A quantum analogue of Fourier analysis on the boolean cube

Ashley Montanaro

Department of Computer Science
University of Bristol
Bristol, UK

QIPC Rome 2009

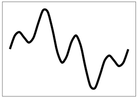
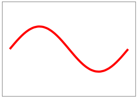
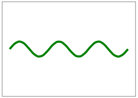
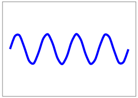
Talk based on joint work with Tobias Osborne

University of Bristol

QICS

Fourier analysis

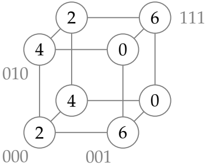
...traditionally looks like this:

 $= 3\times$  $-$  $+2\times$ 

- Given some function $f : \mathbb{R} \to \mathbb{R}$...
- ...we expand it in terms of trigonometric functions $\sin(kx)$, $\cos(kx)$...
- ...in an attempt to understand the structure of f.

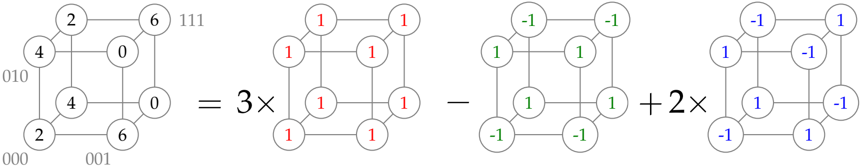
Fourier analysis

In computer science, it's natural to consider functions on the set of n-bit strings – also known as the boolean cube $\{0,1\}^n$:



Fourier analysis

In computer science, it's natural to consider functions on the set of *n*-bit strings – also known as the boolean cube $\{0,1\}^n$:



- Given some function $f : \{0,1\}^n \to \mathbb{R}$...
- ...we expand it in terms of parity functions...
- ...in an attempt to understand the structure of f.

This talk

- The classical theory of Fourier analysis on the boolean cube
- A quantum generalisation
- Application: Testing for Pauli operators
- The qubit depolarising channel
- Application: Spectra of k-local operators

Fourier analysis on the boolean cube

We expand functions $f : \{0,1\}^n \to \mathbb{R}$ in terms of the parity functions

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

also known as the characters of $\mathbb{Z}_2^n$.

Fourier analysis on the boolean cube

We expand functions $f : \{0,1\}^n \to \mathbb{R}$ in terms of the parity functions

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

also known as the characters of $\mathbb{Z}_2^n$.

There are 2^n of these functions, indexed by subsets $S \subseteq \{1,\ldots,n\}$. $\chi_S(x) = -1$ if the no. of bits of x in S set to 1 is odd.

Fourier analysis on the boolean cube

We expand functions $f : \{0,1\}^n \to \mathbb{R}$ in terms of the parity functions

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

also known as the characters of $\mathbb{Z}_2^n$.

There are 2^n of these functions, indexed by subsets $S \subseteq \{1, \ldots, n\}$. $\chi_S(x) = -1$ if the no. of bits of x in S set to 1 is odd.

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

$$f = \sum_{S \subseteq \{1,\ldots,n\}} \hat{f}_S \, \chi_S$$

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

Applications of Fourier analysis on the boolean cube

This approach has led to new results in many areas of classical computer science, including:

- Probabilistically checkable proofs [Håstad '01; Dinur '07; . . .]
- Decision tree complexity [Nisan & Szegedy '94]
- Influence of voters and fairness of elections [Kahn, Kalai, Linial '88; Kalai '02]
- Computational learning theory [Goldreich & Levin '89; Kushilevitz & Mansour '91; . . .]
- Property testing [Bellare et al '95; Matulef et al '09; . . .]

Property testing

The property testing model is defined as follows.

- We are given access to a boolean function f on n bits as a black box which we can query on inputs of our choice.

Property testing

The property testing model is defined as follows.

- We are given access to a boolean function f on n bits as a black box which we can query on inputs of our choice.
- We want to output whether f has some property P, or is "far" from having property P, using a constant number of queries.

Property testing

The property testing model is defined as follows.

- We are given access to a boolean function f on n bits as a black box which we can query on inputs of our choice.
- We want to output whether f has some property P, or is "far" from having property P, using a constant number of queries.
- Sample problem: Determine whether f is linear, or "far" from linear: i.e. differs from all linear functions in a constant fraction of places.

Applications in quantum computation

There have also been some recent applications of Fourier analysis to quantum computer science.

- Quantum algorithms for computational learning
  [Bshouty & Jackson '95; Atici & Servedio '07]
- Quantum communication complexity
  [Klauck '01; Gavinsky et al '07]
- Lower bounds on quantum locally decodable codes
  [Ben-Aroya, Regev, de Wolf '08]
- Quantum algorithms with exponential speed-ups
  [Roetteler '08; AM '08]

A generalisation of Fourier analysis

We would like to generalise these results to a quantum (noncommutative) setting.

A generalisation of Fourier analysis

We would like to generalise these results to a quantum (noncommutative) setting.

Why?

1. Because we can: generalisations are generally interesting
2. The classical theory is very successful – maybe a quantum theory will be too
3. Results in the classical theory become conjectures in the quantum theory

A generalisation of Fourier analysis

We would like to generalise these results to a quantum (noncommutative) setting.

Why?

1. Because we can: generalisations are generally interesting
2. The classical theory is very successful – maybe a quantum theory will be too
3. Results in the classical theory become conjectures in the quantum theory

Our generalisation: instead of decomposing functions $\{0,1\}^n \to \mathbb{C}$, we decompose linear operators on the space of n qubits.

“Fourier analysis” for qubits

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

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

“Fourier analysis” for qubits

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

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

We write a tensor product of Paulis 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 qubits

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

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

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

Any n qubit linear operator f has an expansion

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

for some $\{\hat{f}_{\mathbf{s}}\}$ – the Pauli coefficients of f. This is our analogue of the Fourier expansion of a function $f : \{0, 1\}^n \to \mathbb{C}$.

Norms and closeness

Some definitions we'll need later:

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

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

  where $\{\sigma_j\}$ are the singular values of M.
- Note that $\|M\|_p$ increases with p.

Norms and closeness

Some definitions we'll need later:

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

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

  where $\{\sigma_j\}$ are the singular values of M.
- Note that $\|M\|_p$ increases with p.
- With this definition we have a (quantum) Parseval's equality:

$$\|M\|_2^2 = \sum_{\mathbf{s} \in \{0,1,2,3\}^n} |\hat{M}_{\mathbf{s}}|^2.$$

Norms and closeness

Some definitions we'll need later:

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

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

  where $\{\sigma_j\}$ are the singular values of M.
- Note that $\|M\|_p$ increases with p.
- With this definition we have a (quantum) Parseval's equality:

$$\|M\|_2^2 = \sum_{\mathbf{s} \in \{0,1,2,3\}^n} |\hat{M}_{\mathbf{s}}|^2.$$

- Closeness: Let U and V be two linear operators. Then we say that f and g are ϵ-close if $\|U - V\|_2^2 \leqslant 4\epsilon$.

Quantum property testing

Consider the following representative example:

Pauli testing

Given oracle access to an unknown unitary operator U on n qubits, determine whether U is a Pauli 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:

Pauli testing

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

This problem is a generalisation of classical linearity testing.

We give a test (the quantum Pauli test) that has the following property.

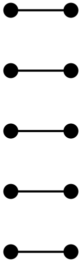
Proposition

Suppose that a unitary operator U passes the quantum Pauli test with probability $1 - \epsilon$. Then U is ϵ-close to a Pauli operator (with phase) $e^{i\phi}\chi_{\mathbf{s}}$.

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

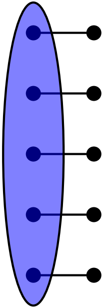
Quantum Pauli testing algorithm (sketch)

1. Apply U to the first halves of n Bell pairs $|\Phi\rangle^{\otimes n}$, resulting in a quantum state $|u\rangle = U \otimes \mathbb{I}|\Phi\rangle^{\otimes n}$.



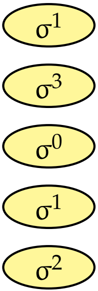
Quantum Pauli testing algorithm (sketch)

1. Apply U to the first halves of n Bell pairs $|\Phi\rangle^{\otimes n}$, resulting in a quantum state $|u\rangle = U \otimes \mathbb{I}|\Phi\rangle^{\otimes n}$.



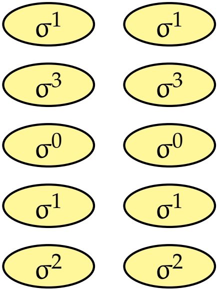
Quantum Pauli testing algorithm (sketch)

1. Apply U to the first halves of n Bell pairs $|\Phi\rangle^{\otimes n}$, resulting in a quantum state $|u\rangle = U \otimes \mathbb{I}|\Phi\rangle^{\otimes n}$.
2. If U is a Pauli then $|u\rangle$ should be an n-fold product of one of four possible states (corresponding to $\sigma^0 \ldots \sigma^3$).



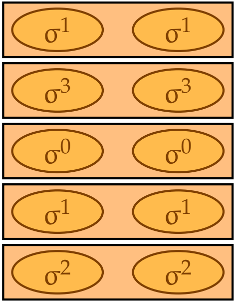
Quantum Pauli testing algorithm (sketch)

1. Apply U to the first halves of n Bell pairs $|\Phi\rangle^{\otimes n}$, resulting in a quantum state $|u\rangle = U \otimes \mathbb{I}|\Phi\rangle^{\otimes n}$.
2. If U is a Pauli then $|u\rangle$ should be an n-fold product of one of four possible states (corresponding to $\sigma^0 \ldots \sigma^3$).
3. Create two copies of $|u\rangle$.



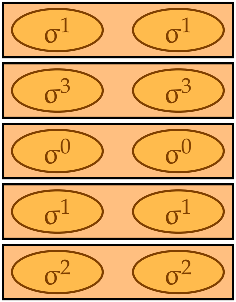
Quantum Pauli testing algorithm (sketch)

1. Apply U to the first halves of n Bell pairs $|\Phi\rangle^{\otimes n}$, resulting in a quantum state $|u\rangle = U \otimes \mathbb{I}|\Phi\rangle^{\otimes n}$.
2. If U is a Pauli then $|u\rangle$ should be an n-fold product of one of four possible states (corresponding to $\sigma^0 \ldots \sigma^3$).
3. Create two copies of $|u\rangle$.
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 Pauli testing algorithm (sketch)

1. Apply U to the first halves of n Bell pairs $|\Phi\rangle^{\otimes n}$, resulting in a quantum state $|u\rangle = U \otimes \mathbb{I}|\Phi\rangle^{\otimes n}$.
2. If U is a Pauli then $|u\rangle$ should be an n-fold product of one of four possible states (corresponding to $\sigma^0 \dots \sigma^3$).
3. Create two copies of $|u\rangle$.
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 Pauli test $\Pr[\text{test accepts}] = \sum_{\mathbf{s}} |\hat{U}_{\mathbf{s}}|^4$, which implies the proposition by Parseval's equality.

The Pauli operators and depolarising noise

The Pauli expansion can help us understand the qubit depolarising channel.

The Pauli operators and depolarising noise

The Pauli expansion can help us understand the qubit depolarising channel.

- Let $\mathcal{D}_\epsilon$ be the qubit depolarising channel with noise rate $1-\epsilon$, i.e.

$$\mathcal{D}_\epsilon(\rho) = \frac{(1-\epsilon)}{2} \operatorname{tr}(\rho)\mathbb{I} + \epsilon\,\rho.$$

The Pauli operators and depolarising noise

The Pauli expansion can help us understand the qubit depolarising channel.

- Let $\mathcal{D}_\epsilon$ be the qubit depolarising channel with noise rate $1 - \epsilon$, i.e.

$$\mathcal{D}_\epsilon(\rho) = \frac{(1-\epsilon)}{2} \operatorname{tr}(\rho)\mathbb{I} + \epsilon\, \rho.$$

- Then

$$\mathcal{D}_\epsilon^{\otimes n}(\rho) = \sum_{\mathbf{s} \in \{0,1,2,3\}^n} \epsilon^{|\mathbf{s}|}\, \hat{\rho}_{\mathbf{s}}\, \chi_{\mathbf{s}}.$$

(this connection goes back at least a decade [Bruss et al '99], and was used in [Kempe et al '08] to give upper bounds on fault-tolerance thresholds)

The Pauli operators and depolarising noise

The Pauli expansion can help us understand the qubit depolarising channel.

- Let $\mathcal{D}_\epsilon$ be the qubit depolarising channel with noise rate $1 - \epsilon$, i.e.

$$\mathcal{D}_\epsilon(\rho) = \frac{(1-\epsilon)}{2} \operatorname{tr}(\rho)\mathbb{I} + \epsilon\, \rho.$$

- Then

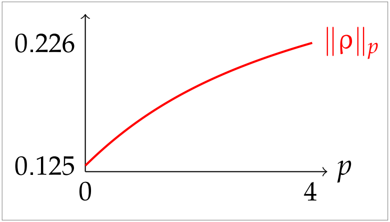
$$\mathcal{D}_\epsilon^{\otimes n}(\rho) = \sum_{\mathbf{s} \in \{0,1,2,3\}^n} \epsilon^{|\mathbf{s}|}\, \hat{\rho}_{\mathbf{s}}\, \chi_{\mathbf{s}}.$$

(this connection goes back at least a decade [Bruss et al '99], and was used in [Kempe et al '08] to give upper bounds on fault-tolerance thresholds)

We are interested in the smoothing effect of this channel.

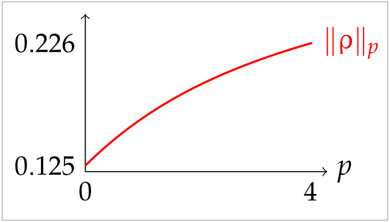
The qubit depolarising channel and p-norms

p-norms of a random quantum state ρ increase with p:

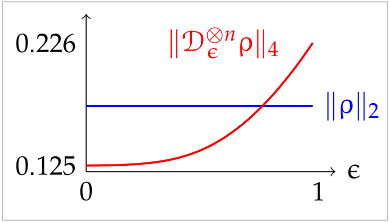


The qubit depolarising channel and p-norms

p-norms of a random quantum state ρ increase with p:



Applying depolarising noise smooths ρ by reducing its higher norms:



Quantum hypercontractivity

Proposition

Let H 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

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

Quantum hypercontractivity

Proposition

Let H 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

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

- This is a quantum generalisation of a hypercontractive inequality of Bonami, Gross and Beckner for functions $f : \{0,1\}^n \to \mathbb{R}$, which is an essential component in many results in classical analysis of boolean functions.

Quantum hypercontractivity

Proposition

Let H 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

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

- This is a quantum generalisation of a hypercontractive inequality of Bonami, Gross and Beckner for functions $f : \{0,1\}^n \to \mathbb{R}$, which is an essential component in many results in classical analysis of boolean functions.
- The quantum proof isn't a simple generalisation of the classical proof, but would be if the maximum output $p \to q$ norm were multiplicative!

Application: Spectra of k-local operators

A Hamiltonian H on n qubits is said to be k-local if it has a decomposition

$$H = \sum_i H_i$$

where each H_i acts nontrivially on at most k sites.

Application: Spectra of k-local operators

A Hamiltonian H on n qubits is said to be k-local if it has a decomposition

$$H = \sum_i H_i$$

where each H_i acts nontrivially on at most k sites.

Our results show that the spectra of k-local operators are "smooth". In particular:

- For any $q \geqslant 2$, $\|H\|_q \leqslant (q-1)^{k/2}\|H\|_2$
- $\text{rank}(H) \geqslant 2^{n-O(k)}$ (a quantum Schwartz-Zippel lemma)
- ...

Conclusions

Summary:

- We've defined a quantum generalisation of the concept of Fourier analysis on the boolean cube.
- Many results from the classical theory have natural quantum analogues.

Conclusions

Summary:

- We've defined a quantum generalisation of the concept of Fourier analysis on the boolean cube.
- Many results from the classical theory 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 operator $U^2 = \mathbb{I}$ has an influential qubit: there is a j such that $\| \operatorname{tr}_j U \otimes \mathbb{I}/2 - U\|_2^2 = \Omega((\log n)/n)$.
- ...

The end

Further reading:

- "Quantum boolean functions", AM & Tobias Osborne, arXiv:0810.2435.
- "Learning and testing algorithms for the Clifford group", Richard Low, arXiv:0907.2833.
- 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:

- “Quantum boolean functions”, AM & Tobias Osborne, arXiv:0810.2435.
- “Learning and testing algorithms for the Clifford group”, Richard Low, arXiv:0907.2833.
- 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!

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).
- Applications to social choice theory and used as part of a proof of the PCP theorem [Dinur '07].

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).
- Applications to social choice theory and used as part of a proof of the PCP theorem [Dinur '07].
- 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).
- Applications to social choice theory and used as part of a proof of the PCP theorem [Dinur '07].
- Proof uses hypercontractivity, and generalises to the quantum case (fairly) straightforwardly, giving:

Quantum FKN theorem

Let U be a unitary operator on n qubits with eigenvalues ± 1. If

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

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

Approximate learning of unitary operators

What does it mean to approximately learn a unitary operator U?

Approximate learning of unitary operators

What does it mean to approximately learn a unitary operator U?

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

Approximate learning of unitary operators

What does it mean to approximately learn a unitary operator U?

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

A natural dynamical counterpart of recent work on "pretty good" state tomography [Aaronson '07].

Approximate learning of unitary operators

What does it mean to approximately learn a unitary operator U?

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

A natural dynamical counterpart of recent work on "pretty good" state tomography [Aaronson '07].

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

Computational learning of unitary operators

"Quantum Goldreich-Levin" algorithm

Given oracle access to a unitary U, 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 $|\hat{U}_{\mathbf{s}}| \geqslant \gamma$, then $\mathbf{s} \in L$; and (2) if $\mathbf{s} \in L$, $|\hat{U}_{\mathbf{s}}| \geqslant \gamma/2$.

Computational learning of unitary operators

"Quantum Goldreich-Levin" algorithm

Given oracle access to a unitary U, and given $\gamma, \delta > 0$, there is a $\mathrm{poly}\left(n, \frac{1}{\gamma}\right) \log\left(\frac{1}{\delta}\right)$-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 $|\hat{U}_{\mathbf{s}}| \geqslant \gamma$, then $\mathbf{s} \in L$; and (2) if $\mathbf{s} \in L$, $|\hat{U}_{\mathbf{s}}| \geqslant \gamma/2$.

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 operators $\sigma_j^s(t) \equiv e^{-itH} \sigma_j^s e^{itH}$ with $\mathrm{poly}(n)$ uses of e^{itH}.

Computational learning of unitary operators

"Quantum Goldreich-Levin" algorithm

Given oracle access to a unitary U, 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 $|\hat{U}_{\mathbf{s}}| \geqslant \gamma$, then $\mathbf{s} \in L$; and (2) if $\mathbf{s} \in L$, $|\hat{U}_{\mathbf{s}}| \geqslant \gamma/2$.

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 operators $\sigma_j^s(t) \equiv e^{-itH}\sigma_j^s e^{itH}$ 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.