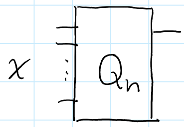
BQP: Efficient Quantum Computation

1. Definition

Let $A = (A_{yes}, A_{no})$ be a promise problem and let $c, s: \mathbb{N} \to [0,1]$ be functions. Then $A \in \mathrm{BQP}(c, s)$ if and only if there exists a *polynomial-time uniform family of quantum circuits* $\{Q_n : n \in \mathbb{N}\}$, where Q_n takes n qubits as input and outputs 1 bit, such that

- if $x \in A_{yes}$ then $\Pr[Q_{|x|}(x) = 1] \geq c(|x|)$, and
- if $x \in A_{no}$ then $\Pr[Q_{|x|}(x) = 1] \leq s(|x|)$.



The class BQP is defined as BQP = BQP(2/3,1/3).

2. Error reduction for BQP

Theorem. Let $p: \mathbb{N} \to \mathbb{N}$ be a polynomially bounded function satisfying $p(n) \geq 2$ for all n. Then it holds that BQP = $\mathrm{BQP}(1 - 2^{-p}, 2^{-p})$.

Idea: repeat the computation many times and take majority vote

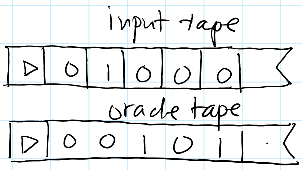
· Chernoff bound.

3. BQP subroutine theorem

Theorem. $\mathrm{BQP}^{\mathrm{BQP}} = \mathrm{BQP}$.

4. Complexity classes of oracle machines

An oracle is a subset $B \subseteq \Sigma^*$, an oracle Turing machine with oracle B attached is a Turing machine which may call the oracle B at intermediate computational steps and the call counts as a **single** step.



$\mathrm{P}^B, \mathrm{NP}^B, \ldots$

extend the ability of the machine

Oracles in the circuit model: in addition to the usual gates, we have a family of big gates $\{O_m\}$ such that

$$O_{|y|}(y) = \begin{cases} 1 & y \in B, \\ 0 & y \notin B. \end{cases}$$

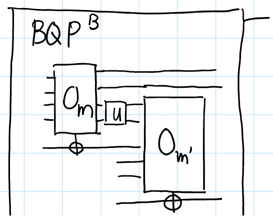
For a complexity class C, we define

$\mathrm{P}^{\mathrm{C}} = \cup_{B \in \mathrm{C}} \mathrm{P}^B$

$\mathrm{NP}^{\mathrm{NP}} \overset{?}{\neq} \mathrm{NP}$

$\mathrm{NP}^{\mathrm{NP}}$ and the polynomial hierarchy

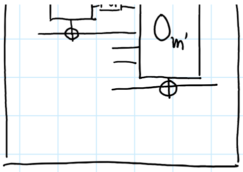
In the quantum case, we adopt the form of the oracle access as $O_m|y, a\rangle = |y, a \oplus O_m(y)\rangle$



5. Proof

What do we need to prove?

5. Proof

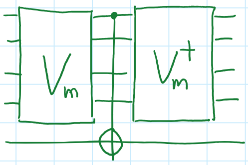


What do we need to prove?

Two difficulties:

1. The output of a BQP circuit is probabilistic
2. We need to simulate the behaviour of the O_m gate on all qubits

1. error reduction
2. $\{V_m\}$ the uniform circuit family for B.



6. Relation with classical friends

- BPP: Same as BQP, but uses (random) classical circuits
- PP: Same as BPP, but with $c > 1/2$ and $s \leq 1/2$ #P
- PSPACE: A promise problem A is in PSPACE if and only if there exists a deterministic Turing machine running in polynomial space that accepts every string $x \in A_{yes}$ and rejects every string $x \in A_{no}$
- PH: Polynomial hierarchy

  Meet more complexity animals at Complexity Zoo!

  P ⊆ BPP ⊆ BQP ⊆ QMA ⊆ PP ⊆ PSPACE

  Conjecture. BQP is not contained in NP and vice versa.

multiplication factoring TQBF

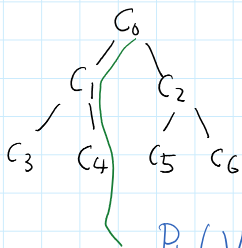
7. BQP vs PP

Counting

Theorem. BQP ⊆ PP.

- GapP functions
- A function $g: \Sigma^* \rightarrow \mathbb{Z}$ is a *GapP function* if there exists a polynomial p and a polynomial-time computable funcion f such that

$$g(x) = \#\{y \in \Sigma^{p(|x|)}: f(x,y) = 0\} - \#\{y \in \Sigma^{p(|x|)}: f(x,y) = 1\}$$
$$= \sum_{y \in \Sigma^{p(|x|)}} (-1)^{f(x,y)}.$$



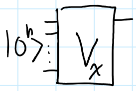
$\Pr_w(V(x,w)=1)$

- Lemma: A promise problem is in PP if and only if there is a GapP function g such that
  a. if $x \in A_{yes}$ then $g(x) > 0$, and
  b. if $x \in A_{no}$ then $g(x) \leq 0$.
- Fact: quantum computational universality of H and Toffoli

Fourier → H, classical →  real amplitudes are enough

- Quantum computing is all about estimating the first entry of unitary circuits

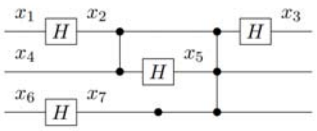
circuits



$$\Pr(\mathcal{U}\text{ accepts}) = \langle 0^n| \mathcal{U}^\dagger (|1\rangle\langle 1| \otimes I)\, \mathcal{U} |0^n\rangle$$

- Encode amplitudes as GapP functions

path integral



C'

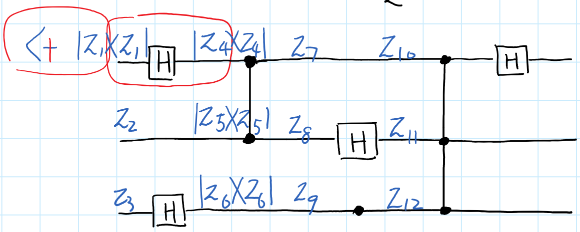
Figure 1: The internal part C' of a circuit C corresponding to the polynomial $x_1x_2 + x_2x_3 + x_4x_5 + x_6x_7 + x_2x_4 + x_2x_5x_7 + x_7$.

Screen clipping taken: 5/9/2020 5:21 PM

f_C over $n+h$ binary variables

$$C = H^{\otimes n}\, C'\, H^{\otimes n}$$

Claim $\langle 0^n| C |0^n\rangle = \dfrac{\mathrm{gap}(f_C)}{2^{h/2+n}}$ $\qquad \langle +^n| C' |+^n\rangle$



C'_z

h: # of H

n: # of qubits

$$C' = \sum_{z_1,\dots} C'_z$$

$$\langle +^n| C'_z |+^n\rangle = \frac{1}{2^{n+h/2}} (-1)^{z_1z_4} (-1)^{z_4z_5} \delta_{z_4z_7} \delta_{z_3z_8} \cdots$$

$$\langle +^n| C' |+^n\rangle = \frac{1}{2^{n+h/2}} \sum_x (-1)^{f_C(x)}$$

arXiv: 1607.08473

8. Exercise 3

Write down a definition of BQP without looking at any reference. Compare it with the definition given above and see if you have missed anything.

9. Exercise 4

Prove the error reduction theorem for BQP.