T_\epsilon f\|_q$ in terms of the norm of a 2×2 matrix whose entries are the norms of the blocks of $T_\epsilon f$.
- Bound the norms of these blocks using the inductive hypothesis.
- The hypercontractive inequality for the base case $n = 1$ then gives an upper bound for this 2×2 matrix norm.

---

[2] C. King, "Inequalities for trace norms of 2x2 block matrices", 2003

Corollaries

There are some interesting corollaries of this result. We only mention one, about the degree of operators.

By analogy with the classical notion of degree, we define

$$\deg(f) = \max_{\mathbf{s}, \hat{f}_{\mathbf{s}} \neq 0} |\mathbf{s}|$$

for n-qubit operators f.

Corollaries

There are some interesting corollaries of this result. We only mention one, about the degree of operators.

By analogy with the classical notion of degree, we define

$$\deg(f) = \max_{\mathbf{s}, \hat{f}_{\mathbf{s}} \neq 0} |\mathbf{s}|$$

for n-qubit operators f. Then:

Different norms of low-degree operators are close

Let f be a Hermitian operator on n qubits with degree at most d. Then, for any $q \geqslant 2$, $\|f\|_q \leqslant (q-1)^{d/2} \|f\|_2$.

Proof of corollary

Different norms of low-degree operators are close

Let f be a Hermitian operator on n qubits with degree at most d. Then, for any $q \geqslant 2$, $\|f\|_q \leqslant (q-1)^{d/2}\|f\|_2$.

The proof is exactly the same as the original classical proof!

$$\|f\|_q^2 = \left\| \sum_{k=0}^{d} f^{=k} \right\|_q^2$$

Proof of corollary

Different norms of low-degree operators are close

Let f be a Hermitian operator on n qubits with degree at most d. Then, for any $q \geqslant 2$, $\|f\|_q \leqslant (q-1)^{d/2}\|f\|_2$.

The proof is exactly the same as the original classical proof!

$$\|f\|_q^2 = \left\|\sum_{k=0}^{d} f^{=k}\right\|_q^2 = \left\|T_{1/\sqrt{q-1}}\left(\sum_{k=0}^{d}(q-1)^{k/2} f^{=k}\right)\right\|_q^2$$

Proof of corollary

Different norms of low-degree operators are close

Let f be a Hermitian operator on n qubits with degree at most d. Then, for any $q \geqslant 2$, $\|f\|_q \leqslant (q-1)^{d/2}\|f\|_2$.

The proof is exactly the same as the original classical proof!

$$\begin{aligned}
\|f\|_q^2 &= \left\|\sum_{k=0}^{d} f^{=k}\right\|_q^2 = \left\|T_{1/\sqrt{q-1}}\left(\sum_{k=0}^{d}(q-1)^{k/2} f^{=k}\right)\right\|_q^2 \\
&\leqslant \left\|\sum_{k=0}^{d}(q-1)^{k/2} f^{=k}\right\|_2^2
\end{aligned}$$

Proof of corollary

Different norms of low-degree operators are close

Let f be a Hermitian operator on n qubits with degree at most d. Then, for any $q \geqslant 2$, $\|f\|_q \leqslant (q-1)^{d/2}\|f\|_2$.

The proof is exactly the same as the original classical proof!

$$
\begin{aligned}
\|f\|_q^2 &= \left\|\sum_{k=0}^{d} f^{=k}\right\|_q^2 = \left\|T_{1/\sqrt{q-1}}\left(\sum_{k=0}^{d}(q-1)^{k/2}f^{=k}\right)\right\|_q^2 \\
&\leqslant \left\|\sum_{k=0}^{d}(q-1)^{k/2}f^{=k}\right\|_2^2 = \sum_{k=0}^{d}(q-1)^k \sum_{\mathbf{s},|\mathbf{s}|=k} \hat{f}_{\mathbf{s}}^2
\end{aligned}
$$

Proof of corollary

Different norms of low-degree operators are close

Let f be a Hermitian operator on n qubits with degree at most d. Then, for any $q \geqslant 2$, $\|f\|_q \leqslant (q-1)^{d/2}\|f\|_2$.

The proof is exactly the same as the original classical proof!

$$\begin{aligned}
\|f\|_q^2 &= \left\| \sum_{k=0}^{d} f^{=k} \right\|_q^2 = \left\| T_{1/\sqrt{q-1}} \left(\sum_{k=0}^{d} (q-1)^{k/2} f^{=k} \right) \right\|_q^2 \\
&\leqslant \left\| \sum_{k=0}^{d} (q-1)^{k/2} f^{=k} \right\|_2^2 = \sum_{k=0}^{d} (q-1)^k \sum_{\mathbf{s}, |\mathbf{s}|=k} \hat{f}_{\mathbf{s}}^2 \\
&\leqslant (q-1)^d \sum_{\mathbf{s}} \hat{f}_{\mathbf{s}}^2
\end{aligned}$$

Proof of corollary

Different norms of low-degree operators are close

Let f be a Hermitian operator on n qubits with degree at most d. Then, for any $q \geqslant 2$, $\|f\|_q \leqslant (q-1)^{d/2}\|f\|_2$.

The proof is exactly the same as the original classical proof!

$$
\begin{aligned}
\|f\|_q^2 &= \left\|\sum_{k=0}^{d} f^{=k}\right\|_q^2 = \left\|T_{1/\sqrt{q-1}}\left(\sum_{k=0}^{d}(q-1)^{k/2}f^{=k}\right)\right\|_q^2 \\
&\leqslant \left\|\sum_{k=0}^{d}(q-1)^{k/2}f^{=k}\right\|_2^2 = \sum_{k=0}^{d}(q-1)^k \sum_{\mathbf{s},|\mathbf{s}|=k}\hat{f}_{\mathbf{s}}^2 \\
&\leqslant (q-1)^d\sum_{\mathbf{s}}\hat{f}_{\mathbf{s}}^2 = (q-1)^d\|f\|_2^2.
\end{aligned}
$$

A quantum FKN theorem

Once the hypercontractive inequality is established, the proof of the classical Friedgut-Kalai-Naor theorem goes through fairly straightforwardly (with one or two caveats).

A quantum FKN theorem

Once the hypercontractive inequality is established, the proof of the classical Friedgut-Kalai-Naor theorem goes through fairly straightforwardly (with one or two caveats).

Quantum FKN theorem

Let f be a QBF. If

$$\sum_{|\mathbf{s}|>1} \hat{f}_{\mathbf{s}}^2 < \epsilon,$$

then there is a constant K such that f is $K\epsilon$-close to being a dictator or constant.

A quantum FKN theorem

Once the hypercontractive inequality is established, the proof of the classical Friedgut-Kalai-Naor theorem goes through fairly straightforwardly (with one or two caveats).

Quantum FKN theorem

Let f be a QBF. If

$$\sum_{|\mathbf{s}|>1} \hat{f}_{\mathbf{s}}^2 < \epsilon,$$

then there is a constant K such that f is $K\epsilon$-close to being a dictator 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.

Examples:

- The Bernstein-Vazirani algorithm learns the class of classical parity functions χ_S exactly with one query.

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.

Examples:

- The Bernstein-Vazirani algorithm learns the class of classical parity functions χ_S exactly with one query.
- Can easily be extended to learn the class of stabilisers $\chi_{\mathbf{s}}$.

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.

Examples:

- The Bernstein-Vazirani algorithm learns the class of classical parity functions χ_S exactly with one query.
- Can easily be extended to learn the class of stabilisers $\chi_{\mathbf{s}}$.
- Robust against perturbation: if f is *close* to a stabiliser operator $\chi_{\mathbf{s}}$, we can find $\mathbf{s}$.

Quantum Goldreich-Levin algorithm

It turns out to be possible to estimate individual Fourier coefficients efficiently.

Lemma

For any $\mathbf{s} \in \{0, 1, 2, 3\}^n$ it is possible to estimate $\hat{f}_{\mathbf{s}}$ to within $\pm\eta$ with probability $1 - \delta$ with $O\left(\frac{1}{\eta^2} \log\left(\frac{1}{\delta}\right)\right)$ uses of f.

Quantum Goldreich-Levin algorithm

It turns out to be possible to estimate individual Fourier coefficients efficiently.

Lemma

For any $\mathbf{s} \in \{0, 1, 2, 3\}^n$ it is possible to estimate $\hat{f}_{\mathbf{s}}$ to within $\pm\eta$ with probability $1 - \delta$ with $O\left(\frac{1}{\eta^2} \log\left(\frac{1}{\delta}\right)\right)$ uses of f.

We can use this result to give the following algorithm for listing the “large” Fourier coefficients of a QBF.

Quantum Goldreich-Levin algorithm

It turns out to be possible to estimate individual Fourier coefficients efficiently.

Lemma

For any $\mathbf{s} \in \{0, 1, 2, 3\}^n$ it is possible to estimate $\hat{f}_{\mathbf{s}}$ to within $\pm\eta$ with probability $1 - \delta$ with $O\left(\frac{1}{\eta^2} \log\left(\frac{1}{\delta}\right)\right)$ uses of f.

We can use this result to give the following algorithm for listing the "large" Fourier coefficients of a QBF.

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 $L = \{\mathbf{s}_1, \mathbf{s}_2, \ldots, \mathbf{s}_m\}$ such that with prob. $1 - \delta$: (1) if $|\hat{f}_{\mathbf{s}}| \geqslant \gamma$, then $\mathbf{s} \in L$; and (2) if $\mathbf{s} \in L$, $|\hat{f}_{\mathbf{s}}| \geqslant \gamma/2$.

Learning quantum dynamics

This is sufficient, in some cases, to learn quantum dynamics.
What does this mean?

Learning quantum dynamics

This is sufficient, in some cases, to learn quantum dynamics. What does this mean?

- Given a Hamiltonian H, define the unitary operator $U = e^{itH}$.

Learning quantum dynamics

This is sufficient, in some cases, to learn quantum dynamics. What does this mean?

- Given a Hamiltonian H, define the unitary operator $U = e^{itH}$.
- We say that we have (γ, ϵ)-*learned* the dynamics of a Hermitian operator M if:

Learning quantum dynamics

This is sufficient, in some cases, to learn quantum dynamics. What does this mean?

- Given a Hamiltonian H, define the unitary operator $U = e^{itH}$.
- We say that we have (γ, ϵ)-*learned* the dynamics of a Hermitian operator M if:
  - given γ uses of U...

Learning quantum dynamics

This is sufficient, in some cases, to learn quantum dynamics. What does this mean?

- Given a Hamiltonian H, define the unitary operator $U = e^{itH}$.
- We say that we have (γ, ϵ)-*learned* the dynamics of a Hermitian operator M if:
  - given γ uses of U...
  - ...we can calculate an approximation $\widetilde{U^\dagger M U}$...

Learning quantum dynamics

This is sufficient, in some cases, to learn quantum dynamics. What does this mean?

- Given a Hamiltonian H, define the unitary operator $U = e^{itH}$.
- We say that we have (γ, ϵ)-*learned* the dynamics of a Hermitian operator M if:
  - given γ uses of U...
  - ...we can calculate an approximation $\widetilde{U^\dagger M U}$...
  - ...such that $\|\widetilde{U^\dagger M U} - U^\dagger M U\|_2^2 \leqslant \epsilon$.

Learning quantum dynamics

This is sufficient, in some cases, to learn quantum dynamics. What does this mean?

- Given a Hamiltonian H, define the unitary operator $U = e^{itH}$.
- We say that we have (γ, ϵ)-*learned* the dynamics of a Hermitian operator M if:
  - given γ uses of U...
  - ...we can calculate an approximation $\widetilde{U^\dagger M U}$...
  - ...such that $\|\widetilde{U^\dagger M U} - U^\dagger M U\|_2^2 \leqslant \epsilon$.
- This means that we can approximately predict the outcome of measurement M.

Example: a 1D spin chain

Consider a Hamiltonian which can be written

$$H = \sum_{j=1}^{n-1} h_j$$

with h_j Hermitian, $\|h_j\|_\infty = O(1)$, and $\mathrm{supp}(h_j) \subset \{j, j+1\}$ for $j \leqslant n-1$.

Example: a 1D spin chain

Consider a Hamiltonian which can be written

$$H = \sum_{j=1}^{n-1} h_j$$

with h_j Hermitian, $\|h_j\|_\infty = O(1)$, and $\mathrm{supp}(h_j) \subset \{j, j+1\}$ for $j \leqslant n-1$.

Theorem

Let $t = O(\log(n))$. Then, with probability $1 - \delta$ we can (γ, ϵ)-learn the quantum boolean functions $\sigma_j^s(t) \equiv e^{-itH}\sigma_j^s e^{itH}$ with $\gamma = \mathrm{poly}(n, 1/\epsilon, \log(1/\delta))$ uses of e^{itH}.

Example: a 1D spin chain

Consider a Hamiltonian which can be written

$$H = \sum_{j=1}^{n-1} h_j$$

with h_j Hermitian, $\|h_j\|_\infty = O(1)$, and $\mathrm{supp}(h_j) \subset \{j, j+1\}$ for $j \leqslant n-1$.

Theorem

Let $t = O(\log(n))$. Then, with probability $1-\delta$ we can (γ, ϵ)-learn the quantum boolean functions $\sigma_j^s(t) \equiv e^{-itH} \sigma_j^s e^{itH}$ with $\gamma = \mathrm{poly}(n, 1/\epsilon, \log(1/\delta))$ uses of e^{itH}.

What does this mean? We can predict the outcome of measuring σ^s on site j after a short time well 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 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 quantum analogues.

We still have many open conjectures...

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 quantum analogues.

We still have many open conjectures...

- For a QBF f acting non-trivially on n qubits, does it hold that $\deg(f) = \Omega(\log n)$?

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 quantum analogues.

We still have many open conjectures...

- For a QBF f acting non-trivially on n qubits, does it hold that $\deg(f) = \Omega(\log n)$?
- Further property testers: locality, dictatorship, ...

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 quantum analogues.

We still have many open conjectures...

- For a QBF f acting non-trivially on n qubits, does it hold that $\deg(f) = \Omega(\log n)$?
- Further property testers: locality, dictatorship, ...
- Does every QBF have an influential qubit?

The end

Further reading:

- Our paper: arXiv: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.
- 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!