Testing quantum satisfiability

Changpeng Shao

Academy of Mathematics and Systems Science, Chinese Academy of Sciences
joint work with Ashley Montanaro and Dominic Verdon
arXiv:2301.10699

Quantum Theory and Operator Theory
BIMSA, August 26 - 30, 2024

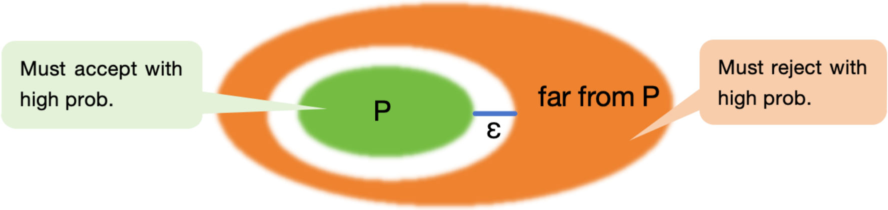
Table of Contents

Property testing

High level idea: Determine whether an unknown "massive object" has some property $\mathcal{P}$ of interest or far from having the property, while inspecting only a tiny fraction of the object.

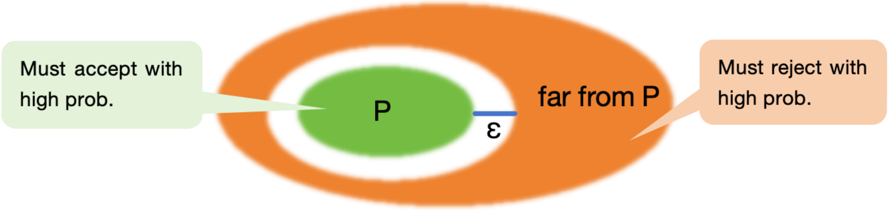
Property testing

"far from" is determined by some distance $\mathrm{dist}(f, \mathcal{P}) := \min_{g \in \mathcal{P}} \mathrm{dist}(f, g)$.



Property testing

“far from” is determined by some distance $\mathrm{dist}(f, \mathcal{P}) := \min_{g \in \mathcal{P}} \mathrm{dist}(f, g)$.



E.g., testing triangle-freeness in a graph:

- accept if triangle-free (i.e., no triangles)
- reject if a constant fraction of edges should be removed in order to be triangle-free.

Importance of property testing

- A relaxation of decision problems:
  - If the object is very large, it is infeasible to examine all of it and we must design algorithms that examine only a small part of the object.
  - The object is not too large to fully examine, but the exact decision problem is NP-hard, e.g., SAT, k-Colorability.

Importance of property testing

- A relaxation of decision problems:
  - If the object is very large, it is infeasible to examine all of it and we must design algorithms that examine only a small part of the object.
  - The object is not too large to fully examine, but the exact decision problem is NP-hard, e.g., SAT, k-Colorability.
- A relaxation of learning problems:
  - Instead of output a good estimate of f when $f \in \mathcal{F}$, we can ask if $f \in \mathcal{F}$ or f is far from $\mathcal{F}$.

Importance of property testing

- A relaxation of decision problems:
  - If the object is very large, it is infeasible to examine all of it and we must design algorithms that examine only a small part of the object.
  - The object is not too large to fully examine, but the exact decision problem is NP-hard, e.g., SAT, k-Colorability.
- A relaxation of learning problems:
  - Instead of output a good estimate of f when $f \in \mathcal{F}$, we can ask if $f \in \mathcal{F}$ or f is far from $\mathcal{F}$.

Usually, testing algorithms are much faster than decision and learning algorithms.

Importance of property testing

- A relaxation of decision problems:
  - If the object is very large, it is infeasible to examine all of it and we must design algorithms that examine only a small part of the object.
  - The object is not too large to fully examine, but the exact decision problem is NP-hard, e.g., SAT, k-Colorability.
- A relaxation of learning problems:
  - Instead of output a good estimate of f when $f \in \mathcal{F}$, we can ask if $f \in \mathcal{F}$ or f is far from $\mathcal{F}$.

Usually, testing algorithms are much faster than decision and learning algorithms. For example, for learning k-junta boolean functions, the learning algorithm costs $\Theta(2^k)$ while the testing algorithm only costs $\Theta(k)$.

An example: BLR linear testing [Blum, Luby and Rubinfeld, STOC 1990]

Given a boolean function $f : \{0,1\}^n \to \{0,1\}$, decide if it is either linear or far from linear.

An example: BLR linear testing [Blum, Luby and Rubinfeld, STOC 1990]

Given a boolean function $f : \{0,1\}^n \to \{0,1\}$, decide if it is either linear or far from linear.

Distance: $\mathrm{dist}(f,g) := |\{x : f(x) \neq g(x)\}|/2^n$.

An example: BLR linear testing [Blum, Luby and Rubinfeld, STOC 1990]

Given a boolean function $f : \{0,1\}^n \to \{0,1\}$, decide if it is either linear or far from linear.

Distance: $\mathrm{dist}(f,g) := |\{x : f(x) \neq g(x)\}|/2^n$.

Goal: Only evaluate f at a few inputs $x_1, \ldots, x_k$, where $k \ll 2^n$ (or $k \ll n$).

An example: BLR linear testing [Blum, Luby and Rubinfeld, STOC 1990]

Given a boolean function $f : \{0,1\}^n \to \{0,1\}$, decide if it is either linear or far from linear.

Distance: $\mathrm{dist}(f,g) := |\{x : f(x) \neq g(x)\}|/2^n$.

Goal: Only evaluate f at a few inputs $x_1, \dots, x_k$, where $k \ll 2^n$ (or $k \ll n$).

The BLR testing algorithm ($k = 3$):

- Choose $x, y \in \{0,1\}^n$ independently and randomly
- Evaluate $f(x), f(y), f(x+y)$
- Accept if $f(x+y) = f(x) + f(y)$

An example: BLR linear testing [Blum, Luby and Rubinfeld, STOC 1990]

Given a boolean function $f : \{0,1\}^n \to \{0,1\}$, decide if it is either linear or far from linear.

Distance: $\mathrm{dist}(f,g) := |\{x : f(x) \neq g(x)\}|/2^n$.

Goal: Only evaluate f at a few inputs $x_1, \ldots, x_k$, where $k \ll 2^n$ (or $k \ll n$).

The BLR testing algorithm ($k = 3$):

- Choose $x, y \in \{0,1\}^n$ independently and randomly
- Evaluate $f(x), f(y), f(x+y)$
- Accept if $f(x+y) = f(x) + f(y)$

This algorithm is a key ingredient in proving the famous PCP theorem, the most important achievement of classical complexity theory in the past quarter century.

Boolean satisfiability problem (SAT problem)

SAT is the problem of deciding if there is an assignment to the variables of a Boolean formula such that the formula is satisfied, i.e., decide if

$$\bigwedge_{s=1}^{N} (y_{s_1} \vee \cdots \vee y_{s_k}) = 1$$

has a solution, where $y_i \in \{x_i, \bar{x}_i\}$ and $x_i \in \{0, 1\}$.

Boolean satisfiability problem (SAT problem)

SAT is the problem of deciding if there is an assignment to the variables of a Boolean formula such that the formula is satisfied, i.e., decide if

$$\bigwedge_{s=1}^{N} (y_{s_1} \vee \cdots \vee y_{s_k}) = 1$$

has a solution, where $y_i \in \{x_i, \bar{x}_i\}$ and $x_i \in \{0, 1\}$.

Cook-Levin Theorem (1971): The first NP-complete problem for $k \geq 3$.

When $k = 2$, it is in P.

Boolean satisfiability problem (SAT problem)

SAT is the problem of deciding if there is an assignment to the variables of a Boolean formula such that the formula is satisfied, i.e., decide if

$$\bigwedge_{s=1}^{N} (y_{s_1} \vee \cdots \vee y_{s_k}) = 1$$

has a solution, where $y_i \in \{x_i, \bar{x}_i\}$ and $x_i \in \{0, 1\}$.

Cook-Levin Theorem (1971): The first NP-complete problem for $k \geq 3$.

When $k = 2$, it is in P.

The PCP theorem: it is NP-hard to distinguish between
(1) an instance of k-SAT is completely satisfiable, or
(2) no more than 99% of its constraints can be satisfied.

Quantum computing basis

A quantum system of n qubits: A Hilbert space

$$\mathcal{H} = \text{span}\{|i_1, \ldots, i_n\rangle : i_1, \ldots, i_n \in \{0, 1\}\},$$

where $|i_1, \ldots, i_n\rangle = |i_1\rangle \otimes \cdots \otimes |i_n\rangle$. Mathematically, we can view

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

The notation $|\cdot\rangle$, called Dirac notation or ket, provides a way to clarify that we are speaking of a column vector. The bra notation $\langle\cdot|$ is used to denote a row vector.

A quantum state $|\psi\rangle = \sum \psi_{i_1,\ldots,i_n} |i_1, \ldots, i_n\rangle$, where $\psi_{i_1,\ldots,i_n} \in \mathbb{C}$ and $\sum |\psi_{i_1,\ldots,i_n}|^2 = 1$.

k-local Hamiltonian

A k-local Hamiltonian H acting on a system of n qubits is a $2^n \times 2^n$ Hermitian matrix that can be written as $H = \sum_i H_i$, where each H_i is Hermitian of operator norm $\|H_i\| \leq 1$ and acts non-trivially only on k out of the n qubits.

k-local Hamiltonian

A k-local Hamiltonian H acting on a system of n qubits is a $2^n \times 2^n$ Hermitian matrix that can be written as $H = \sum_i H_i$, where each H_i is Hermitian of operator norm $\|H_i\| \leq 1$ and acts non-trivially only on k out of the n qubits.

For example, $H = X \otimes I \otimes I + I \otimes Y \otimes I + I \otimes Y \otimes Z$ is 2-local. Sometimes we just write it as $H = X_1 + Y_2 + Y_2 Z_3$.

k-local Hamiltonian

A k-local Hamiltonian H acting on a system of n qubits is a $2^n \times 2^n$ Hermitian matrix that can be written as $H = \sum_i H_i$, where each H_i is Hermitian of operator norm $\|H_i\| \leq 1$ and acts non-trivially only on k out of the n qubits.

For example, $H = X \otimes I \otimes I + I \otimes Y \otimes I + I \otimes Y \otimes Z$ is 2-local. Sometimes we just write it as $H = X_1 + Y_2 + Y_2 Z_3$.

Definition (k-local Hamiltonian problem (k-LH))

- **Input:** $H = \sum_{i=1}^{m} H_i$ *with* $m = \mathrm{poly}(n)$, $a, b \in \mathbb{R}$ *with* $b - a > 1/\mathrm{poly}(n)$.
- **Output:** *Is the smallest eigenvalue of H smaller than a or larger than b?*

k-local Hamiltonian

A k-local Hamiltonian H acting on a system of n qubits is a $2^n \times 2^n$ Hermitian matrix that can be written as $H = \sum_i H_i$, where each H_i is Hermitian of operator norm $\|H_i\| \leq 1$ and acts non-trivially only on k out of the n qubits.

For example, $H = X \otimes I \otimes I + I \otimes Y \otimes I + I \otimes Y \otimes Z$ is 2-local. Sometimes we just write it as $H = X_1 + Y_2 + Y_2 Z_3$.

Definition (k-local Hamiltonian problem (k-LH))

- **Input:** $H = \sum_{i=1}^{m} H_i$ *with* $m = \mathrm{poly}(n)$, $a, b \in \mathbb{R}$ *with* $b - a > 1/\mathrm{poly}(n)$.
- **Output:** *Is the smallest eigenvalue of* H *smaller than* a *or larger than* b*?*

Kitaev (1999): k-LH is QMA-hard, a quantum analog of NP-hard.

k-local Hamiltonian

A k-local Hamiltonian H acting on a system of n qubits is a $2^n \times 2^n$ Hermitian matrix that can be written as $H = \sum_i H_i$, where each H_i is Hermitian of operator norm $\|H_i\| \leq 1$ and acts non-trivially only on k out of the n qubits.

For example, $H = X \otimes I \otimes I + I \otimes Y \otimes I + I \otimes Y \otimes Z$ is 2-local. Sometimes we just write it as $H = X_1 + Y_2 + Y_2 Z_3$.

Definition (k-local Hamiltonian problem (k-LH))

- **Input:** $H = \sum_{i=1}^{m} H_i$ *with* $m = \mathrm{poly}(n)$, $a, b \in \mathbb{R}$ *with* $b - a > 1/\mathrm{poly}(n)$.
- **Output:** *Is the smallest eigenvalue of* H *smaller than* a *or larger than* b*?*

Kitaev (1999): k-LH is QMA-hard, a quantum analog of NP-hard.

Quantum PCP conjecture: k-LH is QMA-hard if $b - a = \Omega(1)$. Still open!

LH is a natural generalisation of SAT

For $C = x_1 \vee x_2 \vee \bar{x}_3$, define

$$H = |001\rangle\langle 001| = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

So $H|i_1, i_2, i_3\rangle = 0$ iff $(i_1, i_2, i_3) \neq (0, 0, 1)$. All these (i_1, i_2, i_3) are solutions of C.

LH is a natural generalisation of SAT

For a general 3-SAT: $C = \wedge_{i=1}^{m} C_i$, we similarly define $H = \sum_{i=1}^{m} H_i$, which is 3-local.

- If $H|i_1, \ldots, i_n\rangle = 0$ then C has a solution,
- If $H|i_1, \ldots, i_n\rangle \neq 0$ for all $i_1, \ldots, i_n$, then C has no solution.

In summary, 3-SAT $\Leftrightarrow$ Is the smallest eigenvalue of H at most 0, or is it at least 1?

Table of Contents

Quantum k-SAT problem: due to Bravyi (arXiv:quant-ph/0602108)

An instance of the problem is defined as follows:

- n qubits

Quantum k-SAT problem: due to Bravyi (arXiv:quant-ph/0602108)

An instance of the problem is defined as follows:

- n qubits
- For every k subset $s = \{s_1, \ldots, s_k\} \subseteq [n] := \{1, 2, \ldots, n\}$, there is a Hermitian projector π_s which acts nontrivially only on the qubits in s. Here Hermitian projector means $\pi_s^\dagger = \pi_s = \pi_s^2$.

Quantum k-SAT problem: due to Bravyi (arXiv:quant-ph/0602108)

An instance of the problem is defined as follows:

- n qubits
- For every k subset $s = \{s_1, \ldots, s_k\} \subseteq [n] := \{1, 2, \ldots, n\}$, there is a Hermitian projector π_s which acts nontrivially only on the qubits in s. Here Hermitian projector means $\pi_s^\dagger = \pi_s = \pi_s^2$.
- We say that the constraint π_s is satisfied for some $|\psi\rangle$ if $(\pi_s \otimes I_{\bar{s}})|\psi\rangle = 0$; that is, $|\psi\rangle$ is in the kernel of the projector $\pi_s \otimes I_{\bar{s}}$.

Quantum k-SAT problem: due to Bravyi (arXiv:quant-ph/0602108)

An instance of the problem is defined as follows:

- n qubits
- For every k subset $s = \{s_1, \ldots, s_k\} \subseteq [n] := \{1, 2, \ldots, n\}$, there is a Hermitian projector π_s which acts nontrivially only on the qubits in s. Here Hermitian projector means $\pi_s^\dagger = \pi_s = \pi_s^2$.
- We say that the constraint π_s is satisfied for some $|\psi\rangle$ if $(\pi_s \otimes I_{\bar{s}})|\psi\rangle = 0$; that is, $|\psi\rangle$ is in the kernel of the projector $\pi_s \otimes I_{\bar{s}}$.

A quantum k-SAT problem is as follows: is there some $|\psi\rangle$ which satisfies all the constraints $\{\pi_s : s \subseteq [n], |s| = k\}$? i.e:

$$\sum_{s \subseteq [n], |s|=k} (\pi_s \otimes I_{\bar{s}})|\psi\rangle = 0.$$

Importance of QSAT

- Quantum complexity theory:
  - Quantum k-SAT and its optimization variant (k-LH), are central to quantum complexity theory, being QMA_1- and QMA-complete problems.

Importance of QSAT

- Quantum complexity theory:
  - Quantum k-SAT and its optimization variant (k-LH), are central to quantum complexity theory, being QMA_1- and QMA-complete problems.
- Frustration-freeness systems:
  - Quantum k-SAT is also relevant to frustration-freeness (no energy increase) in many-body physics (global ground state is also a local ground state).

Connection to classical SAT problem

- Consider the case $k = 2$, then $x_1 \vee x_2 = 1 \Leftrightarrow (x_1, x_2) = (0, 1), (1, 0)$ or $(1, 1)$
- On a quantum computer, $x_1 \vee x_2$ corresponds to $|\phi_{12}\rangle = |0\rangle|0\rangle$
  The solutions correspond to $|\psi_{12}\rangle = a|0\rangle|1\rangle + b|1\rangle|0\rangle + c|1\rangle|1\rangle$
- We can view $|\phi_{12}\rangle$ as a projector $\pi_{12} = |\phi_{12}\rangle\langle\phi_{12}|$. As a result,

$$\pi_{12}|\psi_{12}\rangle = 0.$$

Previous results

- $k = 2$, QSAT is in P
  $O(n^2)$ [Bravyi, Contemporary Mathematics 2006]
  $O(n)$ [Arad et al. Theory of Computing 2015]
- $k = 3$, it is QMA$_1$-complete (a quantum analogue of NP-complete)
  [Gosset, Nagaj, SIAM J Comput, 2012]
- $k \geq 4$, it is QMA$_1$-complete
  [Bravyi, Contemporary Mathematics 2006]
- Some cases that can be solved efficiently
  [Aldi et al. Commun. Math. Phys., 2021]
- Rank 1 case with few constraints:
  [Ambainis, Kempe, Sattath, JACM, 2009]
- Random QSAT problem
  [Laumann et al. Phys. Rev. A 2010]
- ......

Testing QSAT

Given a QSAT instance $\Pi = \{\pi_s : s \subseteq [n], |s| = k\}$, decide if it is satisfiable, i.e., $\sum_{s\subseteq[n],|s|=k} \pi_s|\psi\rangle = 0$ for some $|\psi\rangle$, or ε-far from satisfiable.

Testing QSAT

Given a QSAT instance $\Pi = \{\pi_s : s \subseteq [n], |s| = k\}$, decide if it is satisfiable, i.e., $\sum_{s\subseteq[n],|s|=k} \pi_s|\psi\rangle = 0$ for some $|\psi\rangle$, or ε-far from satisfiable.

Here ε-far means, one must remove $> \varepsilon n^k$ projectors before the instance becomes satisfiable. Namely, if $S \subseteq \binom{[n]}{k}$ is such that

$$\sum_{s\subseteq[n]\setminus S,|s|=k} (\pi_s \otimes I_{\bar{s}})|\psi\rangle = 0$$

for some $|\psi\rangle$, then $|S| > \varepsilon n^k$.

Testing QSAT

Given a QSAT instance $\Pi = \{\pi_s : s \subseteq [n], |s| = k\}$, decide if it is satisfiable, i.e., $\sum_{s \subseteq [n], |s|=k} \pi_s |\psi\rangle = 0$ for some $|\psi\rangle$, or ε-far from satisfiable.

Here ε-far means, one must remove $> \varepsilon n^k$ projectors before the instance becomes satisfiable. Namely, if $S \subseteq \binom{[n]}{k}$ is such that

$$\sum_{s \subseteq [n] \setminus S, |s|=k} (\pi_s \otimes I_{\bar{s}}) |\psi\rangle = 0$$

for some $|\psi\rangle$, then $|S| > \varepsilon n^k$.

We are interested in the case if $|\psi\rangle$ is a product state or not in the above definition, i.e., if $|\psi\rangle = |\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle$.

Previous results

The problem is inspired by classical results for testing satisfiability by Alon and Shapira (2003).

Previous results

The problem is inspired by classical results for testing satisfiability by Alon and Shapira (2003).

They proved that if an SAT instance is ε-far from satisfiable, then most of the induced sets of functions, on sets of variables of size c_k/ε^2, are not satisfiable, where c_k is a constant depending only on k.

Previous results

The problem is inspired by classical results for testing satisfiability by Alon and Shapira (2003).

They proved that if an SAT instance is ε-far from satisfiable, then most of the induced sets of functions, on sets of variables of size c_k/ε^2, are not satisfiable, where c_k is a constant depending only on k.

This provides an efficient algorithm for testing: randomly choose c_k/ε^2 variables and focus on the functions in these variables. Check if it is satisfiable or not. If yes, then accept; otherwise reject.

Previous results

The problem is inspired by classical results for testing satisfiability by Alon and Shapira (2003).

They proved that if an SAT instance is ε-far from satisfiable, then most of the induced sets of functions, on sets of variables of size c_k/ε^2, are not satisfiable, where c_k is a constant depending only on k.

This provides an efficient algorithm for testing: randomly choose c_k/ε^2 variables and focus on the functions in these variables. Check if it is satisfiable or not. If yes, then accept; otherwise reject.

Although the SAT problem is NP-hard, the SAT testing problem can be solved in randomised constant time.

Previous results

The problem is inspired by classical results for testing satisfiability by Alon and Shapira (2003).

They proved that if an SAT instance is ε-far from satisfiable, then most of the induced sets of functions, on sets of variables of size c_k/ε^2, are not satisfiable, where c_k is a constant depending only on k.

This provides an efficient algorithm for testing: randomly choose c_k/ε^2 variables and focus on the functions in these variables. Check if it is satisfiable or not. If yes, then accept; otherwise reject.

Although the SAT problem is NP-hard, the SAT testing problem can be solved in randomised constant time.

A short summary of our results: We proved a similar result for testing QSAT.

Table of Contents

Locally satisfiable by a product state

Let $\Pi = \{\pi_s : s \subseteq [n], |s| = k\}$ be an instance of quantum k-SAT, and let $A := \{a_1, \ldots, a_c\} \subseteq [n]$ be some subset. We say that the instance is locally satisfiable by a product state at A if there exists a product state $|\psi\rangle = |\psi_{a_1}\rangle \otimes \cdots \otimes |\psi_{a_c}\rangle$ such that

$$\sum_{s \subseteq A, |s|=k} (\pi_s \otimes I_{\bar{s}})|\psi\rangle = 0$$

Locally satisfiable by a product state

Let $\Pi = \{\pi_s : s \subseteq [n], |s| = k\}$ be an instance of quantum k-SAT, and let $A := \{a_1, \ldots, a_c\} \subseteq [n]$ be some subset. We say that the instance is locally satisfiable by a product state at A if there exists a product state $|\psi\rangle = |\psi_{a_1}\rangle \otimes \cdots \otimes |\psi_{a_c}\rangle$ such that

$$\sum_{s \subseteq A, |s| = k} (\pi_s \otimes I_{\bar{s}})|\psi\rangle = 0$$

Remark. Note that while being (un)satisfiable or ε-far from satisfiable by a product state are global properties involving all the qubits, being locally satisfiable is a local property involving only a subset of the qubits.

Main theorems

Theorem 1 (Satisfiability implies local satisfiability by a product state with high probability)

Let $\Pi = \{\pi_s : s \subseteq [n], |s| = k\}$ *be a satisfiable instance of quantum* k*-SAT. Let* $c \in \mathbb{N}$ *be fixed and* $c \geq 3$*. Let* $A \subseteq [n]$ *be a subset chosen uniformly at random of size* c*.*

Then the probability that the instance is locally satisfiable by a product state at A *is greater than 0.75 whenever*

$$n \geq 2^{6c}.$$

Main theorems

Theorem 2 (Being ε-far from satisfiable by a product state implies local unsatisfiability by a product state with high probability)

There is a constant $c(k,\varepsilon)$ indepenent of n such that the following holds:

Let $\Pi = \{\pi_s : s \subseteq [n], |s| = k\}$ be any instance of quantum k-SAT which is ε far from satisfiable by a product state.

Then, for a randomly chosen subset $S \subseteq [n]$ of size $c(k,\varepsilon)$, the instance is locally unsatisfiable by a product state at C with probability at least $p > 0.75$.

A corollary

Corollary

With the promise that the instance is either satisfiable or ε-far from satisfiable by a product state, quantum k-SAT can be solved in time polynomial in n.

Proof.

- By Theorem 1, satisfiable $\Rightarrow$ locally satisfiable by a product state.
- By Theorem 2, ε-far from satisfiable $\Rightarrow$ locally unsatisfiable by a product state.
- So all we need to do is check satisfiability by a product state on randomly chosen constant-sized subsets. This can be done, say, by Gröbner basis method.

□

Proof of Theorem 1

Theorem (An equivalent statement)

Let $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$ be any state and let $A \subseteq [n]$ be a subset chosen uniformly at random of size c. The probability that the subspace supp$(\mathrm{Tr}_{\overline{A}}(|\psi\rangle\langle\psi|)) \subseteq (\mathbb{C}^2)^{\otimes c}$ contains a product state is greater than $p \in (0,1)$ whenever $n > \Psi(p,c)$.

Proof. (From states to local satisfiability).

Suppose $\Pi = \{\pi_s : s \subseteq [n], |s| = k\}$ is satisfiable by a solution $|\psi\rangle = \sum_k |\psi_{k1}\rangle_A |\psi_{k2}\rangle_{\overline{A}}$ (the Schmidt decomposition), then

- $\pi_s|\psi\rangle = 0 \Leftrightarrow \pi_s|\psi_{k1}\rangle_A = 0$ $(\forall k)$ for all $s \subseteq A$.

Proof of Theorem 1

Theorem (An equivalent statement)

Let $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$ be any state and let $A \subseteq [n]$ be a subset chosen uniformly at random of size c. The probability that the subspace supp$(\mathrm{Tr}_{\overline{A}}(|\psi\rangle\langle\psi|)) \subseteq (\mathbb{C}^2)^{\otimes c}$ contains a product state is greater than $p \in (0,1)$ whenever $n > \Psi(p,c)$.

Proof. (From states to local satisfiability).

Suppose $\Pi = \{\pi_s : s \subseteq [n], |s| = k\}$ is satisfiable by a solution $|\psi\rangle = \sum_k |\psi_{k1}\rangle_A |\psi_{k2}\rangle_{\overline{A}}$ (the Schmidt decomposition), then

- $\pi_s|\psi\rangle = 0 \Leftrightarrow \pi_s|\psi_{k1}\rangle_A = 0$ $(\forall k)$ for all $s \subseteq A$.
- $\mathrm{Tr}_{\overline{A}}|\psi\rangle\langle\psi| = \sum_k |\psi_{k1}\rangle_A\langle\psi_{k1}|_A \Rightarrow \mathrm{supp}(\mathrm{Tr}_{\overline{A}}|\psi\rangle\langle\psi|) = \mathrm{Span}\{|\psi_{k1}\rangle_A\}$.

Proof of Theorem 1

Theorem (An equivalent statement)

Let $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$ be any state and let $A \subseteq [n]$ be a subset chosen uniformly at random of size c. The probability that the subspace supp$(\mathrm{Tr}_{\overline{A}}(|\psi\rangle\langle\psi|)) \subseteq (\mathbb{C}^2)^{\otimes c}$ contains a product state is greater than $p \in (0,1)$ whenever $n > \Psi(p,c)$.

Proof. (From states to local satisfiability).

Suppose $\Pi = \{\pi_s : s \subseteq [n], |s| = k\}$ is satisfiable by a solution $|\psi\rangle = \sum_k |\psi_{k1}\rangle_A |\psi_{k2}\rangle_{\overline{A}}$ (the Schmidt decomposition), then

- $\pi_s|\psi\rangle = 0 \Leftrightarrow \pi_s|\psi_{k1}\rangle_A = 0 \ (\forall k)$ for all $s \subseteq A$.
- $\mathrm{Tr}_{\overline{A}}|\psi\rangle\langle\psi| = \sum_k |\psi_{k1}\rangle_A\langle\psi_{k1}|_A \Rightarrow \mathrm{supp}(\mathrm{Tr}_{\overline{A}}|\psi\rangle\langle\psi|) = \mathrm{Span}\{|\psi_{k1}\rangle_A\}$.
- Any state in $\mathrm{supp}(\mathrm{Tr}_{\overline{A}}|\psi\rangle\langle\psi|)$ is a local solution of Π. Particularly, if it contains a product state, then the instance Π will be locally satisfiable by a product state.

□

Proof (Cont.)

Proof. (From local satisfiability to states).

- Let $|\psi\rangle$ be a state.

Proof (Cont.)

Proof. (From local satisfiability to states).

- Let $|\psi\rangle$ be a state.
- For every $A \subseteq \binom{[n]}{c}$, let π_A be the projector onto $\ker(\text{Tr}_{\overline{A}}|\psi\rangle\langle\psi|)$. This defines an instance of QSAT.

Proof (Cont.)

Proof. (From local satisfiability to states).

- Let $|\psi\rangle$ be a state.
- For every $A \subseteq \binom{[n]}{c}$, let π_A be the projector onto $\ker(\mathrm{Tr}_{\overline{A}}|\psi\rangle\langle\psi|)$. This defines an instance of QSAT.
- If the instance is locally satisfiable by a product state, then $\mathrm{supp}(\mathrm{Tr}_{\overline{A}}|\psi\rangle\langle\psi|)$ contains a product state.

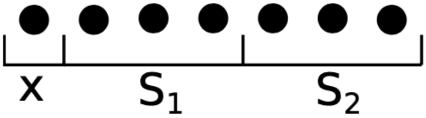
□

Proof of Theorem 1

Lemma (A key Lemma)

Assume that $S_1 \cup S_2 = \{1, \ldots, n\} \backslash \{x\}$, *then one of the following holds:*

1. *The space supp(* $Tr_{S_2} |\psi\rangle\langle\psi|$ *) contains a product state* $|\psi_x\rangle \otimes |\psi_{S_1}\rangle$.
2. *The space supp(* $Tr_{S_1} |\psi\rangle\langle\psi|$ *) contains a product state* $|\psi_x\rangle \otimes |\psi_{S_2}\rangle$.



Proof of Theorem 1

- Randomly choose $x_1 \in \{1, 2, \ldots, n\}$

Proof of Theorem 1

- Randomly choose $x_1 \in \{1, 2, \ldots, n\}$
- Assume that $n-1$ is even and consider all bipartitions $B_1 \cup B_2$ of $V := \{1, 2, \ldots, n\} \backslash \{x_1\}$. By the key lemma, either $\text{supp}(\text{Tr}_{B_1} |\psi\rangle\langle\psi|)$ or $\text{supp}(\text{Tr}_{B_2} |\psi\rangle\langle\psi|)$ has a product state.

Proof of Theorem 1

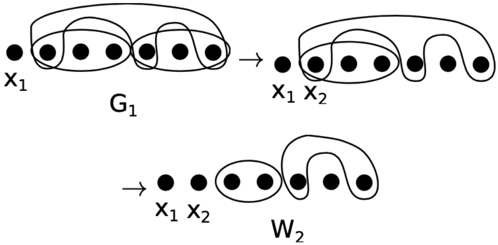
- Randomly choose $x_1 \in \{1, 2, \ldots, n\}$
- Assume that $n-1$ is even and consider all bipartitions $B_1 \cup B_2$ of $V := \{1, 2, \ldots, n\} \backslash \{x_1\}$. By the key lemma, either $\mathrm{supp}(\mathrm{Tr}_{B_1} |\psi\rangle\langle\psi|)$ or $\mathrm{supp}(\mathrm{Tr}_{B_2} |\psi\rangle\langle\psi|)$ has a product state.
- Define a $(n-1)/2$-regular hypergraph G_1 on V, where $E \subseteq V$ is an edge if $\mathrm{supp}(\mathrm{Tr}_{\overline{x_1, E}} |\psi\rangle\langle\psi|)$ has a product state $|\psi_{x_1}\rangle \otimes |\psi_E\rangle$.

Proof of Theorem 1

- Randomly choose $x_2 \in \{1, 2, \ldots, n\} \backslash \{x_1\}$

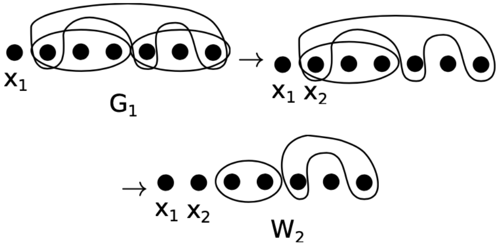
Proof of Theorem 1

- Randomly choose $x_2 \in \{1, 2, \ldots, n\} \backslash \{x_1\}$
- Define a $(n-3)/2$-regular graph W_2 on $\{1, 2, \ldots, n\} \backslash \{x_1, x_2\}$, where the edges are $\{E - x_2 : E$ is an edge of $G_1, x_2 \in E\}$



Proof of Theorem 1

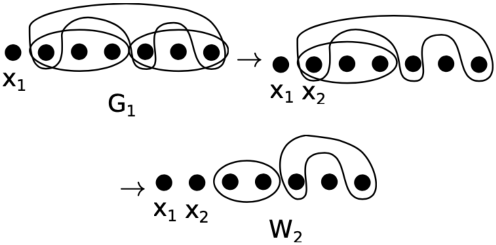
- Randomly choose $x_2 \in \{1, 2, \ldots, n\} \backslash \{x_1\}$
- Define a $(n-3)/2$-regular graph W_2 on $\{1, 2, \ldots, n\} \backslash \{x_1, x_2\}$, where the edges are $\{E - x_2 : E \text{ is an edge of } G_1, x_2 \in E\}$



- Now for every edge $E \in W_2$, we consider all bipartitions and use the Lemma again.

Proof of Theorem 1

- Randomly choose $x_2 \in \{1, 2, \ldots, n\} \backslash \{x_1\}$
- Define a $(n-3)/2$-regular graph W_2 on $\{1, 2, \ldots, n\} \backslash \{x_1, x_2\}$, where the edges are $\{E - x_2 : E \text{ is an edge of } G_1, x_2 \in E\}$



- Now for every edge $E \in W_2$, we consider all bipartitions and use the Lemma again.
- We obtain a regular hypergraph G_2 on the qubits $[n] - \{x_1, x_2\}$, such that for any edge $E \in G_2$ we have $\mathrm{supp}(\mathrm{Tr}_{\overline{\{x_1,x_2\} \sqcup E}}(|\psi\rangle\langle\psi|))$ contains a product state $|\phi_1\rangle \otimes |\phi_2\rangle \otimes |\phi_E\rangle$

Proof of Theorem 1

- We iterate the process to obtain a regular hypergraph G_{c-1} on the qubits $[n] - \{x_1, \ldots, x_{c-1}\}$ such that for any edge $E \in G_{c-1}$ we have

$$\mathrm{supp}(\mathrm{Tr}_{\overline{\{x_1,\ldots,x_{c-1}\}\sqcup E}}(|\psi\rangle\langle\psi|)) \quad \text{contains a product state}$$

$$|\phi_1\rangle \otimes \cdots \otimes |\phi_{c-1}\rangle \otimes |\phi_E\rangle$$

Proof of Theorem 1

- We iterate the process to obtain a regular hypergraph G_{c-1} on the qubits $[n] - \{x_1, \ldots, x_{c-1}\}$ such that for any edge $E \in G_{c-1}$ we have

$$\text{supp}(\mathrm{Tr}_{\overline{\{x_1,\ldots,x_{c-1}\} \sqcup E}}(|\psi\rangle\langle\psi|)) \quad \text{contains a product state}$$

$$|\phi_1\rangle \otimes \cdots \otimes |\phi_{c-1}\rangle \otimes |\phi_E\rangle$$

- When we pick the final qubit x_c, we see that $\text{supp}(\mathrm{Tr}_{\overline{C}}(|\psi\rangle\langle\psi|))$ will contain a product state if x_c lies in an edge of G_{c-1}.

Proof of Theorem 1

- We iterate the process to obtain a regular hypergraph G_{c-1} on the qubits $[n] - \{x_1, \ldots, x_{c-1}\}$ such that for any edge $E \in G_{c-1}$ we have

$$\text{supp}(\mathrm{Tr}_{\overline{\{x_1,\ldots,x_{c-1}\}\sqcup E}}(|\psi\rangle\langle\psi|)) \quad \text{contains a product state}$$

$$|\phi_1\rangle \otimes \cdots \otimes |\phi_{c-1}\rangle \otimes |\phi_E\rangle$$

- When we pick the final qubit x_c, we see that $\text{supp}(\mathrm{Tr}_{\overline{C}}(|\psi\rangle\langle\psi|))$ will contain a product state if x_c lies in an edge of G_{c-1}.
- We can lower bound the edge density and edge size of G_{c-1} using ideas from combinatorics and basic analysis to obtain the theorem.

Proof of Theorem 2 – Main idea

Theorem (Recall)

There is a constant $c(k, \varepsilon)$ independent of n such that the following holds:

Let $\Pi = \{\pi_s : s \subseteq [n], |s| = k\}$ be any instance of quantum k-SAT which is ε far from satisfiable by a product state.

Then, for a randomly chosen subset $A \subseteq [n]$ of size $c(k, \varepsilon)$, the instance is locally unsatisfiable by a product state at A with probability at least 0.75.

Proof of Theorem 2 – Main idea

- A local solution on $A = \{i_1, \dots, i_p\} \subseteq \{1, \dots, n\}$ is a subspace $P_A := V_{i_1} \otimes \cdots \otimes V_{i_p}$, such that for any $|\psi\rangle \in P_A$, we have $\pi_s|\psi\rangle = 0$, where $s \subseteq A$.

Proof of Theorem 2 – Main idea

- A local solution on $A = \{i_1, \ldots, i_p\} \subseteq \{1, \ldots, n\}$ is a subspace $P_A := V_{i_1} \otimes \cdots \otimes V_{i_p}$, such that for any $|\psi\rangle \in P_A$, we have $\pi_s|\psi\rangle = 0$, where $s \subseteq A$.
- Our strategy is to extend a local solution to a global solution gradually. At each step, there appear some $x \notin S$, that are either not extendable, or x can be extended, but the extension after including x is "hard". All these are bad.

Proof of Theorem 2 – Main idea

- A local solution on $A = \{i_1, \ldots, i_p\} \subseteq \{1, \ldots, n\}$ is a subspace $P_A := V_{i_1} \otimes \cdots \otimes V_{i_p}$, such that for any $|\psi\rangle \in P_A$, we have $\pi_s|\psi\rangle = 0$, where $s \subseteq A$.
- Our strategy is to extend a local solution to a global solution gradually. At each step, there appear some $x \notin S$, that are either not extendable, or x can be extended, but the extension after including x is "hard". All these are bad.
- **Lemma 1.** If ε-far, then for any local solution, there are at least $\varepsilon n/5$ bad x.

Proof of Theorem 2 – Main idea

- A local solution on $A = \{i_1, \ldots, i_p\} \subseteq \{1, \ldots, n\}$ is a subspace $P_A := V_{i_1} \otimes \cdots \otimes V_{i_p}$, such that for any $|\psi\rangle \in P_A$, we have $\pi_s|\psi\rangle = 0$, where $s \subseteq A$.
- Our strategy is to extend a local solution to a global solution gradually. At each step, there appear some $x \notin S$, that are either not extendable, or x can be extended, but the extension after including x is "hard". All these are bad.
- **Lemma 1.** If ε-far, then for any local solution, there are at least $\varepsilon n/5$ bad x.
- **Lemma 2.** If extending P_S according to bad x, then it is non-extendable when the length is larger than $5 \cdot 4^{k-1}/\varepsilon$.

Proof of Theorem 2 – Main idea

- A local solution on $A = \{i_1, \dots, i_p\} \subseteq \{1, \dots, n\}$ is a subspace $P_A := V_{i_1} \otimes \cdots \otimes V_{i_p}$, such that for any $|\psi\rangle \in P_A$, we have $\pi_s|\psi\rangle = 0$, where $s \subseteq A$.
- Our strategy is to extend a local solution to a global solution gradually. At each step, there appear some $x \notin S$, that are either not extendable, or x can be extended, but the extension after including x is "hard". All these are bad.
- **Lemma 1.** If ε-far, then for any local solution, there are at least $\varepsilon n/5$ bad x.
- **Lemma 2.** If extending P_S according to bad x, then it is non-extendable when the length is larger than $5 \cdot 4^{k-1}/\varepsilon$.

Thank you very much for listening!