Bounds on the Quantum Satisfiability Threshold

Cristopher Moore
Center for Quantum Information and Control
Computer Science / Physics and Astronomy, UNM
Santa Fe Institute

*joint work with Sergey Bravyi (IBM) and Alexander Russell (Connecticut)*
A phase transition

- Random 3-SAT formulas with $n$ variables and $\alpha n$ clauses
A phase transition

• Search times appear to peak at the transition
Quantum k-SAT [Bravyi]

• Classical SAT: each clause forbids one out of 8 truth values. Think of this as forbidding a basis vector:

\[(x_1 \lor \overline{x_2} \lor x_3) \iff \langle 010| x \rangle = 0\]

• Quantum SAT: forbid an arbitrary vector in \(\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2\),

\[\langle v|x \rangle = 0\]

• For each clause \(c\), we have \(\Pi_c|\psi\rangle = |\psi\rangle\) where

\[\Pi_c = (1 - |v\rangle \langle v|) \otimes 1_{n-3}\]
A local Hamiltonian

- Alternately, ask whether there is a zero-energy state $|\psi\rangle$ of a local, disordered Hamiltonian:

$$H = \sum_c |v\rangle \langle v| \otimes 1$$

- What is its ground state energy? QMA$_1$-complete [Bravyi]

- When are its ground states entangled?
Forbidden and satisfying subspaces

\[ V_{\text{forbidden}} = \text{span} \left\{ |v\rangle \otimes |00\rangle, |v\rangle \otimes |01\rangle, |v\rangle \otimes |10\rangle, |v\rangle \otimes |11\rangle, |00\rangle \otimes |w\rangle, |01\rangle \otimes |w\rangle, |10\rangle \otimes |w\rangle, |11\rangle \otimes |w\rangle \right\} \]

- The satisfying subspace is \( V_{\text{sat}} = V_{\text{forbidden}}^\perp \)

- With probability 1, \( \text{rank} V_{\text{forbidden}} = 8 \), so \( \text{rank} V_{\text{sat}} = 32 - 8 = 24 \)
Generic clause vectors

- These ranks take generic values with probability 1

- Coincidences can only decrease $\text{rank} V_{\text{forbidden}}$, and increase $\text{rank} V_{\text{sat}}$

- For a given hypergraph, if any choice of clause vectors make it unsatisfiable, it is generically unsatisfiable [Laumann et al.]
Random quantum k-SAT formulas

- Two sources of randomness:
  - A random hypergraph with \( n \) vertices and \( m \) hyperedges (clauses), where
    \[
m = \alpha n
    \]
  - Random clause vectors, chosen uniformly from unit-length vectors in \( \mathbb{C}^k \)
- Threshold conjecture:
  \[
  \lim_{n \to \infty} \Pr[H(n, m = \alpha n) \text{ is generically satisfiable}] = \begin{cases} 
    1 & \alpha < \alpha_c \\
    0 & \alpha > \alpha_c 
  \end{cases}
  \]
A classical upper bound

- Compute the expected number of satisfying assignments. For k-SAT,

\[ E[X] = 2^n \left(1 - 2^{-k}\right)^m = \left(2(1 - 2^{-k})^\alpha\right)^n \]

- This is an upper bound on the probability of satisfiability:

\[ \Pr[X > 0] \leq E[X] \]

- This becomes exponentially small when \( \alpha \) is large enough:

\[ \alpha_c \leq \log_{1/(1-2^{-k})} 2 \approx 2^k \ln 2 \]

- This is asymptotically tight [Achlioptas&Moore, Achlioptas&Peres]
A simple quantum upper bound

- Number of solutions is analogous to $\text{rank } V_{\text{sat}}$

- Expectation of a clause projector:

$$\mathbb{E}_v \Pi_c = (1 - \mathbb{E}_v |v\rangle\langle v|) \otimes 1 = (1 - 2^{-k})1$$

- Since the clauses are independent, if $\Pi_{\phi} = \prod_c \Pi_c$ then

$$\text{rank } V_{\text{sat}} \leq \mathbb{E}_\{v\} \text{tr } \Pi_{\phi}^\dagger \Pi_{\phi} = 2^n (1 - 2^{-k})^m$$

- So, the quantum bound is at most the classical one: $\alpha_c^q \leq \alpha_c$

Thursday, October 1, 2009
Quantum SAT is more restrictive

- 2-SAT problem on a star of degree d

- Classical: at least $2^{\lfloor d/2 \rfloor} + 2^{\lceil d/2 \rceil}$ solutions

- Quantum: only $n + 1 = d + 2$
Quantum SAT is more restrictive

• Remember that any choice of forbidden vectors gives an upper bound

• Forbid singlets: $|v\rangle = \frac{1}{\sqrt{2}} (|01\rangle - |10\rangle)$

• $\langle v | \psi \rangle = 0$ if and only if $|\psi\rangle$ is symmetric under transpositions

• If the graph is connected, $|\psi\rangle$ must be symmetric under all permutations
Entangled states
Entangled states

- This 2-SAT formula is satisfiable:
Entangled states

• This 2-SAT formula is satisfiable:
Entangled states

• This 2-SAT formula is satisfiable:

• Is this one?
Entangled states

- This 2-SAT formula is satisfiable:

- Is this one?
Entangled states

- This 2-SAT formula is satisfiable:

- Is this one?

- Classical: of course! Use the new variable to satisfy the new clause.
Entangled states

• This 2-SAT formula is satisfiable:

• Is this one?

• Classical: of course! Use the new variable to satisfy the new clause.

• Quantum: no! In entangled states, single variables don’t have values. Similarly, single variables can’t satisfy entangled clauses.
Better upper bounds

• For any gadget $H$ on $t$ vertices,

$$\mathbb{E}[\Pi_H] = \frac{\text{rank } V_{\text{sat}}(H)}{2^t} \cdot 1$$

• Any time we add a gadget, we reduce the generic rank. With probability 1,

$$\text{rank } V_{\text{sat}}(G \cup H) \leq \frac{\text{rank } V_{\text{sat}}(H) \cdot \text{rank } V_{\text{sat}}(G)}{2^t}$$

• Partition a random hypergraph into gadgets:

$$\text{rank } V_{\text{sat}} \leq 2^n \prod_{i} \frac{\text{rank } V_{\text{sat}}(H_i)}{2^t}$$
The Sunflower

- Partition the hypergraph into \( n_d \) sunflowers of degree \( d \):

\[
\text{This gives:} \quad \text{rank } V_{\text{sat}} \leq 2^n \prod_{d=1}^{\infty} \left( \left( \frac{3}{4} \right)^d \left( \frac{d}{6} + 1 \right) \right)^{n_d}
\]
Sunflower partitions

• Naive: at each step, choose a random vertex, declare it and its clauses to be a sunflower, and remove them

• Continuous time: give each vertex an index $t \in [0, 1]$, and remove in decreasing order

• The degree of a sunflower of index $t$ is the number of clauses whose variables all have index $< t$. Poisson distribution with mean $k\alpha t^{k-1}$

• Setting $\frac{\ln \text{rank } V_{\text{sat}}}{n} = 0$ gives $\alpha_c^q \leq 3.894$

• Greedier partition: taking high-degree vertices first gives $\alpha_c^q \leq 3.689$ (analyze with system of differential equations)
The Nosegay

- Bigger gadgets: more conflict, smaller rank

\[ \alpha_c^q \leq 3.594 \] , far below the classical \[ \alpha_c \approx 4.267 \]
When $k$ is large

- Asymptotically, we have

$$\alpha_c \leq 2^k b$$

- where $b \approx 0.573 < \ln 2$ is the root of $\ln 2 - 2b + \ln(b + 1) = 0$

- Classically,

$$\alpha_c = (1 - o(1)) \leq 2^k \ln 2$$

so the quantum threshold is a constant smaller.
Open questions

• Classical: counting satisfying assignments of a 3-SAT formula is \( \#P\)-complete. Quantum analog: computing \( \text{rank} V_{\text{sat}} \). What is its complexity? Might not be in \( \#P \): entanglement again.

• Similarly, is generic satisfiability of a hypergraph in NP? Is it NP-hard?

• Is there a satisfiable-but-entangled phase, in which random formulas are satisfiable, but all satisfying states are highly entangled?

• Assuming there is a transition, does \( \alpha_c^q \) grow as \( 2^k \)? Does it even grow without bound as \( k \) increases? Best lower bounds so far are less than 1!

• What is the adversarial classical threshold, where the hypergraph is random, but the adversary chooses which literals to negate?
Graph Isomorphism

- Factoring appears to be outside P, but not NP-complete. (Indeed, we believe that BQP does not contain all of NP.)

- Another candidate problem like this:
The Hidden Subgroup Problem

- We have a function $f : G \to X$
- We want to know its symmetries $H \subseteq G$
- Essentially all quantum algorithms that are exponentially faster than classical are of this form:
  - $\mathbb{Z}_n^*$ = factoring
  - $S_n$ = Graph Isomorphism
  - $D_n$ = some cryptographic lattice problems
It turns out that this naïve generalization of Shor’s algorithm doesn’t work: the permutation group $S_n$ is “too non-Abelian.”

Tantalizingly, we know a measurement exists, but we don’t know if we can do it efficiently.

How much can quantum computing really do? How “special” is factoring?
Scattering Algorithms

[Graphs and diagrams with nodes labeled as 'true' and 'false']
Schrödinger’s Equation, Diffraction, and Evolutes
Shameless Plug

Oxford University Press, 2010

THE NATURE of COMPUTATION

Cristopher Moore
Stephan Mertens

Thursday, October 1, 2009
Acknowledgements

- Also, NSF and DTO