The Watrous Post-Quantum Zero-Knowledge Proof

A Crypto Reading Group Talk

by

Xiao Liang

STONY BROOK UNIVERSITY
and
MAX-PLANCK INSTITUTE (SECURITY AND PRIVACY)

Git repo for these slides and LaTeX source code:

Post-Quantum ZK for NP

The model:
- ▶ Classical P and V
- ▶ ZK system for NP languages
- ▶ V^* can be quantum.
  - ▶ Modeled as a quantum polynomial-time (QPT) Turing machine.
  - ▶ equivalently (and more preferred in quantum-computing literature), poly-size quantum circuits.
  - ▶ Non-uniformity: V^* has an auxiliary quantum state that depends only on the security para. n. More accurately,

$$V^* = \{\mathsf{QC}_n, |\psi_n\rangle\}_{n\in\mathbb{N}}$$

Post-Quantum (Black-Box) ZK Is Hard

Why's **rewinding** hard?

- ▶ information gain VS state disturbance
- ▶ the no-cloning theorem

The major result in [Wat06]: a quantum rewinding lemma

Some Historical Notes

Techniques inspired by Marriot-Watrous [MW04]
- ▶ error-gap amplification for QMA using only 1 witness state

First published at STOC'06 [Wat06]
- ▶ explicit connection to [MW04]
- ▶ simple, ad hoc proof
- ▶ this talk mainly focus on this version
- ▶ the notation herein is consistent with this version

Then, on SIAM Journal of Computing in 2009 [Wat09]
- ▶ abstract out a general quantum rewinding lemma
- ▶ hiding the connection with Marriot-Watrous
- ▶ we'll also see a brief discuss of this version

Today's Agenda

- ▶ Prove quantum ZK for the Graph Isomorphism protocol [GMW86] (in detail)
  - ▶ Originally ad hoc [Wat06]
  - ▶ We'll take a general perspective
- ▶ Extends to the Graph-3-coloring Protocol [GMW86] in the ideal Com model (simple)
  - ▶ General quantum rewinding lemma
- ▶ G3C ZK with computationally-secure Com (simple-yet-tedious)
  - ▶ Rewinding lemma in its most general form — allowing small perturbations
  - ▶ the widely-used version in crypto literature

GMW ZK for Graph Isomorphism (GI)

Some Remarks:

- ▶ GI is not known to be NP-complete.
- ▶ the 1st message of the GMW GI protocol is perfectly uniform.

Input for P: statement $(G_0, G_1) \in \mathcal{G}_n \times \mathcal{G}_n$, witness $w = \sigma$ s.t. $\sigma(G_1) = G_0$

Input for V: (G_0, G_1)

1. P samples $\pi \leftarrow S_n$, sends $H = \pi(G_0)$
2. V sends $a \leftarrow \{0, 1\}$
3. P sends $\tau = \pi \circ \sigma^a$

V**'s decision:** accept iff $\tau(G_a) = H$

Classical Sim: guess the bit a

Modeling in Quantum Way

Model a Quantum V^***:** circuit family $\{\mathbf{V}_H\}_{H \in \mathcal{G}_n}$, auxiliary input $|\psi\rangle$

- receives H from P
- Perform $\mathbf{V}_H |\psi\rangle_{\mathsf{W}} |0\rangle_{\mathsf{V}} |0\rangle_{\mathsf{A}} = \alpha_0 |\psi_0\rangle_{\mathsf{WV}} |0\rangle_{\mathsf{A}} + \alpha_1 |\psi_1\rangle_{\mathsf{WV}} |1\rangle_{\mathsf{A}}$
    - V: work space
    - A: single-qubit register to store V^*'s challenge.
    - Note that $\mathbf{V}_H$ operates on space $\mathsf{W} \otimes \mathsf{V} \otimes \mathsf{A}$

Modeling in Quantum Way

View the protocol through a quantum lens:

- ▶ The full space $W \otimes X$, where $X = V \otimes A \otimes Y \otimes B \otimes Z$
- ▶ P performs

$$\mathbf{T} |0\rangle_{\mathsf{YBZ}} = \frac{1}{\sqrt{2n!}} \sum_{b \in \{0,1\}} \sum_{\pi \in S_n} |\pi(G_b)\rangle_{\mathsf{Y}} |b\rangle_{\mathsf{B}} |\pi\rangle_{\mathsf{Z}}$$

- ▶ V apply $\mathbf{V} = \sum_{H \in \mathcal{G}} \mathbf{V}_H \otimes |H\rangle\langle H|_{\mathsf{Y}} \otimes \mathbb{1}_{\mathsf{BZ}}$ on the full space $W \otimes X$
  - ▶ recall that $\mathbf{V}_H$ operates on $|\psi\rangle_{\mathsf{W}} |0\rangle_{\mathsf{V}} |0\rangle_{\mathsf{A}}$
  - ▶ corresponding to the exec. in super-position
  - ▶ Output format:

  $$\alpha_{00} |\psi_{00}\rangle |00\rangle_{\mathsf{AB}} + \alpha_{01} |\psi_{01}\rangle |01\rangle_{\mathsf{AB}} + \alpha_{10} |\psi_{10}\rangle |10\rangle_{\mathsf{AB}} + \alpha_{11} |\psi_{11}\rangle |11\rangle_{\mathsf{AB}}$$

In summary, the protocol up to step 2 is:

$$\underbrace{\mathbf{VT}}_{\text{on } \mathsf{W} \otimes \mathsf{X}} (|\psi\rangle_{\mathsf{W}} |0\rangle_{\mathsf{X=VAYBZ}}) \iff \underbrace{\mathbf{VT}(\mathbb{1}_{\mathsf{W}} \otimes |0\rangle_{\mathsf{X}})}_{\text{only on } \mathsf{W}} |\psi\rangle$$

Measuring the Guess

Define a binary-outcome measurement on the full space $W \otimes X$:

- $\Pi_0 = |0\rangle\langle 0|_{AB}$, $\quad \Pi_1 := \mathbb{1}_{AB} - |0\rangle\langle 0|_{AB} = |1\rangle\langle 1|_{AB}$
- work on the full space $W \otimes X$. Just tensor identities on registers other than AB

Performing $\{\Pi_0, \Pi_1\}$ on $VT\, |\psi\rangle_W\, |0\rangle_X$ boils down to:

- the probability for outcome 0 is $\mathrm{Tr}\left(\langle \psi |\, Q\, |\psi\rangle \right)$
- the probability for outcome 1 is $\mathrm{Tr}\left(\langle \psi |\, (\mathbb{1}_W - Q)\, |\psi\rangle \right)$

where $Q = (\mathbb{1}_W \otimes \langle 0|_X) T^\dagger V^\dagger \Pi_0 TV (\mathbb{1}_W \otimes |0\rangle_X)$.

Two important facts:

- $\{Q, \mathbb{1}_W - Q\}$ form a POVM
- $\mathrm{Tr}\left(\langle \psi |\, Q\, |\psi\rangle \right) = \mathrm{Tr}\left(\langle \psi |\, (\mathbb{1}_W - Q)\, |\psi\rangle \right) = \frac{1}{2}$, independent of $|\psi\rangle$. (Cuz 1st msg. of GI prot. is perfectly uniform.)

$\Rightarrow$ $Q = \mathbb{1}_W - Q = \frac{1}{2}\mathbb{1}_W$

An Important Lemma

Let $\boldsymbol{\Delta}_0 := \mathbb{1}_{\mathsf{W}} \otimes |0\rangle\langle 0|_{\mathsf{X}}$.

► $\boldsymbol{\Delta}_0$ projects register X to all-0 qubits.

► $\boldsymbol{\Delta}_0 = \boldsymbol{\Delta}_0^\dagger$

► $\boldsymbol{\Delta}_1 := \mathbb{1}_{\mathsf{WX}} - \boldsymbol{\Delta}_0$. The $\{\boldsymbol{\Delta}_0, \boldsymbol{\Delta}_1\}$ form a POVM.

LEMMA 1:

For all $|\psi\rangle \in \mathcal{H}(\mathsf{W})$, $|\gamma_0\rangle = |\psi\rangle_{\mathsf{W}} |0\rangle_{\mathsf{X}}$ is an eigenvector of $\underbrace{\boldsymbol{\Delta}_0^\dagger \mathbf{T}^\dagger \mathbf{V}^\dagger \boldsymbol{\Pi}_0 \mathbf{T} \mathbf{V} \boldsymbol{\Delta}_0}_{:=\mathbf{M}}$ with

corresponding eigenvalue $\lambda = 1/2$.

Proof. Recall $\mathbf{Q} = (\mathbb{1}_{\mathsf{W}} \otimes \langle 0|_{\mathsf{X}}) \mathbf{T}^\dagger \mathbf{V}^\dagger \boldsymbol{\Pi}_0 \mathbf{T} \mathbf{V} (\mathbb{1}_{\mathsf{W}} \otimes |0\rangle_{\mathsf{X}}) = \frac{1}{2}\mathbb{1}_{\mathsf{W}}$.

$$\Rightarrow \boldsymbol{\Delta}_0^\dagger \mathbf{T}^\dagger \mathbf{V}^\dagger \boldsymbol{\Pi}_0 \mathbf{T} \mathbf{V} \boldsymbol{\Delta}_0 = (\mathbb{1}_{\mathsf{W}} \otimes |0\rangle_{\mathsf{X}}) \mathbf{Q} (\mathbb{1}_{\mathsf{W}} \otimes \langle 0|_{\mathsf{X}}) = \frac{1}{2}\mathbb{1}_{\mathsf{W}} \otimes |0\rangle\langle 0|_{\mathsf{X}}$$

$$\Rightarrow \forall |\psi\rangle, \boldsymbol{\Delta}_0^\dagger \mathbf{T}^\dagger \mathbf{V}^\dagger \boldsymbol{\Pi}_0 \mathbf{T} \mathbf{V} \boldsymbol{\Delta}_0 \underbrace{|\psi\rangle_{\mathsf{W}} |0\rangle_{\mathsf{X}}}_{|\gamma_0\rangle} = (\frac{1}{2}\mathbb{1}_{\mathsf{W}} \otimes |0\rangle\langle 0|_{\mathsf{X}}) \underbrace{|\psi\rangle_{\mathsf{W}} |0\rangle_{\mathsf{X}}}_{|\gamma_0\rangle} = \frac{1}{2} \underbrace{|\psi\rangle_{\mathsf{W}} |0\rangle_{\mathsf{X}}}_{|\gamma_0\rangle}$$

Marriot-Watrous Lemma

Given unitary $\mathbf{U}$, proj. mnt. $\{\mathbf{\Pi}_0, \mathbf{\Pi}_1\}$ and $\{\mathbf{\Delta}_0, \mathbf{\Delta}_1\}$. Assume $|\gamma_0\rangle$ is an evec. of $\mathbf{\Delta}_0\mathbf{U}^\dagger\mathbf{\Pi}_0\mathbf{U}\mathbf{\Delta}_0$ with eval. λ. Define

$$|\delta_0\rangle := \frac{\mathbf{\Pi}_0\mathbf{U}|\gamma_0\rangle}{\sqrt{\lambda}}, \quad |\delta_1\rangle := \frac{\mathbf{\Pi}_0\mathbf{U}|\gamma_0\rangle}{\sqrt{1-\lambda}}, \quad |\gamma_1\rangle := \frac{\mathbf{\Delta}_1\mathbf{U}^\dagger|\delta_0\rangle}{\sqrt{1-\lambda}}.$$

Then, $\langle\gamma_0|\gamma_1\rangle = \langle\delta_0|\delta_1\rangle = 0$ and

$$\mathbf{U}|\gamma_0\rangle = \sqrt{\lambda}|\delta_0\rangle + \sqrt{1-\lambda}|\delta_1\rangle \qquad \mathbf{U}^\dagger|\delta_0\rangle = \sqrt{\lambda}|\gamma_0\rangle + \sqrt{1-\lambda}|\gamma_1\rangle$$
$$\mathbf{U}|\gamma_1\rangle = \sqrt{1-\lambda}|\delta_0\rangle - \sqrt{\lambda}|\delta_1\rangle \qquad \mathbf{U}^\dagger|\delta_1\rangle = \sqrt{1-\lambda}|\gamma_0\rangle - \sqrt{\lambda}|\gamma_1\rangle$$

(draw the evolution diagram)

$|\gamma_0\rangle \qquad |\delta_0\rangle \qquad |\gamma_0\rangle \qquad |\delta_0\rangle \qquad |\gamma_0\rangle \quad \cdots$

$|\delta_1\rangle \qquad |\gamma_1\rangle \qquad |\delta_1\rangle \qquad |\gamma_0\rangle \quad \cdots$
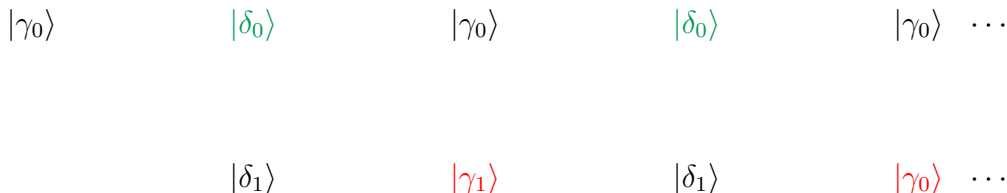
In Our Setting: Marriot-Watrous + Post-Mnt. Selection

In our setting, we have $\mathbf{U} = \mathbf{VT}$, $\lambda = 1/2$, and $|\gamma_0\rangle = |\psi\rangle_{\mathsf{W}} |0\rangle_{\mathsf{X}}$

Lemma 2 $\Rightarrow$ $|\gamma_0\rangle = \frac{1}{\sqrt{2}} |\delta_0\rangle + \frac{1}{\sqrt{2}} |\delta_1\rangle$, and the following:

$$|\delta_0\rangle = \sqrt{2}\mathbf{\Pi}_0\mathbf{VT} |\gamma_0\rangle, \quad \mathbf{T}^\dagger\mathbf{V}^\dagger |\delta_1\rangle = \frac{1}{\sqrt{2}} |\gamma_0\rangle - \frac{1}{\sqrt{2}} |\gamma_1\rangle, \quad \mathbf{VT}(\frac{1}{\sqrt{2}} |\gamma_0\rangle + \frac{1}{\sqrt{2}} |\gamma_1\rangle) = |\delta_0\rangle$$

Starting with $|\gamma_0\rangle \to \mathbf{VT} |\gamma_0\rangle \to$ measurement $\{\mathbf{\Pi}_0, \mathbf{\Pi}_1\}$:

▶ w.p. $1/2$, it is $|\delta_0\rangle$ — we are done!
▶ w.p. $1/2$, it is $|\delta_1\rangle$
  ▶ Key observation: $\mathbf{T}^\dagger\mathbf{V}^\dagger |\delta_1\rangle = \frac{1}{\sqrt{2}} |\gamma_0\rangle - \frac{1}{\sqrt{2}} |\gamma_1\rangle$
  ▶ If we can flip the phase of the 2nd term $\Rightarrow$ $\frac{1}{\sqrt{2}} |\gamma_0\rangle + \frac{1}{\sqrt{2}} |\gamma_1\rangle$.
  ▶ Then, simply do $\mathbf{VT}(\frac{1}{\sqrt{2}} |\gamma_0\rangle + \frac{1}{\sqrt{2}} |\gamma_1\rangle) = |\delta_0\rangle$

Yes, we can! (next slide)

Phase Flip for the 2nd Term

We want: $\frac{1}{\sqrt{2}} |\gamma_0\rangle - \frac{1}{\sqrt{2}} |\gamma_1\rangle \quad \to \quad \frac{1}{\sqrt{2}} |\gamma_0\rangle + \frac{1}{\sqrt{2}} |\gamma_1\rangle$

Recall the following

- $|\gamma_0\rangle = |\psi\rangle_\mathsf{W} |0\rangle_\mathsf{X}$ and $\mathbf{\Delta}_0 = \mathbb{1}_\mathsf{W} \otimes |0\rangle\langle 0|_\mathsf{X}$
- $\Rightarrow \quad \mathbf{\Delta}_0 |\gamma_0\rangle = |\gamma_0\rangle$
- Lemma 2 says $|\gamma_1\rangle = \sqrt{2}\mathbf{\Delta}_1 \mathbf{T}^\dagger \mathbf{V}^\dagger |\delta_0\rangle \quad \Rightarrow \quad \mathbf{\Delta}_0 |\gamma_1\rangle = 0$

Therefore, it is not hard to come up with the following idea:

$$\underbrace{(2\mathbf{\Delta}_0 - \mathbb{1}_\mathsf{WX})}_{=\mathbf{\Delta}_0 - \mathbf{\Delta}_1}(\frac{1}{\sqrt{2}} |\gamma_0\rangle - \frac{1}{\sqrt{2}} |\gamma_1\rangle) = \frac{2}{\sqrt{2}}\mathbf{\Delta}_0 |\gamma_0\rangle - \frac{2}{\sqrt{2}}\mathbf{\Delta}_0 |\gamma_1\rangle - \frac{1}{\sqrt{2}} |\gamma_0\rangle + \frac{1}{\sqrt{2}} |\gamma_1\rangle$$

$$= \frac{2}{\sqrt{2}} |\gamma_0\rangle - 0 - \frac{1}{\sqrt{2}} |\gamma_0\rangle + \frac{1}{\sqrt{2}} |\gamma_1\rangle$$

$$= \frac{1}{\sqrt{2}} |\gamma_0\rangle + \frac{1}{\sqrt{2}} |\gamma_1\rangle$$

Summarizing the Watrous Simulator

- ▶ Start with $|\gamma_0\rangle_{\mathsf{XW}} = |\psi\rangle_{\mathsf{X}} |0\rangle_{\mathsf{W}}$
- ▶ Perform $\mathbf{VT} |\gamma_0\rangle_{\mathsf{XW}}$
- ▶ Perform measurement $\{\mathbf{\Pi}_0, \mathbf{\Pi}_1\}$
    - ▶ If outcome is 0 — guessed correctly (in $|\delta_0\rangle$). Go next step.
    - ▶ Otherwise, we are in $|\delta_1\rangle = \sqrt{2}\mathbf{\Pi}_1 \mathbf{VT} |\gamma_0\rangle$.
        - ▶ Perform $\mathbf{T}^\dagger \mathbf{V}^\dagger |\delta_1\rangle = \frac{1}{\sqrt{2}} |\gamma_0\rangle - \frac{1}{\sqrt{2}} |\gamma_1\rangle$
        - ▶ Perform $(2\mathbf{\Delta}_0 - \mathbb{1}_{\mathsf{WX}})(\frac{1}{\sqrt{2}} |\gamma_0\rangle - \frac{1}{\sqrt{2}} |\gamma_1\rangle) = \frac{1}{\sqrt{2}} |\gamma_0\rangle + \frac{1}{\sqrt{2}} |\gamma_1\rangle$
        - ▶ Perform $\mathbf{VT}(\frac{1}{\sqrt{2}} |\gamma_0\rangle + \frac{1}{\sqrt{2}} |\gamma_1\rangle) = |\delta_0\rangle$. Go next step.
- ▶ Sim can finish the last round as the honest prover.

Extending to G3C—Idealized Com Model (1/3)

- The graph-3-coloring (G3C) problem is NP-complete
- will use the G3C classical ZK proof from [GMW86]
- $\Pr[\text{Guess correctly}] = \frac{1}{m}$, where $m = $ # edges.
- $\Pr[\text{Guess correctly}] \perp |\psi\rangle$?
    - 1st msg using perfect-binding (PB) Com
    - What about binding? — Collapse-binding suffices [Unr16]
    - We assume an ideal Com for simplicity: perfect-hiding and perfectly-binding
    - Extends to PB and CH Com later

Extending to G3C—Idealized Com Model (2/3)
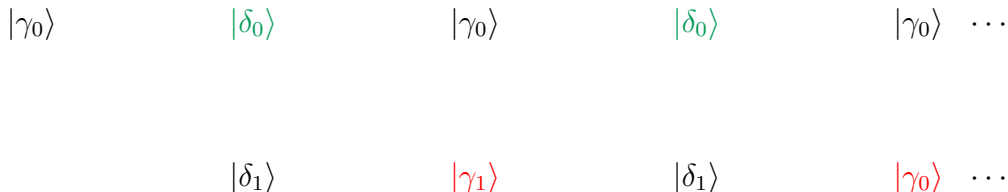
Key ingredients for the GI simulator:

- Define an operator: $\mathbf{\Delta}_0^\dagger \mathbf{T}^\dagger \mathbf{V}^\dagger \mathbf{\Pi}_0 \mathbf{T} \mathbf{V} \mathbf{\Delta}_0 \ (=: \mathbf{M})$
- An technical Lemma 1: $\lambda = \frac{1}{2} \quad (\perp \ |\psi\rangle)$
- Invoke Marriot-Watrous Lemma 2 with $\lambda = \frac{1}{2}$:
  - Voilà 😊! We can get $|\delta_0\rangle$ within ≤ 2 steps

What will change for the G3C protocol?

- $\mathbf{M}$ defined as before ($\mathbf{T}$ modified in the natural way)
- Lemma 1: $\lambda = \frac{1}{m} \quad (\perp \ |\psi\rangle)$
- Invoke Marriot-Watrous Lemma 2 with $\lambda = \frac{1}{m}$:
  - 🙁! no guarantee for $|\delta_0\rangle$ within ≤ 2 steps
- Solution: use the full power of Matrriot-Watrous analysis (next slide).

Extending to G3C—Idealized Com Model (3/3)

(draw the evolution diagram in the current setting)

$|\gamma_0\rangle$ $|\delta_0\rangle$ $|\gamma_0\rangle$ $|\delta_0\rangle$ $|\gamma_0\rangle$ $\cdots$

$|\delta_1\rangle$ $|\gamma_1\rangle$ $|\delta_1\rangle$ $|\gamma_0\rangle$ $\cdots$

The main take-away:

- $\mathbf{U}|\gamma_0\rangle = \sqrt{\lambda}|\delta_0\rangle + \sqrt{1-\lambda}|\delta_1\rangle$ $\mathbf{U}^\dagger|\delta_0\rangle = \sqrt{\lambda}|\gamma_0\rangle + \sqrt{1-\lambda}|\gamma_1\rangle$, where $\lambda = 1/m$.
  $\mathbf{U}|\gamma_1\rangle = \sqrt{1-\lambda}|\delta_0\rangle - \sqrt{\lambda}|\delta_1\rangle$ $\mathbf{U}^\dagger|\delta_1\rangle = \sqrt{1-\lambda}|\gamma_0\rangle - \sqrt{\lambda}|\gamma_1\rangle$
- Measure $\{\mathbf{\Pi}_0, \mathbf{\Pi}_1\}$ at each $|\delta\rangle$, if results in $|\delta_1\rangle$:
  - $\mathbf{U}(2\mathbf{\Delta} - \mathbb{1})\mathbf{U}^\dagger|\delta_1\rangle = 2\sqrt{p(1-p)}|\delta_0\rangle + (1-2p)|\delta_1\rangle$
- Measure $\{\mathbf{\Pi}_0, \mathbf{\Pi}_1\}$. Go to $|\delta_1\rangle$ w.p. $(1-2p)$.
- Keep failing after t iteration: $1 - (1-p)(1-2p)^t$. Then Chernoff bound.

The General Quantum Rewinding Lemma (Exact)

LEMMA 3: EXACT QUANTUM REWINDING [WAT09]

Q is a QC works on $|\psi\rangle$ and with $\Pr[\text{success}] = p \; (\perp |\psi\rangle)$ outputs $|\delta_0\rangle$. Then, for any $\varepsilon > 0$, there exists another QC **R** of size

$$O\left(\frac{\log(1/\varepsilon)}{p(1-p)} \cdot \text{size}(\mathbf{Q})\right)$$

such that for every input $|\psi\rangle$, the output ρ of **R** satisfies $\text{Tr}(\rho \, |\delta_0\rangle\langle\delta_0|) \geq 1 - \varepsilon$.

- ▶ "Exact" refers to the face that $p \perp |\psi\rangle$.
- ▶ The $\frac{\log(1/\varepsilon)}{p(1-p)}$ is due to Chernoff bound.
- ▶ Only need poly-size for a negligible ε.
- ▶ For the trace, the closer to 1, the better.

The Version Allowing Small Perturbations

LEMMA 4: QUANTUM REWINDING WITH SMALL PERTURBATIONS [WAT09, SEC. 4.2]

Let $\mathbf{Q}$, $|\psi\rangle$, and $|\delta_0\rangle$ as before. But $\Pr[\text{success}] = p(|\psi\rangle)$ now depends on $|\psi\rangle$.
Let $p_0, q \in (0, 1)$ and $\varepsilon \in (0, 1/2)$ be real numbers such that

$\quad$ (1). $|p(\psi) - q| < \varepsilon$ $\quad$ (2). $p_0 \leq p(\psi)$ $\quad$ (3). $p_0(1 - p_0) \leq q(1 - q)$

Then, for any $\varepsilon > 0$, there exists another QC $\mathbf{R}$ of size $O\left(\frac{\log(1/\varepsilon)}{p_0(1-p_0)} \cdot \text{size}(\mathbf{Q})\right)$
such that for every input $|\psi\rangle$, the output ρ of $\mathbf{R}$ satisfies:

$$\text{Tr}(\rho \,|\delta_0\rangle\langle\delta_0|) \geq 1 - 16\varepsilon \frac{\log^2(1/\varepsilon)}{p_0^2(1 - p_0)^2}.$$

Proof at a high-level:

► Consider each eigen-space separately (next slide).
► For detailed calculation, see [Wat09, Sec. 4.2].

Proof Sketch for Lemma 4

Proof Sketch:

- ▶ In Lemma 1, $|\gamma_0\rangle = |\psi\rangle_\mathsf{W} |0\rangle_\mathsf{X}$ is no longer an evec. of $\mathbf{M}$
  - ▶ The reason: $|\psi\rangle_\mathsf{W}$ is not an evec. of $\mathbf{Q}$
- ▶ (mental exper.) Thus, decomp. $|\psi\rangle$ in the evecs $\{|\psi_i\rangle\}_{i \in [\mathsf{dim}]}$ of $\mathbf{Q}$
- ▶ (mental exper.) For each i, we obtain Lemmas 1 and 2
- ▶ (mental exper.) In the Marriot-Watrous procedure, in each egein space:
  $$\mathbf{VT} |\psi_i\rangle_\mathsf{W} |0\rangle_\mathsf{X} = \sqrt{p(|\psi_i\rangle)} |\delta_0(|\psi_i\rangle)\rangle + \sqrt{1 - p(|\psi_i\rangle)} |\delta_1(|\psi_i\rangle)\rangle$$
- ▶ (mental exper.) Define a unitary $\mathbf{N}$ such that for all $i \in [\mathsf{dim}]$:
  $$\sqrt{p(|\psi_i\rangle)} |\delta_0(|\psi_i\rangle)\rangle + \sqrt{1 - p(|\psi_i\rangle)} |\delta_1(|\psi_i\rangle)\rangle \to \sqrt{q} |\delta_0(|\psi_i\rangle)\rangle + \sqrt{1 - q} |\delta_1(|\psi_i\rangle)\rangle$$
- ▶ (mental exper.) Ready to apply the Exact Rewinding Lemma 3 (w/ p_0 as we don't know p.) Need $p_0(1 - p_0) \leq q(1 - q)$

In summary, this is a Sim w/ an imaginary operator $\mathbf{N}$, giving the same trace bound as in Lemma 3. But for the real Sim, there is no $\mathbf{N}$.

- ▶ Doesn't matter. $\mathbf{N}$ only affects the trace bound negligibly.
- ▶ By tedious-yet-elementary linear algebra (see [Wat09, Sec. 4.2]).

References

[GMW86] Oded Goldreich, Silvio Micali, and Avi Wigderson. Proofs that yield nothing but their validity and a methodology of cryptographic protocol design (extended abstract). In *27th Annual Symposium on Foundations of Computer Science, Toronto, Canada, 27-29 October 1986*, pages 174–187. IEEE Computer Society, 1986.

[MW04] Chris Marriott and John Watrous. Quantum arthur-merlin games. In *19th Annual IEEE Conference on Computational Complexity (CCC 2004), 21-24 June 2004, Amherst, MA, USA*, pages 275–285. IEEE Computer Society, 2004.

[Unr16] Dominique Unruh. Computationally binding quantum commitments. In Marc Fischlin and Jean-Sébastien Coron, editors, *Advances in Cryptology - EUROCRYPT 2016 - 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, May 8-12, 2016, Proceedings, Part II*, volume 9666 of *Lecture Notes in Computer Science*, pages 497–527. Springer, 2016.

[Wat06] John Watrous. Zero-knowledge against quantum attacks. In Jon M. Kleinberg, editor, *Proceedings of the 38th Annual ACM Symposium on Theory of Computing, Seattle, WA, USA, May 21-23, 2006*, pages 296–305. ACM, 2006.

[Wat09] John Watrous. Zero-knowledge against quantum attacks. *SIAM J. Comput.*, 39(1):25–58, 2009.