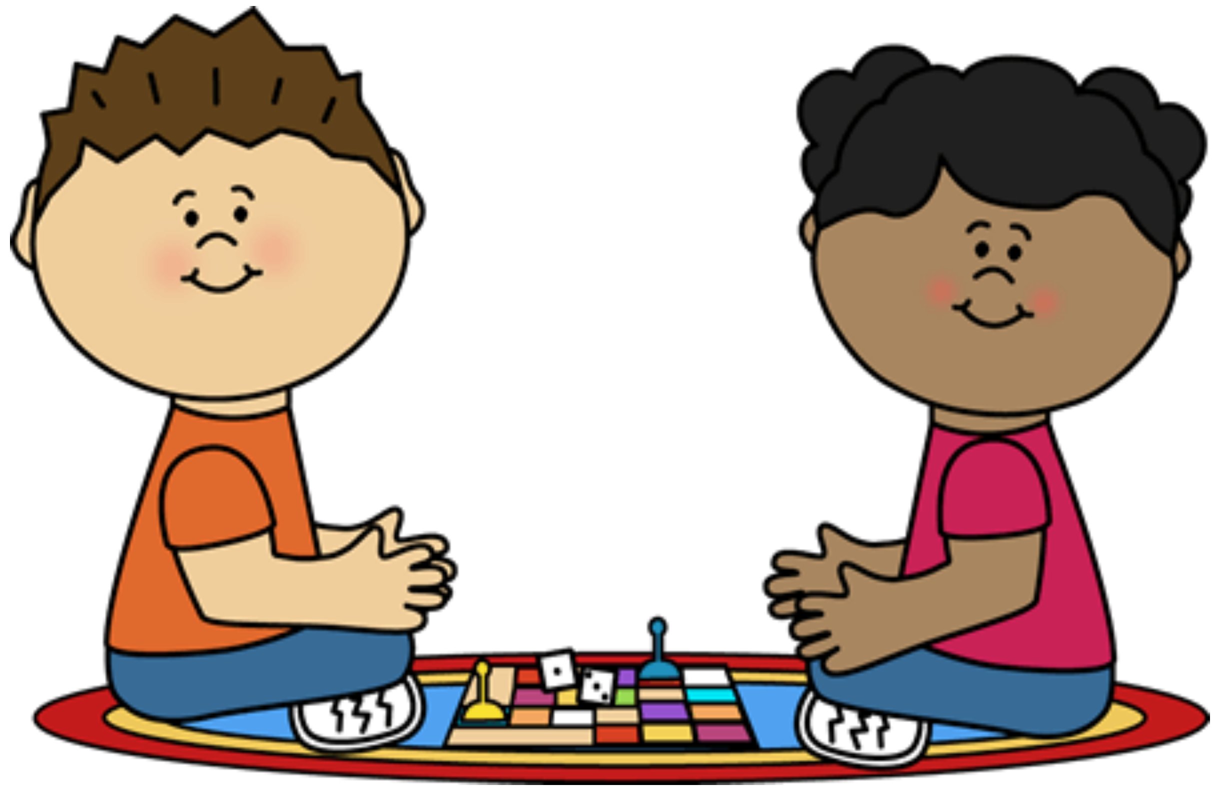
A study of one-turn quantum refereed games



Soumik Ghosh, 29th June, 2020.

Let us start with QMA….

Sends quantum proof ρ

Referee

Alice (the yes prover)

QRG(1) is a generalization

Alice (the yes prover)

Sends quantum state ρ

Bob (the no prover)

Sends quantum state σ

Referee

Proper definitions

That of a “referee”….

Definition 8. A referee is a polynomial-time generated family

$$R = \{R_x : x \in \Sigma^*\}$$

of quantum circuits which has the following features, for each $x \in \Sigma^*$:

1. The inputs to the circuit R_x can be divided into two registers: an n-qubit register A and an m-qubit register B, where n and m are polynomially bounded functions.
2. The output of the circuit R_x is a single qubit, which is measured in the standard basis immediately after running the circuit.

Define…

$$\omega(R_x) = \max_{\rho \in \mathrm{D}(\mathcal{A})} \min_{\sigma \in \mathrm{D}(\mathcal{B})} \langle 1|R_x(\rho \otimes \sigma)|1\rangle.$$

That of QRG(1)….

Definition 9. A promise problem $A = (A_{\text{yes}}, A_{\text{no}})$ is contained in the complexity class $\mathrm{QRG}(1)_{\alpha,\beta}$ if there exists a referee $R = \{R_x : x \in \Sigma^*\}$ such that the following properties are satisfied:

1. For every string $x \in A_{\text{yes}}$, it is the case that $\omega(R_x) \geq \alpha$.
2. For every string $x \in A_{\text{no}}$, it is the case that $\omega(R_x) \leq \beta$.

We also define $\mathrm{QRG}(1) = \mathrm{QRG}(1)_{2/3,1/3}$.

What do we know about QRG(1)?

Trivial facts:

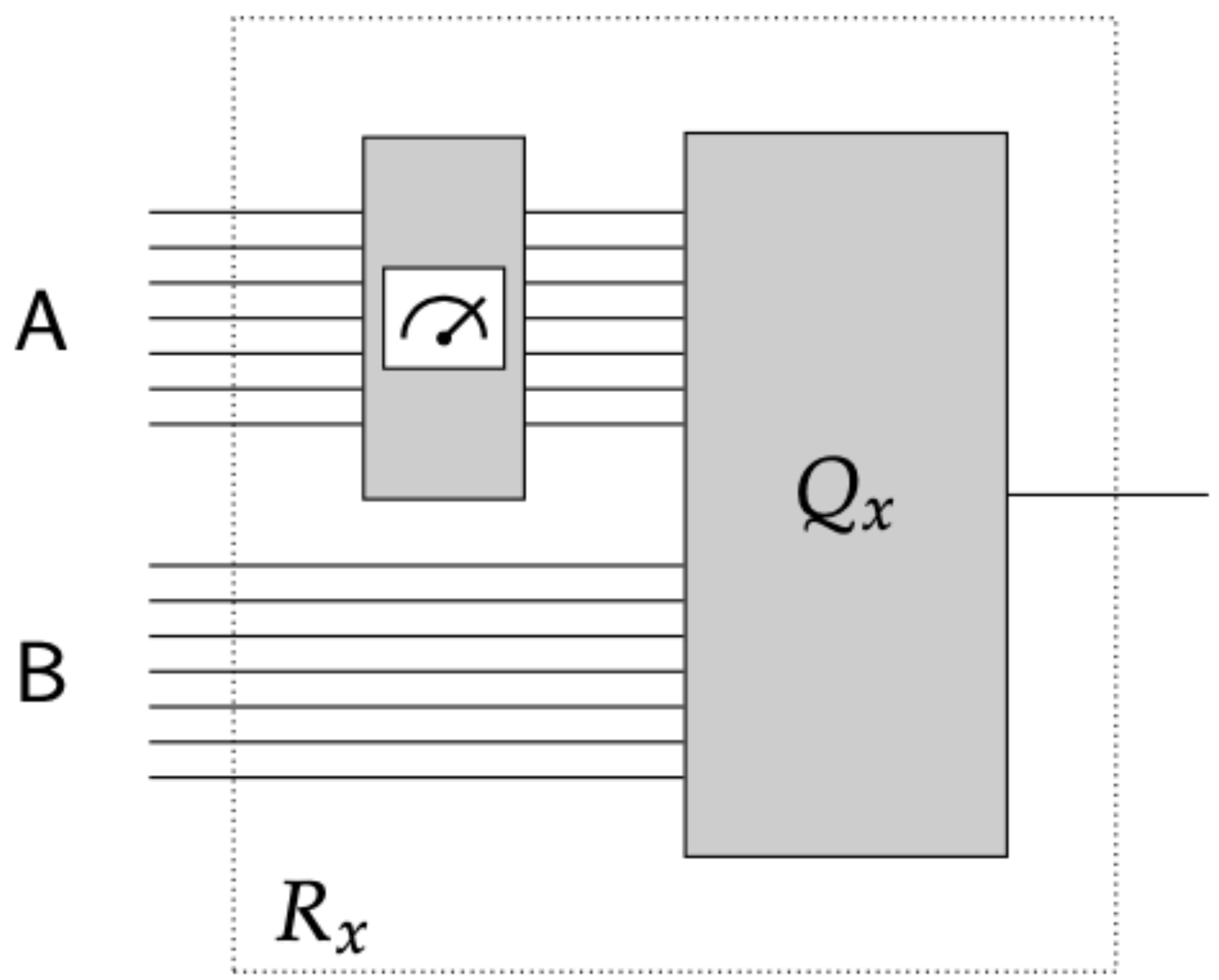
1. Contains QMA (just neglect the no proof).
2. Contains co-QMA (just neglect the yes proof).
3. Error reduction by parallel repetition.

Non-trivial facts:

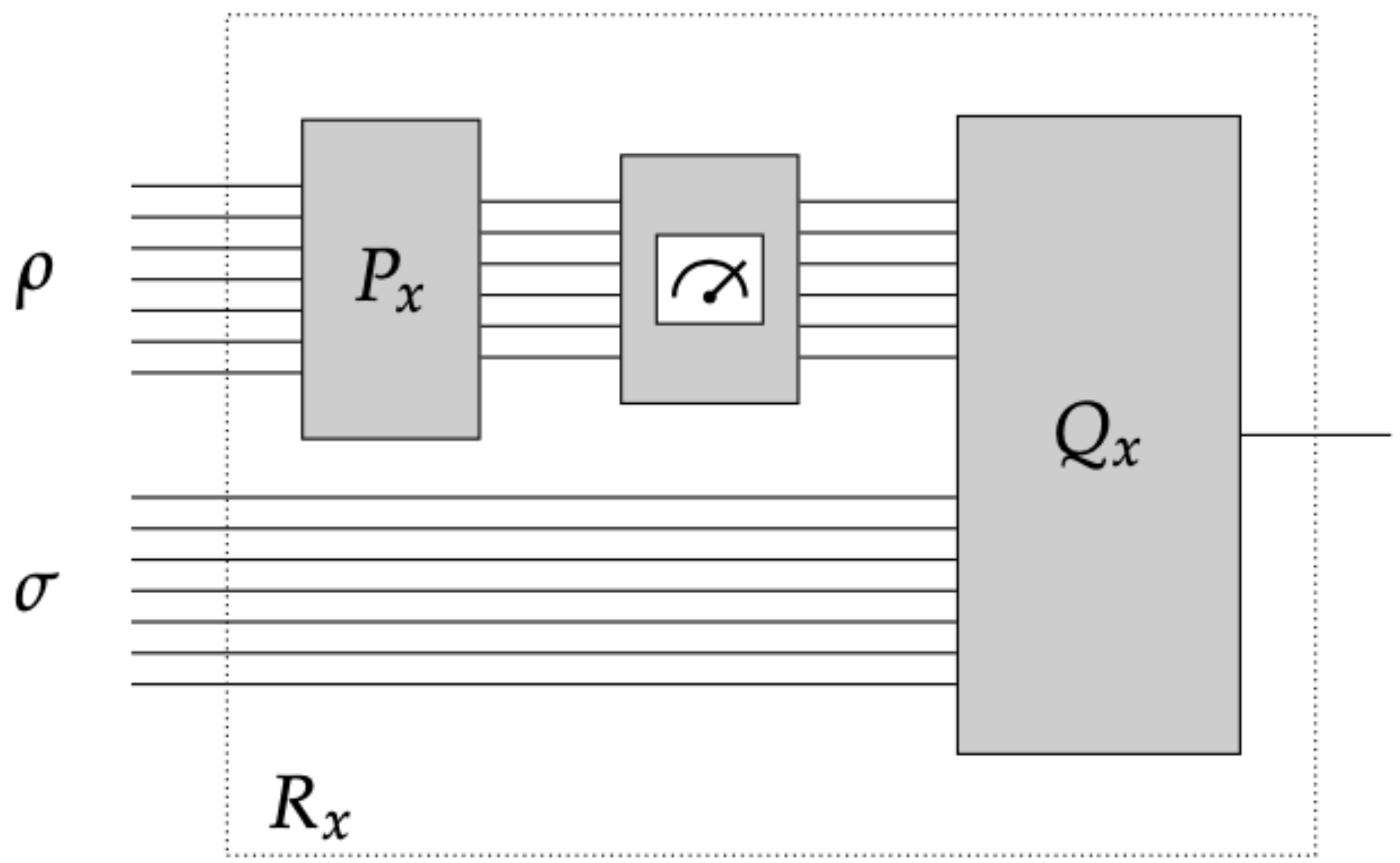
1. Contained in PSPACE (proved by Rahul Jain and John Watrous, 2009).
2. $\mathrm{QRG}(1) = \mathrm{P}^{\mathrm{QRG}(1)}$ (folklore result, elucidated in thesis).

Contributions of this thesis

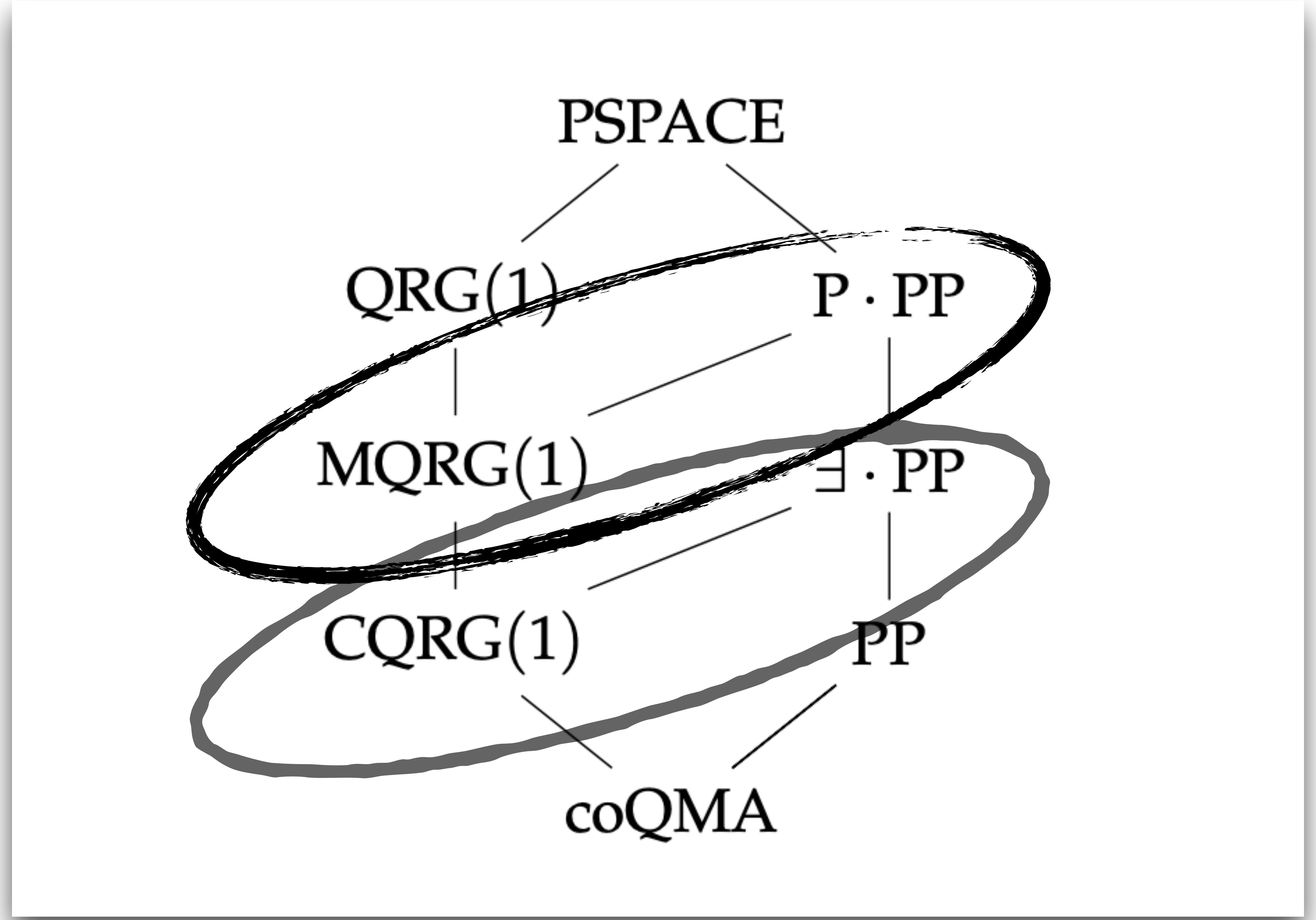
Two new classes:



CQRG(1)



MQRG(1)



Hasse diagram showing the inclusions

What are those funny classes?

$\exists \cdot \mathrm{PP}$

Definition 12. The complexity class $\exists \cdot \mathrm{PP}$ contains all promise problems $A = (A_{\text{yes}}, A_{\text{no}})$ for which there exists a language $B \in \mathrm{PP}$ and a polynomially bounded function p such that these two implications hold:

$$x \in A_{\text{yes}} \Rightarrow \left\{y \in \Sigma^p : \langle x, y\rangle \in B\right\} \neq \varnothing,$$
$$x \in A_{\text{no}} \Rightarrow \left\{y \in \Sigma^p : \langle x, y\rangle \in B\right\} = \varnothing.$$

$\mathrm{P} \cdot \mathrm{PP}$

Definition 13. The complexity class $\mathrm{P} \cdot \mathrm{PP}$ contains all promise problems $A = (A_{\text{yes}}, A_{\text{no}})$ for which there exists a language $B \in \mathrm{PP}$ and a polynomially bounded function p such that these two implications hold:

$$x \in A_{\text{yes}} \Rightarrow \left|\left\{y \in \Sigma^p : \langle x, y\rangle \in B\right\}\right| > \frac{1}{2} \cdot 2^p,$$
$$x \in A_{\text{no}} \Rightarrow \left|\left\{y \in \Sigma^p : \langle x, y\rangle \in B\right\}\right| \leq \frac{1}{2} \cdot 2^p.$$

First tool….

A Chernoff-type bound, but for matrices! Proved by Tropp, 2011.

Corollary 20. *Let d and N be positive integers, let $\eta, \varepsilon \in [0,1]$ with $\eta > \varepsilon$ be real numbers, and let $X_1, \ldots, X_N$ be independent and identically distributed operator-valued random variables having the following properties:*

1. *Each X_k takes $d \times d$ positive semidefinite operator values satisfying $X_k \leq \mathbb{1}$.*
2. *The minimum eigenvalue of the expected operator $\mathrm{E}(X_k)$ satisfies $\lambda_{\min}(\mathrm{E}(X_k)) \geq \eta$.*

It is the case that

$$\Pr\left(\lambda_{\min}\left(\frac{X_1 + \cdots + X_N}{N}\right) < \eta - \varepsilon\right) \leq d \exp(-2N\varepsilon^2).$$

Second tool…..

Brief description: gives us a PP language!

Lemma 22. *Let $\{Q_x : x \in \Sigma^*\}$ be a polynomial-time generated family of quantum circuits, where each circuit Q_x takes as input a k-qubit register* Y *and an m-qubit register* B*, for polynomially bounded functions k and m, and outputs a single qubit. For each $x \in \Sigma^*$ and $y \in \Sigma^k$, define an operator*

$$S_{x,y} = (\langle y| \otimes \mathbb{1}_{\mathsf{B}}) Q_x^* (|1\rangle\langle 1|) (|y\rangle \otimes \mathbb{1}_{\mathsf{B}}).$$

For every polynomially bounded function N, there exists a language $B \in \mathrm{PP}$ for which the following implications are true for all $x \in \Sigma^*$ and $y_1, \ldots, y_N \in \Sigma^k$:

$$\lambda_{min}\left(\frac{S_{x,y_1} + \cdots + S_{x,y_N}}{N}\right) \geq \frac{2}{3} \quad \Rightarrow \quad (x, y_1 \cdots y_N) \in B,$$

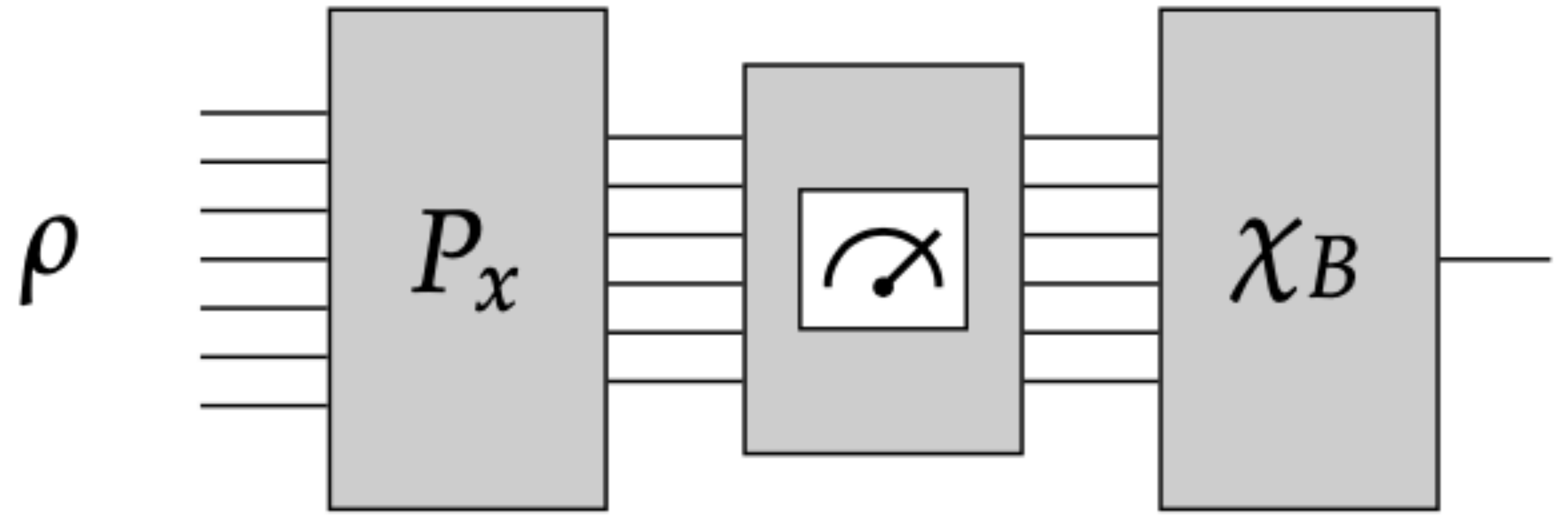
$$\lambda_{min}\left(\frac{S_{x,y_1} + \cdots + S_{x,y_N}}{N}\right) \leq \frac{1}{3} \quad \Rightarrow \quad (x, y_1 \cdots y_N) \notin B.$$

31

Idea of the proof: similar to Marriott Watrous but without in-place error amplification

More tools…..

A complexity class called QMA.C



Definition 24. For a given complexity class $\mathcal{C}$, the complexity class QMA $\cdot$ $\mathcal{C}$ contains all promise problems $A = (A_{\text{yes}}, A_{\text{no}})$ for which there exists a polynomial-time generated family of quantum circuits $\{P_x : x \in \Sigma^*\}$, where each P_x takes $n = n(|x|)$ input qubits and outputs $k = k(|x|)$ qubits, along with a language $B \in \mathcal{C}$, such that the following implications hold.

1. If $x \in A_{\text{yes}}$, then there exists a density operator ρ on n qubits for which
$$\Pr\big(P_x(\rho) \in B\big) \geq \frac{2}{3}.$$
2. If $x \in A_{\text{no}}$, then for every density operator ρ on n qubits,
$$\Pr\big(P_x(\rho) \in B\big) \leq \frac{1}{3}.$$

Fact: $\mathbb{QMA} \cdot \mathbb{C}$ is contained in $\mathbb{P} \cdot \mathbb{C}$, when $\mathbb{C}$ is P or PP

Idea of proof: Gap.C functions!

Definition 2. Let $\mathcal{C}$ be any complexity class of languages over the alphabet Σ. A function $f : \Sigma^* \to \mathbb{Z}$ is a Gap $\cdot\, \mathcal{C}$ function if there exist languages $A, B \in \mathcal{C}$ and a polynomially bounded function p such that

$$f(x) = \left|\{y \in \Sigma^p : \langle x, y\rangle \in A\}\right| - \left|\{y \in \Sigma^p : \langle x, y\rangle \in B\}\right|$$

for all $x \in \Sigma^*$.

First result

Definition 12. The complexity class $\exists \cdot \mathrm{PP}$ contains all promise problems $A = (A_{\text{yes}}, A_{\text{no}})$ for which there exists a language $B \in \mathrm{PP}$ and a polynomially bounded function p such that these two implications hold:

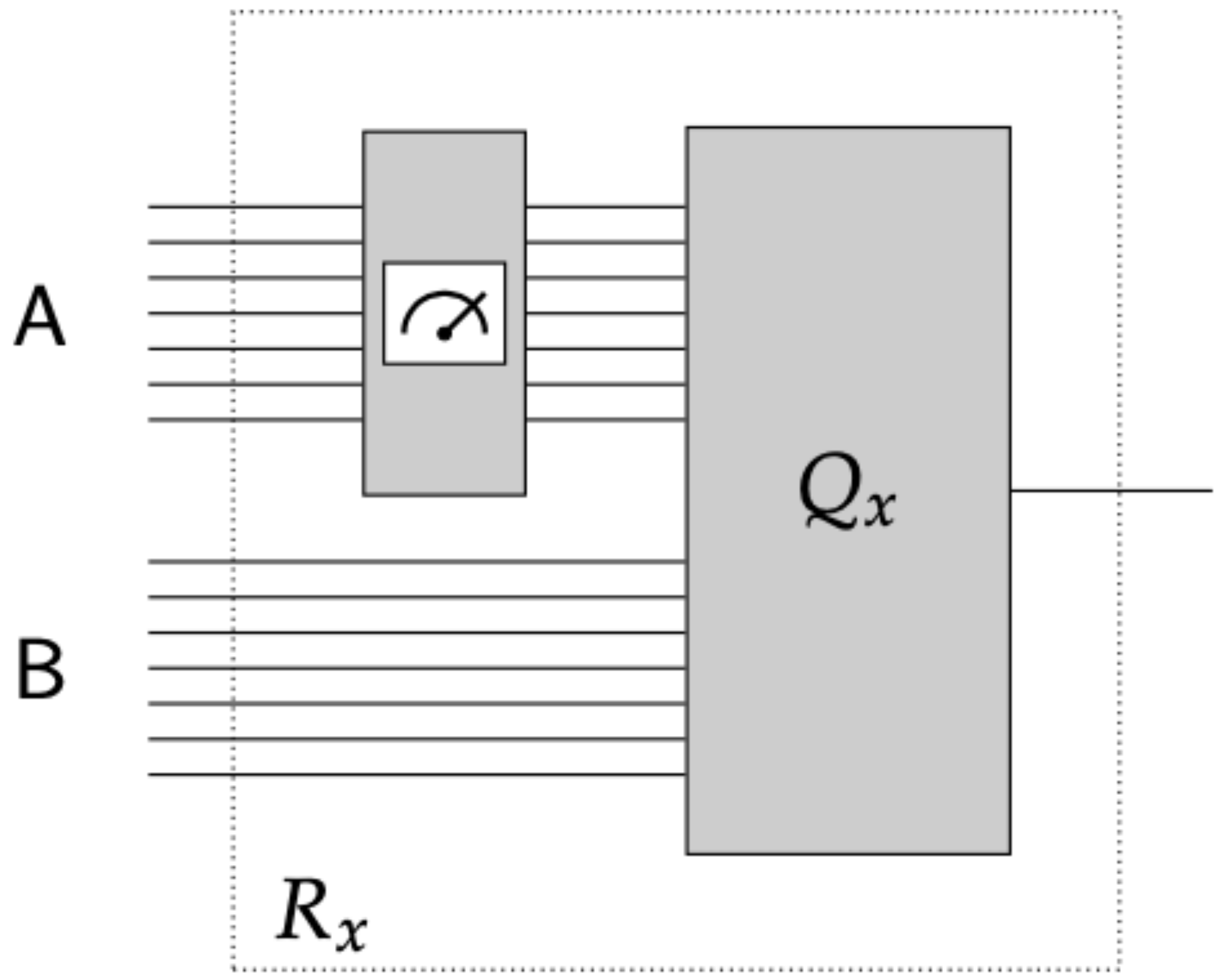
$$x \in A_{\text{yes}} \Rightarrow \left\{ y \in \Sigma^p : \langle x, y \rangle \in B \right\} \neq \varnothing,$$
$$x \in A_{\text{no}} \Rightarrow \left\{ y \in \Sigma^p : \langle x, y \rangle \in B \right\} = \varnothing.$$

$$\mathrm{CQRG}(1) \subseteq \exists \cdot \mathrm{PP}$$

Existence of a polynomial length string.
Use the matrix bound of Tool 1 + probabilistic method.

Existence of a PP language.
Use Tool 2.

Setting things up…



Observation: Alice is restricted to a classical strategy!

Let Alice send an optimal classical probability distribution “p” over

$y \in \Sigma^n$.

Define $$S_{x,y} = (\langle y| \otimes \mathbb{1}_{\mathcal{B}}) Q_x^* (|1\rangle\langle 1|) (|y\rangle \otimes \mathbb{1}_{\mathcal{B}})$$

Probability that Alice wins when Bob plays optimally: $$\lambda_{\min}\left(\sum_{y \in \Sigma^n} p(y) S_{x,y}\right)$$

Hurdle: “p” may not have a polynomial length description

Brief proof idea

Take $N = 72(m+2)$, where m is the number of Bob's qubits.
Consider an N-tuple of strings $\langle y_1, y_2, \ldots, y_N \rangle$ for $y_i \in \Sigma^n$.

Define a distribution "q" as follows:

$$q(y) = \frac{\left|\{j \in \{1,\ldots,N\} \,:\, y = y_j\}\right|}{N}$$

(Intuition: choose an index uniformly at random!)

By the matrix tail bound, there exists a "q" that is a good approximation to "p"!

"q" has a polynomial length description!

Probability Alice wins when she plays “q”:

$$\lambda_{\min}\left(\frac{S_{x,y_1} + \cdots + S_{x,y_N}}{N}\right)$$

Use second tool to get the PP language B!

Lemma 22. *Let $\{Q_x : x \in \Sigma^*\}$ be a polynomial-time generated family of quantum circuits, where each circuit Q_x takes as input a k-qubit register* Y *and an m-qubit register* B*, for polynomially bounded functions k and m, and outputs a single qubit. For each $x \in \Sigma^*$ and $y \in \Sigma^k$, define an operator*

$$S_{x,y} = (\langle y| \otimes \mathbb{1}_{\mathsf{B}})Q_x^*(|1\rangle\langle 1|)(|y\rangle \otimes \mathbb{1}_{\mathsf{B}}).$$

For every polynomially bounded function N, there exists a language $B \in \mathrm{PP}$ for which the following implications are true for all $x \in \Sigma^*$ and $y_1, \ldots, y_N \in \Sigma^k$:

$$\lambda_{min}\left(\frac{S_{x,y_1} + \cdots + S_{x,y_N}}{N}\right) \geq \frac{2}{3} \quad \Rightarrow \quad (x, y_1 \cdots y_N) \in B,$$

$$\lambda_{min}\left(\frac{S_{x,y_1} + \cdots + S_{x,y_N}}{N}\right) \leq \frac{1}{3} \quad \Rightarrow \quad (x, y_1 \cdots y_N) \notin B.$$

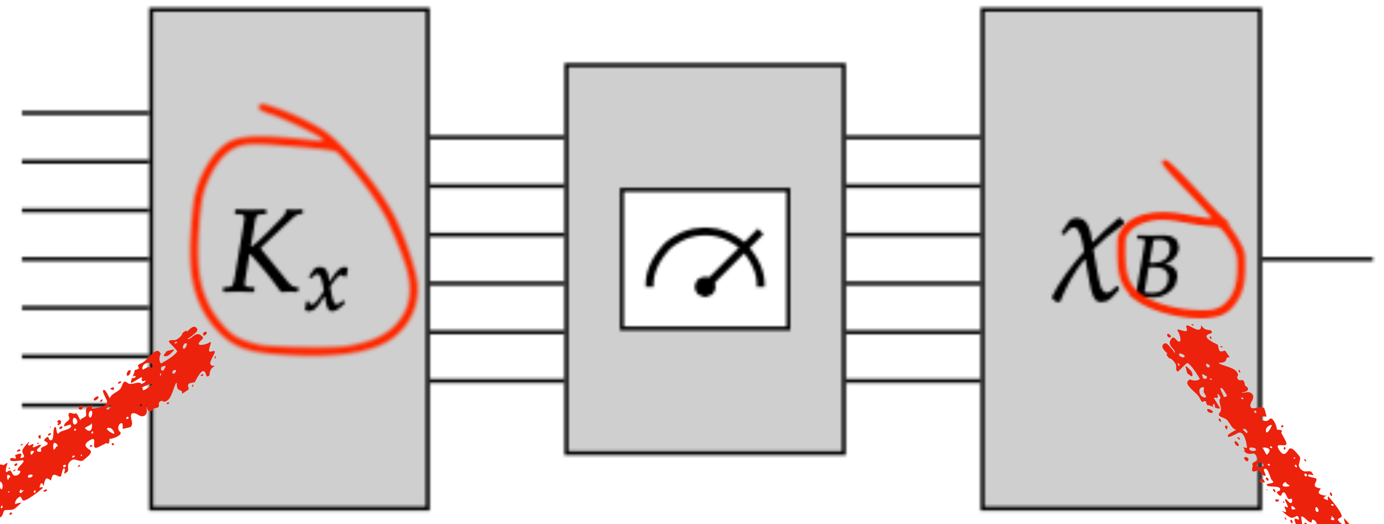
31

Combine the two (polynomial description + PP language), and we have our proof

Second result: $\mathrm{MQRG}(1) \subseteq \mathrm{P} \cdot \mathrm{PP}$

We will prove:

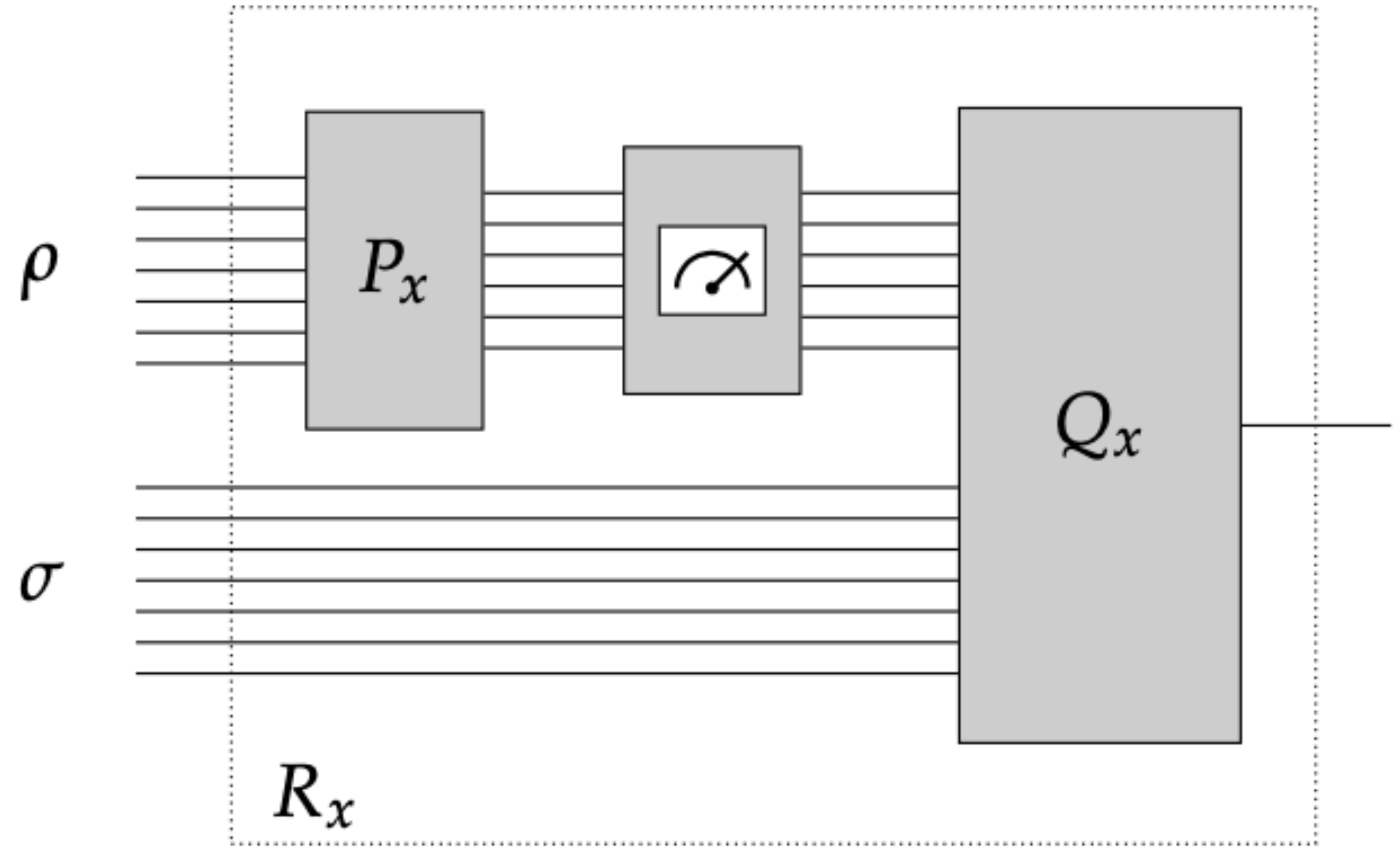
$\mathrm{MQRG}(1) \subseteq \mathrm{QMA} \cdot \mathrm{PP}$



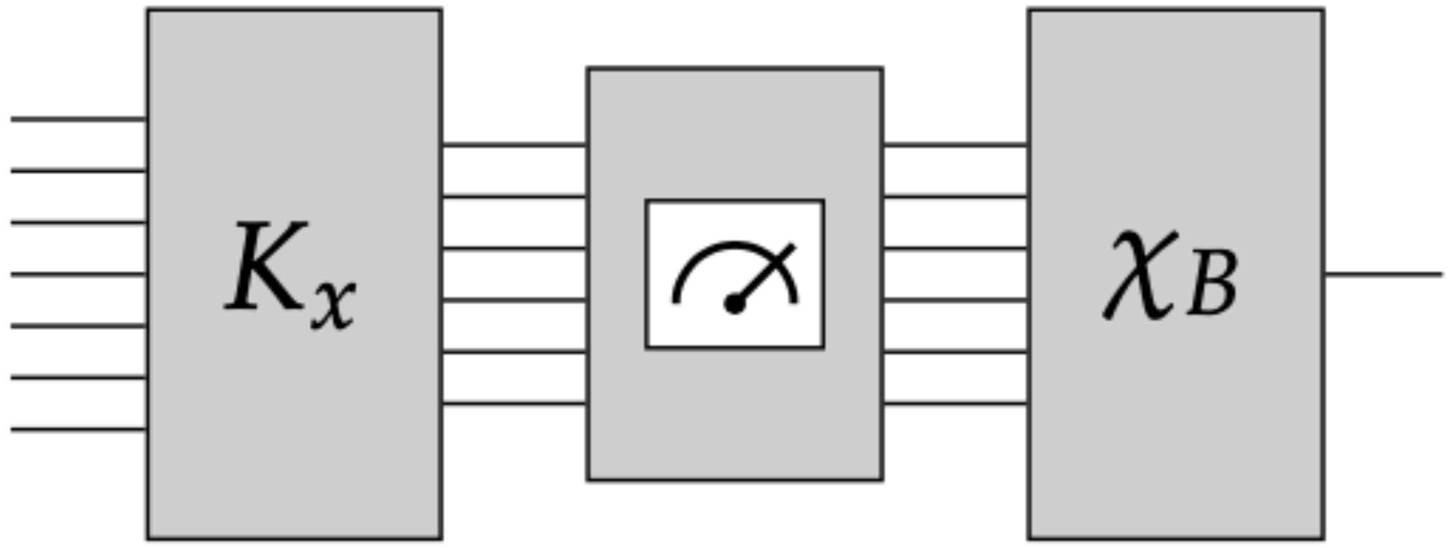
We will define this channel.
Justification uses the matrix tail bound from before.

Existence of PP language B.
Argued for same as before, using the “second” tool.

Setting things up



MQRG(1)



QMA.C

Define: $K_x = |x\rangle\langle x| \otimes P_x^{\otimes N}$

Assuming Bob plays optimally, the language B can be found the same way as before, by applying the “second” tool.

Proof outline

Take: $\xi = \rho^{\otimes N}$

Can prove using the matrix tail bound, similar to before.

It now suffices to prove:

Completeness. If it is the case that $x \in A_{\text{yes}}$, then there must exist a state $\xi \in \mathrm{D}(\mathcal{A}^{\otimes N})$ such that

$$\Pr(K_x(\xi) \in B) \geq \frac{2}{3}.$$

Soundness. If it is the case that $x \in A_{\text{no}}$, then for every state $\xi \in \mathrm{D}(\mathcal{A}^{\otimes N})$ it must be that

$$\Pr(K_x(\xi) \in B) \leq \frac{1}{3}.$$

Slightly more involved because there may be entanglement across N registers.
Proved using a conditional variant of Hoeffding's inequality.

Conclusion

$$\mathrm{CQRG}(1) \subseteq \exists \cdot \mathrm{PP}$$

Proved two containments.

$$\mathrm{MQRG}(1) \subseteq \mathrm{P} \cdot \mathrm{PP}$$

Future work:

1. Oracle separations. Is there an oracle separating PP/AWPP from QRG(1)?
2. Facts about QRG(1) where both provers are classical.
3. Is QRG(1) contained somewhere in the counting hierarchy?

Thank you!