PIMS-MITACS
Summer School on Quantum Information Science

Quantum proofs

June 2003

Alain Tapp

IRO, Université de Montréal

Proofs

A proof system should have the following properties.

Completeness: every true statement should have a proof.

Soundness: no false statement should have a proof.

Usefulness: it should be easy to verify the correcteness of a proof regardless of how hard it might be to find one.

A simple proof system

$$S = \{n \mid n \text{ is a positive composite number}\}$$

$\langle n, p, q \rangle$ is a proof if that *n* is in *S* if

$$n = pq, \;\; 1 < p < n, \;\; 1 < q < n$$

It might be hard to find such a proof
but it is easy to verify its correcteness.

The class NP

A set (*of strings*) is in NP if there is a polynomial time algorithm *V* such that:

$$\square x \square S,\ \square p \quad \text{such that } V(x, p) = \text{true}$$

$$\square x \square S,\ \square p \quad V(x, p) = \text{false}$$

NP is the class of sets (*of string*) having polinomial time chechable proof system.

World tour problem

The world tour (a.k.a. Traveling salesman) **problem:** Given a list of cities and a cost to travel between each pair of cities, is there a tour that costs less than *c*?

IF there are *n* cities to be visited there are *(n-1)!* possible tours. One might have to compute the cost of every tour before finding one with cost less than *c*. The set is in NP: given a list of cities, a table of cost, a budget and a tour, it is possible to verify the that the tour is within the budget in polynomial time.

World tour problem

Budget 720k

	Montréal	Calgary	Paris	Tokyo
Montréal	0	50k	100k	300k
Calgary	40k	0	160k	250k
Paris	120k	170k	0	320k
Tokyo	310k	260k	330k	0

There are 6 possible tours

Montréal 50k Calgary 160k Paris 320k Tokyo 310k Montréal=840k

Montréal 100k Paris 320k Tokyo 260k Calgary 40k Montréal=720k

Problems in NP

Scheduling: Giving a list of courses with the students attending, is it possible to produce a schedule using *k* periods without any conflict?

Clique: given a graph *G*, is there a clique of size at least *k* in *G*?

Quadratic residuosity: given *a*,*b* and *c*, is there a $x < c$ such that $x^2 = a \bmod b$?

NP-Complete

A problem is in P if there is a polynomial time algorithm to solve it.

A problem is NP-Complete if it is in NP and if every problem in NP reduces to it in polynomial time.

Scheduling, Clique, Quadratic residuosity, Traveling salesman are NP-Complete.

The most important question in complexity is: Is P=NP?

NP and the quantum computer

A problem is in BQP if there is a polynomial time quantum algorithm to solve it.

No NP-Complete problem is known to be in BQP.

Using Grover’s algorithm it is possible to obtain a quadratic speedup on the quantum computer.

Quantum proof

What happens if we consider quantum proofs?

A classical proof is a string; a quantum proof has to be a quantum state.

A classical proof is verified by a classical program.

A quantum proof would be verified by a quantum circuit.

Classical proof systems are usualy deterministic; a quantum proof might as well be probabilistic.

Does there exist problems that don’t have a short classical proof but have a short quantum proof?

QMA

A set *S* (of strings) has a quantum is in QMA if there exists a polynomial time algorithm *V* such that:

$$\square x \square S,\ \square\left|\square\right\rangle \ \text{ such that } \ \text{Prob}\big(V(x,\left|\square\right\rangle) = \text{true}\big) \geq \frac{2}{3}$$

$$\square x \square S,\ \square\left|\square\right\rangle \ \ \text{Prob}\big(V(x,\left|\square\right\rangle) = \text{false}\big) \square \frac{1}{3}$$

Is there some problem in QMA not known to be in NP?

Finite group

A finite group is a set *G* with an operation * such that:

Closure

$$\square x, y \square G \qquad x \square y \square G$$

Associativity

$$\square x, y, z \square G \qquad (x \square y) \square z = x \square (y \square z)$$

Neutral element

$$\square 1 \square G \text{ such that } \square x \square G \quad x \square 1 = 1 \square x = x$$

Inverse

$$\square x \square G, \square y \quad \text{with} \quad x \square y = y \square x = 1$$

Example of a finite group (1)

$$a \equiv b \bmod c \quad \square \quad \square k,\ kc + b = a \quad \square \quad \text{rest of } \frac{a}{c} \text{ is } b$$

$$25 \equiv 4 \bmod 7 \quad \text{for} \quad 3 \cdot 7 + 4 = 25$$

Integer mod *n* with addition forms a finite group

$$(x + y) + z \equiv x + (y + z) \bmod n$$

$$x + 0 \equiv 0 + x \equiv 0 \bmod n$$

$$x + (n \square x) \equiv (n \square x) + x \equiv n \equiv 0 \bmod n$$

Example of a finite group (2)

Integer mod *p* with multiplication forms a finite group when *p* is prime.

Clearly

$$(x \square y) \square z \equiv x \square (y \square z) \bmod p$$

$$x \square 1 \equiv 1 \square x \equiv x \bmod p$$

Fermat's theorem says

$$\square x, x^{p \square 1} \equiv 1 \bmod p$$

$$x \square x^{p \square 2} \equiv x^{p \square 2} \square x \equiv 1 \bmod p$$

$$1 \square 1 \equiv 2 \square 4 \equiv 3 \square 5 \equiv 4 \square 2 \equiv 5 \square 3 \equiv 6 \square 6 \equiv 1 \bmod 7$$

Example of a finite group (3)

Modular arithmetic nicely generalizes to *n* by *n* matrices of integers mod *p*.

The multiplication is done modulo *p*.

The set of all *n* by *n* invertible matrices mod *p* forms a group (Matrix group).

The neutral element is the identity matrix.

Example of finite group

A simple way to define a group is to consider the subset of a group *G* defined by some generators.

A group $G' \subseteq G$ can be defined by *k* generating elements $g_1, g_2, \ldots, g_k$.

$G \supseteq G' = \langle g_1, g_2, \ldots, g_k \rangle$ is the set of elements that can be obtained by the multiplication of some generator.

Group membership: a natural question is:
Given generators $g_1, g_2, \ldots, g_k$, is *h* in the group *G′*?

Example of finite group

Consider the group *G′* generated by (mod *7*)

$$m_1 = \begin{bmatrix} 1 & 4 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 3 \end{bmatrix} \qquad m_2 = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 2 & 0 & 1 \end{bmatrix} \qquad m_3 = \begin{bmatrix} 1 & 6 & 3 \\ 1 & 1 & 0 \\ 1 & 0 & 2 \end{bmatrix}$$

Does *m* belong to *G′* ?

$$m = \begin{bmatrix} 1 & 1 & 4 \\ 3 & 3 & 4 \\ 3 & 6 & 2 \end{bmatrix} \qquad m = m_3 \cdot m_1 \cdot m_2 \cdot m_3$$

In that case it is true and easy to verify.
What about the general case?

Group membership problem

Group membership: Given generators $g_1, g_2, \ldots, g_k$, is h in the group obtained by multiplication of the generators? $h \in \langle g_1, g_2, \ldots, g_k \rangle$?

For all groups, group membership is in NP.

For some groups, like the matrix group, it is not known if group non-membership is in NP.

No short proofs are known in general for non-membership of a group.

For any group, group non-membership is in QMA.

The quantum proof

For the group

$$G' = \langle g_1, g_2, \ldots, g_k \rangle$$

The state

$$|G'\rangle = \frac{1}{|G'|} \sum_{g \in G'} |g\rangle$$

is a quantum proof for non-membership for any *h* not in G′.

(Note: this state might be difficult to create.)

Properties of $|G^{\perp}\rangle$

For any *h* in *G* let $$|hG^{\perp}\rangle = \frac{1}{|G^{\perp}|}\sum_{g\in G^{\perp}} |h\oplus g\rangle$$

$h \in G^{\perp}$	$h \notin G^{\perp}$
$\forall g, h\oplus g \in G^{\perp}$ $\forall g_1, g_2 \in G,\quad h\oplus g_1 \neq h\oplus g_2$	$\forall g, h\oplus g \notin G^{\perp}$
$\langle G^{\perp}\vert hG^{\perp}\rangle = 1$	$\langle G^{\perp}\vert hG^{\perp}\rangle = 0$

Testing membership

Knowing *h*, there are unitary transformations *U*

$$\forall g \in G, \quad U|g\rangle = |h \circ g\rangle$$

and *U′*

$$\forall g \in G, \quad U'|0\rangle|g\rangle = |g\rangle \quad U'|1\rangle|g\rangle = |h \circ g\rangle$$

Consider

$$U'\frac{\left(|0\rangle + |1\rangle\right)}{\sqrt{2}}\,|G\rangle = \frac{U'|0\rangle|G\rangle + U'|1\rangle|G\rangle}{\sqrt{2}} = \frac{|0\rangle|G\rangle + |1\rangle|hG\rangle}{\sqrt{2}}$$

$$H|0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \qquad H|1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle \square |1\rangle\right)$$

$$U\square\frac{\left(|0\rangle + |1\rangle\right)}{\sqrt{2}} \qquad |G\square\rangle = \frac{|0\rangle|G\square\rangle + |1\rangle|hG\square\rangle}{\sqrt{2}}$$

We apply *H* to the first qubit and obtain

$$\frac{\left(H|0\rangle\right)|G\square\rangle + \left(H|1\rangle\right)|hG\square\rangle}{\sqrt{2}} = \frac{1}{2}|0\rangle\left(|G\square\rangle + |hG\square\rangle\right) + \frac{1}{2}|1\rangle\left(|G\square\rangle \square |hG\square\rangle\right)$$

$h \square G[$	$h \square G[$
$\|G\square\rangle = \|hG\square\rangle$ $\|0\rangle\|G\square\rangle$ $\Pr[1] = 0$	$\langle G\square\|hG\square\rangle = 0$ $\Pr[1] = \frac{1}{2}$

Soundness

If the the state we start with is the right one, we can test non-membership probabilistically.

Maybe in the case where *h* is a member there exists a state that will succeed with some probability.

We need a way to verify or ensure that the state is the correct one.

Increasing the quality of the proof

Before we use the test to verify that *h* is not in the group we will generate (using the generator) several elements of *G′* and perform the test with them.

If the state is $|G'\rangle$ then all tests will succeed and the state will remain unchanged. Otherwise, one of the tests will fail or we will obtain a state almost equal to $|G'\rangle$

Increasing the quality of the proof

We are provided with the state $\left|K\right\rangle$
We perform the test with element *g*

$$U\square\frac{\left(\left|0\right\rangle+\left|1\right\rangle\right)}{\sqrt{2}}\left|K\right\rangle=\frac{U\square\left|0\right\rangle\left|K\right\rangle+U\square\left|1\right\rangle\left|K\right\rangle}{\sqrt{2}}=\frac{\left|0\right\rangle\left|K\right\rangle+\left|1\right\rangle\left|gK\right\rangle}{\sqrt{2}}$$

$$\frac{\left(H\left|0\right\rangle\right)K\rangle+\left(H\left|1\right\rangle\right)hK\rangle}{\sqrt{2}}=\frac{1}{2}\left|0\right\rangle\left(\left|K\right\rangle+\left|gK\right\rangle\right)+\frac{1}{2}\left|1\right\rangle\left(\left|K\right\rangle\square\left|gK\right\rangle\right)$$

$$\left|K\right\rangle+\left|gK\right\rangle\square\ \mathrm{L}\ \square\ \left|G\right\rangle$$

The resulting state when the test succeeds is *better* than the original state.