ON THE ADDITIVE AND MULTIPLICATIVE ADVERSARY METHODS

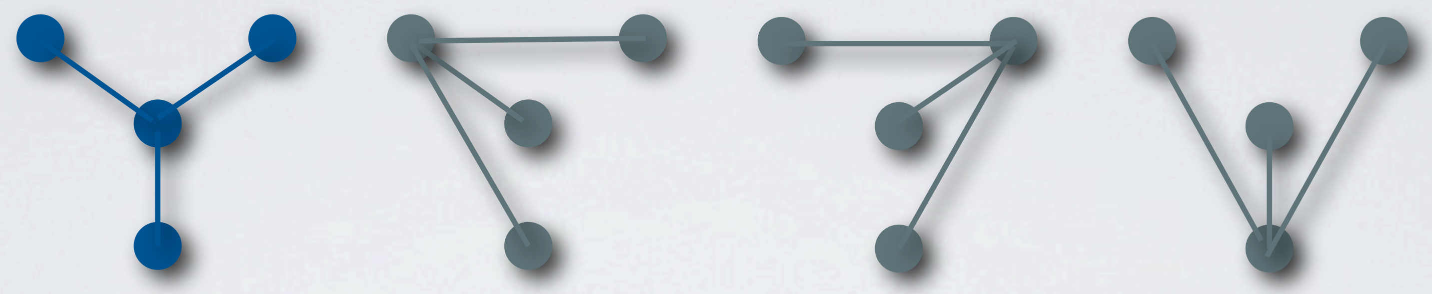
L. Magnin (U. Paris 11, U. Brussels, NEC Labs)
M. Roetteler (NEC Labs)
J. Roland (NEC Labs)

QIP'11, Singapore, 1.11.11

QUANTUM STATE GENERATION

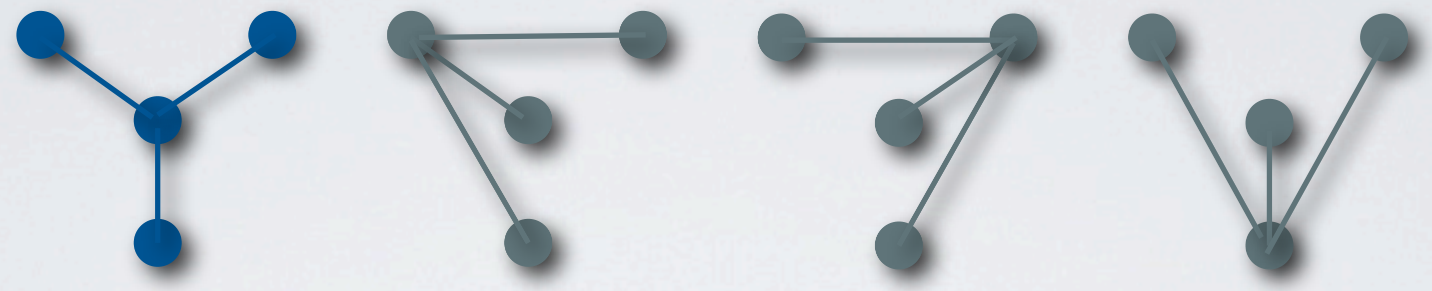
[Folklore] One way to solve Graph Isomorphism

Create the uniform superposition on permuted graphs



Example: $$\frac{1}{\sqrt{N!}} \sum_{\pi \in S_N} |G^{\pi}\rangle$$

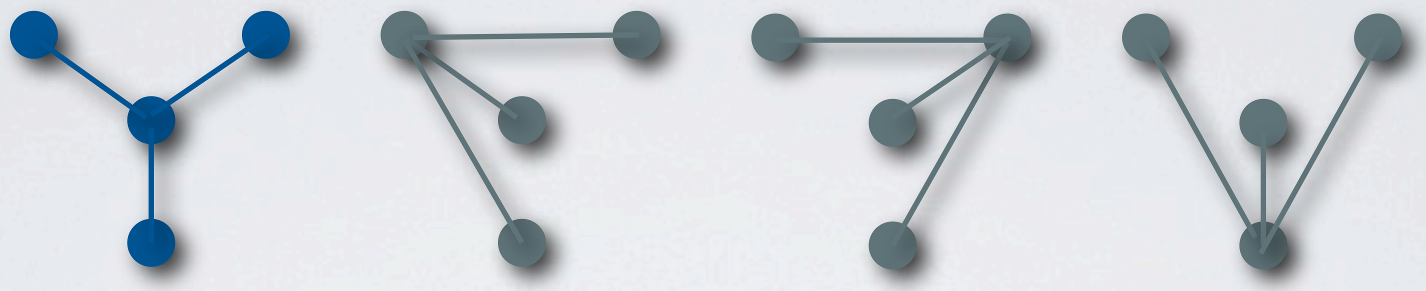
[Folklore] One way to solve Graph Isomorphism
Create the uniform superposition on permuted graphs



Example: $\frac{1}{\sqrt{N!}} \sum_{\pi \in S_N} |G^\pi\rangle$ Easy to do: $\frac{1}{\sqrt{N!}} \sum_{\pi \in S_N} |\pi\rangle|G^\pi\rangle$

QUANTUM STATE GENERATION

[Folklore] One way to solve Graph Isomorphism
Create the uniform superposition on permuted graphs



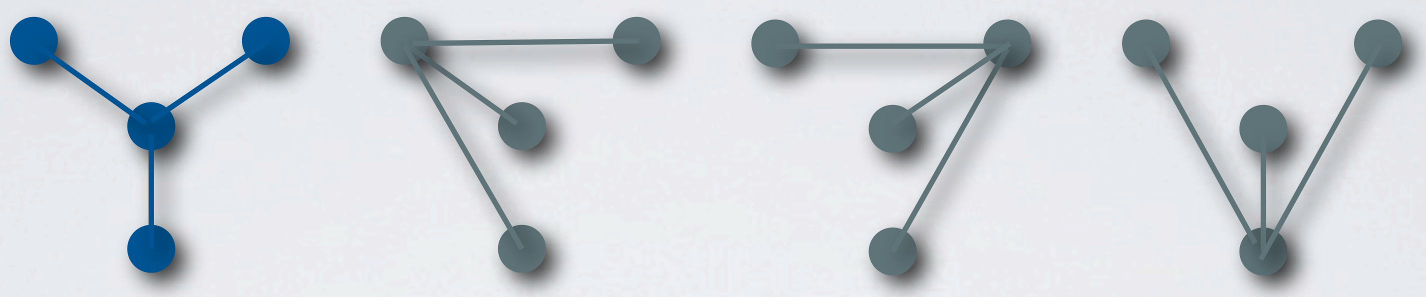
Example: $\frac{1}{\sqrt{N!}} \sum_{\pi \in S_N} |G^\pi\rangle$ Easy to do: $\frac{1}{\sqrt{N!}} \sum_{\pi \in S_N} |\pi\rangle |G^\pi\rangle$

Time Complexity?

- Open question (exponential upper bound)
- Let's try something simpler: query complexity

QUANTUM STATE GENERATION

[Folklore] One way to solve Graph Isomorphism
Create the uniform superposition on permuted graphs



Example: $\frac{1}{\sqrt{N!}} \sum_{\pi \in S_N} |G^\pi\rangle$ Easy to do: $\frac{1}{\sqrt{N!}} \sum_{\pi \in S_N} |\pi\rangle |G^\pi\rangle$

Time Complexity?

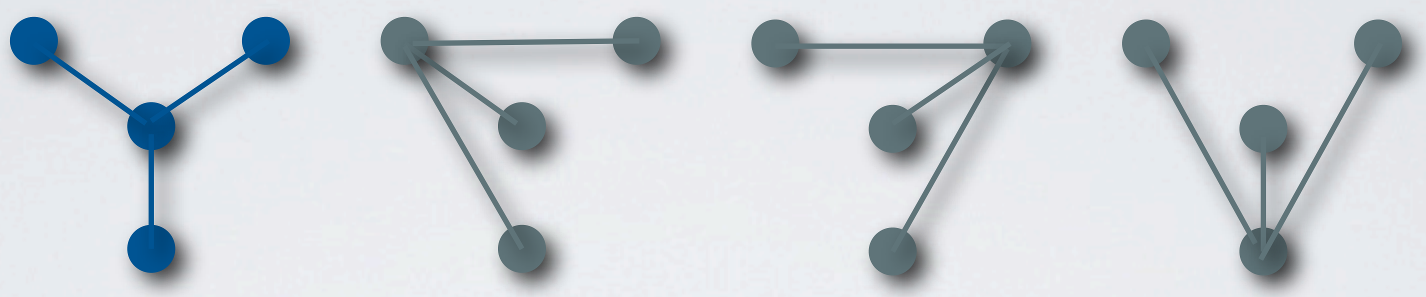
- Open question (exponential upper bound)
- Let's try something simpler: query complexity

f injective $[N] \to [M]$

$$\frac{1}{\sqrt{N}} \sum_{x \in [N]} |f(x)\rangle \qquad\qquad \frac{1}{\sqrt{N}} \sum_{x \in [N]} |x\rangle |f(x)\rangle$$

QUANTUM STATE GENERATION

[Folklore] One way to solve Graph Isomorphism
Create the uniform superposition on permuted graphs



Example: $\frac{1}{\sqrt{N!}} \sum_{\pi \in S_N} |G^\pi\rangle$ Easy to do: $\frac{1}{\sqrt{N!}} \sum_{\pi \in S_N} |\pi\rangle|G^\pi\rangle$

Time Complexity?

- Open question (exponential upper bound)
- Let's try something simpler: query complexity

INDEX ERASURE PROBLEM [Shi'02]

Given an injective function $f : [N] \longrightarrow [M]$ as an oracle
create the state $|\psi_f^{\odot}\rangle = \frac{1}{\sqrt{N}} \sum_{x \in [N]} |f(x)\rangle$

QUERY COMPLEXITY

QUANTUM STATE GENERATION PROBLEM

Given a function $f \in F$ as an oracle $O_f : |x\rangle|s\rangle \mapsto |x\rangle|f(x) \oplus s\rangle$ create a state ε-close to a target state $|\psi_f^{\odot}\rangle$

$Q_\varepsilon(\psi)$ Minimal number of queries that solve the problem over all algorithms.

QUANTUM PROBLEMS

Example: Index Erasure

CLASSICAL PROBLEMS (Tutorial by Ben Reichardt)

Creating $|\psi_f\rangle$ is computing a function

Example: search $\psi_f = \bigoplus_i f(x_i)$

QUERY COMPLEXITY

QUANTUM STATE GENERATION PROBLEM

Given a function $f \in F$ as an oracle $O_f : |x\rangle|s\rangle \mapsto |x\rangle|f(x) \oplus s\rangle$ create a state ε-close to a target state $|\psi_f^{\odot}\rangle$

$Q_\varepsilon(\psi)$ Minimal number of queries that solve the problem over all algorithms.

NEW

joint work with Ambainis

Complexity $\Theta(\sqrt{N})$

QUANTUM PROBLEMS

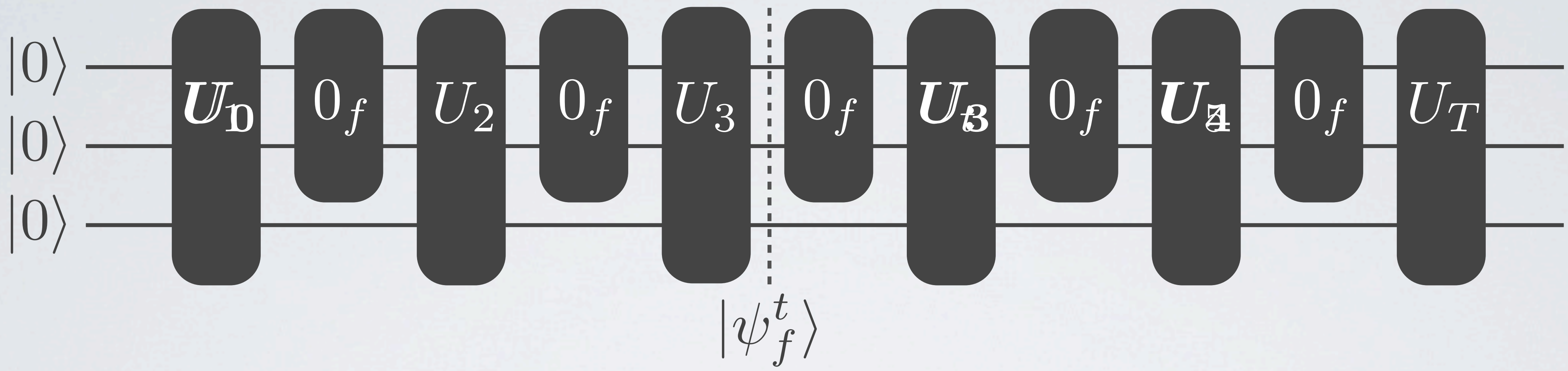
Example: Index Erasure

CLASSICAL PROBLEMS (Tutorial by Ben Reichardt)

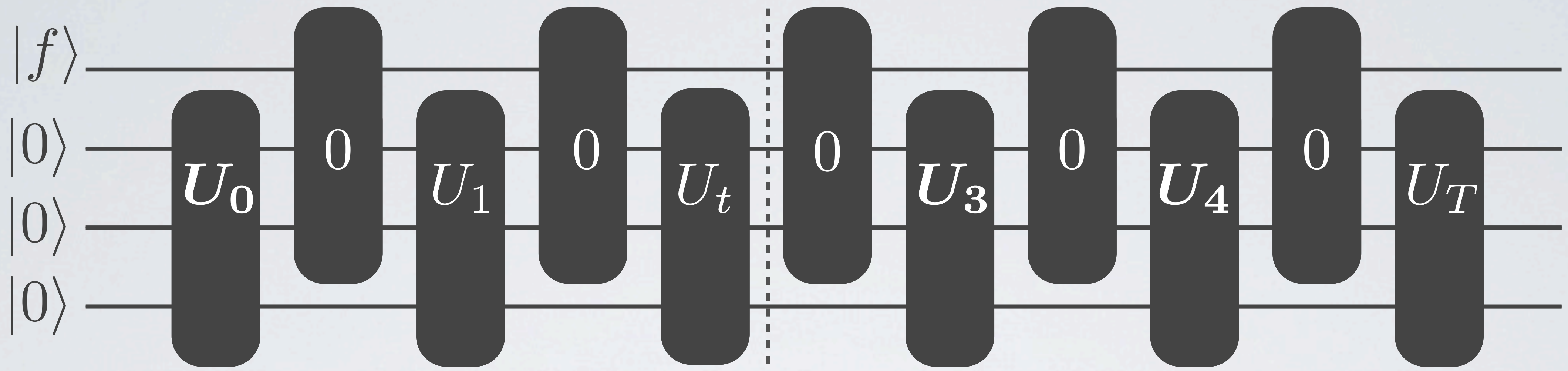
Creating $|\psi_f\rangle$ is computing a function

Example: search $\psi_f = \bigoplus_i f(x_i)$

PRINCIPLES BEHIND THE ADVERSARY METHODS



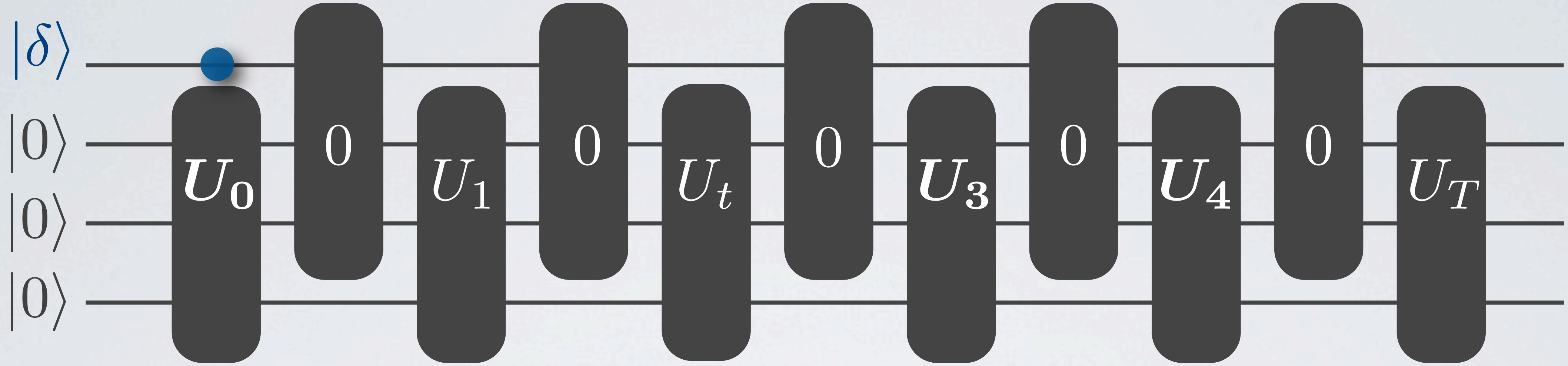
PRINCIPLES BEHIND THE ADVERSARY METHODS



$$|\Psi_f^t\rangle = |f\rangle|\psi_f^t\rangle$$

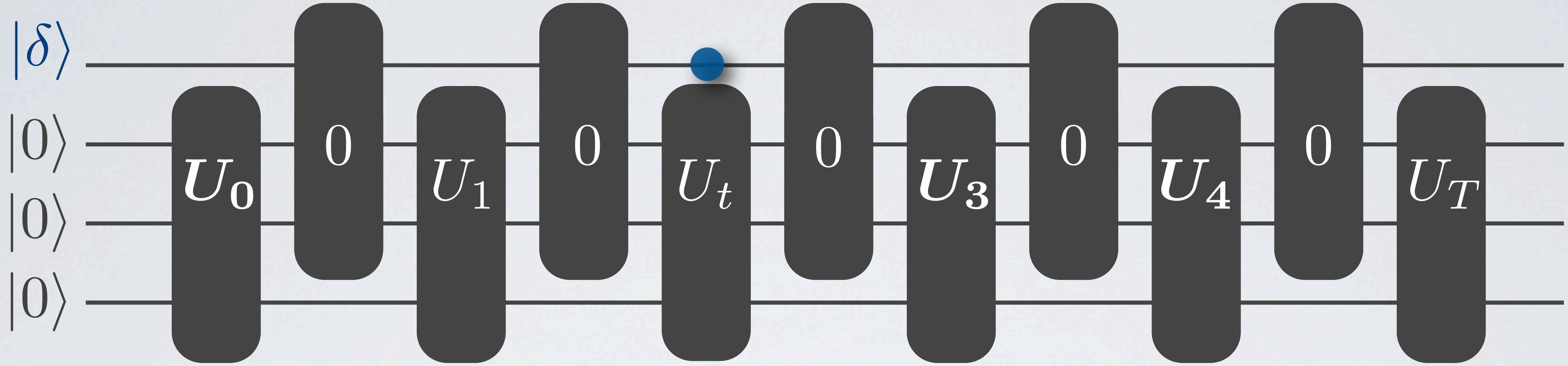
PRINCIPLES BEHIND THE ADVERSARY METHODS

$|\delta\rangle = 1/|F| \sum |f\rangle$



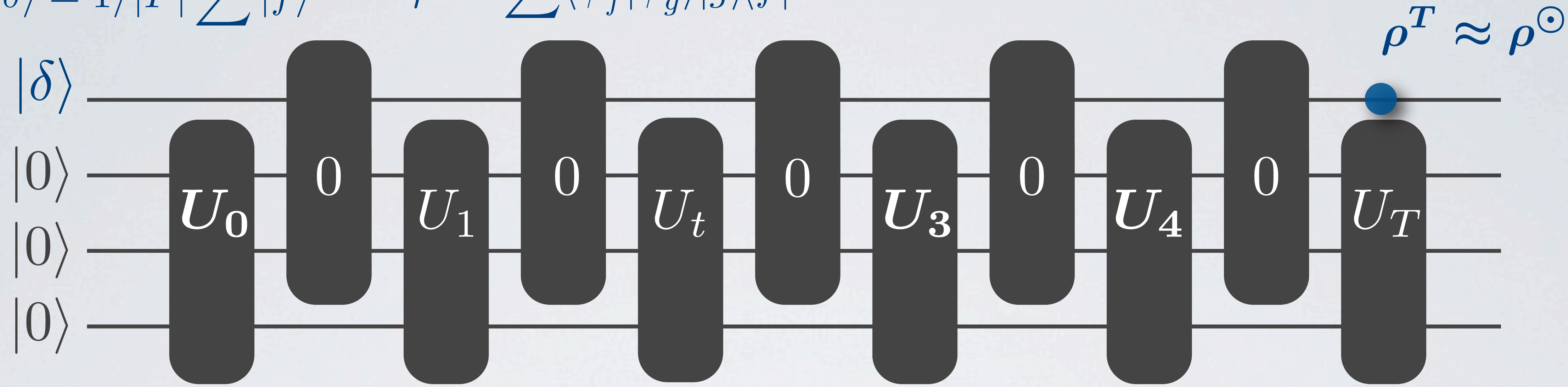
PRINCIPLES BEHIND THE ADVERSARY METHODS

$|\delta\rangle = 1/|F| \sum |f\rangle$ $\qquad$ $\rho^t = \sum \langle \psi_f^t | \psi_g^t \rangle |g\rangle\langle f|$

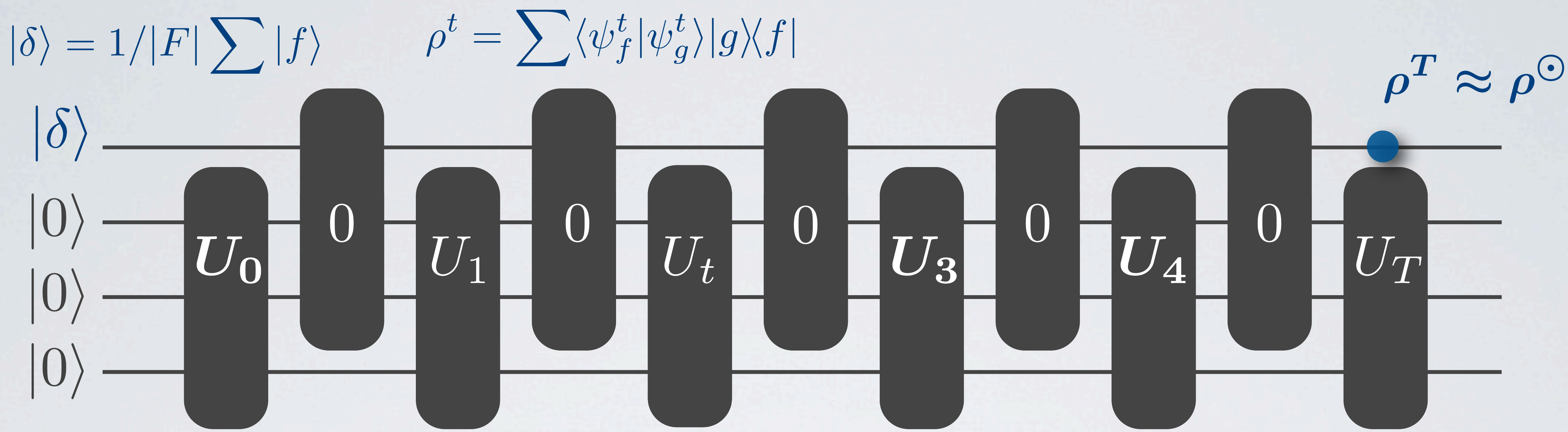


PRINCIPLES BEHIND THE ADVERSARY METHODS

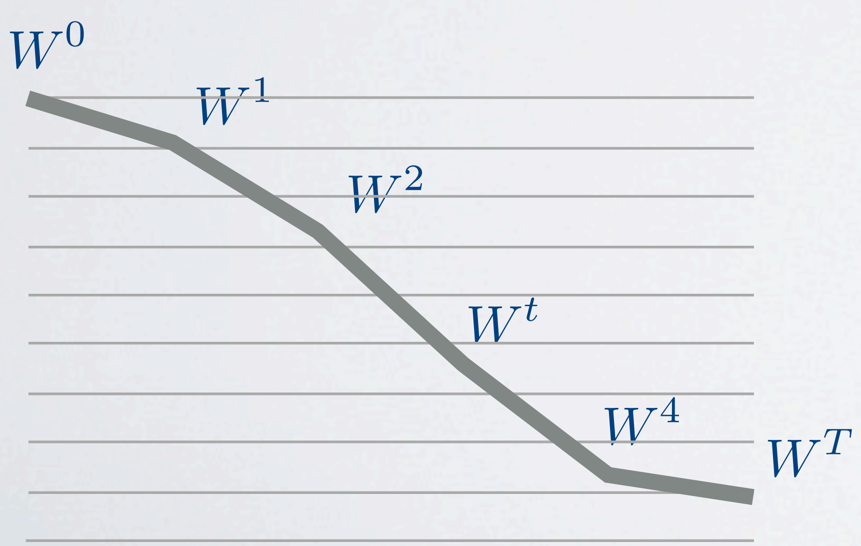
$|\delta\rangle = 1/|F| \sum |f\rangle$ $\rho^t = \sum \langle\psi_f^t|\psi_g^t\rangle |g\rangle\langle f|$



PRINCIPLES BEHIND THE ADVERSARY METHODS



Progress function $\boldsymbol{W^t = \sum \Gamma_{fg} \langle \psi_f^t | \psi_g^t \rangle = \mathrm{tr}[\Gamma \rho^t]}$



- Initial value (high)
- Progress done by one query (limited)
- Final value (low, depends on the success probability)

ADVERSARIES FOR CLASSICAL PROBLEMS

97 [BBBV'97] Hybrid argument

00 [Amb'00] Adversary method

03 [Amb'03]

04 [LM'04] Several variations (and many more)

05 [Amb'05]

06 [SŠ'06] All these methods are equivalent

07 [HLŠ'07] Additive method (negative weights) $W^t - W^{t+1}$

08 [Špa'08] Multiplicative method W^t / W^{t+1}

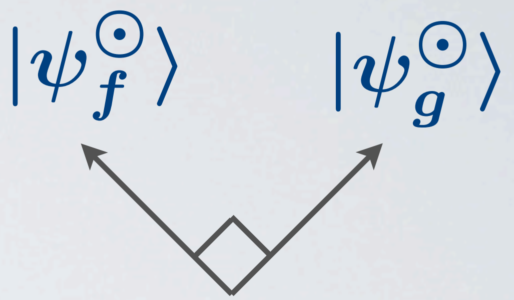
09 [Reï'09] The additive method is tight for all functions

10 [LMRŠ'10] in the bounded-error model

ADVERSARY MATRICES, FIRST APPROACH

$$W^t = \mathrm{tr}[\Gamma \rho^t] = \sum \Gamma_{fg} \langle \psi_f^t | \psi_g^t \rangle$$

For computing functions (classical) :



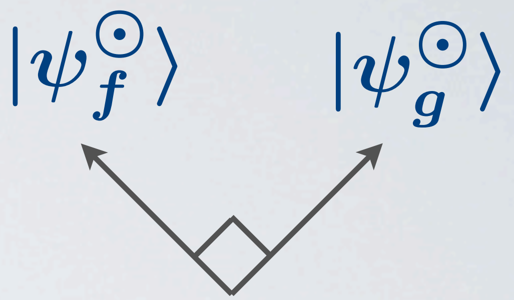
Conditions on Γ: ❶ definite positive

❷ $\Gamma_{fg} = 0$ when $|\psi_f^{\odot}\rangle = |\psi_g^{\odot}\rangle$

ADVERSARY MATRICES, FIRST APPROACH

$$W^t = \mathrm{tr}[\Gamma \rho^t] = \sum \Gamma_{fg} \langle \psi_f^t | \psi_g^t \rangle$$

For computing functions (classical) :

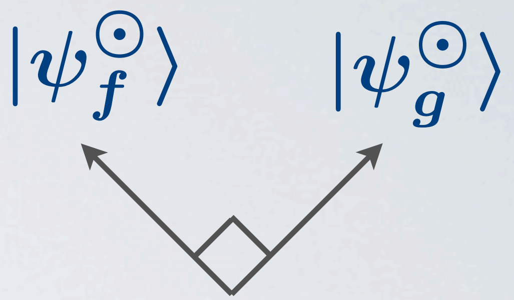


Conditions on Γ: ❶ definite positive

❷ $\mathrm{tr}[\Gamma(\rho^{\odot} \circ M)] = 0, \ \forall M$

ADVERSARY MATRICES, FIRST APPROACH

$$W^t = \mathrm{tr}[\Gamma \rho^t] = \sum \Gamma_{fg} \langle \psi_f^t | \psi_g^t \rangle$$



For computing functions (classical) :

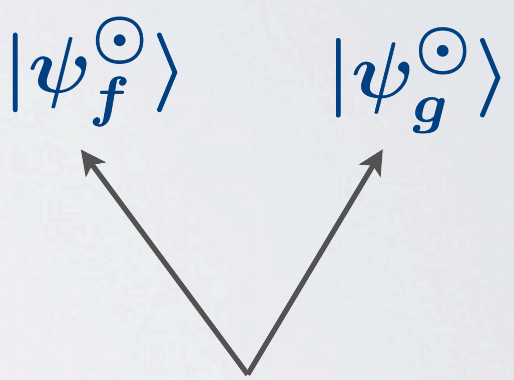
Conditions on Γ: ❶ definite positive

❷ $\mathrm{tr}[\Gamma(\rho^{\odot} \circ M)] = 0, \ \forall M$

[this work]

For quantum state generation:

- non-orthogonal output states



ADDITIVE METHOD:

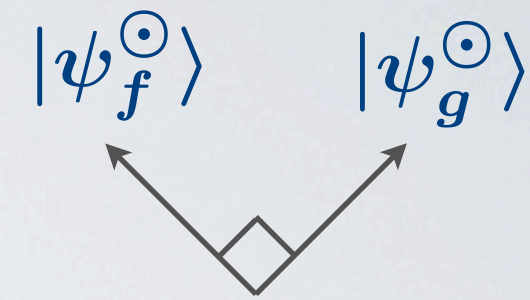
Conditions on Γ: ❶ definite positive

❷ $\mathrm{tr}[\Gamma(\rho^{\odot} \circ M)] = 0, \ \forall M \succeq 0, M_{ii} = 1$

ADVERSARY MATRICES, FIRST APPROACH

$$W^t = \mathrm{tr}[\Gamma\rho^t] = \sum \Gamma_{fg}\langle\psi_f^t|\psi_g^t\rangle$$

For computing functions (classical) :



Conditions on Γ: ❶ definite positive

❷ $\mathrm{tr}[\Gamma(\rho^\odot \circ M)] = 0, \ \forall M$

[this work]

For quantum state generation:

- non-orthogonal output states

too restrictive for small success probability

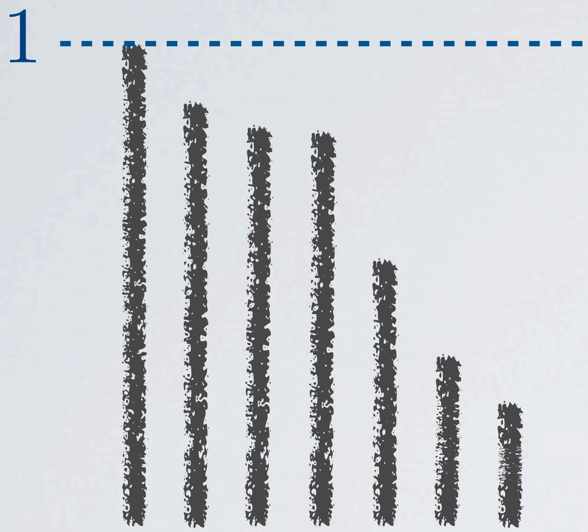
ADDITIVE METHOD:

Conditions on Γ: ❶ definite positive

❷ $\mathrm{tr}[\Gamma(\rho^\odot \circ M)] = 0, \ \forall M \succeq 0, M_{ii} = 1$

NEW METHOD: HYBRID

Eigenvalues of $\mathbf{\Gamma}$

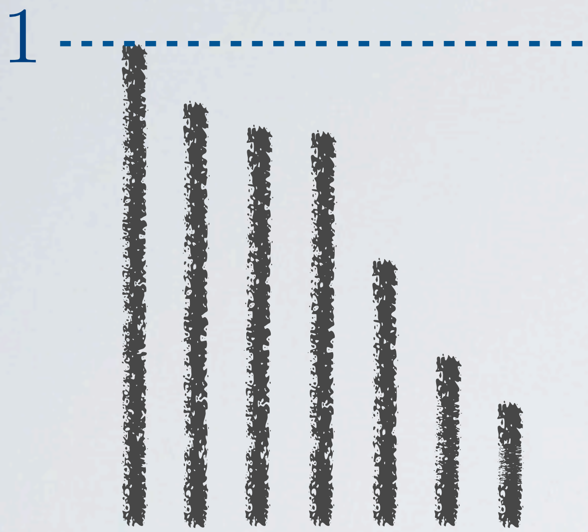


Conditions on $\mathbf{\Gamma}$, hybrid method

$\mathbf{\Gamma} \preceq \mathbb{I}$

NEW METHOD: HYBRID

Eigenvalues of $\boldsymbol{\Gamma}$



Overlap of $\boldsymbol{\rho}^{\mathbf{0}}$ and $\boldsymbol{\Gamma}$

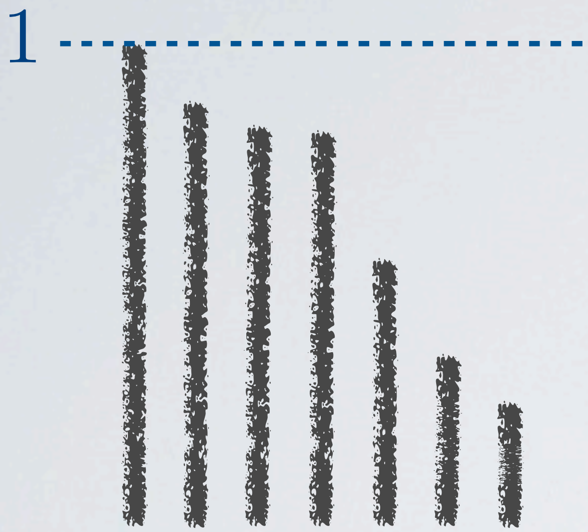
Conditions on $\boldsymbol{\Gamma}$, hybrid method

$$\boldsymbol{\Gamma} \preceq \mathbb{I}$$

$$\boldsymbol{\Gamma}|\delta\rangle = |\delta\rangle$$

NEW METHOD: HYBRID

Eigenvalues of $\boldsymbol{\Gamma}$



Overlap of $\boldsymbol{\rho}^{\mathbf{0}}$and $\boldsymbol{\Gamma}$

Overlap of $\boldsymbol{\rho}^{\odot}$ and $\boldsymbol{\Gamma}$

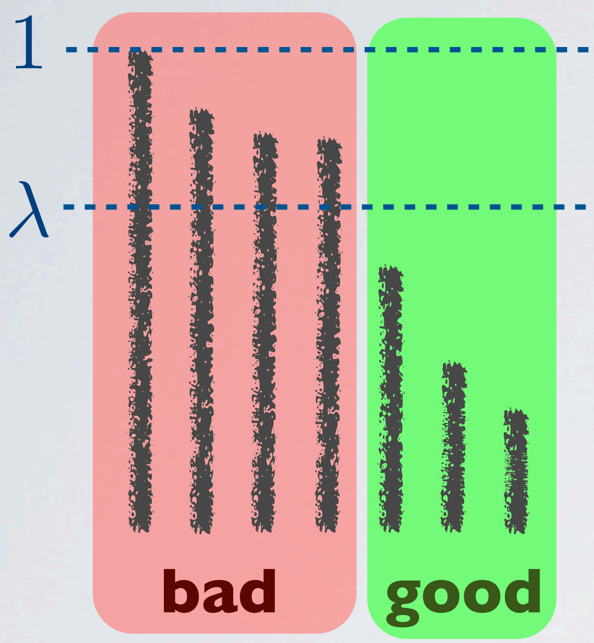
Conditions on $\boldsymbol{\Gamma}$, hybrid method

$$\boldsymbol{\Gamma} \preceq \boldsymbol{I\!I}$$

$$\boldsymbol{\Gamma}|\delta\rangle = |\delta\rangle$$

NEW METHOD: HYBRID

Eigenvalues of $\mathbf{\Gamma}$



Conditions on $\mathbf{\Gamma}$, hybrid method

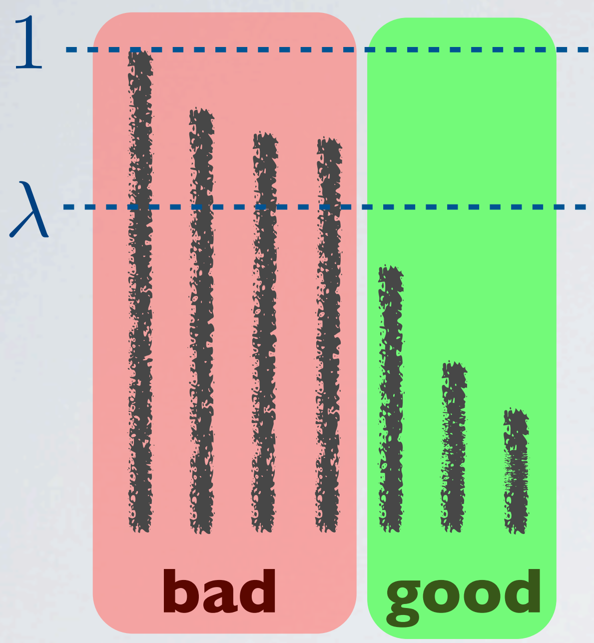
$$\mathbf{\Gamma} \preceq \mathbb{I}$$
$$\mathbf{\Gamma}|\delta\rangle = |\delta\rangle$$
$$\mathrm{tr}[\Pi_{\mathrm{bad}}(\rho^{\odot} \circ M)] \leq \eta$$

Overlap of ρ^0 and $\mathbf{\Gamma}$

Overlap of $\rho^{\odot}$ and $\mathbf{\Gamma}$

NEW METHOD: HYBRID

Eigenvalues of $\mathbf{\Gamma}$



Overlap of ρ^0 and $\mathbf{\Gamma}$

Overlap of $\rho^\odot$ and $\mathbf{\Gamma}$

Conditions on $\mathbf{\Gamma}$, hybrid method

$$\mathbf{\Gamma} \preceq \mathbb{I}$$
$$\mathbf{\Gamma}|\delta\rangle = |\delta\rangle$$
$$\mathrm{tr}[\Pi_{\mathrm{bad}}(\rho^\odot \circ M)] \leq \eta$$

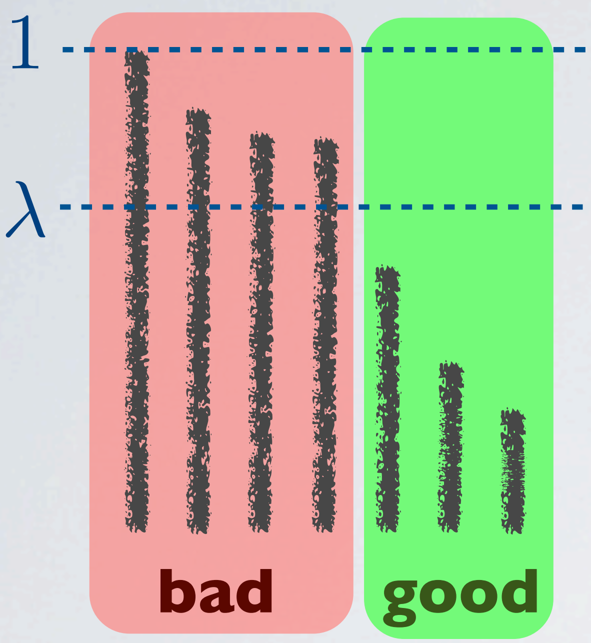
Initial value: $W^0 = 1$

Final value: $W^T \leq (1-\lambda)(\sqrt{1-\varepsilon} - \sqrt{\eta})^2$

Progress: $|W^{t+1} - W^t| \leq \max_x ||\mathbf{\Gamma}_x - \mathbf{\Gamma}||$

NEW METHOD: HYBRID

Eigenvalues of $\boldsymbol{\Gamma}$



Overlap of ρ^0 and $\boldsymbol{\Gamma}$

Overlap of $\rho^{\odot}$ and $\boldsymbol{\Gamma}$

Conditions on $\boldsymbol{\Gamma}$, hybrid method

$$\Gamma \preceq I\!I$$
$$\Gamma|\delta\rangle = |\delta\rangle$$
$$\mathrm{tr}[\Pi_{\mathrm{bad}}(\rho^{\odot} \circ M)] \leq \eta$$

Initial value: $W^0 = 1$

Final value: $W^T \leq (1-\lambda)(\sqrt{1-\varepsilon} - \sqrt{\eta})^2$

Progress: $|W^{t+1} - W^t| \leq \max_x ||\Gamma_x - \Gamma||$

THEOREM

$\mathrm{MADV}_\varepsilon \geq \mathrm{ADV}_\varepsilon^{\mathrm{Hyb}} \geq \mathrm{ADV}_\varepsilon^{\pm} / 60$

SYMMETRIZATION

2 technical difficulties:

- Designing a « good » adversary matrix
- Computing the norm $||\boldsymbol{\Gamma}_{\boldsymbol{x}} - \boldsymbol{\Gamma}||$

Solution:

- Using the symmetries of the problem

Index Erasure: $|\psi_{f}^{\odot}\rangle = \frac{1}{\sqrt{N}} \sum_{x \in [N]} |f(x)\rangle$ $\quad f : [N] \mapsto [M]$

SYMMETRIZATION

2 technical difficulties:

- Designing a « good » adversary matrix
- Computing the norm $||\mathbf{\Gamma}_{\boldsymbol{x}} - \mathbf{\Gamma}||$

Solution:

- Using the symmetries of the problem

Index Erasure: $|\psi_{\boldsymbol{f}}^{\odot}\rangle = \frac{\mathbf{1}}{\sqrt{\boldsymbol{N}}} \sum_{\boldsymbol{x} \in [\boldsymbol{N}]} |\boldsymbol{f}(\boldsymbol{x})\rangle$ $\quad \boldsymbol{f} : [\boldsymbol{N}] \mapsto [\boldsymbol{M}]$

Invariant by permutations of the inputs

$\forall \pi \in S_N, |\psi_{f\circ\pi}^{\odot}\rangle = |\psi_{f}^{\odot}\rangle$

SYMMETRIZATION

2 technical difficulties:

- Designing a « good » adversary matrix
- Computing the norm $||\mathbf{\Gamma}_{\boldsymbol{x}} - \mathbf{\Gamma}||$

Solution:

- Using the symmetries of the problem

Index Erasure: $|\psi_{\boldsymbol{f}}^{\odot}\rangle = \frac{\mathbf{1}}{\sqrt{\boldsymbol{N}}} \sum_{\boldsymbol{x}\in[\boldsymbol{N}]} |\boldsymbol{f}(\boldsymbol{x})\rangle$ $\quad \boldsymbol{f} : [\boldsymbol{N}] \mapsto [\boldsymbol{M}]$

Invariant by permutations of the inputs

$\forall \pi \in S_N, |\psi_{f\circ\pi}^{\odot}\rangle = |\psi_f^{\odot}\rangle$

The circuit should have this symmetry

USING SYMMETRIES

- π permutation on the inputs
- τ permutation on the outputs

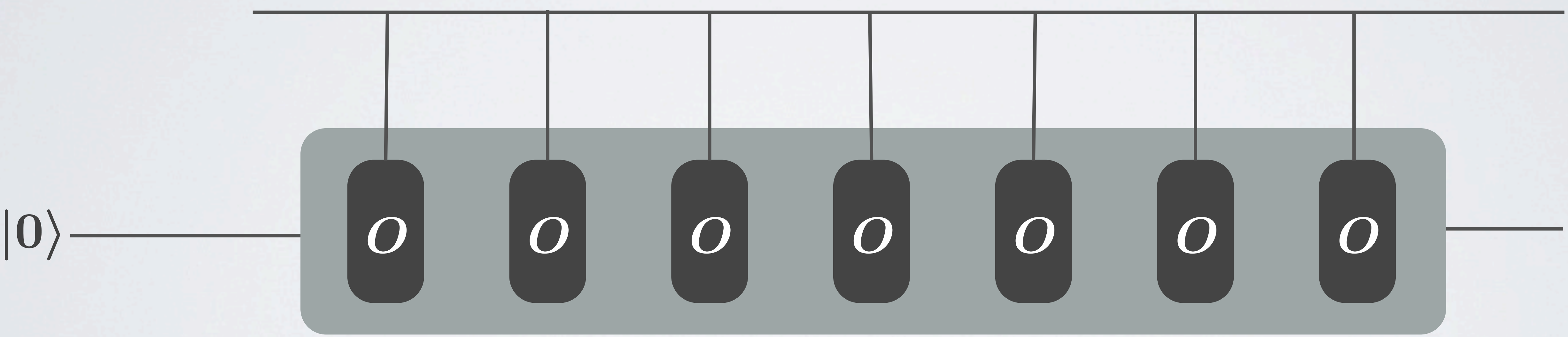
$$f_{\pi,\tau} = \tau \circ f \circ \pi$$

$$U_{\pi\tau}|f\rangle = |f_{\pi\tau}\rangle$$

AUTOMORPHISM GROUP G [HLŠ'07]

$\forall (\pi,\tau) \in G,\ \forall f \in F,\ f_{\pi\tau} \in F$

$\forall (\pi,\tau) \in G$ there exists a unitary $V_{\pi\tau}|\psi_f^{\odot}\rangle = |\psi_{f_{\pi\tau}}^{\odot}\rangle$



USING SYMMETRIES

π permutation on the inputs

τ permutation on the outputs

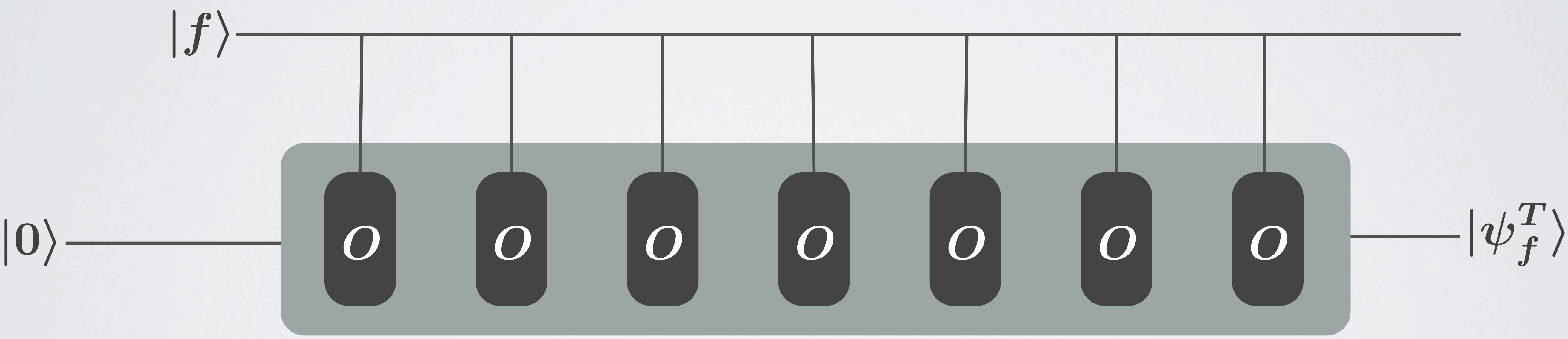
$f_{\pi,\tau} = \tau \circ f \circ \pi$

$U_{\pi\tau}|f\rangle = |f_{\pi\tau}\rangle$

AUTOMORPHISM GROUP G [HLŠ'07]

$\forall(\pi,\tau) \in G,\ \forall f \in F,\ f_{\pi\tau} \in F$

$\forall(\pi,\tau) \in G$ there exists a unitary $V_{\pi\tau}|\psi_f^{\odot}\rangle = |\psi_{f_{\pi\tau}}^{\odot}\rangle$



USING SYMMETRIES

π permutation on the inputs

τ permutation on the outputs

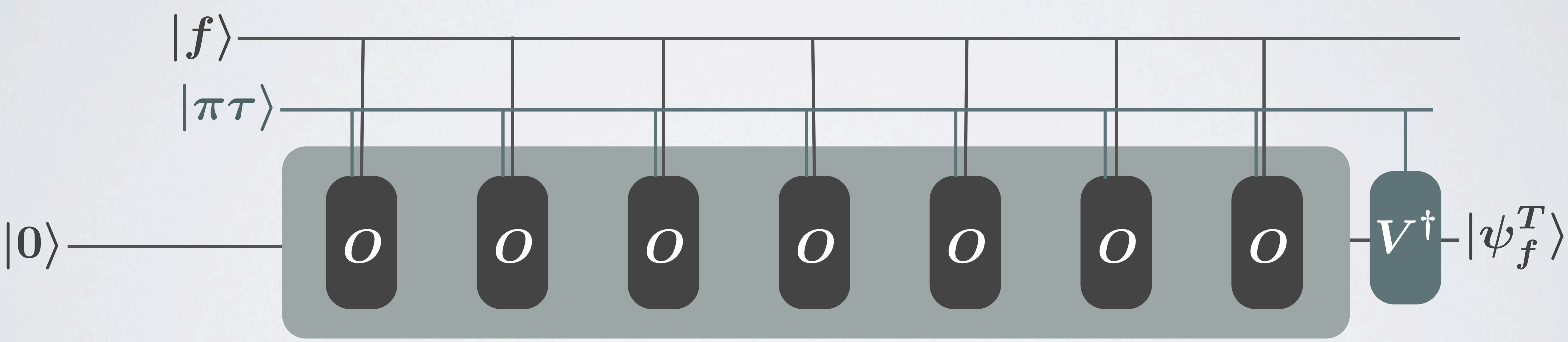
$$f_{\pi,\tau} = \tau \circ f \circ \pi$$

$$U_{\pi\tau}|f\rangle = |f_{\pi\tau}\rangle$$

AUTOMORPHISM GROUP G [HLŠ'07]

$\forall(\pi,\tau) \in G,\ \forall f \in F, f_{\pi\tau} \in F$

$\forall(\pi,\tau) \in G$ there exists a unitary $V_{\pi\tau}|\psi_f^{\odot}\rangle = |\psi_{f_{\pi\tau}}^{\odot}\rangle$



USING SYMMETRIES

π permutation on the inputs

τ permutation on the outputs

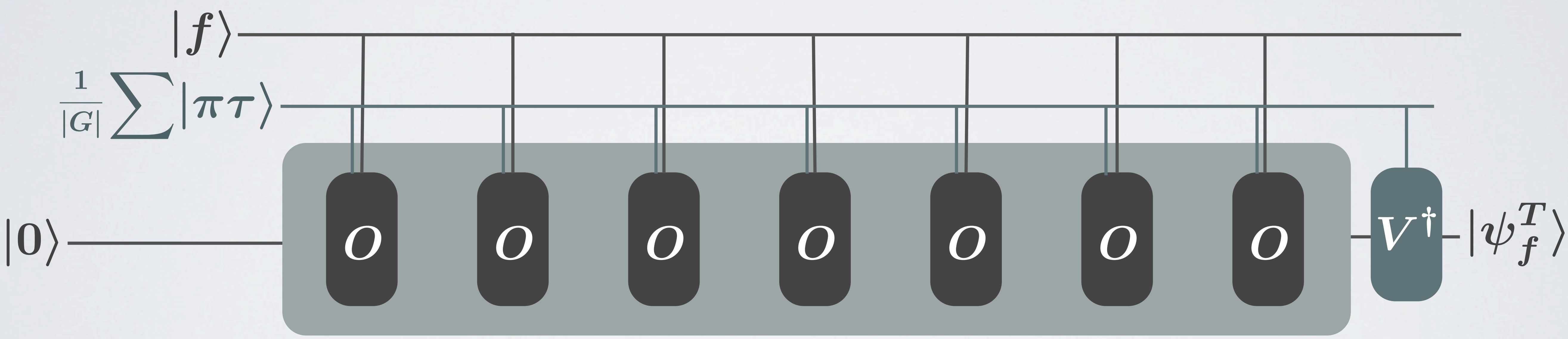
$f_{\pi,\tau} = \tau \circ f \circ \pi$

$U_{\pi\tau}|f\rangle = |f_{\pi\tau}\rangle$

AUTOMORPHISM GROUP G [HLŠ'07]

$\forall(\pi, \tau) \in G, \ \forall f \in F, f_{\pi\tau} \in F$

$\forall(\pi, \tau) \in G$ there exists a unitary $V_{\pi\tau}|\psi_f^{\odot}\rangle = |\psi_{f_{\pi\tau}}^{\odot}\rangle$



USING SYMMETRIES

π permutation on the inputs

τ permutation on the outputs

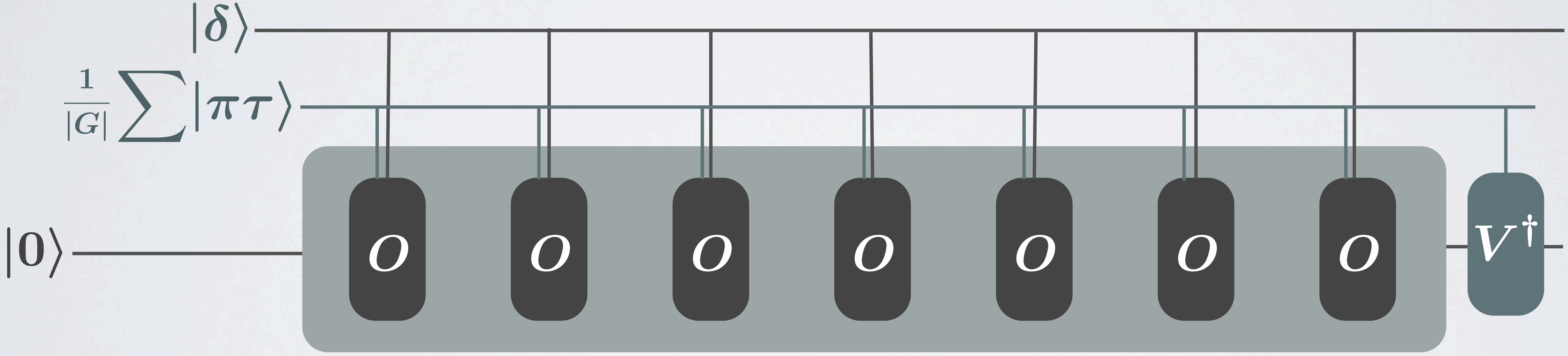
$$f_{\pi,\tau} = \tau \circ f \circ \pi$$

$$U_{\pi\tau}|f\rangle = |f_{\pi\tau}\rangle$$

AUTOMORPHISM GROUP G [HLŠ'07]

$\forall(\pi,\tau) \in G,\ \forall f \in F,\ f_{\pi\tau} \in F$

$\forall(\pi,\tau) \in G$ there exists a unitary $V_{\pi\tau}|\psi_f^{\odot}\rangle = |\psi_{f_{\pi\tau}}^{\odot}\rangle$



USING SYMMETRIES

π permutation on the inputs

τ permutation on the outputs

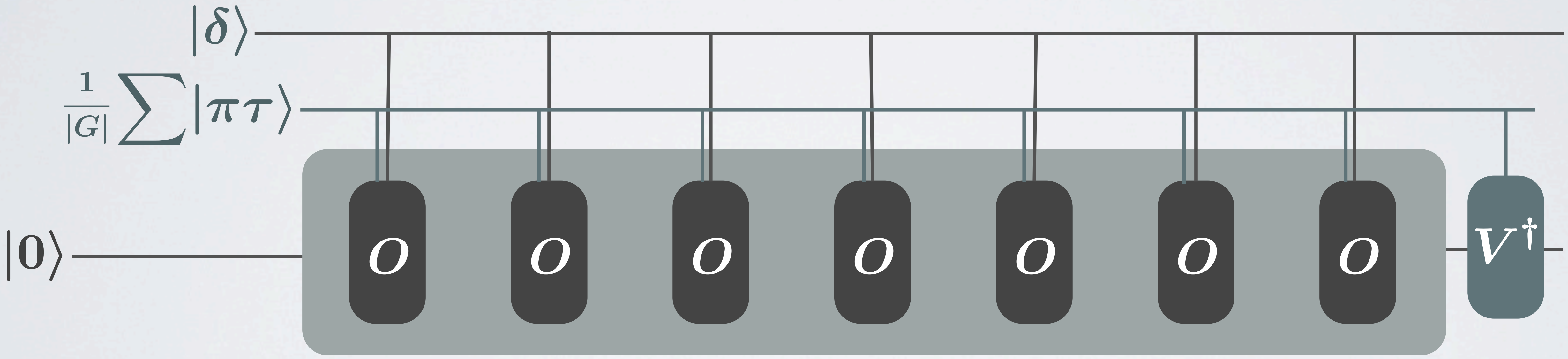
$f_{\pi,\tau} = \tau \circ f \circ \pi$

$U_{\pi\tau}|f\rangle = |f_{\pi\tau}\rangle$

AUTOMORPHISM GROUP G [HLŠ'07]

$\forall(\pi,\tau) \in G,\ \forall f \in F,\ f_{\pi\tau} \in F$

$\forall(\pi,\tau) \in G$ there exists a unitary $V_{\pi\tau}|\psi_f^{\odot}\rangle = |\psi_{f_{\pi\tau}}^{\odot}\rangle$



Symmetry of the oracle state: $U_{\pi\tau}\rho^t U_{\pi\tau}^\dagger = \rho^t$

Γ can be chosen with the same symmetries: $U_{\pi\tau}\,\Gamma U_{\pi\tau}^\dagger = \Gamma$

USING SYMMETRIES

π permutation on the inputs

τ permutation on the outputs

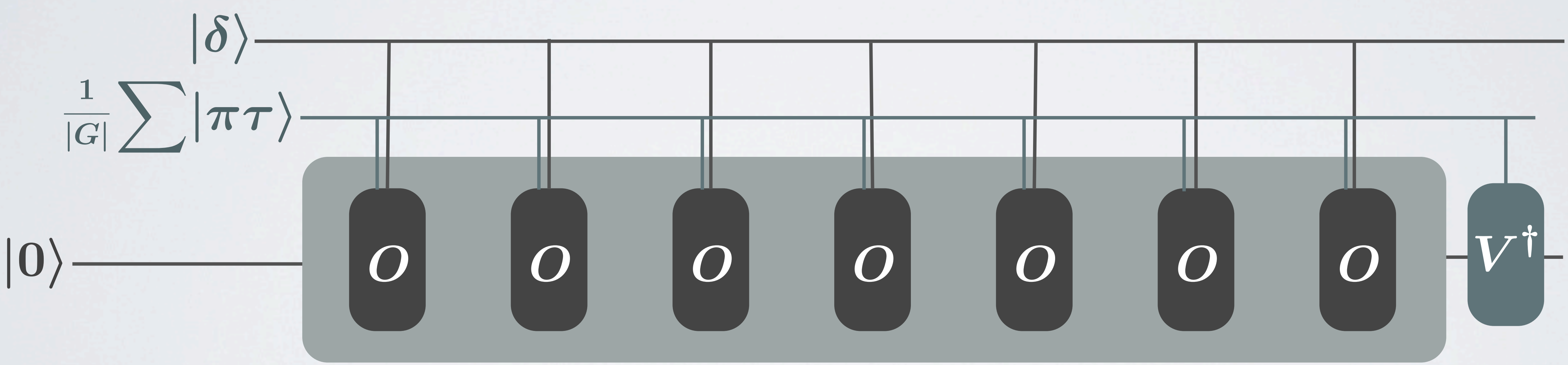
$f_{\pi,\tau} = \tau \circ f \circ \pi$

$U_{\pi\tau}|f\rangle = |f_{\pi\tau}\rangle$

AUTOMORPHISM GROUP G [HLŠ'07]

$\forall(\pi,\tau) \in G,\ \forall f \in F, f_{\pi\tau} \in F$

$\forall(\pi,\tau) \in G$ there exists a unitary $V_{\pi\tau}|\psi_f^{\odot}\rangle = |\psi_{f_{\pi\tau}}^{\odot}\rangle$



Symmetry of the oracle state: $U_{\pi\tau}\rho^t U_{\pi\tau}^\dagger = \rho^t$

Γ can be chosen with the same symmetries: $U_{\pi\tau}\,\Gamma U_{\pi\tau}^\dagger = \Gamma$

$\mathcal{U} : (\pi,\tau) \mapsto U_{\pi\tau}$ is a representation of G

USING SYMMETRIES WHEN $\mathcal{U}$ IS MULTIPLICITY-FREE

USING SYMMETRIES WHEN $\mathcal{U}$ IS MULTIPLICITY-FREE

$\Gamma = \sum_k \gamma_k \Pi_k$ where Π_k is the k-th irrep of G

USING SYMMETRIES WHEN $\mathcal{U}$ IS MULTIPLICITY-FREE

$\boldsymbol{\Gamma} = \sum_k \gamma_k \boldsymbol{\Pi}_k$ where $\boldsymbol{\Pi}_k$ is the k-th irrep of G

$$G_x = \{(\pi, \tau) \in G \;:\; \pi(x) = x\}$$

$$G_{xy} = \{(\pi, \tau) \in G \;:\; \pi(x) = x, \tau(y) = y\}$$

l is an irrep of G_x with multiplicity m_l

$$\|\boldsymbol{\Gamma}_x - \boldsymbol{\Gamma}\| = \max_l \left\|\boldsymbol{\Delta}_x^l\right\|$$

USING SYMMETRIES WHEN $\mathcal{U}$ IS MULTIPLICITY-FREE

$\boldsymbol{\Gamma = \sum_k \gamma_k \Pi_k}$ where $\boldsymbol{\Pi_k}$ is the $\boldsymbol{k}$-th irrep of $\boldsymbol{G}$

$$\boldsymbol{G_x = \{(\pi,\tau) \in G \ : \ \pi(x) = x\}}$$

$$\boldsymbol{G_{xy} = \{(\pi,\tau) \in G \ : \ \pi(x) = x, \tau(y) = y\}}$$

depends on the overlap of irreps of G, G_x and G_{xy}

$\boldsymbol{l}$ is an irrep of $\boldsymbol{G_x}$ with multiplicity $\boldsymbol{m_l}$

$$\boldsymbol{\|\Gamma_x - \Gamma\| = \max_l \left\|\Delta_x^l\right\|}$$

large size: |F| x |F|
index erasure $N!\binom{M}{N}$.

small size: $m_l \times m_l$
index erasure 3×3

USING SYMMETRIES WHEN $\mathcal{U}$ IS MULTIPLICITY-FREE

$$\boldsymbol{\Gamma} = \sum_k \gamma_k \boldsymbol{\Pi}_k$$ where $\boldsymbol{\Pi}_k$ is the k-th irrep of G

$$G_x = \{(\pi, \tau) \in G \;:\; \pi(x) = x\}$$

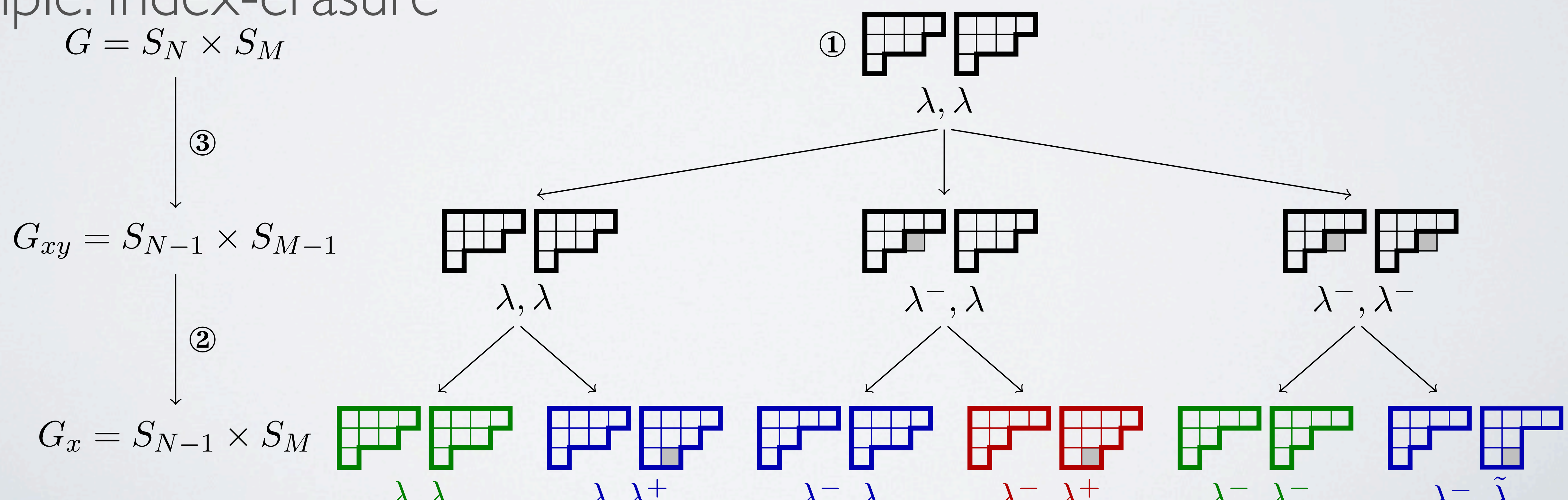
$$G_{xy} = \{(\pi, \tau) \in G \;:\; \pi(x) = x, \tau(y) = y\}$$

l is an irrep of G_x with multiplicity m_l

depends on the overlap of irreps of G, G_x and G_{xy}

$$\|\boldsymbol{\Gamma}_x - \boldsymbol{\Gamma}\| = \max_l \left\| \boldsymbol{\Delta}_x^l \right\|$$

Example: Index-erasure



STRONG DIRECT PRODUCT THEOREM

Assume: multiplicative lower bound complexity for QSG is T.
Complexity of solving QSG on k independent instances?

- Upper bound $O(kT)$
- Lower bound?

STRONG DIRECT PRODUCT THEOREM

Assume: multiplicative lower bound complexity for QSG is T.
Complexity of solving QSG on k independent instances?

- Upper bound $O(kT)$
- Lower bound?

STRONG DIRECT PRODUCT THEOREM

The success probability of an algorithm solving QSG on k independent instances with less than $kT/10$ queries is exponentially small in k.

$$\mathrm{MADV}_{\epsilon'}^{(k)} \leq \frac{k}{10}\mathrm{MADV}_{\epsilon}$$

OPEN QUESTIONS

QUERY COMPLEXITY

- Optimality for quantum state generation?
- Strong direct product theorem holds for *all functions*?
  - quantum state generation problems?

PROVING LOWER BOUNDS

- New lower bounds? (Set equality)
- Shorter/Simpler proofs?
- What about Graph Isomorphism?

Acknowledgments of support:

Thank you for your attention!

Methods + Application to Index erasure:
arXiv:1012.2112 [quant-ph]

A SHORT BIBLIOGRAPHY

[Amb'00]	STOC'00
[Amb'03]	FOCS'03
[Amb'05]	arxiv:quant-ph/0508200
[BBBV'97]	SIAM J. Comput, 1997
[HLŠ'07]	STOC'07
[LM'04]	CCC'04
[LMRŠ'10]	arxiv:1011.3020 [quant-ph]
[Rei'09]	FOCS'09
[Špa'08]	CCC'08
[Shi'02]	FOCS'02
[SŠ'06]	Th. Comput. 2006