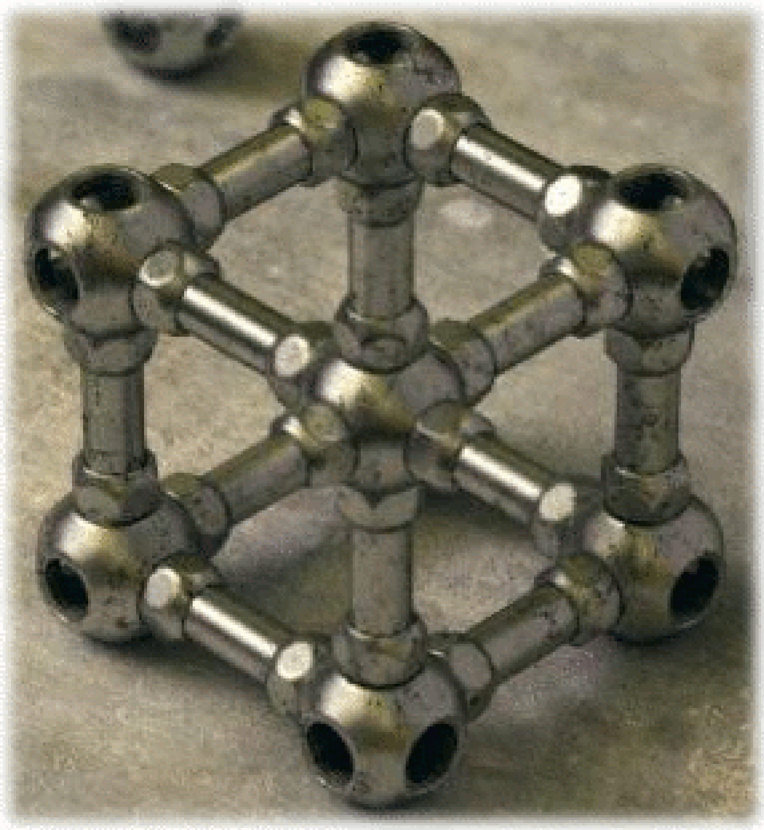

Classical and quantum satisfiability [1]

Author(s):

Anderson de Araújo

Marcelo Finger

[1] This work was supported by Fapesp Project LogProb, grant 2008/03995-5, São Paulo, Brazil.

Classical and quantum satisfiability

Anderson de Araújo   Marcelo Finger

Institute of Mathematics and Statistics
Departament of Computer Science
University of São Paulo

Objectives

General: To analyze the main quantum and classical time-complexity classes (*P*, *NP*, *BQP* and *QMA*), studying *NP* and *QMA* complete problems.

Objectives

General: To analyze the main quantum and classical time-complexity classes (*P*, *NP*, *BQP* and *QMA*), studying *NP* and *QMA* complete problems.

Specific: To show that the existing quantum versions of the satisfiability problem (*SAT*) do not allow an adequate logical analysis of the relationship between *NP* and *QMA*.

Motivation

General: There are quantum algorithms that efficiently solves some important problems, for example: (1) *Shor's algorithm* is a quantum algorithm for integer factorization which takes time $O((\log n)^3)$; (2) *Grover's algorithm* is a quantum algorithm for searching an unsorted database with n entries in $O(\sqrt{n})$ time.

Motivation

General: There are quantum algorithms that efficiently solves some important problems, for example: (1) *Shor's algorithm* is a quantum algorithm for integer factorization which takes time $O((\log n)^3)$; (2) *Grover's algorithm* is a quantum algorithm for searching an unsorted database with n entries in $O(\sqrt{n})$ time.

Specific: There are classical and quantum problems that *at first glance* seem similar, notably: *probabilistic satisfiability problem* (*PSAT*) and *quantum satisfiability problem* (*QSAT*). Both are probabilistic problems and can be viewed as linear program problems. In (Finger and de Bona, 2010), a polynomial-time reduction of *PSAT* to *SAT* was given. *PSAT* is *NP*-complete and *QSAT* is *QMA*-complete. So...

Problem

Can we use *PSAT* and *QSAT* to compare the classes *NP* and *QMA*?

Strategy

- To put *SAT* and *QSAT* in the same framework.
- To investigate whether all *SAT*-instances are *QSAT*-instances, and vice-versa.

Quantum satisfiability problem (Kitaev-Bravyi)

Input: A set with m local density matrices $|v_m\rangle\langle v_m| \otimes I_{n-k}$ defined on a Hilbert space $\mathcal{H}^{\otimes n}$ of n qubits (dimension 2^n), where each $|v_m\rangle$ is a vector in the subspace $\mathcal{H}^{\otimes k} \subseteq \mathcal{H}^{\otimes n}$ and I_{n-k} is the identity operator on $\mathcal{H}^{\otimes n-k}$. For $|v_m\rangle\langle v_m| \otimes I_{n-k} = (a^m_{ij})$, the condition of *locality* means that a^m_{ij} is given with $poly(n)$ many bits.

Quantum satisfiability problem (Kitaev-Bravyi)

Input: A set with m local density matrices $|v_m\rangle\langle v_m| \otimes I_{n-k}$ defined on a Hilbert space $\mathcal{H}^{\otimes n}$ of n qubits (dimension 2^n), where each $|v_m\rangle$ is a vector in the subspace $\mathcal{H}^{\otimes k} \subseteq \mathcal{H}^{\otimes n}$ and I_{n-k} is the identity operator on $\mathcal{H}^{\otimes n-k}$. For $|v_m\rangle\langle v_m| \otimes I_{n-k} = (a^m_{ij})$, the condition of *locality* means that a^m_{ij} is given with $poly(n)$ many bits.

Problem: Is there a vector $|v\rangle$ in $\mathcal{H}^{\otimes n}$ such that

$$\sum_{l=1}^{m} \langle v|(|v_l\rangle\langle v_l| \otimes I_{n-k})|v\rangle = 0?$$

Or, for each vector $|v\rangle$ in $\mathcal{H}^{\otimes n}$, is it true that

$$\sum_{l=1}^{m} \langle v|(|v_l\rangle\langle v_l| \otimes I_{n-k})|v\rangle \geq \epsilon, \text{ where } \epsilon \geq n^{-\alpha} \text{ for}$$
$\alpha = O(1)$ is a fixed precision parameter?

Intuition behind QSAT

- The reduzed density matrices $|v_I\rangle\langle v_I| \otimes I_{n-k}$ correspond to unsatisfying assignments of clauses ψ_I of a propositional formula ϕ in CNF.

Intuition behind QSAT

- The reduzed density matrices $|v_l\rangle\langle v_l| \otimes I_{n-k}$ correspond to unsatisfying assignments of clauses ψ_l of a propositional formula ϕ in CNF.
- A vector $|v\rangle$ in $\mathcal{H}^{\otimes n}$ is such that $|v_l\rangle\langle v_l| \otimes I_{n-k}|v\rangle = 0$ if, and only if, v is an assignment to the n variables which satisfies the clause ψ_l.

Intuition behind QSAT

- The reduzed density matrices $|v_l\rangle\langle v_l| \otimes I_{n-k}$ correspond to unsatisfying assignments of clauses ψ_l of a propositional formula ϕ in CNF.
- A vector $|v\rangle$ in $\mathcal{H}^{\otimes n}$ is such that $|v_l\rangle\langle v_l| \otimes I_{n-k}|v\rangle = 0$ if, and only if, v is an assignment to the n variables which satisfies the clause ψ_l.
- ϕ is satisfiable if, and only if, $\sum_{l=1}^{m}\langle v|(|v_l\rangle\langle v_l| \otimes I_{n-k})|v\rangle = 0$ for some $|v\rangle \in \mathcal{H}^{\otimes n}$.

Example (Aharonov and Naveh, 2002)

For the clause $\psi_l = x \vee y \vee \neg z$, we have the Hermitian matrix

$$H_l = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} = |001\rangle\langle 001|,$$

since (001) is the only unsatisfying assignment for ψ_l. In this case, v is an assignment to the n variables which satisfies the clause ψ_l if, and only if, $|v\rangle$ in $\mathcal{H}^{\otimes n}$ is such that $H_l \otimes I_{n-3}|v\rangle = 0$.

Some difficulties in the previous example

- It does not work a clause $\psi'_l = \neg x_1 \vee x_2 \vee \neg x_3$ in *QSAT*: (101) is the only unsatisfying assignment in this case and H'_l will not be a density matrix since $\mathtt{tr}(H'_l) > 1$.

Some difficulties in the previous example

- It does not work a clause $\psi'_l = \neg x_1 \vee x_2 \vee \neg x_3$ in *QSAT*: (101) is the only unsatisfying assignment in this case and H'_l will not be a density matrix since $\mathtt{tr}(H'_l) > 1$.
- This shows that it is necessary a condition of normalization.

Some difficulties in the previous example

- It does not work a clause $\psi'_l = \neg x_1 \vee x_2 \vee \neg x_3$ in *QSAT*: (101) is the only unsatisfying assignment in this case and H'_l will not be a density matrix since $\mathtt{tr}(H'_l) > 1$.
- This shows that it is necessary a condition of normalization.
- Moreover, the matrices only have elements 0 and 1, but the original problem is general: any polynomial computable complex number which satisfies the condition of normalization can be an element of the matrices.

$QSAT^l$: *a logical version of QSAT*

- Let ψ_l be a clause of a propositional formula ϕ in CNF with degree (k, n), where k is the number of literal in each clause and n the number of variables in ϕ. A *quantum assigment to* ψ_l is a $2^n \times 2^n$-matrix $\|\psi_l\|_v$ on $\mathbb{C}_2^{\otimes n}$ such that

$$\|\psi_l\|_v = A_l(|v(x_{l_1})\cdots v(x_{l_k})\rangle\langle v(x_{l_1})\cdots v(x_{l_k})| \otimes I_{n-k}),$$

where $\{x_{l_1}, \ldots, x_{l_k}\} = var(\psi_l)$, $v \in Eval(\phi)$ is such that, for all l with $1 \leq l \leq m$, $\hat{v}(\psi_l) = 0$, A_l is matrix for which $\mathtt{tr}(\|\psi_l\|_v) = 1$, $\|\psi_l\|_v = \|\psi_l\|_v^{T*}$, $\langle u| \, \|\psi_l\|_v \, |u\rangle \geq 0$ for all $|u\rangle \in \mathbb{C}_2^{\otimes n}$ and $a^l_{ij} \neq 0$ for $i = j$ but $a^l_{ij} = 0$ for $i \neq j$.

$QSAT^l$: *a logical version of* $QSAT$

- Let ψ_l be a clause of a propositional formula ϕ in CNF with degree (k, n), where k is the number of literal in each clause and n the number of variables in ϕ. A *quantum assigment to* ψ_l is a $2^n \times 2^n$-matrix $\|\psi_l\|_v$ on $\mathbb{C}_2^{\otimes n}$ such that

$$\|\psi_l\|_v = A_l(|v(x_{l_1})\cdots v(x_{l_k})\rangle\langle v(x_{l_1})\cdots v(x_{l_k})| \otimes I_{n-k}),$$

  where $\{x_{l_1}, \ldots, x_{l_k}\} = var(\psi_l)$, $v \in Eval(\phi)$ is such that, for all l with $1 \leq l \leq m$, $\hat{v}(\psi_l) = 0$, A_l is matrix for which $\mathtt{tr}(\|\psi_l\|_v) = 1$, $\|\psi_l\|_v = \|\psi_l\|_v^{T*}$, $\langle u| \, \|\psi_l\|_v \, |u\rangle \geq 0$ for all $|u\rangle \in \mathbb{C}_2^{\otimes n}$ and $a_{ij}^l \neq 0$ for $i = j$ but $a_{ij}^l = 0$ for $i \neq j$.
- Given an $\epsilon \geq n^{-\alpha}$ for $\alpha = O(1)$, ϕ is *quantum satisfiable* if there is $|w\rangle \in \mathbb{C}_2^{\otimes n}$ for which $|v\rangle = |w\rangle + |v(x_1)\cdots v(x_n)\rangle$ is such that

$$\sum_{l=1}^{m} \langle v|(|v_l\rangle\langle v_l| \otimes I_{n-k})|v\rangle = 0.$$

  Otherwise, ϕ is *quantum unsatisfiable*, i.e., for each vector $|v\rangle$ in $\mathcal{H}^{\otimes n}$, is it true that

$$\sum_{l=1}^{m} \langle v|(|v_l\rangle\langle v_l| \otimes I_{n-k})|v\rangle \geq \epsilon$$

Another example

Take the formula $\phi = (x \vee \neg y) \wedge (x \vee z)$. The assigment $v \in Eval(\phi)$ such that $v(x) = 0$, $v(y) = 1$ and $v(z) = 0$ is such that $\hat{v}(x \vee \neg y) = \hat{v}(\neg x \vee z) = 0$ and so $\hat{v}(\phi) = 0$. In this case,

$$|v(x)v(y)\rangle\langle v(x)v(y)| = |01\rangle\langle 01| = |0\rangle \otimes |1\rangle\langle 0| \otimes \langle 1| = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

and

$$|v(x)v(z)\rangle\langle v(x)v(z)| = |00\rangle\langle 00| = |0\rangle \otimes |0\rangle\langle 0| \otimes \langle 0| = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

As $k = 2$ and $n = 3$, $\|x \vee \neg y\|_v$ and $\|x \vee z\|_v$ are, respectively, the following matrices:

$$A_1 \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, A_2 \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

for some appropriate 8×8-matrices A_1 and A_2.

However, $|v(x)v(y)v(z)\rangle = |010\rangle = |0\rangle \otimes |1\rangle \otimes |0\rangle$ is the vector

$$\begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

Since $A_1 \|x \vee \neg y\|_v |v(x)v(y)v(z)\rangle = 0$ but $A_1 \|x \vee z\|_v |v(x)v(y)v(z)\rangle \neq 0$ for any matrices A_1 and A_2, we conclude that ϕ is quantum unsatisfiable.

$QSAT^{l}$ *is not an adequate generalization of* SAT

Theorem

Let ϕ be a propositional formula in CNF with degree (k, n) such that $var(\phi) = \{x_1, \ldots, x_n\}$. Suppose that ϕ is satisfiable and ψ_p as well as ψ_q are clauses of ϕ such that $var(\psi_p) \neq var(\psi_q)$. Then, there exists an assigment $v \in Eval(\phi)$ such that, for all l, $\hat{v}(\psi_l) = 0$ but there is no vector $|w\rangle$ in $\mathbb{C}_2^{\otimes n}$ such that, for $|v\rangle = |w\rangle + |v(x_1) \cdots v(x_n)\rangle$, both $\langle v| \, \|\psi_p\|_v \, |v\rangle = 0$ and $\langle v| \, \|\psi_q\|_v \, |v\rangle = 0$.

Proof (idea).

- Permutations of the conjunctions and disjunctions ocurring in ϕ do not change its classical truth-value.
- Put the literals of ψ_p and ψ_q that have different variables in the same position in $\|\psi_p\|_v$ and $\|\psi_q\|_v$.

□

Present work

- The logical relationship between *SAT* and *QSAT* was made explicit. It was shown that the connection between them is only superficial and not deep enough to allow a direct comparison between *NP* and *QMA*.

Present work

- The logical relationship between *SAT* and *QSAT* was made explicit. It was shown that the connection between them is only superficial and not deep enough to allow a direct comparison between *NP* and *QMA*.
- Variations of *QSAT* more closed to *PSAT* are just stoquastic versions of *QSAT*. Thus, the same limitations exhibited here also are applicable to them.

Present work

- The logical relationship between *SAT* and *QSAT* was made explicit. It was shown that the connection between them is only superficial and not deep enough to allow a direct comparison between *NP* and *QMA*.
- Variations of *QSAT* more closed to *PSAT* are just stoquastic versions of *QSAT*. Thus, the same limitations exhibited here also are applicable to them.
- Is there a *QMA*-complete problem that, from a logical point of view, is an appropriate quantum generalization of *SAT*?

Future work

- If $QSAT^{I}$ is QMA-complete, then the answer is "No!" and perhaps this fact can be used to show that $NP \not\subseteq QMA$.

Future work

- If $QSAT^I$ is QMA-complete, then the answer is "No!" and perhaps this fact can be used to show that $NP \not\subseteq QMA$.
- If $QSAT^I$ is *not* QMA-complete, then the answer is, perhaps, "Yes!" and we don't know what say about the question "$NP \subseteq QMA$?"!