Estimating and Interpreting Resource Measures via Quantum Algorithms

Mark M. Wilde

School of Electrical and Computer Engineering, Cornell University

Joint work with Margarite LaBorde and Soorya Rethinasamy

Available as arXiv:2105.12758

Quantum Resources Workshop, Singapore, December 2022

Collaborators

Margarite LaBorde

Soorya Rethinasamy

Motivation

- Symmetry plays a fundamental role in physics
- Applications include entanglement, thermodynamics, coherence, reference frames, metrology, etc.
- Common theme is that symmetric states are not useful, whereas asymmetric ones are
- Motivates the resource theory (RT) of asymmetry

Outline

- Goal: Devise quantum algorithms that test symmetry
- Outcomes:
  - 1) Operational meanings of fidelity resource monotones
  - 2) Tested performance using variational approach
  - 3) (Unexpected) Three new resource theories related to asymmetry

Overview of Results

Test	Algorithm	Acceptance Probability
G-Bose symmetry	1	$\max_{\sigma \in \text{B-Sym}_G} F(\rho, \sigma)$
G-symmetry	2	$\max_{\sigma \in \text{Sym}_G} F(\rho, \sigma)$
G-Bose symmetric extendibility	3	$\max_{\sigma \in \text{BSE}_G} F(\rho, \sigma)$
G-symmetric extendibility	4	$\max_{\sigma \in \text{SymExt}_G} F(\rho, \sigma)$

Preliminaries

- Let $\{U(g)\}_{g \in G}$ denote a unitary representation of a group G
- Let $\Pi^G \equiv \frac{1}{|G|} \sum_{g \in G} U(g)$ denote the group projection
- For systems A and B, we use $\{U_A(g)\}_{g \in G}$ and $\{V_B(g)\}_{g \in G}$ for unitary representations of G
- Corresponding projections are $\Pi_A^G \equiv \frac{1}{|G|} \sum_{g \in G} U_A(g)$ and $\Pi_B^G \equiv \frac{1}{|G|} \sum_{g \in G} V_B(g)$

Fidelity

- Fidelity of states ω and τ is a measure of their similarity

$$F(\omega,\tau) \equiv \left\| \sqrt{\omega}\sqrt{\tau} \right\|_1^2$$

- Equal to one iff $\omega = \tau$ and equal to zero iff $\omega \perp \tau$

- Data processing inequality: For a channel $\mathcal{N}$,

$$F(\omega,\tau) \le F(\mathcal{N}(\omega), \mathcal{N}(\tau))$$

- Uhlmann's theorem: $F(\omega,\tau) = \max_U |\langle \psi^\omega | U \otimes I | \psi^\tau \rangle|^2$

Warmup! RT of Bose Asymmetry - Statics

- A state σ is G-Bose symmetric if $\sigma = \Pi^G \sigma \Pi^G$
- Let BSym_G denote the set of Bose symmetric states:

$$\mathrm{BSym}_G \equiv \{\sigma : \sigma \in \text{States}, \sigma = \Pi^G \sigma \Pi^G\}$$

Measure of Bose Asymmetry

- Simple measure of Bose asymmetry for a state ρ:

$$\mathrm{Tr}[\Pi^G \rho]$$

- Observe that $\mathrm{Tr}[\Pi_G \rho] = 1$ if and only if ρ is G-Bose symmetric

- Theorem:

$$\mathrm{Tr}[\Pi^G \rho] = \max_{\sigma \in \mathrm{BSym}_G} F(\rho, \sigma)$$

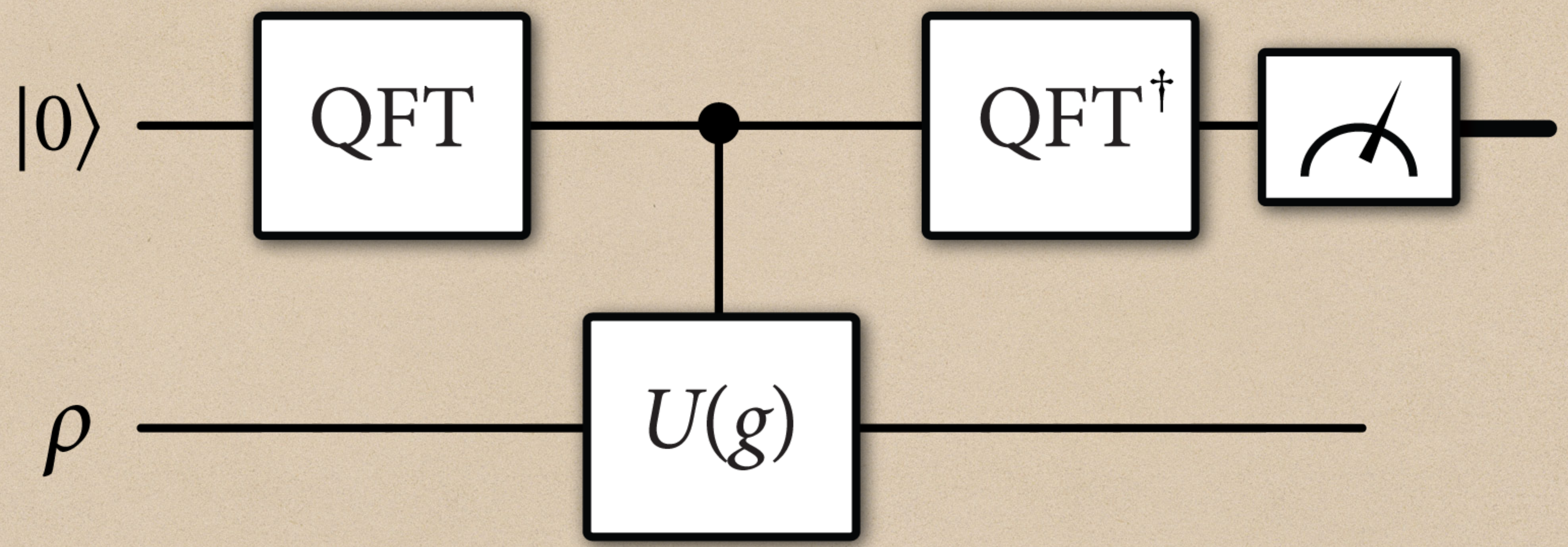
RT of Bose Asymmetry - Dynamics

- A channel $\mathcal{N}_{A\to B}$ is G-Bose symmetric if

$$(\mathcal{N}_{A\to B})^{\dagger}(\Pi_B^G) \geq \Pi_A^G$$

- Follows that $\mathcal{N}_{A\to B}(\sigma_A)$ is G-Bose symmetric if $\mathcal{N}_{A\to B}$ and σ_A are
- Conclude that $\mathrm{Tr}[\Pi^G \rho]$ is a resource monotone

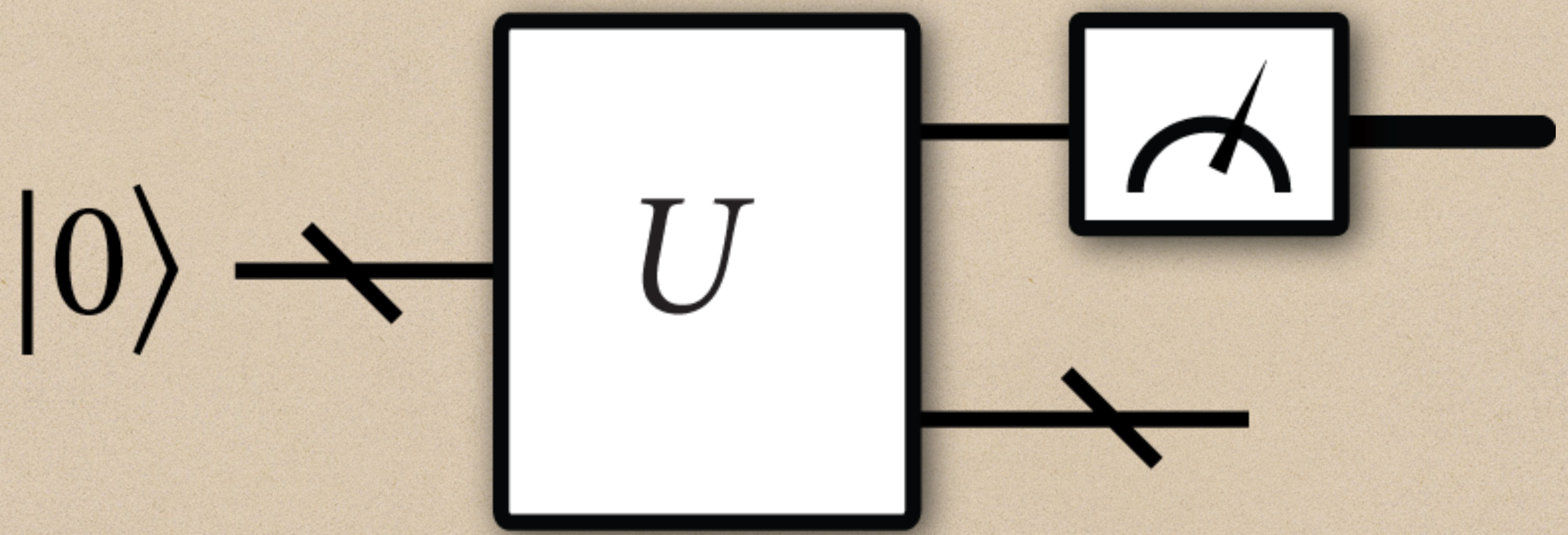
Algorithm for Testing G-Bose Symmetry



- Accept if measurement gives all zeros outcome
- Algorithm's acceptance probability $= \mathrm{Tr}[\Pi_G \rho]$
- Gives operational meaning to resource monotone $\mathrm{Tr}[\Pi^G \rho]$

BQP in a Nutshell

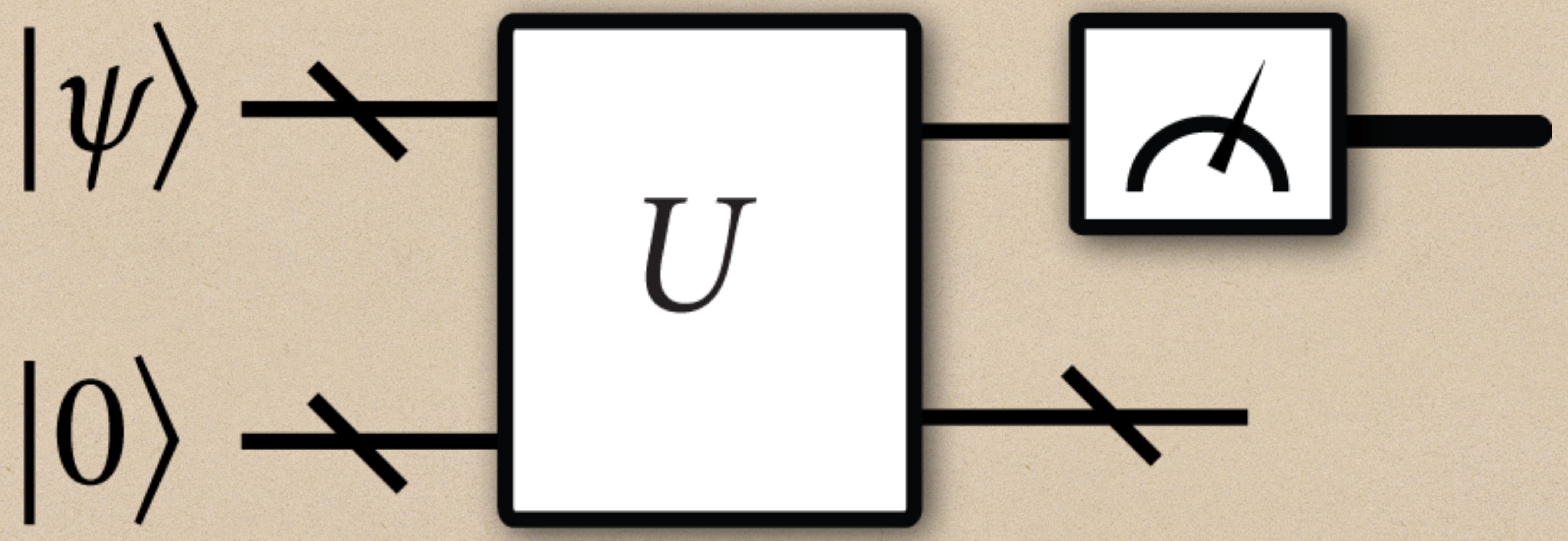
- BQP stands for "bounded error quantum polynomial time"
- Problems that are efficiently decidable by a quantum computer



- The world is now spending billions based on the P $\subsetneq$ BQP belief

QMA in a Nutshell

- QMA stands for "quantum Merlin Arthur"
- Problems believed to be hard for a quantum computer to decide

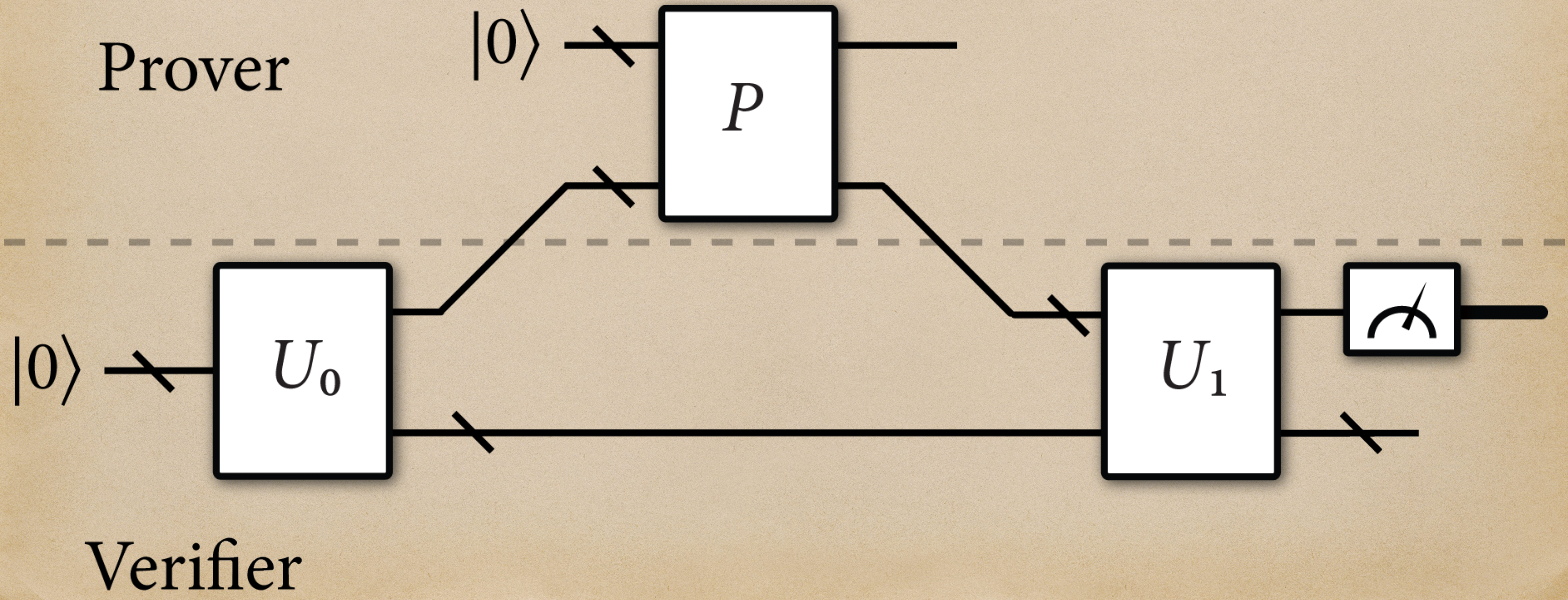


- Model is that $|\psi\rangle$ is a state that is difficult to prepare on a quantum computer
- Assumption: quantum prover with unbounded computational resources prepares $|\psi\rangle$

Quantum Interactive Proofs (QIP)

- Perspective: QMA is a communication protocol in which the prover sends a quantum message to the verifier
- BQP involves no messages sent from the prover to the verifier
- Taking this concept further, allow for prover and verifier to exchange more messages (called "quantum interactive proof")
- Interaction can allow for solving more difficult problems, i.e., an omniscient but untrustworthy teacher ("dancing with the devil")

QIP(2) - Two Messages Exchanged

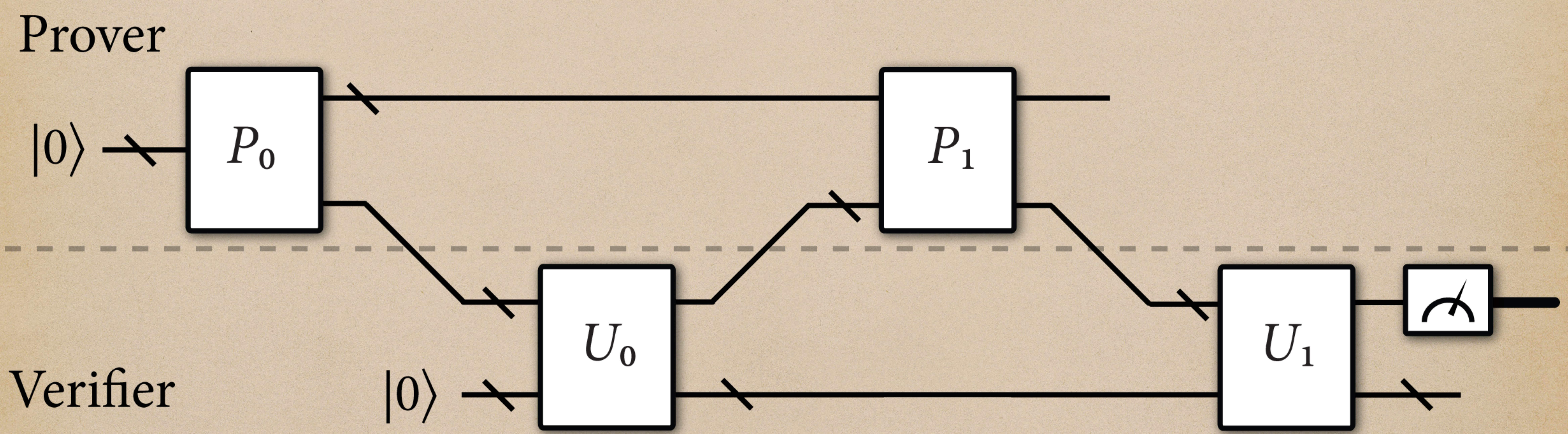


QIP(2)-Complete Problem

- Given circuits to realize a channel $\mathcal{N}$ and a state ρ, estimate

$$\max_{\sigma \in \text{States}} F(\rho, \mathcal{N}(\sigma))$$

QIP(3) - Three Messages Exchanged



QIP(3)-Complete Problem

- Given circuits to realize quantum channels $\mathcal{N}$ and $\mathcal{M}$, estimate

$$\max_{\rho,\sigma \in \text{States}} F(\mathcal{N}(\rho), \mathcal{M}(\sigma))$$

RT of Asymmetry - Statics

- A state ρ is G-symmetric if $[U(g), \rho] = 0$ for all $g \in G$
- Equivalently, ρ is G-symmetric if $\rho = U(g)\rho U(g)^\dagger$ for all $g \in G$

  or if $\rho = \mathcal{T}_G(\rho)$ where the twirl channel is defined as

$$\mathcal{T}_G(\,\cdot\,) \equiv \frac{1}{|G|} \sum_{g \in G} U(g)(\,\cdot\,)U(g)^\dagger$$

- Let Sym denote the set of G-symmetric states:

$$\text{Sym} \equiv \{\sigma : \sigma \in \text{States},\ \sigma = \mathcal{T}_G(\sigma)\}$$

RT of Asymmetry - Dynamics

- A channel $\mathcal{N}_{A\to B}$ is G-symmetric if

$$\mathcal{N}_{A\to B} \circ \mathcal{U}_A(g) = \mathcal{V}_B(g) \circ \mathcal{N}_{A\to B} \quad \forall g \in G$$

- Follows that $\mathcal{N}_{A\to B}(\sigma_A)$ is G-symmetric if $\mathcal{N}_{A\to B}$ and σ_A are
- Conclude that $\max_{\sigma \in \mathrm{Sym}_G} F(\rho, \sigma)$ is a resource monotone

G-Symmetric Purifications

- Theorem: If ρ is G-symmetric, $\exists$ a purification ψ_G^ρ that is G-Bose symmetric, i.e., satisfying

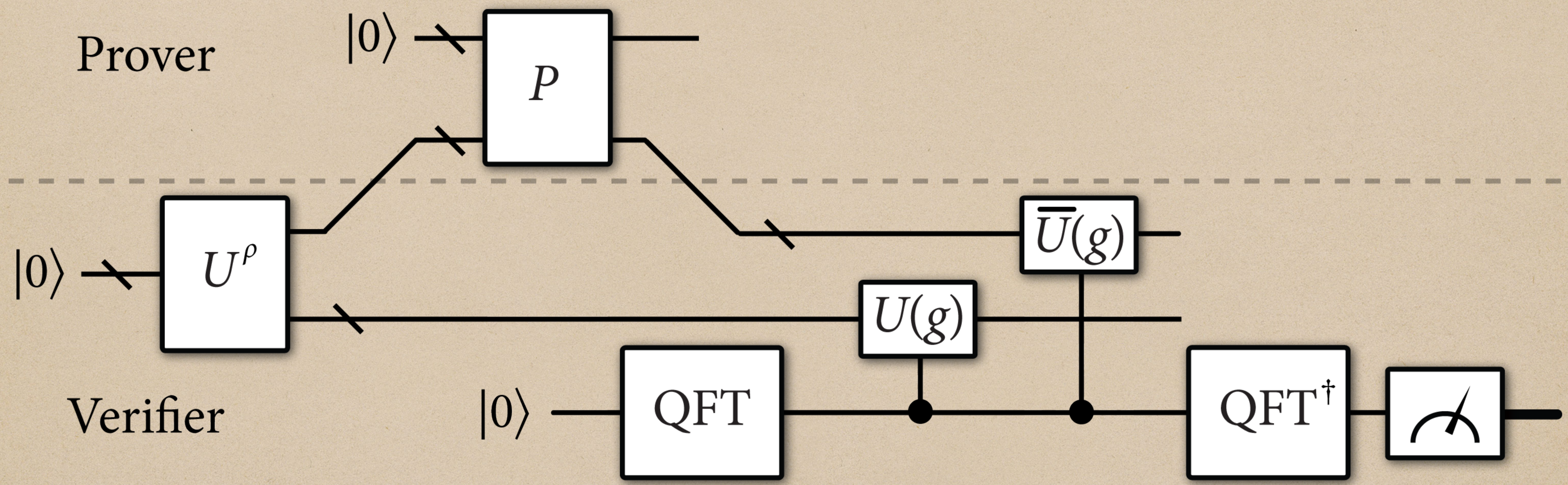
$$|\psi_G^\rho\rangle = \overline{U}(g) \otimes U(g) |\psi_G^\rho\rangle \quad \forall g \in G$$

- Thus, if ρ is G-symmetric, $\exists$ unitary P such that $|\psi_G^\rho\rangle = P \otimes I |\psi^\rho\rangle$

G-Symmetry Testing

- Suppose ∃ a quantum circuit that prepares a purification ψ^ρ of ρ
- Idea: Send the purifying system to the prover, and then do a test to check for G-Bose symmetry of the resulting state

G-Symmetry Testing in QIP(2)



- Theorem: Acceptance probability equals max. sym. fidelity:

$$\max_{P_{S'E\to\hat{S}E'}} \left\| \Pi^G_{S\hat{S}} P_{S'E\to\hat{S}E'} |\psi^\rho\rangle_{S'S} |0\rangle_E \right\|_2^2 = \max_{\sigma\in\mathrm{Sym}_G} F(\rho,\sigma)$$

Two Other Resource Theories

- RT of Bose asymmetric unextendibility
- RT of asymmetric unextendibility

(*k*-Bose-unextendibility and *k*-unextendibility are special cases)

RT of Bose Asymmetric Unextendibility - Statics

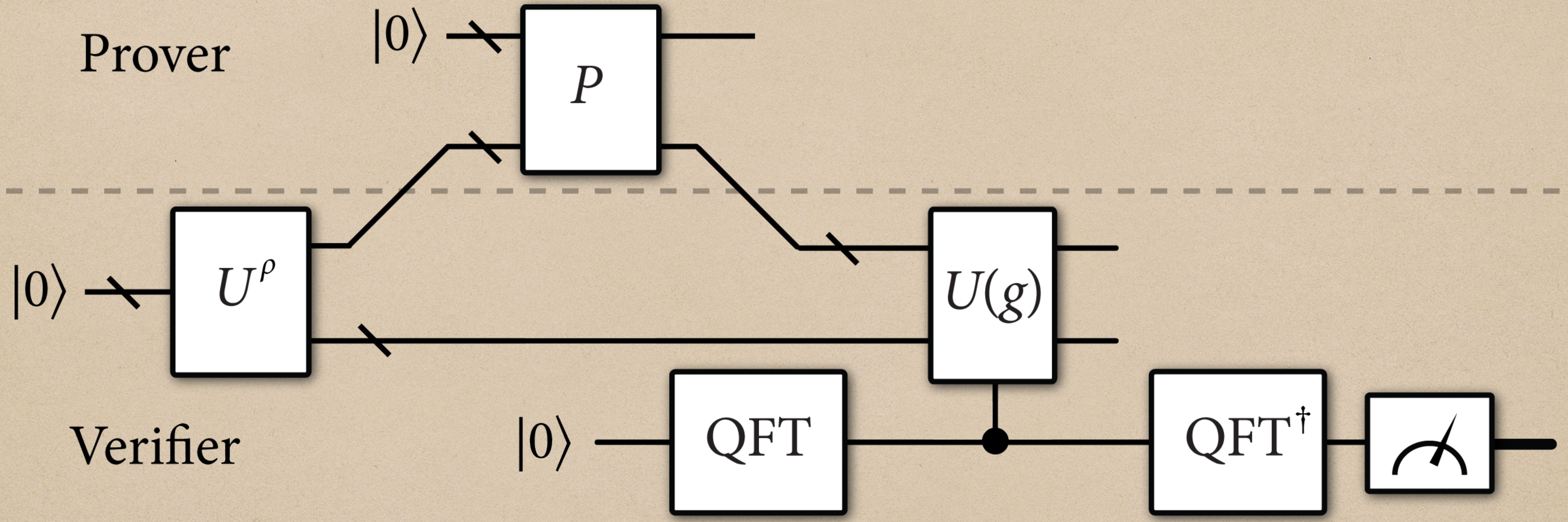
- A state σ_S is Bose-symmetric extendible if
  - $\exists$ a state ω_{RS} such that $\mathrm{Tr}_R[\omega_{RS}] = \sigma_S$
  - $\omega_{RS} = \Pi^G_{RS}\omega_{RS}\Pi^G_{RS}$ where $\Pi^G_{RS} \equiv \dfrac{1}{|G|}\sum_{g\in G} U_{RS}(g)$
- Let BSE_G denote the set of Bose symmetric extendible states:

$$\mathrm{BSE}_G \equiv \left\{\sigma_S : \exists \omega_{RS} \in \mathrm{States}, \mathrm{Tr}_R[\omega_{RS}] = \sigma_S, \omega_{RS} = \Pi^G_{RS}\omega_{RS}\Pi^G_{RS}\right\}$$

RT of Bose Asymmetric Unextendibility - Dynamics

- A channel $\mathcal{N}_{S\to S'}$ is Bose-symmetric extendible if
  - $\exists$ a channel $\mathcal{M}_{RS\to R'S'}$ such that $\mathrm{Tr}_{R'} \circ \mathcal{M}_{RS\to R'S'} = \mathcal{N}_{S\to S'} \circ \mathrm{Tr}_R$
  - $\mathcal{M}_{RS\to R'S'}$ is Bose symmetric: $(\mathcal{M}_{RS\to R'S'})^\dagger(\Pi^G_{R'S'}) \geq \Pi^G_{RS}$
- Golden rule holds: $\mathcal{N}_{S\to S'}(\sigma_S)$ is BSE if $\mathcal{N}_{S\to S'}$ and σ_S are

G-BSE Testing in QIP(2)



- Theorem: Acceptance probability equals max. sym. fidelity:

$$\max_{P_{S'E\to RE'}} \left\| \Pi^G_{RS} P_{S'E\to RE'} |\psi\rangle_{S'S} |0\rangle_E \right\|_2^2 = \max_{\sigma\in \mathrm{BSE}_G} F(\rho,\sigma)$$

RT of Asymmetric Unextendibility - Statics

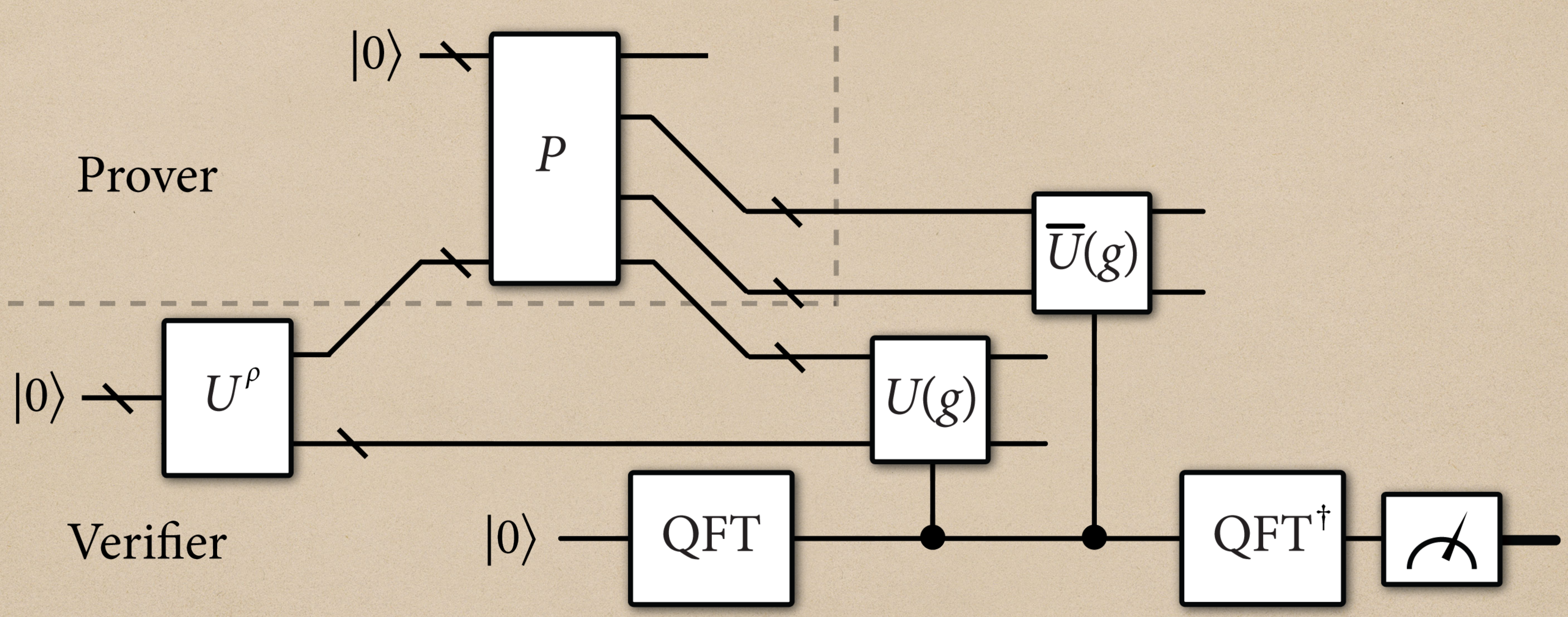
- A state σ_S is symmetric extendible if
  - $\exists$ a state ω_{RS} such that $\mathrm{Tr}_R[\omega_{RS}] = \sigma_S$
  - $\omega_{RS} = U_{RS}(g)\omega_{RS}U_{RS}(g)^\dagger \quad \forall g \in G$
- Let SymExt_G denote the set of symmetric extendible states:

$$\mathrm{SymExt}_G \equiv \left\{\sigma_S : \exists\omega_{RS} \in \mathrm{States}, \mathrm{Tr}_R[\omega_{RS}] = \sigma_S, \omega_{RS} = \mathcal{T}^G_{RS}(\omega_{RS})\right\}$$

RT of Asymmetric Unextendibility - Dynamics

- A channel $\mathcal{N}_{S\to S'}$ is symmetric extendible if
  - $\exists$ a channel $\mathcal{M}_{RS\to R'S'}$ such that $\mathrm{Tr}_{R'} \circ \mathcal{M}_{RS\to R'S'} = \mathcal{N}_{S\to S'} \circ \mathrm{Tr}_R$
  - $\mathcal{M}_{RS\to R'S'}$ is symmetric:
    $\mathcal{M}_{RS\to R'S'} \circ \mathcal{U}_{RS}(g) = \mathcal{V}_{R'S'}(g) \circ \mathcal{M}_{RS\to R'S'} \quad \forall g \in G$
- Golden rule holds: $\mathcal{N}_{S\to S'}(\sigma_S)$ is sym. ext. if $\mathcal{N}_{S\to S'}$ and σ_S are

G-SE Testing in QIP(2)



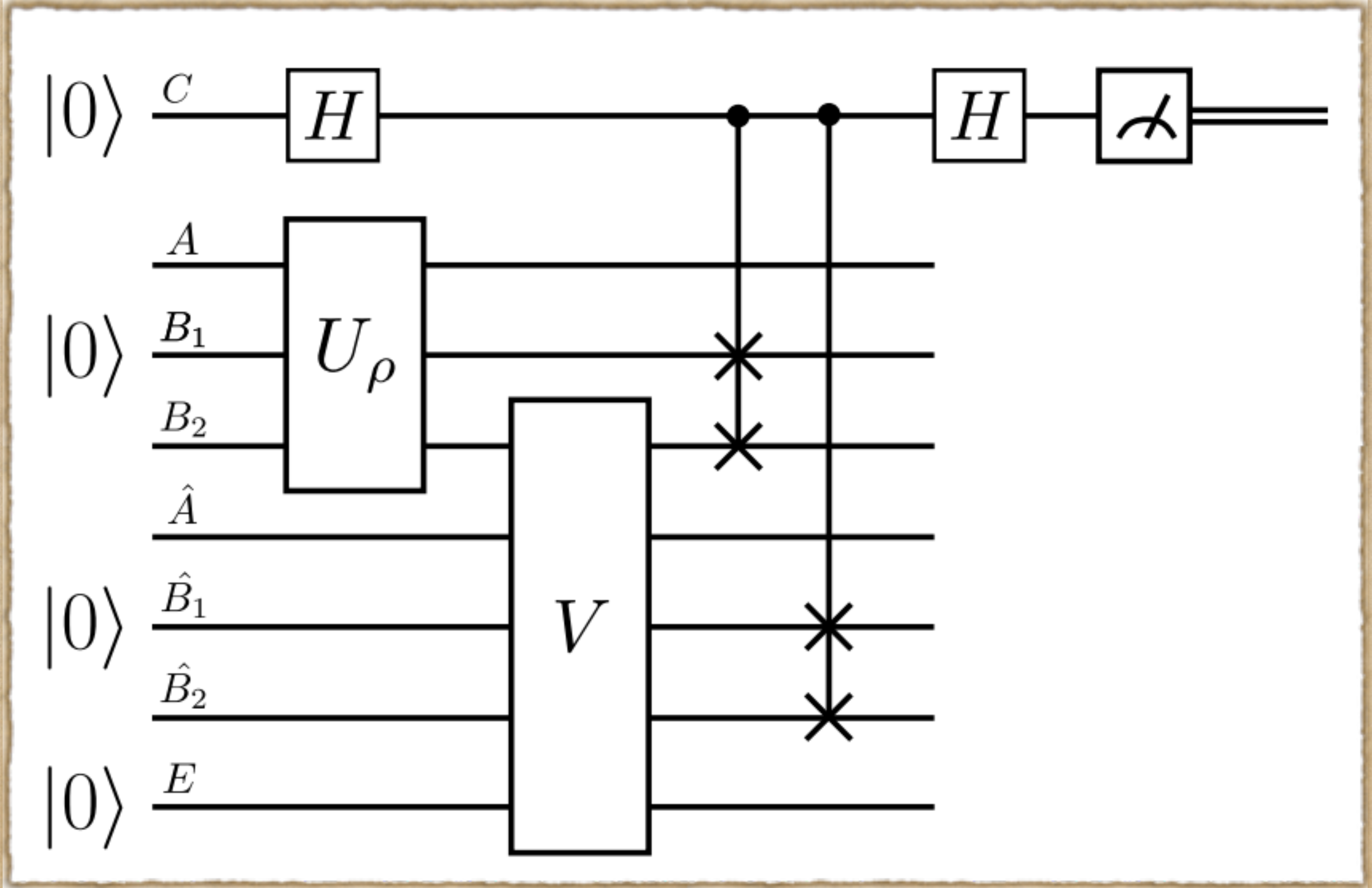
- Theorem: Acceptance probability equals max. sym. fidelity:

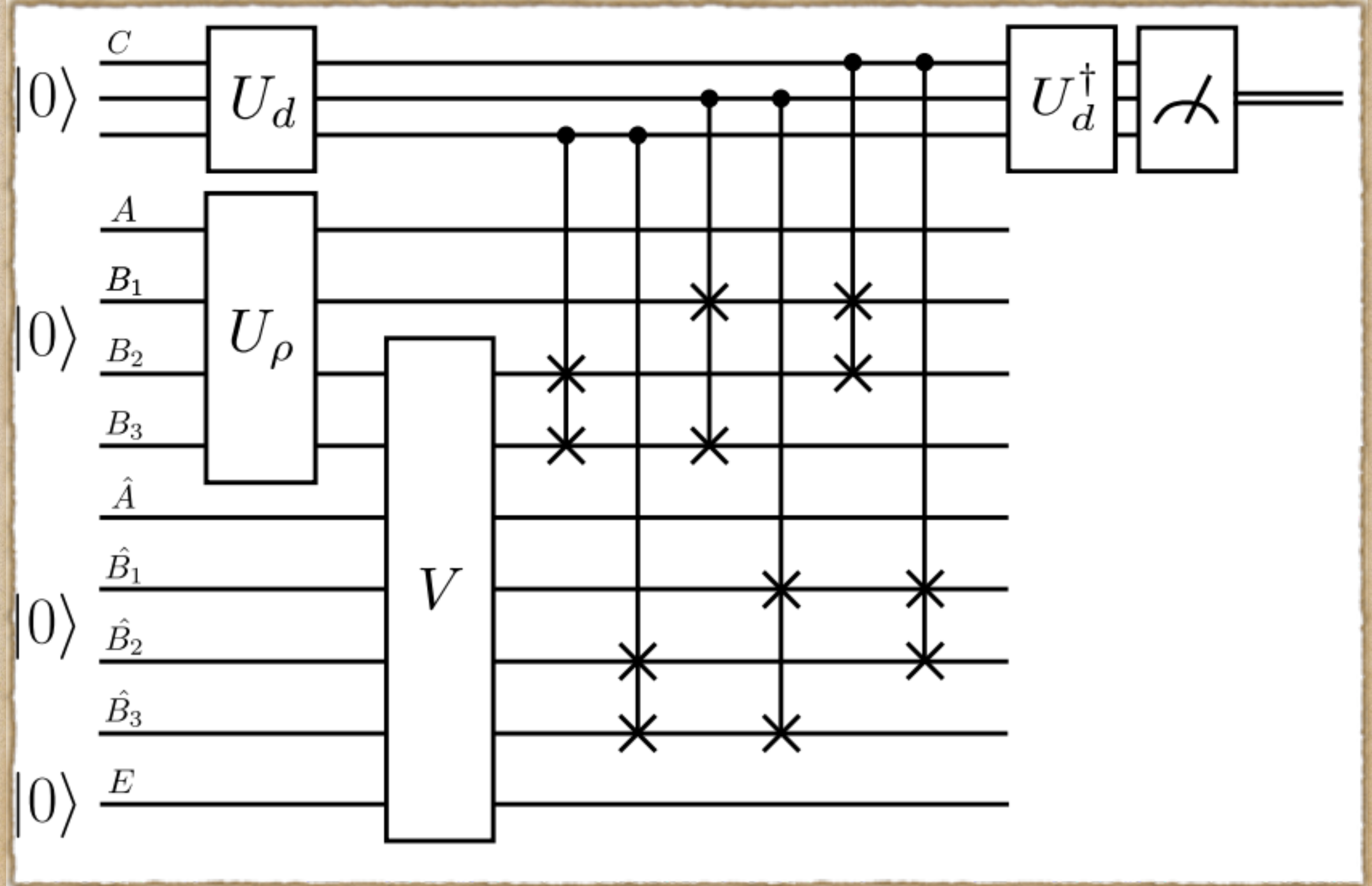
$$\max_{P_{S'E\to R\hat{R}\hat{S}E'}} \left\| \Pi^G_{RS\hat{R}\hat{S}} P_{S'E\to R\hat{R}\hat{S}E'} |\psi\rangle_{S'S} |0\rangle_E \right\|_2^2 = \max_{\sigma\in \mathrm{SymExt}_G} F(\rho,\sigma)$$

Variational Algorithms for Symmetry Testing

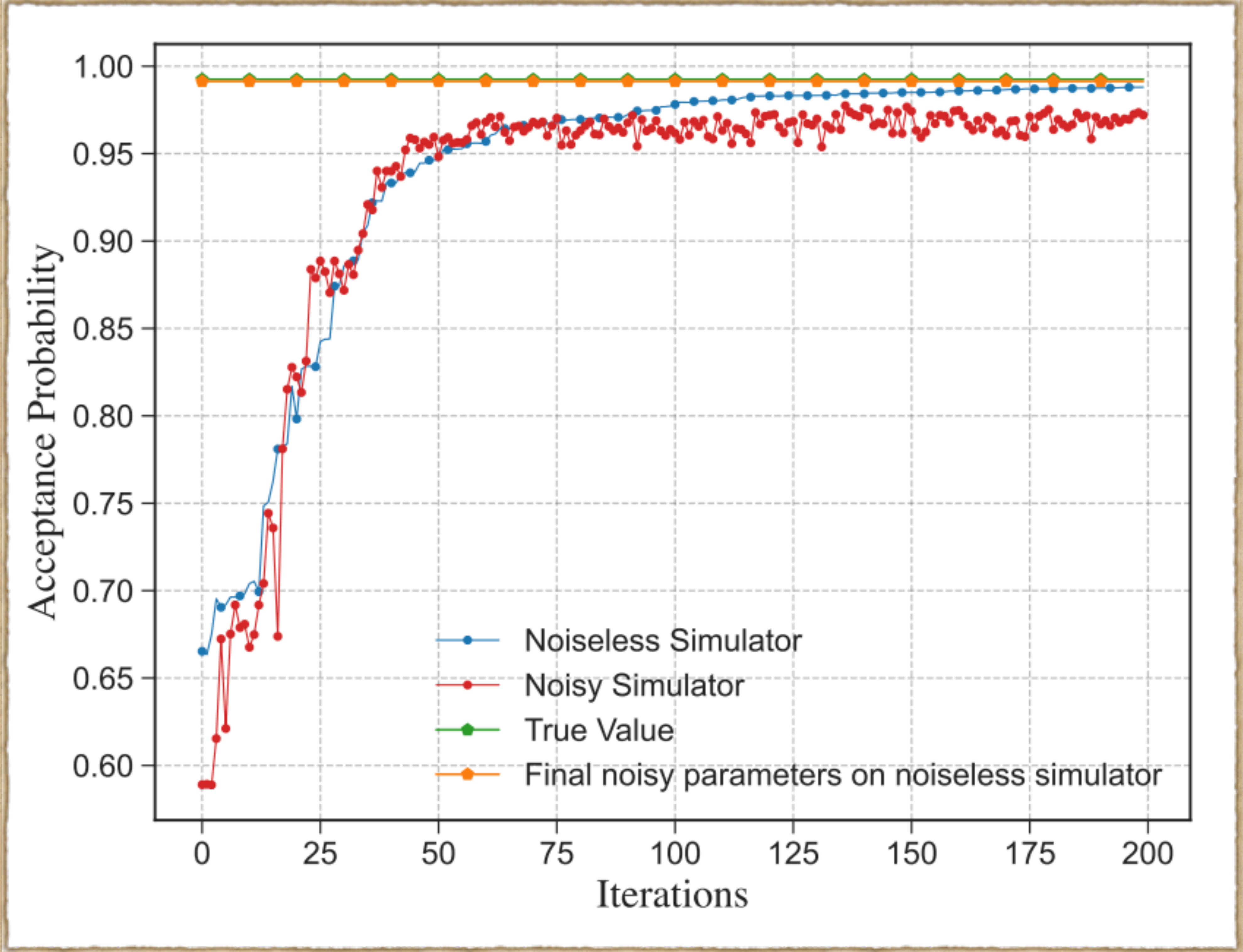
- idea: replace prover with a parameterized circuit and use a hybrid classical-quantum approach to estimate acceptance probability

- Examples of testing two- and three-extendibility

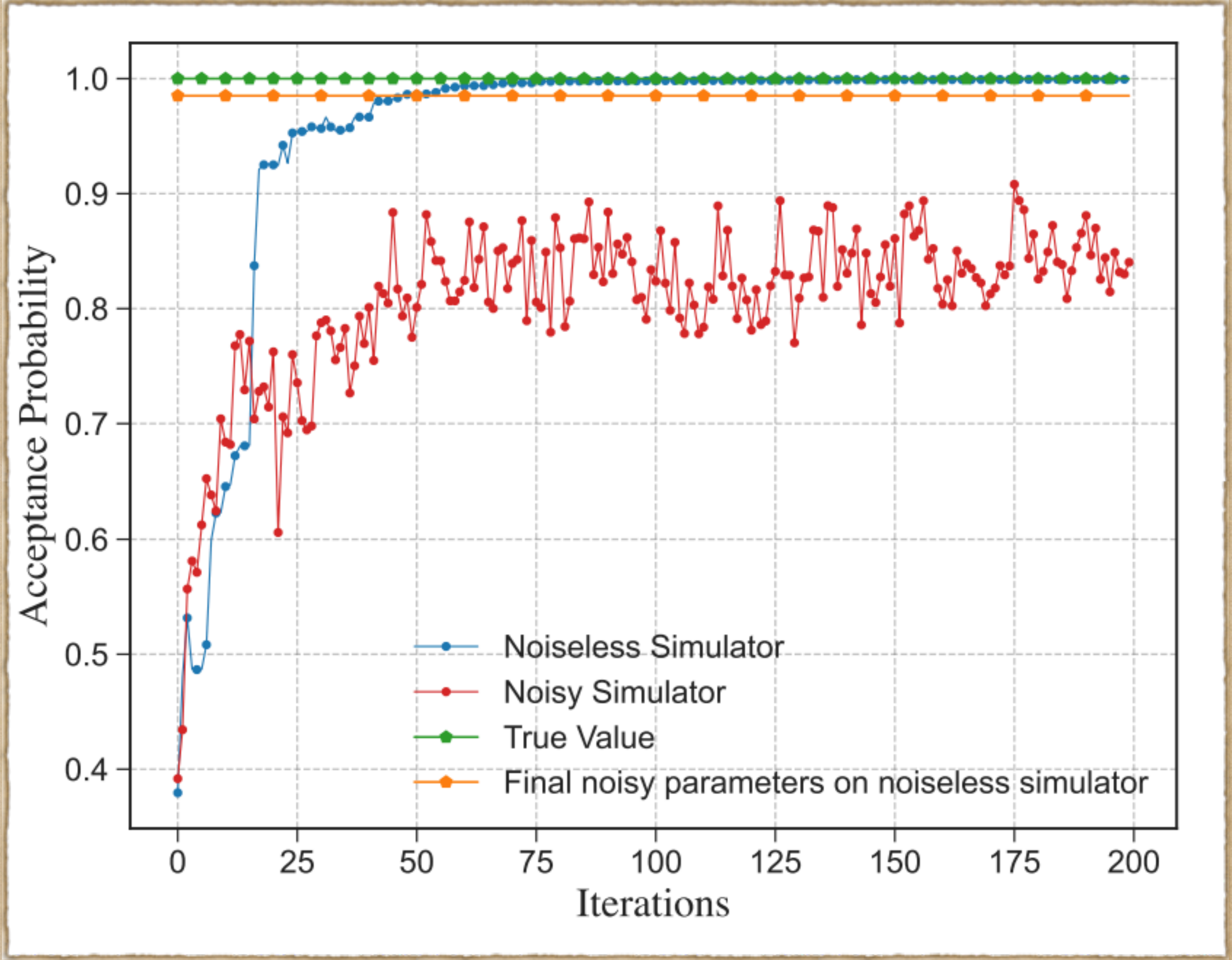




Performance of Variational Algorithms



two-extendibility



three-extendibility

In each case, tested a separable state

Summary

Test	Algorithm	Acceptance Probability
G-Bose symmetry	1	$\max_{\sigma \in \text{B-Sym}_G} F(\rho, \sigma)$
G-symmetry	2	$\max_{\sigma \in \text{Sym}_G} F(\rho, \sigma)$
G-Bose symmetric extendibility	3	$\max_{\sigma \in \text{BSE}_G} F(\rho, \sigma)$
G-symmetric extendibility	4	$\max_{\sigma \in \text{SymExt}_G} F(\rho, \sigma)$

Outlook

- Would like to implement larger instances of algorithms on existing quantum computers
- Would like to modify these algorithms to learn symmetries
- Estimate other resource measures?
- Can we incorporate catalysts, correlated catalysts, marginal catalysts, analystic catalysts, masochistic catalysts, activistic catalysts, panelists of catalysts? :)