Quantum Algorithms
Lecture 27
The quantum analogue of NP: the class BQNP I

Zhejiang University

Another complexity classes

It is possible to construct quantum analogues not only for the class P, but also for other classical complexity classes. This is not a routine process, but suitable generalizations often come up naturally. We will consider the class NP as an example.

Another example — the class IP and its quantum analogue QIP. Authors also mention that the quantum analogue of PSPACE equals PSPACE. In 2009 it was proven that QIP=PSPACE, so IP=QIP=PSPACE=quantum PSPACE.

Modification of classical definitions

Partially defined function

Quantum computation, as well as probabilistic computation, is more naturally described using partially defined functions.

A partially defined Boolean function is a function

$$F\colon B^n \to \{0,1,\text{“}undefined\text{”}\}$$

In this section, it will be tacitly understood that by Boolean function we mean partially defined Boolean function.

Notations

One more comment regarding notation: we have used the symbol P both for the class of polynomially computable functions and for the class of polynomially decidable predicates; now we act analogously, using the notations P, NP, etc. for classes of partially defined functions.

P, of course, denotes the class of polynomially computable partially defined functions. We introduce a modified definition of the class NP.

Definition

A function $F: B^n \to \{0,1,\text{“}undefined\text{”}\}$ belongs to the class NP if there is a partially defined function $R \in P$ in two variables such that

$$F(x) = 1 \Rightarrow \exists y((|y| < q(|x|)) \wedge (R(x,y) = 1))$$
$$F(x) = 0 \Rightarrow \forall y((|y| < q(|x|)) \Rightarrow (R(x,y) = 0))$$

As before, $q(\cdot)$ is a polynomial.

Logical expression $(|y| < q(|x|)) \Rightarrow (R(x,y) = 0)$ means that if $|y| < q(|x|)$, then $R(x,y) = 0$.

If y is not of polynomial length, then condition of $R(x,y) = 0$ is not mandatory.

Probabilistic case

What would change if in Definition we replaced the condition $R \in P$ by the condition $R \in BPP$? First of all, we would get a different, broader, class, which we could denote by BNP. However, for this class there is another, standard, notation — MA, indicating that it falls into a hierarchy of classes defined by Arthur-Merlin games. We have mentioned Arthur and Merlin in connection with the definition of NP. We have also discussed games corresponding to other complexity classes (in Section 5.1).

Probabilistic case

Traditionally, the term “Arthur-Merlin games” is used for probabilistic games in which Arthur is a polynomial Turing machine whereas Merlin is all-powerful; before each move Arthur flips coins so that both players see them. The order of the letters in the symbol MA indicates the order of the moves: at first Merlin communicates y, then Arthur checks the truth of the predicate $R(x, y)$, by a polynomial probabilistic computation. The message y is sometimes called a “proof”; it may be hard to find but easy to check.

MA case

Example of MA class will be resembling our definition for quantum NP – in case of MA probabilistic TM receives a proof y from Merlin, and then TM processes this proof probabilistically. We will see how it works in quantum case.

Quantum definition by analogy

BQNP definition

A function $F\colon B^n \to \{0,1,\text{“}undefined\text{”}\}$ belongs to the class BQNP if there exists a polynomial classical algorithm that computes a function $x \to Z(x)$, where $Z(x)$ is a description of a quantum circuit, realizing an operator $U_x\colon B^{\otimes N_x} \to B^{\otimes N_x}$ such that

$$F(x)=1 \implies \exists\,|\xi\rangle \in \mathcal{B}^{\otimes m_x}\ \mathbf{P}\left(U_x|\xi\rangle \otimes |0^{N_x-m_x}\rangle,\ \mathcal{M}\right) \geq p_1,$$

$$F(x)=0 \implies \forall\,|\xi\rangle \in \mathcal{B}^{\otimes m_x}\ \mathbf{P}\left(U_x|\xi\rangle \otimes |0^{N_x-m_x}\rangle,\ \mathcal{M}\right) \leq p_0.$$

BQNP definition

$$F(x)=1 \implies \exists\,|\xi\rangle \in \mathcal{B}^{\otimes m_x}\ \mathbf{P}\Big(U_x|\xi\rangle \otimes |0^{N_x-m_x}\rangle,\ \mathcal{M}\Big) \geq p_1,$$

$$F(x)=0 \implies \forall\,|\xi\rangle \in \mathcal{B}^{\otimes m_x}\ \mathbf{P}\Big(U_x|\xi\rangle \otimes |0^{N_x-m_x}\rangle,\ \mathcal{M}\Big) \leq p_0.$$

Here $M = C(|1\rangle) \otimes B^{\otimes(N_x-1)}$, and p_0, p_1 satisfy the condition $p_1 - p_0 \geq \Omega(n^{-\alpha})$ for some constant $\alpha \geq 0$. The quantifiers of $|\xi\rangle$ include only vectors of unit length. (We will use an analogous convention further on in this section, pushing numeric factors outside the $|\cdot\rangle$ sign.)

The vector $|\xi\rangle$ plays the role of a proof. Note that $m_x \leq N_x \leq |Z(x)| = poly(|x|)$ since the algorithm is polynomial.

Amplification of probabilities

If $F \in BQNP$, then it likewise satisfies a variant of BQNP Definition in which the numbers p_0, p_1 ($p_1 - p_0 \geq \Omega(n^{-\alpha})$) are replaced by

$$p_1' = 1 - \varepsilon, p_0' = \varepsilon, \varepsilon = \exp(-\Omega(n^{\beta}))$$

where β is an arbitrary positive constant.

Proof - keypoints

- $k = poly(n)$ copies of the circuit realizing the operator $U = U_x$;
- majority function (where $p = (p0 + p1)/2$):

$$G(z_1, \ldots, z_k) = \begin{cases} 1 & \text{if } \sum_{j=1}^{k} z_j \geq pk, \\ 0 & \text{if } \sum_{j=1}^{k} z_j < pk, \end{cases}$$

- Merlin may attempt to deceive Arthur by sending him a message that is not factorable into the tensor product, so additional analysis is needed, because copy-approach will not work.

Proof – density matrix

Merlin submits any density matrix $\rho \in L(B^{\otimes km})$. It is like k copies, each of size m, but here we have a density matrix, so it is not like copies.

In simplified terms, we get probabilities to have a specific value a in first qubit of m-bit portion of ρ after applying U.

$$\mathbf{P}(z_1, \ldots, z_k | \rho) = \mathrm{Tr}\left(X^{(z_1)} \otimes \cdots \otimes X^{(z_k)} \rho\right),$$

$$X^{(a)} = \mathrm{Tr}_{[m+1,\ldots,N]}\left(U^\dagger \Pi_1^{(a)} U \left(I_{\mathcal{B}^{\otimes m}} \otimes |0^{N-m}\rangle\langle 0^{N-m}|\right)\right).$$

Proof – probabilities

In case of $F(x) = 1$, Merlin can just send tensored copies of convincing quantum state. In this case lower bound for probabilities will be investigated, to see that the probability is $\geq pk$.

In the opposite case, $F(x) = 0$, we will obtain an upper bound for the probability over all density matrices ρ.

Proof – probabilities

Authors consider conditional probabilities over basis vectors. Since we are interested in function G, where we are interested to check cases where number of outcomes 1 equals pk, derived formulas use combinations formula (from combinatorics):

$$C(n,k) = \binom{n}{k} = \frac{n!}{k!\,(n-k)!}$$

Then probability estimates use Chernoff's inequality.

Remarks

Authors mention that diagonalization of both $X^{(0)}$ and $X^{(1)}$ over the same basis was important, it simplifies analysis so we considered basis states.

In nontrivial complexity classes probability amplification does not affect the class, since additional resources for amplification are incomparably small for resource constraints of the complexity class.

Complete problems

Karp reducibility

A predicate $L1$ is reducible to a predicate $L2$ if there exists a function $f \in P$ such that $L1(x) = L2(f(x))$ for any input string x.

We say that f reduces $L1$ to $L2$. Notation: $L1 \propto L2$.

Karp reducibility is also called "polynomial reducibility".

NP-completeness

A predicate $L \in NP$ is NP-complete if any predicate in NP is reducible to it.

If some NP-complete predicate can be computed in time $T(n)$, then any NP-predicate can be computed in time $poly(n) + T(poly(n))$. Therefore, if some NP-complete predicate belongs to P, then P = NP. Put is this way: if P ≠ NP (which is probably true), then no NP-complete predicate belongs to P.

Complete problem

Consider a function F which is defined on a subset of the words of this form:
$z = \{(description\ of\ a\ quantum\ circuit\ U), p0, p1\}$
where by description of a circuit we mean its approximate realization in the standard basis, and $p0$, $p1$ are such that $p1 - p0 \geq \Omega(n^{-\alpha})$ (n is the size of the circuit, $\alpha > 0$ is a constant).

Complete problem

The function F is defined as follows:

- $F(z) = 1 \Leftrightarrow$ there exists a vector $|\xi\rangle$, on which we get 1 in the first bit with probability greater than $p1$;
- $F(z) = 0 \Leftrightarrow$ for all $|\xi\rangle$ the probability of getting 1 in the first bit is smaller than $p0$.

The problem is complete because it is equal to the Definition of class BQNP. Therefore, it is easy to reduce any BQNP problem to this one.

3-CNF

Recall that a CNF (conjunctive normal form) is a conjunction of clauses; each clause is a disjunction of literals; each literal is either a variable or a negation of a variable. If each clause contains at most three literals, we get a 3-CNF.

$(x1 \vee \neg x2 \vee x3) \wedge (\neg x1 \vee x4 \vee \neg x5)$

A quantum analog of 3-CNF — the local Hamiltonian (locality is the analogue of the condition that the number of variables in each clause is bounded).

Hermitian matrix

Normal matrix: $AA^H = A^H A$, unitary: $AA^H = A^H A = I$.

Hermitian matrix: $A^H = A$.

For an Hermitian matrix:

- all eigenvalues are real,
- eigenvectors corresponding to distinct eigenvalues are orthogonal,
- there exists an orthogonal basis of the whole space, consisting of eigenvectors.

Thus all Hermitian matrices are diagonalizable.

Reminder: density matrices are Hermitian nonnegative operators with trace 1.

k-local Hamiltonian

An operator H: $B^{\otimes n} \to B^{\otimes n}$ is called a k-local Hamiltonian if it is expressible in the form

$$H = \sum_j H_j[S_j]$$

where each term $H_j \in L(B^{\otimes |S_j|})$ is a Hermitian operator acting on a set of qubits S_j, $|S_j| \leq k$.

In addition, authors put a normalization condition, namely, $0 \leq H_j \leq 1$, meaning that both H_j and $I - H_j$ are nonnegative.

The local Hamiltonian

z={description of a k-local Hamiltonian H, a, b} where $k = O(1)$, $0 \leq a < b$, $b - a = \Omega(n^{-\alpha})$ ($\alpha > 0$ is a constant). Then

- $F(x) = 1 \iff H$ has an eigenvalue not exceeding a,
- $F(x) = 0 \iff$ all eigenvalues of H are greater than b.

LH belongs to BQNP

$$H = \sum_j H_j[S_j]$$

Authors construct a circuit W that can be applied to a state $|\eta\rangle \in B^{\otimes n}$ so as to produce a result 1 or 0 (“yes” or “no”): it says whether Arthur accepts the submitted state or not.

The answer "yes" will occur with probability $p = 1 - r^{-1}\langle\eta|H|\eta\rangle$.

Number of terms r means how many such $H_j[S_j]$ we have.

LH belongs to BQNP

Authors use the result of Problem 11.8: POVM measurement can be represented as an isometric embedding into a larger space, followed by a projective measurement.

In the proof each Hermitian term H_j is represented in orthogonal basis of eigenvectors:

$$H_j = \sum_s \lambda_s |\psi_s\rangle \langle\psi_s|$$

Then authors represent $|\eta\rangle = \sum_s y_s |\psi_s\rangle$ as the expansion of $|\eta\rangle$ in the orthogonal system of eigenvectors of H_j.

LH belongs to BQNP

The measuring operator is designed in a way that it picks random term H_j from Hamiltonian H, then applies the corresponding measurement operator:

$$W_j : |\psi_s, 0\rangle \mapsto |\psi_s\rangle \otimes \left(\sqrt{\lambda_s}|0\rangle + \sqrt{1-\lambda_s}|1\rangle\right)$$

Analysis of probabilities gives the following formula:

$$\mathbf{P}(1) = \sum_j \frac{1}{r}\mathbf{P}_j(1) = \sum_j \frac{1}{r}\left(1 - \langle\eta|H_j|\eta\rangle\right) = 1 - r^{-1}\langle\eta|H|\eta\rangle$$

Local Hamiltonian – another description

The local Hamiltonian problem

Suppose that M is a Hermitian matrix whose rows and columns are indexed by strings of length n for some integer $n \geq 1$. Then M is said to be k-local if and only if it can be expressed as

$$M = P_\pi (A \otimes I) P_\pi^{-1}$$

for an arbitrary matrix A indexed by Σ^k, P_π a permutation matrix defined by

$$P_\pi |x_1 \ldots x_n\rangle = |x_{\pi(1)} \ldots x_{\pi(n)}\rangle$$

for some permutation $\pi \in S_n$, and I denoting the identity matrix indexed by Σ^{n-k}.

The local Hamiltonian problem

M is a matrix that arises from a "gate" on k qubits, but where the gate is described by a $2^k \times 2^k$ Hermitian matrix A rather than a unitary matrix. It is possible to express such a matrix compactly by specifying A along with the bit-positions on which A acts.

The local Hamiltonian problem

A k-local matrix assigns a real number (typically thought of as representing energy) to any quantum state on n qubits. This number depends only on the reduced state of the k qubits where M acts nontrivially, and can be thought of as a locally defined penalty on a given quantum state. Loosely speaking, the k-local Hamiltonian problem asks whether there exists a quantum state that can significantly avoid a collection of such penalties.

THE k-LOCAL HAMILTONIAN PROBLEM

Input: A collection $H_1, \ldots, H_m$ of k-local Hermitian matrices with entries indexed by strings of length n and satisfying $\|H_j\| \leq 1$ for $j = 1, \ldots, m$.

Yes: There exists an n-qubit quantum state $|\Psi\rangle$ such that $\langle\Psi|H_1 + \cdots + H_m|\Psi\rangle \leq -1$.

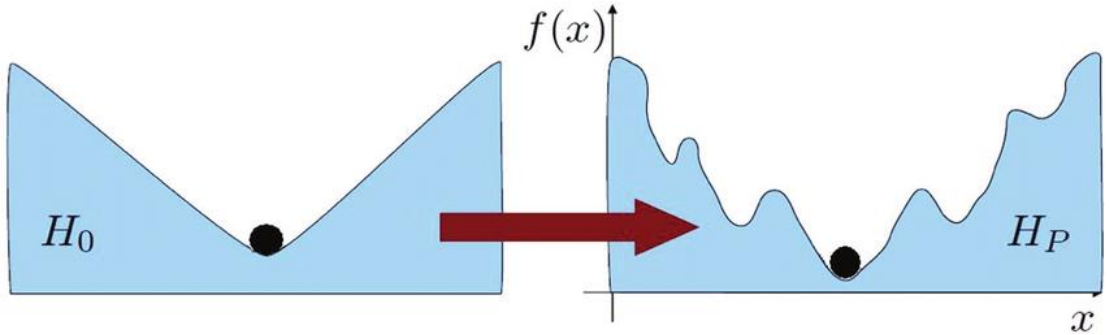
No: For every n-qubit quantum state $|\Psi\rangle$ it holds that $\langle\Psi|H_1 + \cdots + H_m|\Psi\rangle \geq 1$.

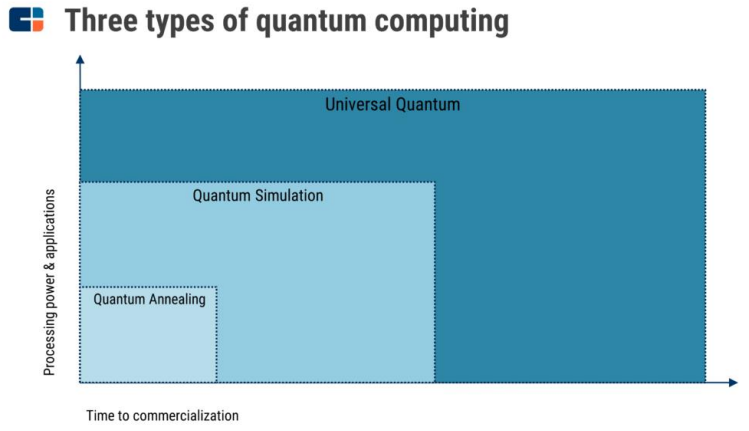
Theorem

The 2-local Hamiltonian problem is complete for QMA with respect to Karp reductions.

The completeness of this problem has been shown to be closely related to the universality of the so-called adiabatic model of quantum computation.

QMA is currently widely used to name the class BQNP. QMA = Quantum Merlin-Arthur.





Another description of the problem

Decide, whether the ground state energy (i.e., lowest eigenvalue) of a given k-local Hamiltonian is at most some given number a or at least $a + 1/poly(n)$. Determining the ground state energy of a given physical system is extremely important in physics and chemistry.

We can just let the quantum witness be the ground state (i.e., an eigenstate for the lowest eigenvalue) and measure its energy using the Hamiltonian, which is the observable corresponding to total energy.

Several Variants of the local Hamiltonian problem

The 2-local Hamiltonian problem remains QMA-complete when the local Hamiltonians are restricted to nearest neighbor interactions on a two-dimensional array of qubits. The hardness of the local Hamiltonian problem with nearest-neighbor interactions on one-dimensional systems is known to be QMA-complete for 12 dimensional particles in place of qubits, but is open for smaller systems including qubits.

Thank you for your attention!