# Quantum Complexity Theory

## Journey to 1990 - 2010

Hee Ryang Choi

SNU SQRT

October 27, 2022

# Overview

1. BQP
   - Polynomial-time generated circuit families
   - Definition and Problems
   - Error Reduction and Subroutine
   - Bounds of BQP
2. QMA
   - Definition and Problems
   - Error Reduction
   - Other Properties of QMA
3. QIP
   - Definition and Properties
   - Quantum Statistically Zero Knowledge
   - Multiple Proof

# Overview

# Encoding

For any quantum circuit formed from the gates, there could be encoding which is a binary string using any number of different schemes.

- Sensibility : Every quantum circuit is encoded by at least one binary string, and every binary string encodes at most one quantum circuit.
- Efficiency : There is a fixed polynomial-bounded function $p$ such that every circuit of size $N$ has an encoding with length at most $p(N)$.
- Non-compressibility : It is not possible to work with encoding schemes that allow for meaningfully short encodings of circuits.

# Quantum circuit families

So any quantum circuit represents a finite computation with some fixed number of input and output qubits, quantum algorithms are modelled by families of quantum circuits.

## Polynomial-time generated

Let $S \subseteq \Sigma^*$ be any set of strings. Then a collection $\{\mathbf{Q}_x : x \in S\}$ of quantum circuits is said to be polynomial-time generated if there exists a polynomial-time deterministic Turing Machine that, on every input $x \in S$, outputs an encoding of $\mathbf{Q}_x$

# BQP

## BQP

Let $A = (A_{yes}, A_{no})$ be a promise problem and let $a, b : \mathbf{N} \to [0, 1]$ be functions. Then $A \in BQP(a, b)$ if and only if there exists a polynomial-time generated family of quantum circuits $\mathbf{Q} = \{\mathbf{Q}_n : n \in \mathbf{N}\}$, where each circuit $\mathbf{Q}_n$ takes $n$ input qubits and produces one output qubit, that satisfies the following properties.

- If $x \in A_{yes}$ then $Pr[\mathbf{Q}\ accepts\ x] \geq a(|x|)$
- If $x \in A_{no}$ then $Pr[\mathbf{Q}\ accepts\ x] \leq b(|x|)$

Also, the class BQP defined as BQP = BQP$(\frac{2}{3}, \frac{1}{3})$

# Recall : P

A language $L$ is in $P$ if and only if there exists a polynomial-time generated circuit family of Boolean circuits $\{C_n : n \in \mathbf{N}\}$, such that

- For all $n \in \mathbf{N}$, $C_n$ takes $n$ bits as input and outputs 1 bit
- For all $x$ in $L$, $C_{|x|}(x) = 1$
- For all $x$ not in $L$, $C_{|x|}(x) = 0$

# Recall : BPP

A language $L$ is in $P$ if and only if there exists a polynomial bounded function $r$ and a polynomial-time generated circuit family of Boolean circuits $\{C_n : n \in \mathbf{N}\}$, such that

- For all $n \in \mathbf{N}$, $C_n$ takes $n + r(n)$ bits as input and outputs 1 bit
- For all $x$ in $L$, $Pr(C_{|x|}(x) = 1) \geq 2/3$
- For all $x$ not in $L$, $Pr(C_{|x|}(x) = 0) \geq 2/3$

where $y \in \Sigma^{r(|x|)}$ is chosen uniformly random in both cases.

# BQP vs BPP

From definition, it is trivial that $BPP \subseteq BQP$. There are several problems known to be in BQP, but not known(also generally not) in BPP. Here are examples.

- Integer Factoring and Discrete Logarithm Problems
- Simulation of Quntum Systems(Universal Quantum Simulator)
- Approximating the Jones Polynomial at certain roots of unity
- Harrow-Hassidim-Lloyd algorithm

# BQP-complete

## APPROX-QCIRCUIT-PROB problem

Given a description of a quantum circuit $C$ acting on $n$ qubits with $m$ gates, where $m$ is a polynomial in $n$ and each gate acts on one or two qubits, and two numbers $\alpha, \beta \in [0, 1]$, $\alpha > \beta$, distinguish between the following two cases:

- measuring the first qubit of the state $C|0\rangle^{\otimes n}$ yields $|1\rangle$ with probability $\geq \alpha$
- measuring the first qubit of the state $C|0\rangle^{\otimes n}$ yields $|1\rangle$ with probability $\leq \beta$

Our claim is that any BQP problem reduces to APPROX-QCIRCUIT-PROB problem.

# BQP-complete

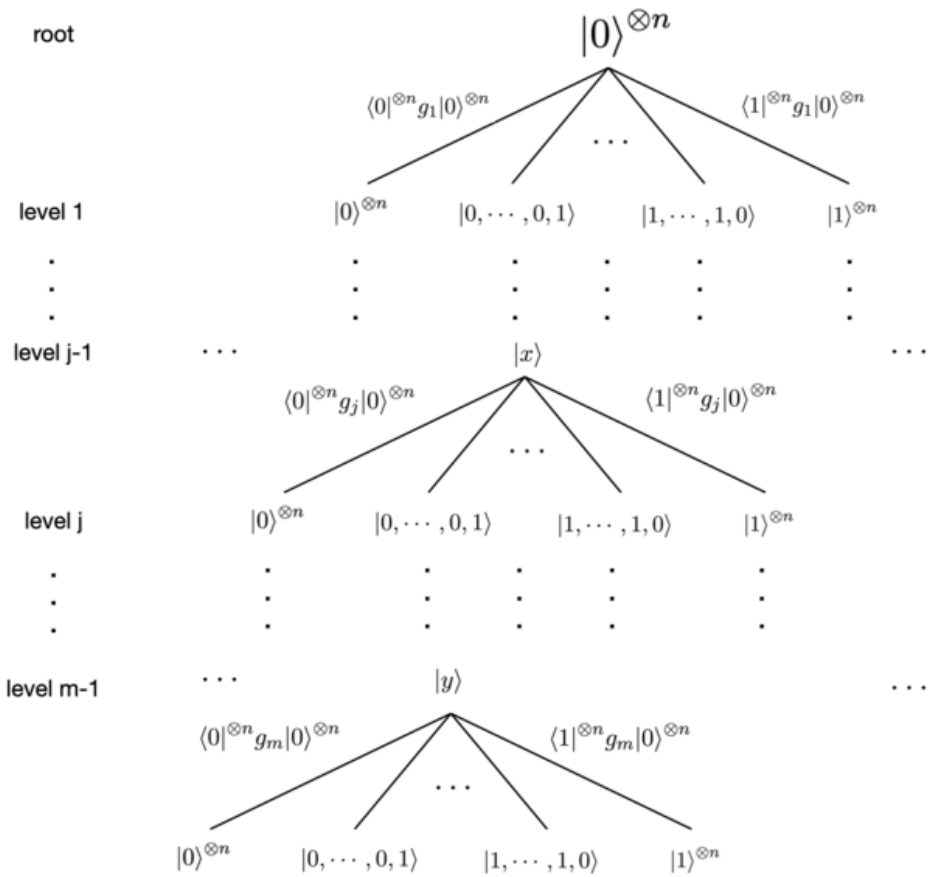
Suppose we have an algorithm $A$ that solves APPROX - QCIRCUIT - PROB. We can set parameters of $A$ as $\alpha = 2/3$ and $\beta = 1/3$, with circuit $C$. Now consider BQP. For any $L \in BQP$, there exists family of quantum circuits $\{\mathbf{Q}_n : n \in \mathbf{N}\}$. For each $|x\rangle$, we can construct a circuit $C_x$ such that $C_x |0\rangle^{\otimes n} = |x\rangle$. Then just combine two circuits to get $C' = C_x Q_n$, so $C' |0\rangle^{\otimes n} = Q_n |x\rangle$. This is BQP itself.

# BQP vs EXP

Since we have exponential power, given a quantum circuit $C$, we can use classical computer to simulate each gate in $C$ to get the final state.

Formally, let $C$ be a circuit given by APPROX - QCIRCUIT - PROB. Let $|\psi_0\rangle = |0\rangle^{\otimes n}$ and $|\psi_i\rangle$ be the state after $i$-th gate in t circuit is applied to $|\psi_{i-1}\rangle$. Each state can be represented in a classical computer as a unit vector in $\mathbf{C}^{2^n}$, where gate as a unit vector in $\mathbf{C}^{2^n \times 2^n}$. Hence final state can be computed in $O(m2^{2n})$ time.

# BQP vs PSPACE



# BQP vs NP

Contrary to intuition, it is believed that NPs will not be included in BQP. This is because quantum computers can implement superposition, but cannot compute all states at the same time as nondeterministic computer.

For example, consider Grover's algorithm. It is necessary to apply Grover's algorithm $O(\sqrt{2^n})$ times to find a desired one in a set of n-bit strings(this is called query - complexity).

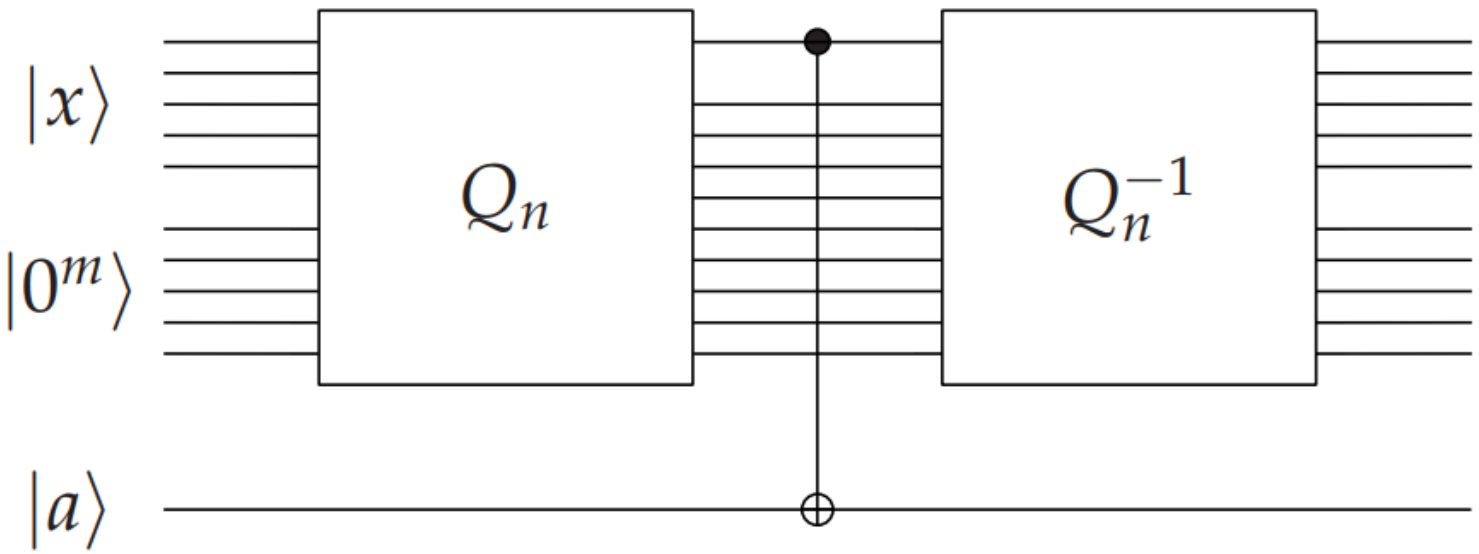
# BQP Error Reduction

## Error Reduction for BQP

Suppose that $a, b : \mathbf{N} \to [0, 1]$ are polynomial time computable functions and $p : \mathbf{N} \to \mathbf{N}$ is a polynomial bounded function such that $a(n) - b(n) \geq 1/p(n)$ for all but finitely many $n \in \mathbf{N}$. Then for every choice of a polynomial bounded function $q : \mathbf{N} \to \mathbf{N}$ satisfying $q(n) \geq 2$ for all but finitely many $n \in \mathbf{N}$, it holds that

$$BQP(a, b) = BQP = BQP(1 - 2^{-q}, 2^{-q}) \tag{1}$$

# BQP Subroutine Theorem



# BQP Subroutine Theorem

Suppose $A = (A_{yes}, A_{no})$ is a promise problem in BQP. Then for any choice of a polynomial bounded function $p$ there exists a polynomial bounded function $q$ and a polynomial time generated family of unitary quantum circuits $\{R_n : n \in \mathbf{N}\}$ with the following properties :

- Each circuit $R_n$ implements a unitary operation $U_n$ on $n + q(n) + 1$ qubits.
- For every $x \in A_{yes}$ and $a \in \Sigma$ it holds that

$$\langle x, 0^m, a \oplus 1 | \, U_n \, | x, 0^m, a \rangle \geq 1 - 2^{-p(n)} \tag{2}$$

- For every $x \in A_{no}$ and $a \in \Sigma$ it holds that

$$\langle x, 0^m, a | \, U_n \, | x, 0^m, a \rangle \geq 1 - 2^{-p(n)} \tag{3}$$

# GapP Function

## GapP Function

A function $f : \Sigma^* \to \mathbf{Z}$ is said to be GapP function if there exists a polynomial time nondeterministic Turing Machine $M$ such that $f(x) = \#M(x) - \#\bar{M}(x)$ for all $x \in \Sigma^*$.

GapP function is exactly the closure of #P under subtraction. Also, it has all the other closure properties of #P, such as addition, multiplication, binomial coefficients.

# GapP Function

## Fenner-Fortnow-Kurtz Theorem

Let $f$ be a GapP function and $q$ a polynomial. Then the following are GapP functions :

- $-f(x)$
- $\Sigma_{|y|\leq q(|x|)} f(\langle x, y\rangle)$
- $\Pi_{0\geq|y|\leq q(|x|)} f(\langle x, y\rangle)$

Also we can define or redefine some classes using GapP functions.

# GapP Function

## PP

A language $L$ is in $PP$ if and only if there exists a GapP function $f$ and for all $x \in \Sigma^*$, such that

- If $x \in L$, then $f(x) > 0$
- If $x \notin L$, then $f(x) < 0$

## AWPP

A language $L$ is in $PP$ if and only if there exists a GapP function $f$, polynomial time computable function $g$ such that for all $x \in \Sigma^*$ and $m \geq |x|$, $0 < f(x, 1^m) < g(1^m)$ and

- If $x \in L$, then $f(x, 1^m)) \geq (1 - 2^{-q(m)} g(1^m)$
- If $x \notin L$, then $f(x, 1^m)) \leq 2^{-q(m)} g(1^m)$

# GapP Function

## Acceptance Lemma of GapP Function

For any Quantum Turing Machine M runnig in time bounded by a polynomial $t(n)$, there is a GapP function $f$ such that for all inputs $x$,

$$Pr(M(x)accepts) = \frac{f(x)}{5^{2t(|x|)}} \tag{4}$$

Here, Quantum Turing Machine is not defined yet. You can intuitively think that Quantum Turing Machine is Deterministic Turing Machine with another tape, which allows us to use qubits.

# GapP Function

Proof of Lemma 3.2. We can assume that $M$ has at most $2^t$ configurations. Let $U$ be the transition matrix of $M$. By the discussion in Section 2.3 we can assume the entries of $U$ are of the form $w/5$ for $w$ an integer between $-5$ and 5. By the nature of a transition matrix, we can compute the $(i, j)$ entry of $U$ in time polynomial in $|x|$.

Let $V = 5U$ so $V$ has only integral entries. Let $\vec{\alpha}$ be the initial configuration amplitude vector as described in Section 2.3. Let $\vec{\beta} = V^t \cdot \vec{\alpha}$. Note that each $\beta_i$, a component of $\vec{\beta}$ corresponding to configuration $C_i$, is an exponential sum of a polynomial product of polynomial-time computable entries of $V$. By Theorem 2.2, we have that each $\beta_i$ is a **GapP** function.

Let $f(x)$ be $\beta_i^2$ where $C_i$ is the accepting configuration of $M(x)$. Again by Theorem 2.2 we have $f(x)$ is a **GapP** function. We have that $f(x, m)/5^{t(|x|)^2}$ is the acceptance probability of $M(x)$. ∎

# GapP Function

Proof of Theorem 3.1. Fix a language $L$ in **BQP** and a polynomial $q$. Let $M$ be a polynomial-time quantum Turing machine that on input $(x, 1^m)$ accepts for $x$ in $L$ with probability at least $1 - 2^{-q(m)}$ and accepts for $x$ not in $L$ with probability at most $2^{-q(m)}$.

Fix $x$ and $m$ with $m \geq |x|$. Then there is a polynomial $t(m)$ that bounds the running time of $M(x, 1^m)$. By Lemma 3.2 there is a **GapP** function $f$ such that $f(x, 1^m)/5^{2t(m)}$ is the acceptance probability of $M(x, 1^m)$. We can thus fulfill the requirements of Definition 2.5 by letting $g(1^m) = 5^{2t(m)}$. ∎

So, $BQP \subseteq AWPP$. Also it is known that $PP^{AWPP} = PP$, which means $AWPP$ is low for $PP$. Now we can conclude that $PP^{BQP} = PP$.

# GapP Function

**Theorem 3.3 (Li)** **AWPP** *is low for* **PP**, *i.e.*, $\mathbf{PP}^{\mathbf{AWPP}} = \mathbf{PP}$.

For completeness we sketch the proof of Theorem 3.3.

Proof Sketch. Suppose $L$ is in $\mathbf{PP}^A$ for some $A$ in **AWPP**. By Definition 2.3, there is some $h \in \mathbf{GapP}^A$ such that for $x \in L$, $h(x) \geq 1$ and $h(x) \leq -1$ otherwise. Let $M^A$ be a relativized nondeterministic polynomial-time Turing machine such that $h(x)$ is the difference of the number of accepting and rejecting computations of $M^A(x)$. We assume without loss of generality that for every $A$ and $x$ each computation path of $M^A(x)$ makes the same number of queries.

Pick a polynomial $q(n)$ such that for strings of length $n$, $M^A$ has less than $2^{q(n)/2}$ computation paths. Let $f$ and $g$ be **GapP** and polynomial-time computable functions defined for $A$ and $q$ as in Definition 2.5. Let $N$ be a nondeterministic polynomial-time Turing machine such that $f(x, 1^m)$ is the difference of the number of accepting and rejecting paths of $N(x, 1^m)$.

Create a new nondeterministic polynomial-time Turing machine $M'$ as follows. On input $x$, simulate $M^A(x)$. Every time $M$ makes a query $y$ to $A$, simulate $N(y, 1^{|x|})$. If $N$ accepts then continue the computation of $M$ assuming $y$ is in $A$. If $N$ rejects then continue the computation of $M$ assuming $y$ is not in $A$.

By the choice of $q$, the mistakes made by the wrong simulation, even totaled over every computation path of $M^A(x)$, are not enough to affect the sign of the difference of the number of accepting and rejecting paths of $M'$. ∎

# Known Bounds of BQP

There are several known bounds(or unbounds) of BQP. Here, $A$ means there exists an oracle for proposition.

- $BQP^A \neq BPP^A$
- $BQP^A \not\subseteq MA^A$
- $BQP^A \not\subseteq PH^A$
- $BQP^A \not\subseteq Mod_p^A$ for prime $p$
- $NP^A \not\subseteq BQP^A$
- $SZK^A \not\subseteq BQP^A$

Here we will see brief proof of last two relations.

# NP vs BQP

Let's take a quick look first. Starting with a uniform superposition

$$|\psi_0\rangle = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle \,. \tag{5}$$

It is easily seen that the separation after one query(with phase inversion of the term corresponding to the nonempty location) is maximized by a unitary evolution to

$$|\psi_1(y)\rangle = \frac{1}{\sqrt{2^n}} \sum_x (-1)^{\delta_{x,y}} |x\rangle = |\psi_0\rangle - \frac{2}{\sqrt{2^n}} |y\rangle \,. \tag{6}$$

You can see that the probability is a quadratic jump from 1 to 4, which can be generalized as $4k^2/2^n$.

# NP vs BQP

## Bad Simulation Accuracy Theorem

If two unit-length superpositions are within Euclidean distance $\epsilon$, then observing the two superpositions gives samples from distributions which are within total distance at most $4\epsilon$.

## Query Magnitude

Let $|\phi_i\rangle$ be the superposition of $M^A$ on input $x$ at time $i$. We denote by $q_y(|\phi_i\rangle)$ the sum of squared magnitudes in $|\phi_i\rangle$ of configurations of $M$ which are querying the oracle on string y. We refer to $q_y(|\phi_i\rangle)$ as the query magnitude of $y$ in $|\phi_i\rangle$

# NP vs BQP

## Superposition Accuracy Theorem

Let $|\phi_i\rangle$ be the superposition of $M^A$ on input $x$ at time $i$. Let $\epsilon > 0$, $F \subseteq [0, T-1] \times \Sigma^*$ be a set of time-strings pairs such that $\Sigma_{(i,y)\in F} q_y(|\phi_i\rangle) \leq \epsilon^2/T$. Now suppose the answer to each query $(i,j) \in F$ is modified to some arbitrary fixed $a_{i,y}$. Let $|\phi'_i\rangle$ be the time $i$ superposition of $M$ on input $x$ with oracle $A$ modified as stated above. Then $\| |\phi_T\rangle - |\phi'_T\rangle \| \leq \epsilon$.

# NP vs BQP

**Proof.** Let $U$ be the unitary time evolution operator of $M^A$. Let $A_i$ denote an oracle such that if $(i, y) \in F$ then $A_i(y) = a_{i,y}$ and if $(i, y) \notin F$ then $A_i(y) = A(y)$. Let $U_i$ be the unitary time evolution operator of $M^{A_i}$. Let $|\phi_i\rangle$ be the superposition of $M^A$ on input $x$ at time $i$. We define $|E_i\rangle$ to be the error in the $i^{th}$ step caused by replacing the oracle $A$ with $A_i$. Then

$$|E_i\rangle = U_i|\phi_i\rangle - U|\phi_i\rangle.$$

So we have

$$|\phi_T\rangle = U|\phi_{T-1}\rangle = U_T|\phi_{T-1}\rangle - |E_{T-1}\rangle = \cdots = U_T \cdots U_1|\phi_0\rangle - \sum_{i=0}^{T-1} U_{T-1} \cdots U_i|E_i\rangle.$$

Since all of the $U_i$ are unitary, $|U_{T-1} \cdots U_i|E_i\rangle| = ||E_i\rangle|$.

The sum of squared magnitudes of all of the $E_i$ is equal to $\sum_{(i,y)\in F} q_y(|\phi_i\rangle)$ and therefore at most $\frac{\varepsilon^2}{T^2}$. In the worst case, the $U_{T-1} \cdots U_i|E_i\rangle$s could interfere constructively; however, the squared magnitude of their sum is at most $T$ times the sum of their squared magnitudes, i.e. $\varepsilon^2$. Therefore $||\phi_T\rangle - |\phi'_T\rangle| \leq \varepsilon$. □

# NP vs BQP

**Corollary 3.4** *Let $A$ be an oracle over alphabet $\Sigma$. For $y \in \Sigma^*$, let $A_y$ be any oracle such that $\forall x \neq y\ A_y(x) = A(x)$. Let $|\phi_i\rangle$ be the time $i$ superposition of $M^A$ on input $x$ and $|\phi_i\rangle^{(y)}$ be the time $i$ superposition of $M^{A_y}$ on input $x$. Then for every $\varepsilon > 0$, there is a set $S$ of cardinality at most $\frac{2T^2}{\varepsilon^2}$ such that $\forall y \notin S\ \left||\phi_T\rangle - |\phi_T\rangle^{(y)}\right| \leq \varepsilon$.*

**Proof.** Since each $|\phi_t\rangle$ has unit length, $\sum_{i=0}^{T-1}\sum_y q_y(|\phi_i\rangle) \leq T$. Let $S$ be the set of strings $y$ such that $\sum_{i=0}^{T-1} q_y(|\phi_i\rangle) \geq \frac{\varepsilon^2}{2T}$. Clearly $\text{card}(S) \leq \frac{2T^2}{\varepsilon^2}$.

If $y \notin S$ then $\sum_{i=0}^{T-1} q_y(|\phi_i\rangle) < \frac{\varepsilon^2}{2T}$. Therefore by Theorem 3.3 $\forall y \notin S\ \left||\phi_i\rangle - |\phi_i\rangle^{(y)}\right| \leq \varepsilon$. □

# NP vs BQP

## NP vs BQP

For any $T(n)$ which is $o(2^{n/2})$, relative to a random oracle, with probability 1, $BQPTime(T(n))$ does not contain $NP$.

# NP vs BQP

Let us fix an arbitrary length-preserving function from strings of lengths other than $n$ over alphabet $\Sigma$. Let $\mathcal{C}$ denote the set of oracles consistent with this arbitrary function. Let $\mathcal{A}$ be the set of oracles in $\mathcal{C}$ such that $1^n$ has no inverse (does not belong to $\mathcal{L}_A$). If the oracle answers to length $n$ strings are chosen uniformly at random, then the probability that the oracle is in $\mathcal{A}$ is at least $1/4$. This is because the probability that $1^n$ has no inverse is $(\frac{2^n-1}{2^n})^{2^n}$ which is at least $1/4$ (for $n$ sufficiently large). Let $\mathcal{B}$ be the set of oracles in $\mathcal{C}$ such that $1^n$ has a unique inverse. As above, the probability that a randomly chosen oracle is in $\mathcal{B}$ is $(\frac{2^n-1}{2^n})^{2^n-1}$ which is at least $1/e$.

Given an oracle $A$ in $\mathcal{A}$, we can modify its answer on any single input, say $y$, to $1^n$ and therefore get an oracle $A_y$ in $\mathcal{B}$. We will show that for most choices of $y$, the acceptance probability of $M^A$ on input $1^n$ is almost equal to the acceptance probability of $M^{A_y}$ on input $1^n$. On the other hand, $M^A$ must reject $1^n$ and $M^{A_y}$ must accept $1^n$. Therefore $M$ cannot accept both $\mathcal{L}_A$ and $\mathcal{L}_{A_y}$. By working through the details more carefully, it is easy to show that $M$ fails on input $1^n$ with probability at least $1/8$ when the oracle is a uniformly random function on strings of length $n$, and is an arbitrary function on all other strings.

# NP vs BQP

Let $A_y$ be the oracle such that $A_y(y) = 1^n$ and $\forall z \neq y\ A_y(z) = A(z)$. By Corollary 3.4 there is a set $S$ of at most $338T^2(n)$ strings such that the difference between the $i^{th}$ superposition of $M^{A_y}$ on input $1^n$ and $M^A$ on input $1^n$ has norm at most $1/13$. Using Theorem 3.1 we can conclude that the difference between the acceptance probabilities of $M^{A_y}$ on input $1^n$ and $M^A$ on input $1^n$ is at most $1/13 \times 4 < 1/3$. Since $M^{A_y}$ should accept $1^n$ with probability at least $2/3$ and $M^A$ should reject $1^n$ with probability at least $2/3$, we can conclude that $M$ fails to accept either $\mathcal{L}_A$ or $\mathcal{L}_{A_y}$.

So, each oracle $A \in \mathcal{A}$ for which $M$ correctly decides whether $1^n \in \mathcal{L}_A$ can, by changing a single answer of $A$ to $1^n$, be mapped to at least $(2^n - \text{card}(S)) \geq 2^{n-1}$ different oracles $A_f \in \mathcal{B}$ for which $M$ fails to correctly decide whether $1^n \in \mathcal{L}_{A_f}$. Moreover, any particular $A_f \in \mathcal{B}$ is the image under this mapping of at most $2^n - 1$ oracles $A \in \mathcal{A}$, since where it now answers $1^n$, it must have given one of the $2^n - 1$ other possible answers. Therefore, the number of oracles in $\mathcal{B}$ for which $M$ fails must be at least $1/2$ the number of oracles in $\mathcal{A}$ for which $M$ succeeds. So, calling $a$ the number of oracles in $\mathcal{A}$ for which $M$ fails, $M$ must

Theorem 3.1 means Bad Simulation Accuracy Theorem.

# NP vs BQP

fail for at least $a + 1/2(\text{card}(\mathcal{A}) - a)$ oracles. Therefore $M$ fails to correctly decide whether $1^n \in \mathcal{L}_A$ with probability at least $(1/2)P[\mathcal{A}] \geq 1/8$.

It is easy to conclude that $M$ decides membership in $\mathcal{L}_A$ with probability 0 for a uniformly chosen oracle $A$. □

# BQP vs SZK

## Quantum Collision Lower Bound

To decide whether a function $X : \{1, \cdots, n\} \to \{1, \cdots, n\}$ is one-to-one or two-to-one, lower bound of $\Omega(n^{1/5})$ on the number of queries needed by a quantum computer to solve this problem.

# BQP vs SZK

However, proof of $SZK^A \not\subseteq BQP^A$ does not need collision lower bound theorem. For suppose that a verifier $V$ and prover $P$ both have oracle access to a sequence $X = x_1 \cdots x_{2^n}$, which is either one-to-one or two-to-one. To verify with zero knowledge that $X$ is one-to-one, $V$ can repeatedly choose an $i \in_R \{1, \cdots, 2^n\}$ and send $x_i$ to $P$, whereupon $P$ must send $i$ back to $V$. Thus, using standard diagonalization trick, we can produce an oracle $A$.

# BQP vs NIPZK

**Theorem 3.1.** *There exists an oracle $A$ such that* $\mathrm{NIPZK}^A \not\subseteq \mathrm{BQP}^A$.

It suffices to demonstrate a NIPZK algorithm for $\mathrm{Col}_n^2$. The algorithm, inspired by the algorithm for uniformity testing given by Malka [7], proceeds as follows. The prover divides the shared random string into two strings $r_1$ and $r_2$, each of length $n$. For each $r_i$, it chooses uniformly a string $x_i$ with $X(x_i) = r_i$. It then sends the chosen $x_i$ to the verifier. The verifier accepts if $X(x_i) = r_i$ for both $i$.

We now prove the algorithm is NIPZK. First, we prove its completeness. If $X$ is one-to-one, then its image equals its codomain, and so the $x_i$ can always be selected to be valid, regardless of the $r_i$. Thus the verifier will always accept any one-to-one function.

Next, we prove its soundness. If $X$ is two-to-one, then half of its codomain is not in its image. Thus, with probability $\frac{3}{4}$, at least one of $r_1$ or $r_2$ is not in the image of $X$. Thus, with probability $\frac{3}{4}$, the prover cannot select $x_i$ that the verifier will accept. Thus the soundness error is $\frac{1}{4}$.

Next, we prove its perfect zero-knowledge property. The simulator can simply randomly pick two inputs $x_1$ and $x_2$, then run them through $X$ to get appropriate $r_i$. Since the $x_i$ are selected uniformly, when $X$ is one-to-one the $r_i$ are also uniformly distributed. Furthermore, for those $r_i$, there is only one possible pair of $x_i$; thus the simulator can exactly recreate the distribution over inputs to the verifier. From there, it can simply perfectly simulate any verifier on those inputs.

Thus $\mathrm{Col}_n^2 \in \mathrm{NIPZK}$, and the theorem follows as above.

# Overview

# Definition of QMA

Note that QMA is not a quantum analogue of MA, but a quantum analogue of NP.

## Definition of QMA

Let $A = (A_{yes}, A_{no})$ be a promise problem and let $p$ be a polynomial bounded function, $a, b : \mathbf{N} \to [0, 1]$ be functions. Then $A \in QMA_p(a, b)$ if and only if there exists a polynomial-time generated family of quantum circuits $\mathbf{Q} = \{\mathbf{Q}_n : n \in \mathbf{N}\}$, where each circuit $\mathbf{Q}_n$ takes $n + p(n)$ input qubits and produces one output qubit, that satisfies the following properties.

- Completeness : For all $x \in A_{yes}$ there exists a $p(|x|)$-qubit quantum state $\rho$ such that $Pr(Q \text{ accepts } (x, \rho) \geq a(|x|)$.
- Soundness : For all $x \in A_{no}$ and all $p(|x|)$-qubit quantum state $\rho$ it holds that $Pr(Q \text{ accepts } (x, \rho) \leq b(|x|)$.

Also, the class QMA defined as $QMA = U_p QMA_p(\frac{2}{3}, \frac{1}{3})$

# Recall : NP

A language $L$ is in $NP$ if and only if there exists a deterministic Turing Machine $M$, polynomials $p$ and $q$, such that

- For all $x$ and $y$, $M$ runs in time $p(|x|)$ on input $(x, y)$
- For all $x$ in $L$, there exists a string $y$ of length $q(|x|)$ such that $M(x, y) = 1$
- For all $X$ not in $L$ and all strings $y$ of length $q(|x|)$, $M(x, y) = 0$

# The Local Hamiltonian Problem

A k-local Hamiltonian $H$ is a Hermitian matrix acting on $n$ qubits which can represented as the sum of $m$ Hamiltonian terms acting upon at most $k$ qubits each.

$$H = \sum_{i=1}^{m} H_i \tag{7}$$

The general k-local Hamiltonian problem is, given a k-local Hamiltonian $H$, to find the smallest eigenvalue $\lambda$ of $H$. This problem can be converted into decision version(promise problem) by defining $\alpha, \beta$ for $\lambda \leq \beta$ or if $\lambda \geq \alpha$.

# The Local Hamiltonian Problem

k-local Hamiltonian problem has following known properties :

- QMA-complete when $k = O(logn)$
- QMA-complete when $k = 3$ and norm of $H_i$ is $O(1)$, which means constant norms
- QMA-complete when 2-local on a 2-D Lattice

# Classical : SAT problem

A propositional logic formula, also called Boolean expression, is built from variables, operators AND (conjunction, also denoted by $\wedge$), OR (disjunction, $\vee$), NOT (negation, $\neg$), and parentheses. A formula is said to be satisfiable if it can be made TRUE by assigning appropriate logical values (i.e. TRUE, FALSE) to its variables. The Boolean satisfiability problem (SAT) is, given a formula, to check whether it is satisfiable.

# QUANTUM CIRCUIT-SAT

Problem: Given a quantum circuit $V$ on $n$ witness qubits and $m = \text{poly}(n)$ ancilla qubits, determine whether:

(yes case) $\exists$ $n$-qubit state $|\psi\rangle$ such that $V(|\psi\rangle|0\ldots0\rangle)$ accepts with probability $\geqslant b$, i.e. outputs a state with $|1\rangle$ on the first qubit with amplitude-squared $\geqslant b$

(no case) $\forall$ $n$-qubit state $|\psi\rangle$, $V(|\psi\rangle|0\ldots0\rangle)$ accepts with probability $\leqslant a$,

promised one of these to be the case,
where $b - a \geqslant 1/\text{poly}(n)$ and $|0\ldots0\rangle$ is the all-zero $m$-qubit ancilla state.

Note : QMA-complete

# QUANTUM NON-IDENTITY CHECK

Problem: Given a unitary $U$ implemented by a quantum circuit on $n$ qubits, determine whether $U$ is *not* close to a trivial unitary (the identity times a phase), i.e.,
determine whether:

(yes case) $\forall \phi \in [0, 2\pi), \left\| U - e^{i\phi} \mathbb{1} \right\| \geqslant b$

(no case) $\exists \phi \in [0, 2\pi)$ such that $\left\| U - e^{i\phi} \mathbb{1} \right\| \leqslant a$,

promised one of these to be the case,
where $b - a \geqslant 1/\mathrm{poly}(n)$.

Note : QMA-complete, even for small-depth quantum circuits. Have reduction to QCSAT.

# DETECTING INSECURE QUANTUM ENCRYPTION

**Definition 2.3** ($\epsilon$-private channel)**.** *Suppose $E$ is a channel taking as input an integer $k \in \{1, \ldots, K\}$ and quantum state in space $\mathcal{H}_1$, and producing a quantum output in space $\mathcal{H}_2$, with dim $\mathcal{H}_1 \leqslant$ dim $\mathcal{H}_2$. Let $E_k$ be the quantum channel where the integer input is fixed as $k$. Let $\Omega$ be the completely depolarizing channel that maps all density matrices to the maximally mixed state. $E$ is an $\epsilon$-private channel if $\| \frac{1}{K} \sum_k E_k - \Omega \|_\diamond \leqslant \epsilon$ (so if the key $k$ is not known, the output of $E$ gives almost no information about the input) and there is a polysize decryption channel $D$ (operating on the same space as $E$) such that $\forall k, \| D_k \circ E_k - \mathbb{1} \|_\diamond \leqslant \epsilon$ (i.e. if $k$ is known, the output can be reversed to obtain the input).*

# DETECTING INSECURE QUANTUM ENCRYPTION

Problem: Let $\delta \in (0, 1]$. Given circuit $E$, which upon input $k$ implements channel $E_k$ acting from space $\mathcal{H}_1$ to $\mathcal{H}_2$ (with $\dim \mathcal{H}_1 \leqslant \dim \mathcal{H}_2$),
determine whether:

(yes case) $\exists$ subspace $S$, with $\dim S \geqslant (\dim \mathcal{H}_1)^{1-\delta}$, such that for any $k$ and any reference space $\mathcal{R}$, if $\rho$ is a density matrix on $S \otimes \mathcal{R}$ then $\|(E_k \otimes \mathbb{1}_R)(\rho) - \rho\|_{tr} \leqslant \epsilon$

(no case) $E$ is an $\epsilon$-private channel,

promised one of these to be the case,
where $1 > \epsilon \geqslant 2^{-\text{poly}}$.

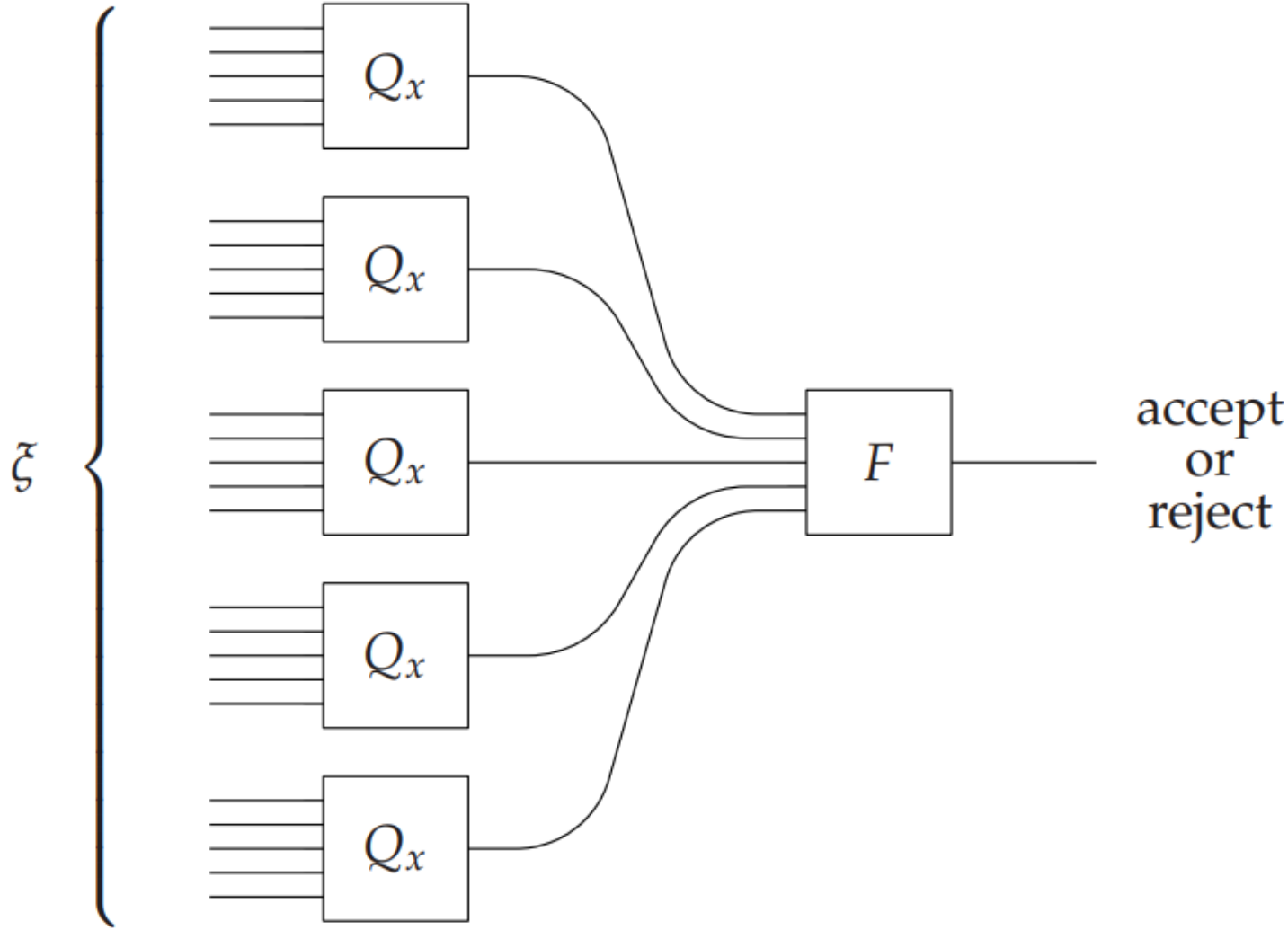
Note : QMA-complete for $0 < \epsilon < 1/8$

# GROUP NON-MEMBERSHIP PROBLEM

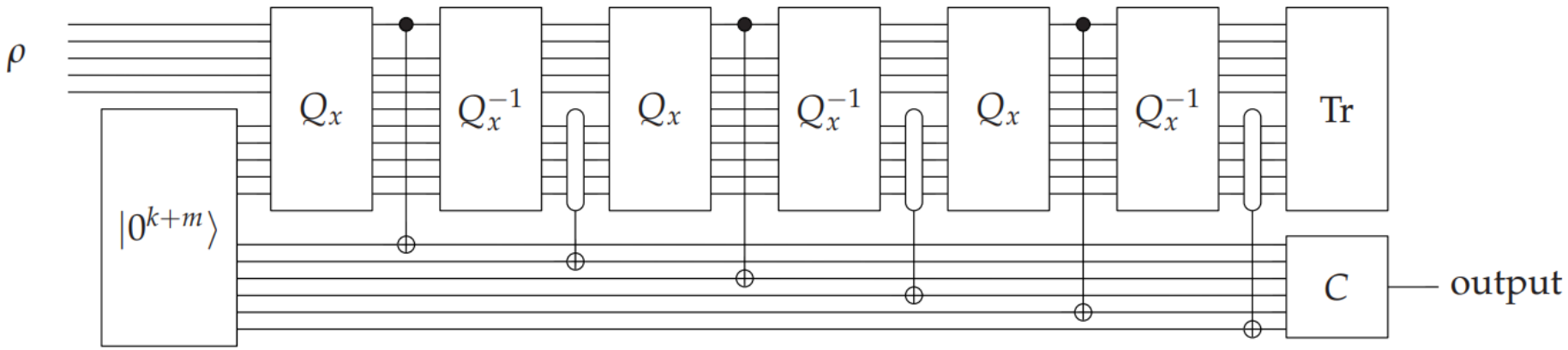
Group elements $h_1, \cdots, h_k$ and $g$ from some finite group $G$. Let $H = \langle h_1, \cdots, h_k \rangle$ be the subgroup generated by $h_1, \cdots, h_k$. Yes instance means $g \notin H$, No instance means $g \in H$.

This problem has several very interesting properties. First, it is expected that this problem is not QMA-Complete. This is uncommon for vascuous(where every answer resolves to yes or no) promise problems. Second, it is also known that this problem not expected to belong to NP.

# Weak Error Reduction Procedure



# Strong Error Reduction Procedure



# Error Reduction of QMA

## Error Reduction of QMA

Suppose that $a, b : \mathbf{N} \to [0, 1]$ are polynomial time computable functions and $q : \mathbf{N} \to \mathbf{N}$ is a polynomial bounded function such that $a(n) - b(n) \geq 1/q(n)$ for all but finitely many $n \in \mathbf{N}$. Then for every choice of polynomial bounded functions $p, r : \mathbf{N} \to \mathbf{N}$ such that $r(n) \geq 2$ for all but finitely many n, it holds that

$$QMA_p(a, b) = QMA_p(1 - 2^{-r}, 2^{-r}) \tag{8}$$

# Containment of QMA in PP

By means of strong error reduction of QMA, it can be proved that QMA is contained in PP as follows. Suppose that some promise problem $A = (A_{yes}, A_{no})$ is contained in QMA. Then QMA Error Reduction, it holds that

$$A \in QMA_p(1 - 2^{-(p+2)}, 2^{-(p+2)}) \tag{9}$$

for some polynomial bounded function $p$. Now consider an algorithm that does not receive any quantum proof, but instead just randomly guesses a quantum proof on $p$ qubits and feeds this proof into a verification procedure having completeness and soundness probabilities consistent with above inclusion. This algorithm accepts every string $x \in A_{yes}$ with probability at least $2^{-(p(|x|)+1)}$ and accepts every string $x \in A_{no}$ with probability at most $2^{-(p(|x|)+2)}$

# Containment of QMA in PP

This algorithm accepts every string $x \in A_{yes}$ with probability at least $2^{-(p(|x|)+1)}$ and accepts every string $x \in A_{no}$ with probability at most $2^{-(p(|x|)+2)}$. Both of these probabilities are exponentially small, but the separation between them is enough to establish that $A \in PP$.

# QCMA : Quantum Analogue of MA

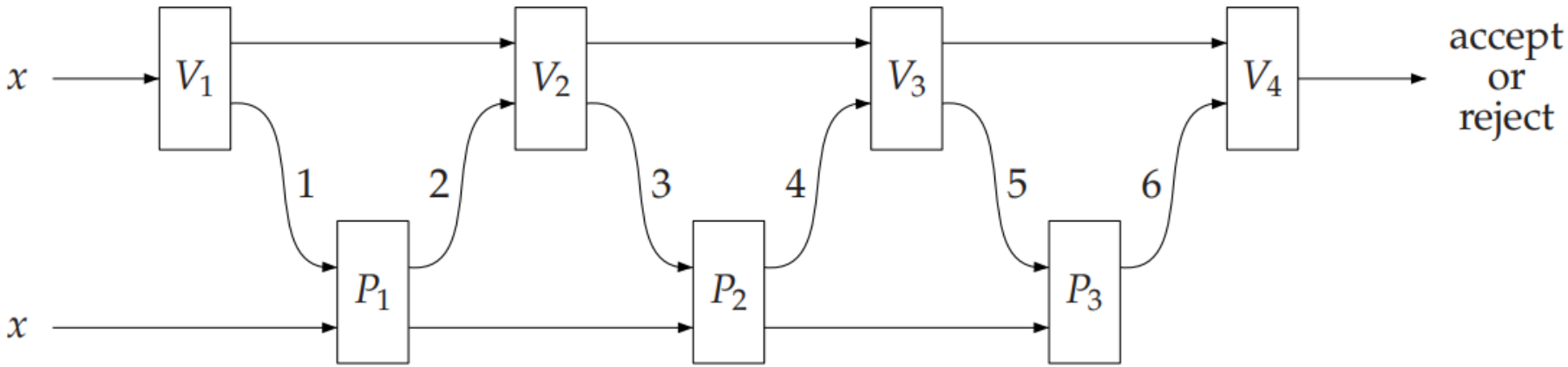
## Definition of QCMA

Let $A = (A_{yes}, A_{no})$ be a promise problem and let $p$ be a polynomial bounded function. Then $A \in QCMA$ if and only if there exists a polynomial-time generated family of quantum circuits $\mathbf{Q} = \{\mathbf{Q}_n : n \in \mathbf{N}\}$, where each circuit $\mathbf{Q}_n$ takes $n + p(n)$ input qubits and produces one output qubit, that satisfies the following properties.

- Completeness : For all $x \in A_{yes}$ there exists a string $y \in \Sigma^{p(|x|)}$ such that $Pr(Q \text{ accepts } (x, y) \geq 2/3$.
- Soundness : For all $x \in A_{no}$ and all strings $y \in \Sigma^{p(|x|)}$ it holds that $Pr(Q \text{ accepts } (x, y) \leq 1/3$.

# Overview

# Quantum Interactive Proof System



# Quantum Interactive Proof System

The Quantum Verifier can be described by a polynomial time generated family of quantum circuits, for some polynomial bounded function $p$.

$$V = \{V_j^n : n \in \mathbf{N}, j \in \{1, \cdots, p(n)\}\} \tag{10}$$

The inputs and outputs of verifier's circuits are divided into two categories; private memory qubits and message qubits. The memory qubits are retained by the verifier, while the message qubits are sent to, or received from, the prover. In similar way, prover can be defined as family of arbitrary quantum operations interface with a given verifier.

$$P = \{P_j^n : n \in \mathbf{N}, j \in \{1, \cdots, q(n)\}\} \tag{11}$$

Note that there is no computational limit for prover.

# Quantum Interactive Proof System

## QIP

Let $A = (A_{yes}, A_{no})$ be a promise problem, let $m$ be a polynomial bounded function, and let $a, b : \mathbf{N} \to [0, 1]$ be polynomial time computable functions. Then $A \in QIP(m, a, b)$ if and only if there exists an $m$-message quantum verifier $V$ with the following properties :

- Completeness : For all $x \in A_{yes}$, there exists a quantum prover $P$ that causes $V$ to accept $x$ with probability at least $a(|x|)$.
- Soundness : For all $x \in A_{no}$, every quantum prover $P$ causes $V$ to accept $x$ with probability at most $b(|x|)$.

Also define $QIP(m) = QIP(m, 2/3, 1/3)$ for each polynomial bounded function $m$ and define $QIP = \cup_m QIP(m)$, where the union is over all polynomial bounded functions $m$.

# Known Properties of QIP

- $PSPACE \subseteq QIP$ follows directly from $IP = PSPACE$. Early 2010s, it also discovered that $QIP \subseteq PSPACE$, so $PSPACE = QIP$.
- $QIP \subseteq EXP$.
- $QIP(0) = BQP$
- $QIP(1) = QMA$.
- $QIP(k) = QIP$ for all $k \in \mathbf{N}, k > 0$.
- $QSZK \subseteq QIP$.

# QIP Reduction

## QIP Reduction

Let $a, b : \mathbf{N} \to [0, 1]$ be polynomial time computable functions and $p$ be a polynomial bounded function such that $a(n) - b(n) \geq 1/p(n)$ for all but finitely many $n \in \mathbf{N}$. Also let $m$ and $r$ be polynomial bounded functions. Then

$$QIP(m, a, b) \subseteq QIP(3, 1, 2^{-r}). \tag{12}$$

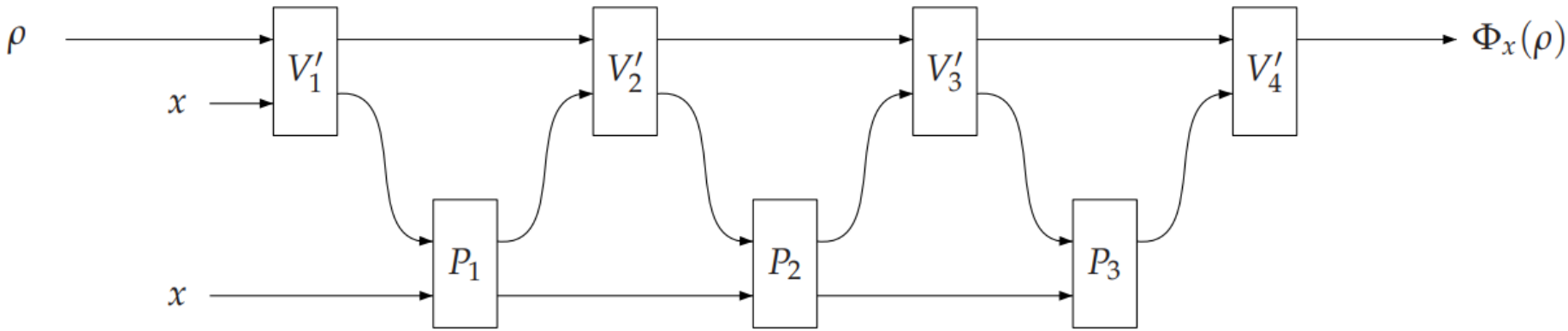
# THE QUANTUM CIRCUIT DISTINGUISHABILITY PROBLEM

The problem that determine whether the operations induced by two quantum circuits are significantly different, or approximately same, defined as below, is QIP-complete problem.

- Input : Quantum circuits $Q_0$ and $Q_1$, both taking $n$ input qubits and producing $m$ output qubits.
- Yes : $\delta(Q_0, Q_1) \geq 2/3$.
- No : $\delta(Q_0, Q_1) \leq 1/3$.

Here, a norm $\delta$ is a diamond norm commonly used to measure the distance between two quantum operations. We've already seen it before in Universality Theorem.

# Quantum Statistically Zero Knowledge



# Quantum Statistically Zero Knowledge

The proof system $(V, P)$ is said to be quantum statistical zero knowledge if, for any choice of a polynomial time non-honest verifier $V'$, there exists a polynomial time generated family $\{Q_x : x \in \Sigma^*\}$ of quantum circuits for which $\delta(\Phi_x, Q_x)$ is negligible(which means, statistically ignorable) for every $x]in A_{yes}$.

Also, A promise problem $A = (A_{yes}, A_{no})$ is in QSZK if and only if it has a statistical zero knowledge proof system.

# Quantum Statistically Zero Knowledge

QSZK related with some other complexity classes as follows :

- Statistical zero knowledge quantum interactive proof systems can be parallelized to two messages. It follows that $QSZK \subseteq QIP(2)$.
- QSZK is closed under complementation.
- $QSZK \subseteq PSPACE$.

It is also known that THE QUANTUM STATE DISTINGUISHABILITY PROBLEM and quantum analogue of ENTROPY DIFFERENCE PROBLEM is QSZK-complete.

# THE QUANTUM STATE DISTINGUISHABILITY PROBLEM

- Input : Quantum circuits $Q_0$ and $Q_1$, both taking no input qubits and producing $m$ output qubits. Let $\rho_0$ and $\rho_1$ be the density matrices corresponding to the outputs of these circuits.
- Yes : $\delta(\rho_0, \rho_1) \geq 2/3$.
- No : $\delta(\rho_0, \rho_1) \leq 1/3$.

Note : This problem is QSZK-complete.

# Multiple Proof

### $MIP^*$

A promise problem $A = (A_{yes}, A_{no})$ is in $MIP^*$ if and only if there exists a multiple prover interactive proof system for $A$ wherein the verifier is classical and the provers may share an arbitrary entangled stated.

### QMIP

A promise problem $A = (A_{yes}, A_{no})$ is in QMIP if and only if ther exists a multi prover quantum interactive system for $A$.

# Multiple Proof

For quantum states, general question can be raised; really multi proof system is better than single proof system? For example, in the case of two quantum proofs versus one, consider the following Arthur's simulation of two quantum proofs by a single quantum proof:

- Given a single quantum proof that is expected to be a tensor product of two pure quantum states, Arthur first runs some preprocessing to rule out any quantum proof far from states of a tensor product of two pure quantum states, and then performs the verification procedure of original two-proof system.

# Multiple Proof

Problem here is that: Is there any physical method - POVM(positive operator-valued measure) measurement - that determines whether a given unknown state is in a tensor product form or even maximally entangled?

## POVM

A positive operator-valued measure(POVM) on a Hilbert space **H** is defined to be a set $\mathbf{M} = \{M_1, \cdots, M_k\}$ of nonnegative Hermitian operators over **H** such that $\sum_{i=1}^{k} M_i = I_{\mathbf{H}}$.

To clarify this, let's consider the **fidelity** between two density operators $\rho$ and $\sigma$ in set of density operators over **H** which is defined by $F(\rho, \sigma) = tr\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}$.

# Multiple Proof

## No Efficient POVM Theorem

Suppose that one of the following two is true for a given proof $|\psi\rangle \in \mathbf{H}^{\otimes 2}$ of $2n$ qubits :

- $|\psi\rangle\langle\psi|$ is in $H_0 = \{|\psi_0\rangle\langle\psi_0| : |\psi_0\rangle \in \mathbf{H}^{\otimes 2}, \exists\, |a\rangle, |b\rangle \in \mathbf{H}, |\psi_0\rangle = |a\rangle \otimes |b\rangle\}$
- $|\psi\rangle\langle\psi|$ is in $H_1 = \{|\psi_1\rangle\langle\psi_1| : |\psi_1\rangle \in \mathbf{H}^{\otimes 2}$ is maximally entangled $\}$

Then, in determining which statement is true, no POVM measurement is better than the trivial strategy in which one guesses at random without any operation at all.

# Multiple Proof

*Proof.* Let $\boldsymbol{M} = \{M_0, M_1\}$ be a POVM on $\mathcal{H}^{\otimes 2}$. With $\boldsymbol{M}$ we conclude $|\Psi\rangle\langle\Psi| \in \mathsf{H}_i$ if $\boldsymbol{M}$ results in $i$, $i \in \{0,1\}$. Let $\mathrm{P}^{\boldsymbol{M}}_{i\to j}(|\Psi\rangle\langle\Psi|)$ denote the probability that $|\Psi\rangle\langle\Psi| \in \mathsf{H}_j$ is concluded by $\boldsymbol{M}$ while $|\Psi\rangle\langle\Psi| \in \mathsf{H}_i$ is true. We want to find the measurement that minimizes $\mathrm{P}^{\boldsymbol{M}}_{0\to 1}(|\Psi\rangle\langle\Psi|)$ keeping the other side of error small enough. More precisely, we consider $\mathcal{E}$ defined and bounded as follows.

$$
\begin{aligned}
\mathcal{E} &\stackrel{\text{def}}{=} \min_{\boldsymbol{M}} \left\{ \max_{\rho\in\mathsf{H}_0} \mathrm{P}^{\boldsymbol{M}}_{0\to 1}(\rho) \colon \max_{\rho\in\mathsf{H}_1} \mathrm{P}^{\boldsymbol{M}}_{1\to 0}(\rho) \le \delta \right\} \\
&\ge \min_{\boldsymbol{M}} \left\{ \int_{\rho\in\mathsf{H}_0} \mathrm{P}^{\boldsymbol{M}}_{0\to 1}(\rho)\mu_0(\mathrm{d}\rho) \colon \int_{\rho\in\mathsf{H}_1} \mathrm{P}^{\boldsymbol{M}}_{1\to 0}(\rho)\mu_1(\mathrm{d}\rho) \le \delta \right\} \\
&= \min_{\boldsymbol{M}} \left\{ \mathrm{P}^{\boldsymbol{M}}_{0\to 1}\left( \int_{\rho\in\mathsf{H}_0} \rho\mu_0(\mathrm{d}\rho) \right) \colon \mathrm{P}^{\boldsymbol{M}}_{1\to 0}\left( \int_{\rho\in\mathsf{H}_1} \rho\mu_1(\mathrm{d}\rho) \right) \le \delta \right\},
\end{aligned}
$$

where each $\mu_i$ is an arbitrary probability measure in $\mathsf{H}_i$. It follows that $\mathcal{E}$ is larger than the error probability in distinguishing $\int_{\rho\in\mathsf{H}_0} \rho\mu_0(\mathrm{d}\rho)$ from $\int_{\rho\in\mathsf{H}_1} \rho\mu_1(\mathrm{d}\rho)$.

# Multiple Proof

Take $\mu_0$ as a uniform distribution over the set $\{|e_i\rangle\langle e_i| \otimes |e_j\rangle\langle e_j|\}_{1\le i,j\le d}$, that is, $\mu_0(|e_i\rangle\langle e_i| \otimes |e_j\rangle\langle e_j|) = \frac{1}{d^2}$ for each $i$ and $j$, where $\{|e_i\rangle\}$ is an orthonormal basis of $\mathcal{H}$, and take $\mu_1$ as a uniform distribution over the set $\{|g_{k,l}\rangle\langle g_{k,l}|\}_{1\le k,l\le d}$, that is, $\mu_1(|g_{k,l}\rangle\langle g_{k,l}|) = \frac{1}{d^2}$ for each $k$ and $l$, where

$$|g_{k,l}\rangle = \frac{1}{d}\sum_{j=1}^{d}\left(e^{2\pi\sqrt{-1}\frac{jk}{d}}|e_j\rangle \otimes |e_{(j+l) \bmod d}\rangle\right).$$

This $\{|g_{k,l}\rangle\}$ forms an orthonormal basis of $\mathcal{H}^{\otimes 2}$ [15], and thus

$$\int_{\rho\in\mathsf{H}_0} \rho\mu_0(\mathrm{d}\rho) = \int_{\rho\in\mathsf{H}_1} \rho\mu_1(\mathrm{d}\rho) = \frac{1}{d^2} I_{\mathcal{H}^{\otimes 2}}.$$

Hence we have the assertion. □

# Multiple Proof

## k-QMA Theorem

$QMA(k, c, s) = QMA(2, 2/3, 1/3)$ for any polynomial bounded function $k : \mathbf{Z} \to \mathbf{N}$ satisfying $k \geq 2$ and any two sided bounded error probability $(c, s)$ if and only if $QMA(2, c, s)$ coincides with $QMA(2, 2/3, 1/3)$.