Quantum Proofs

John Watrous

School of Compupter Science
and
Institute for Quantum Computing

University of Waterloo

August 10, 2006

Promise problems

A **promise problem** is a computational problem where two disjoint sets of inputs (*yes* inputs and *no* inputs) must be distinguished.

The GRAPH ISOMORPHISM problem will serve as a helpful example:

GRAPH ISOMORPHISM

Input:	Two simple, undirected graphs G_0 and G_1.
Yes:	G_0 and G_1 are isomorphic ($G_0 \cong G_1$).
No:	G_0 and G_1 are not isomorphic ($G_0 \ncong G_1$).

There may be “don’t care” inputs: we do not require every input to be either a yes or a no input.

Some basic complexity classes

Computational complexity theory studies classes of promise problems, often defined by resource constraints.

P The class of promise problems solvable in **polynomial time** on a deterministic Turing machine.

BPP The class of promise problems solvable in **polynomial time** on a **bounded error** probabilistic Turing machine (correct on every input with probability at least 99/100).

PP The class of promise problems solvable in **polynomial time** on an **unbounded error** probabilistic Turing machine (correct on every input with probability greater than 1/2).

PSPACE The class of promise problems solvable in **polynomial space** on a deterministic Turing machine.

EXP The class of promise problems solvable in **exponential time** on a deterministic Turing machine.

The class NP

A promise problem A is in the class NP if and only if there exists:

- a polynomial p (which specifies the *proof length*)
- a polynomial-time *verification procedure* V.

such that these two properties are satisfied:

1. Completeness. If a string x is a *yes* input, then there **exists** a string y of length $p(|x|)$ causing V to *accept*:

$$\exists\, y : V(x, y) = 1.$$

The string y is a **proof** (or **certificate** or **witness**) that x is a *yes* input.

2. Soundness. If a string x is a *no* input, then **no** string y of length $p(|x|)$ causes V to accept:

$$\forall\, y : V(x, y) = 0.$$

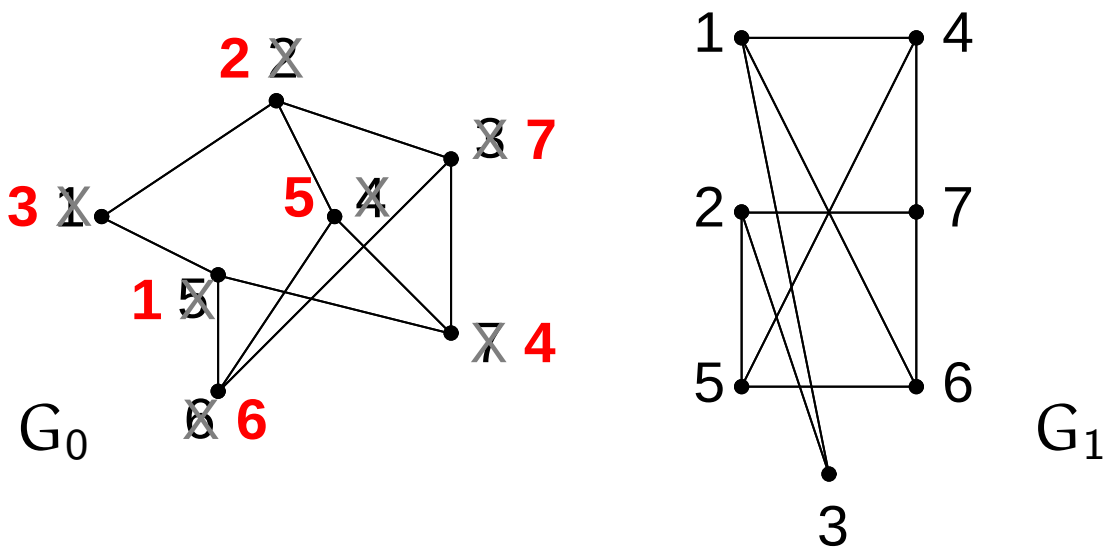
Example: GRAPH ISOMORPHISM is in NP

GRAPH ISOMORPHISM

Input: Two simple, undirected graphs G_0 and G_1.

Yes: G_0 and G_1 are isomorphic ($G_0 \cong G_1$)

No: G_0 and G_1 are not isomorphic ($G_0 \ncong G_1$)



The proof can be a description of an isomorphism:

$1 \to 3, \quad 2 \to 2, \quad 3 \to 7, \quad 4 \to 5, \quad 5 \to 1, \quad 6 \to 6, \quad 7 \to 4.$

Closure under complement?

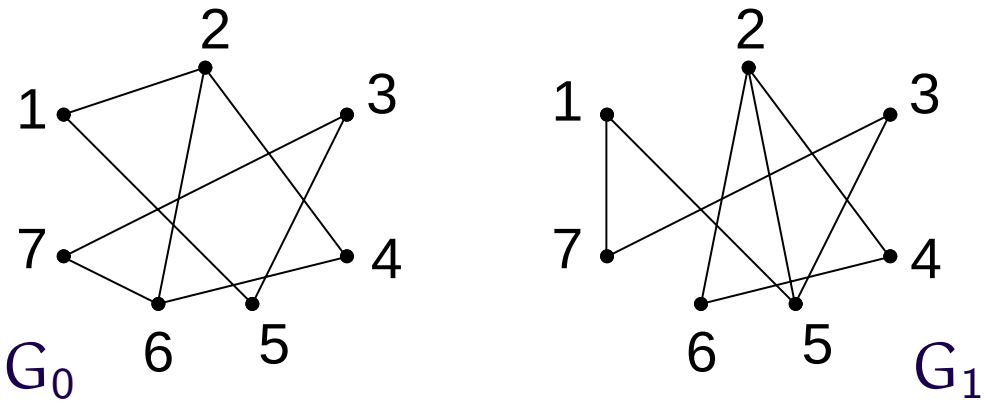
Graph Non-Isomorphism

Input: Two simple, undirected graphs G_0 and G_1.

Yes: G_0 and G_1 are not isomorphic ($G_0 \ncong G_1$).

No: G_0 and G_1 are isomorphic ($G_0 \cong G_1$).

Consider certifying that these two graphs are **non-isomorphic**:



It is not known whether or not this problem is in NP. . . an efficient **general** method would be required.

The class MA

MA is defined similarly to NP, except that the verification procedure is probabilistic. . . a promise problem A is in MA if and only if there exists:

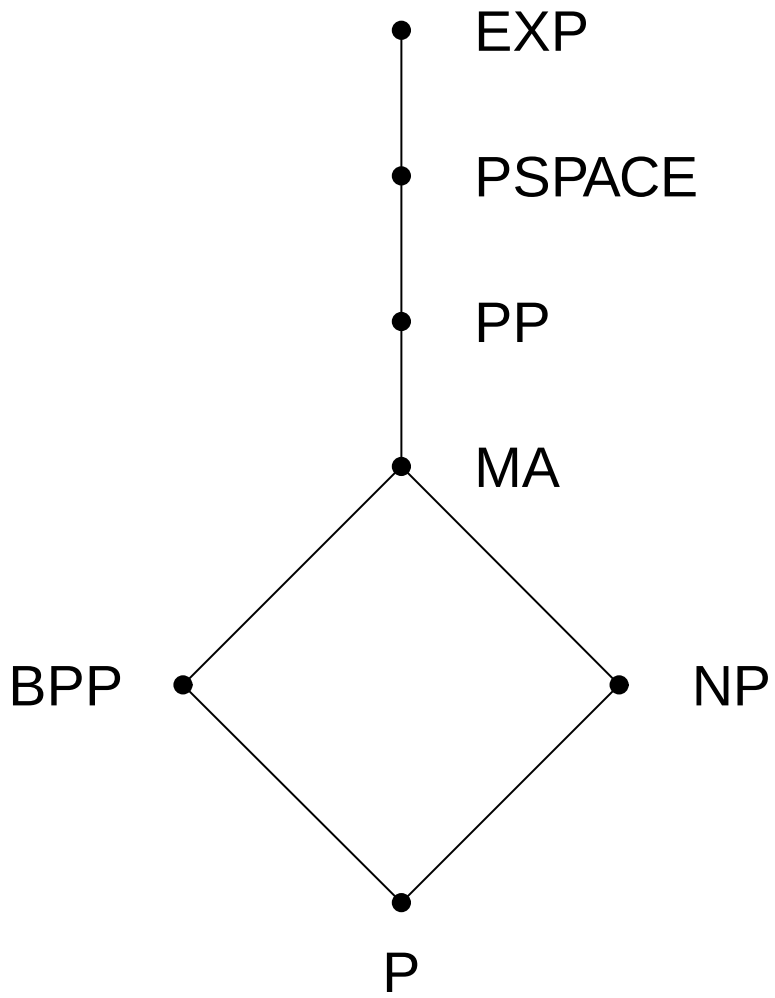
- a polynomial p
- a polynomial-time **probabilistic** verification procedure V

such that similar properties to before are satisfied:

1. Completeness. If x is a *yes* input, then there exists a string y of length $p(|x|)$ such that V accepts (x, y) with probability at least $99/100$.

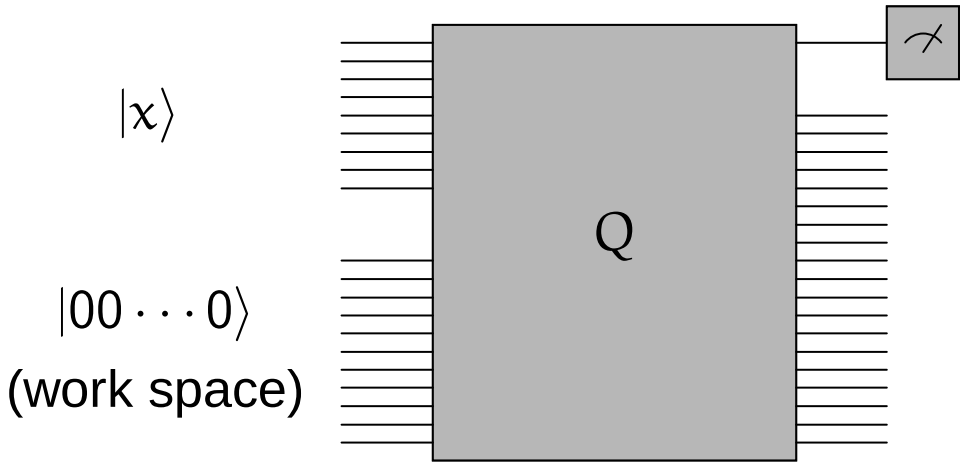
2. Soundness. If x is a *no* input, then V rejects (x, y) for every string y of length $p(|x|)$ with probability at least $99/100$.

Diagram of classes



BQP

A promise problem A is in BQP if there exists a family* of polynomial-size quantum circuits that work like this:



If x is a *yes* input, then

$$\Pr[Q \textit{ accepts } x] \geqslant 99/100.$$

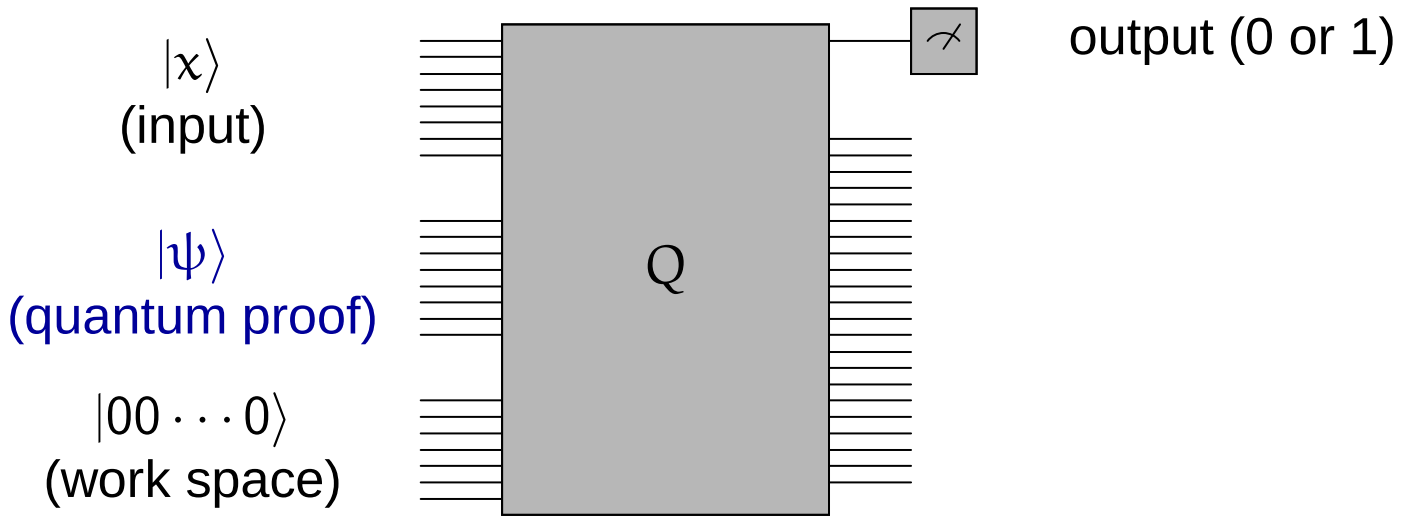
If x is a *no* input, then

$$\Pr[Q \textit{ rejects } x] \geqslant 99/100.$$

QMA: a quantum analogue of NP

A promise problem A is in **QMA** if there exists:

- a polynomial p, and
- a family of polynomial-size circuits as follows:

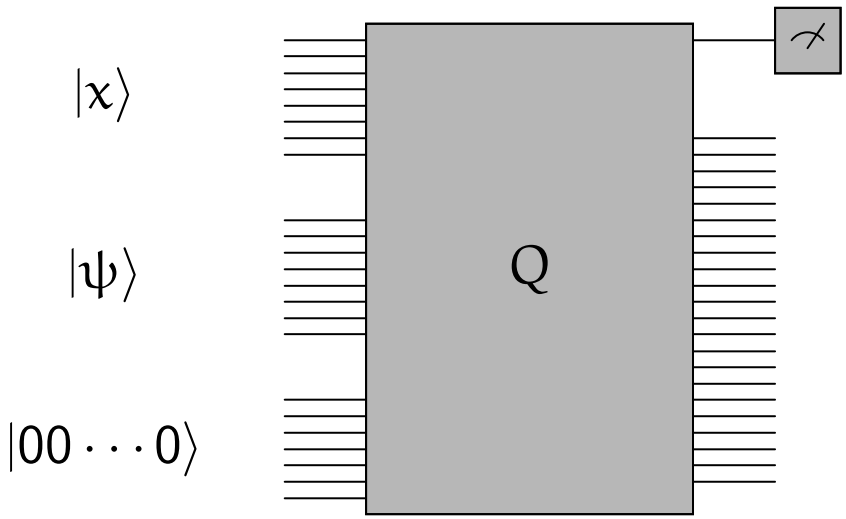


As for NP and MA, the polynomial p specifies the size of the proof: $|\psi\rangle$ is a $p(|x|)$-qubit state.

QMA: conditions on verification procedure

1. Completeness.

If x is a *yes* input, then there must **exist** a quantum state $|\psi\rangle$ that causes Q to accept with high probability:

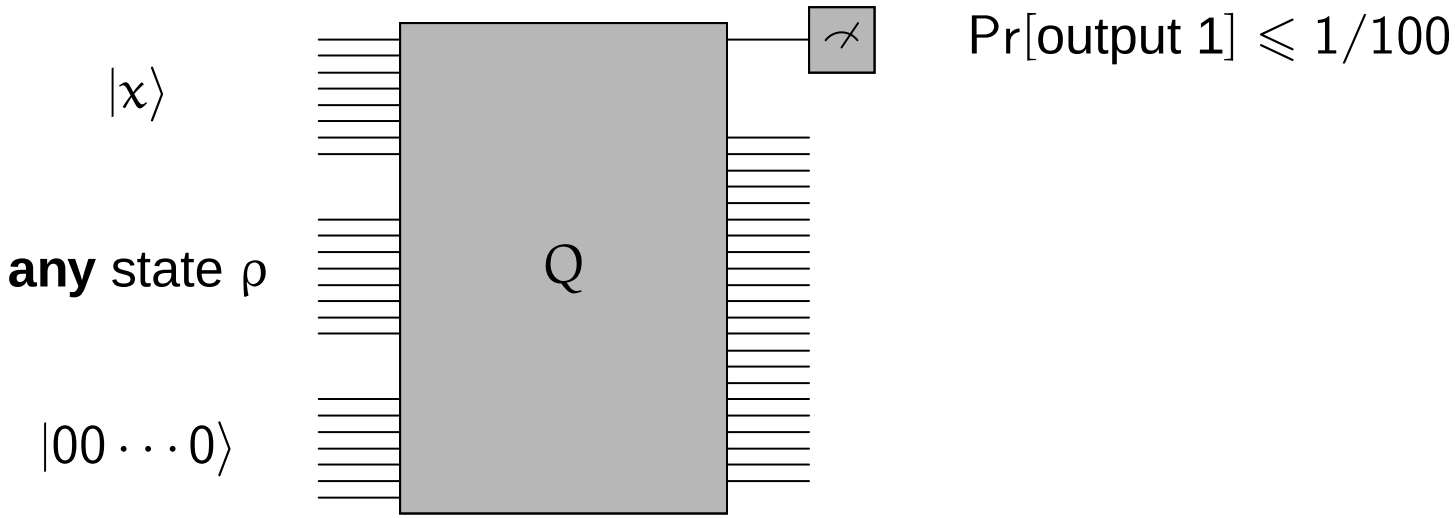


$\Pr[\text{output } 1] \geqslant 99/100$

QMA: conditions on verification procedure

2. Soundness.

If x is a *no* input, then **no** choice of a quantum state $|\psi\rangle$ causes Q to accept, except with very small probability:



Some basic facts about QMA

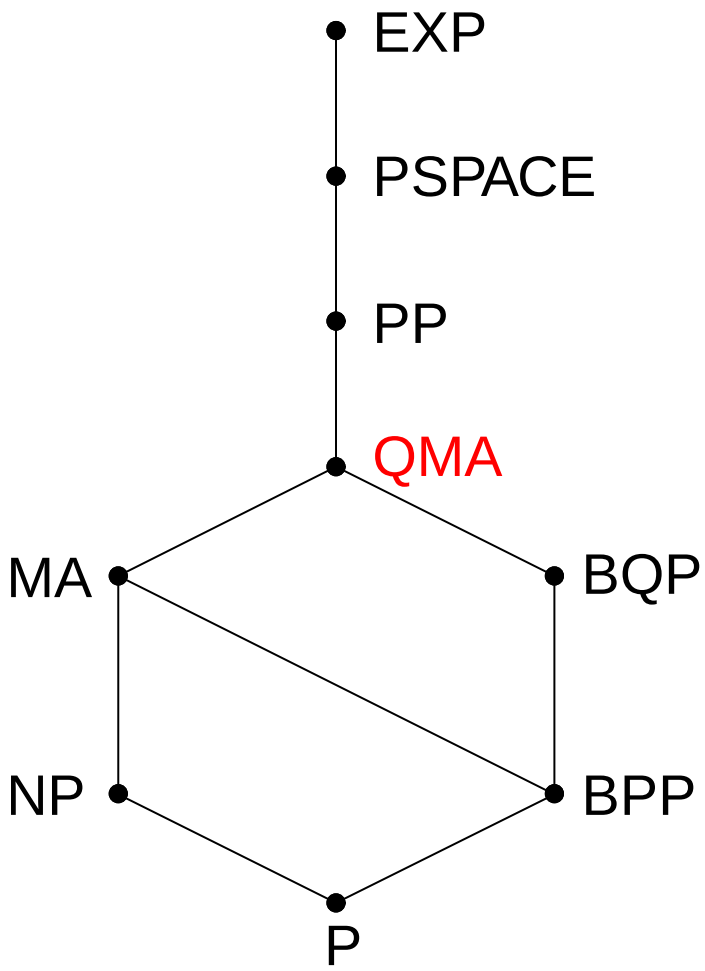
1. **Strong error reduction.**
   There is nothing special about the constant 99/100 in the definition.
   We can require

   completeness probability: $1 - 2^{-q(|x|)}$

   soundness probability: $2^{-q(|x|)}$

   without changing the class.
   This error reduction can be done independently of the proof length.
   [MARRIOTT & W., 2004.]
2. **Upper bound.**
   QMA $\subseteq$ PP. [KITAEV & W., 2000; VYALYI, 2003; MARRIOTT & W., 2004]
3. **Existence of an interesting complete promise problem.**
   The 2-LOCAL HAMILTONIAN problem is complete for QMA
   [KEMPE, KITAEV & REGEV, 2004.]
   (Loosely speaking: quantum analogue of the Cook-Levin Theorem.)

Diagram of classes



Group-theoretic problems

Let G be a **finite group** whose elements can be represented (uniquely) by strings of a given length n.

Efficient computation of group operations:

Given two elements $g, h \in G$, it is assumed that the group operations can be efficiently implemented by quantum circuits:

1. **Multiplication:** $|g\rangle\,|h\rangle \mapsto |g\rangle\,|gh\rangle$.
2. **Inverse:** $|g\rangle \mapsto |g^{-1}\rangle$.

Abstraction:

It is sometimes helpful to view such a group as a **black box group**; the group operations are performed by a black box (or group oracle), and string representatives of elements are independent of group structure.

Group membership

GROUP MEMBERSHIP

Input: Group elements $g_1, \ldots, g_k$ and h of G.

Yes: $h \in \langle g_1, \ldots, g_k \rangle$.

No: $h \notin \langle g_1, \ldots, g_k \rangle$.

- GROUP MEMBERSHIP $\in$ NP [BABAI AND SZEMERÉDY, 1984]
  The proof follows from the *Reachability Lemma*: every element in the subgroup $\langle g_1, \ldots, g_k \rangle$ has a short *straight-line program* that starts with $g_1, \ldots, g_k$.
- GROUP NON-MEMBERSHIP is **not** known to be in NP (or in MA).
  There are group oracles relative to which it is provably not the case [BABAI, 1991; W., 2000].

Quantum proofs for non-membership

Theorem [W., 2000]

GROUP NON-MEMBERSHIP is in QMA.

The idea behind the proof of this theorem is simple—the quantum state that proves

$$h \notin H \stackrel{\text{def}}{=} \langle g_1, \ldots, g_k \rangle$$

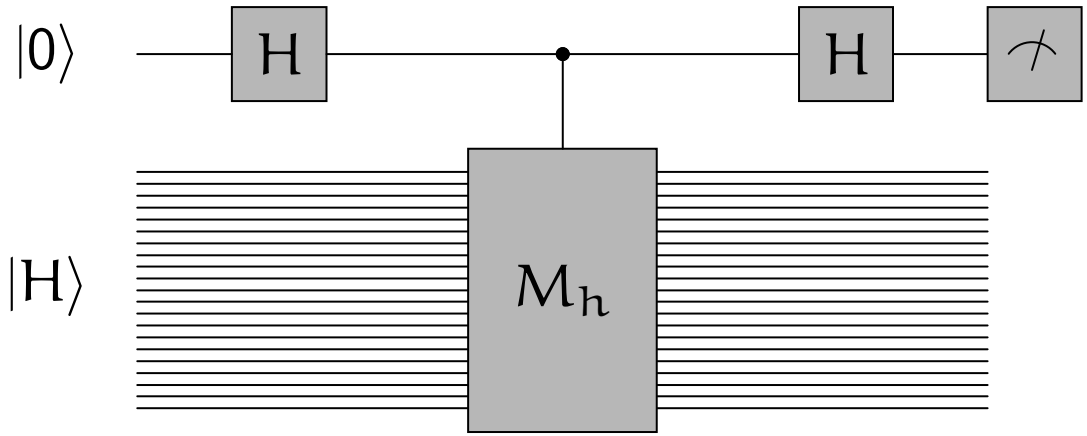
will be the uniform pure state over the elements of H:

$$|H\rangle = \frac{1}{\sqrt{|H|}} \sum_{a \in H} |a\rangle \, .$$

(It is independent of the element h.)

Quantum proofs for non-membership

Suppose that you have a copy of the state $|\mathrm{H}\rangle$. You can use this state to efficiently test membership of h in H as follows ...



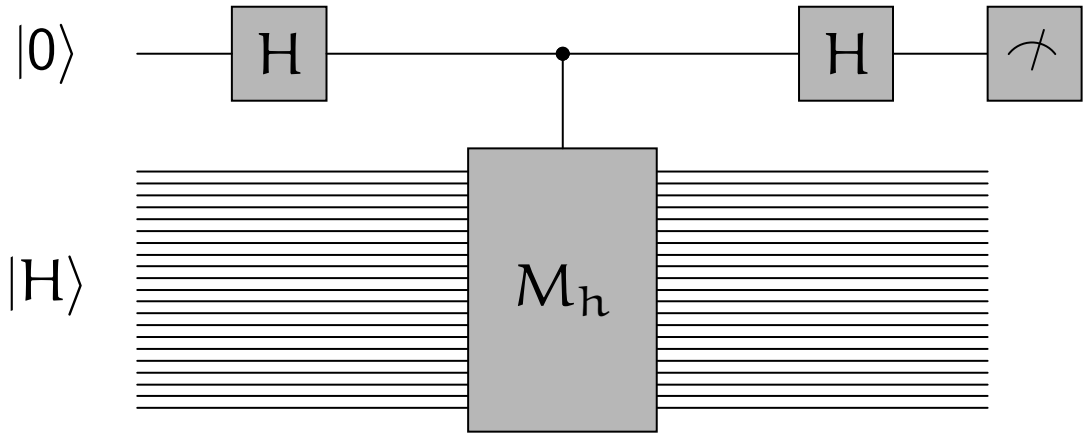
Case 1: $\mathrm{h} \in \mathrm{H}$**.** We have

$$\mathrm{M_h}\,|\mathrm{H}\rangle = |\mathrm{hH}\rangle = |\mathrm{H}\rangle\,;$$

the controlled-multiplication has **no effect**. As $\mathrm{H}^2\,|0\rangle = |0\rangle$, so the measurement outcome is **0** (with certainty).

Quantum proofs for non-membership

Suppose that you have a copy of the state $|\mathrm{H}\rangle$. You can use this state to efficiently test membership of $\mathfrak{h}$ in H as follows ...



Case 2: $\mathfrak{h} \notin \mathrm{H}$**.** We have

$$\mathrm{M}_{\mathfrak{h}} |\mathrm{H}\rangle = |\mathfrak{h}\mathrm{H}\rangle \perp |\mathrm{H}\rangle ;$$

the controlled-multiplication **acts as a measurement** of the first qubit. Both before and after the second Hadamard transform, it will be **totally mixed**. The measurement outcome is a **uniform random bit.**

But we can't trust the proof...

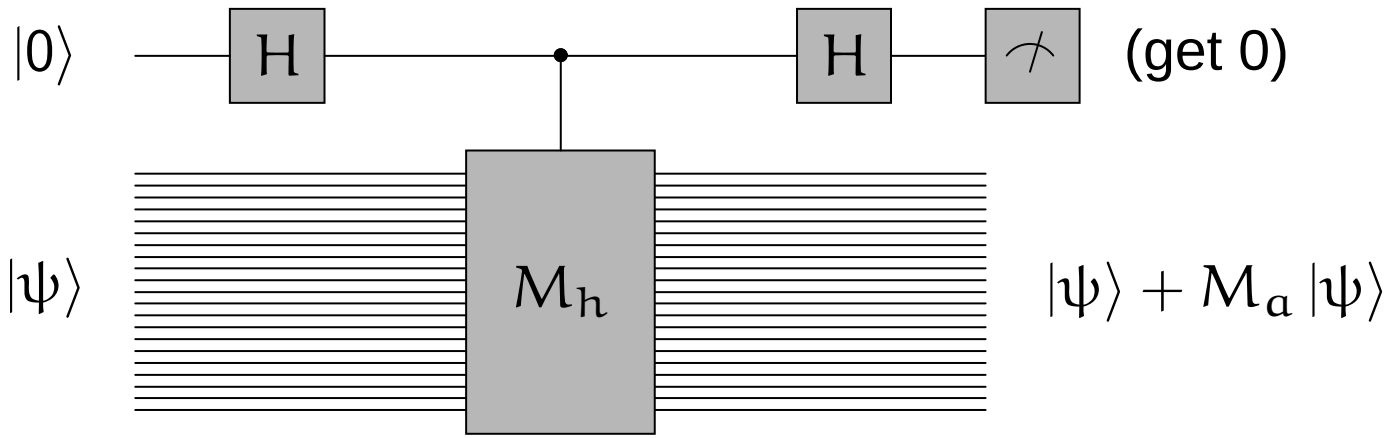
Suppose that $|\psi\rangle$ is the quantum state that supposedly proves $\mathfrak{h} \notin \mathrm{H}$. Unfortunately we cannot trust that $|\psi\rangle = |\mathrm{H}\rangle$, so we need to process $|\psi\rangle$ before running the membership test.

Imagine that instead of running the membership test with $\mathfrak{h}$, we run the test with some element $\mathfrak{a} \in \mathrm{H}$. It should reveal that $\mathfrak{a} \in \mathrm{H}$, because it is!

If the test indicates $\mathfrak{a} \notin \mathrm{H}$, then we know $|\psi\rangle \neq |\mathrm{H}\rangle$; **the proof is invalid** so **reject**.

Conditioned on the test indicating $\mathfrak{a} \in \mathrm{H}$, what happens to the proof?

Modified proof



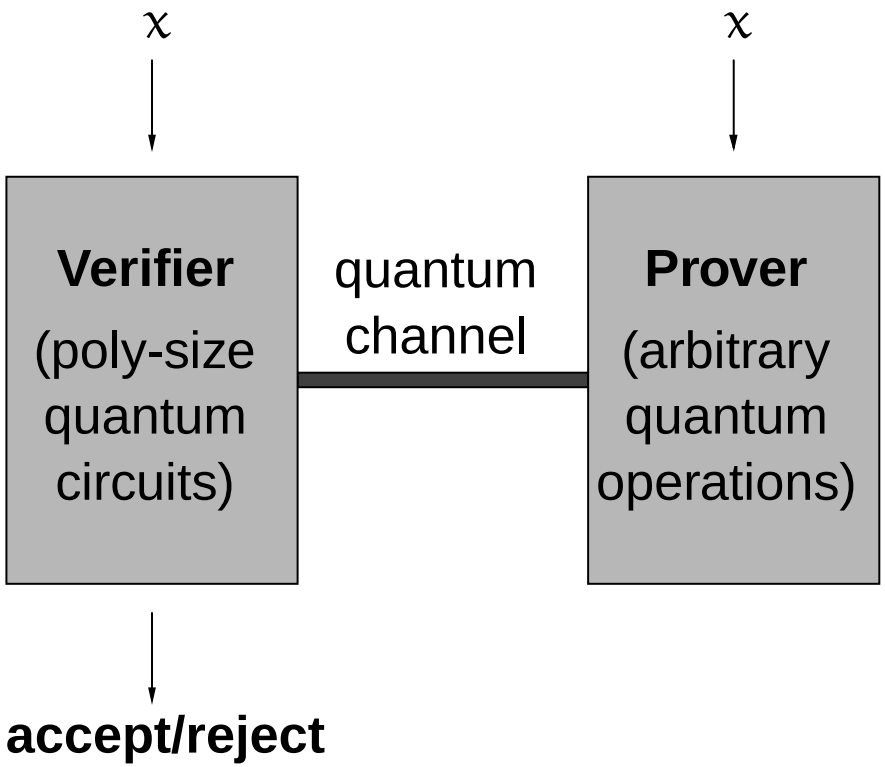
Repeat for a well-chosen set of elements $a_1, \ldots, a_k$; conditioned on success for each test, we will have a state very close to

$$\sum_{a \in H} M_a |\psi\rangle \quad \text{(normalized)}.$$

This state is invariant under left multiplication by elements in H; if $h \in H$, the test will falsely conclude $h \notin H$ with very small probability.

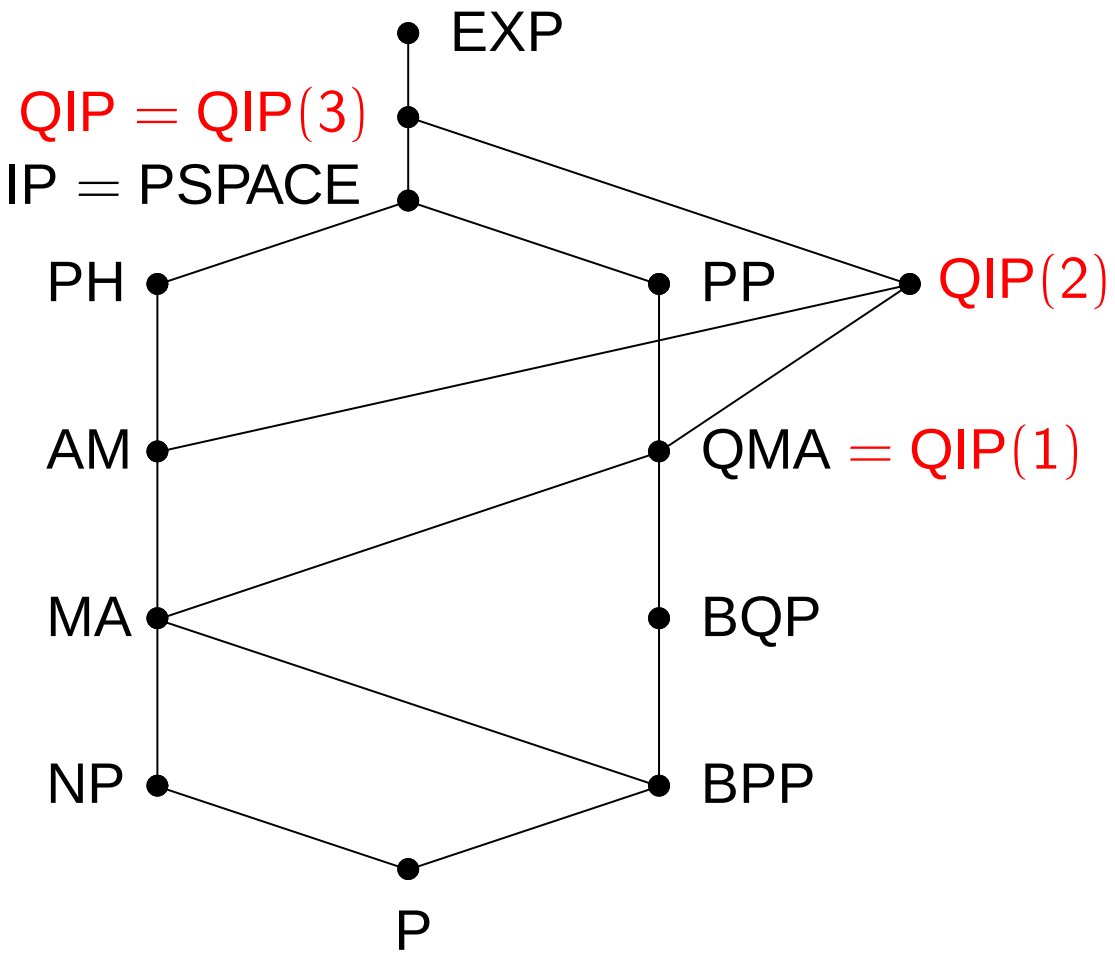
Quantum interactive proof systems

The quantum interactive proof system model works similarly to QMA, except that an **interaction** occurs between the verification procedure and a **prover**.



The model's **classical** counterpart is very important and well-studied in complexity theory.

Diagram of complexity classes



Open problems

1. Place interesting problems in QMA.
   - Is GRAPH NON-ISOMORPHISM in QMA?
   - Is GROUP ORDER in QMA?
2. Many questions about the classes QMA, QIP(2), and QIP remain unanswered.
   - Is QIP(2) $\subseteq$ PSPACE?
   - Improve PSPACE $\subseteq$ QIP $\subseteq$ EXP.
   - Is QIP closed under complementation?
3. There are interesting variants of these models for which little is known:
   - “Multiple Merlins”. . . are two quantum proofs better than one?
   - Multiprover interactive proofs. . .