

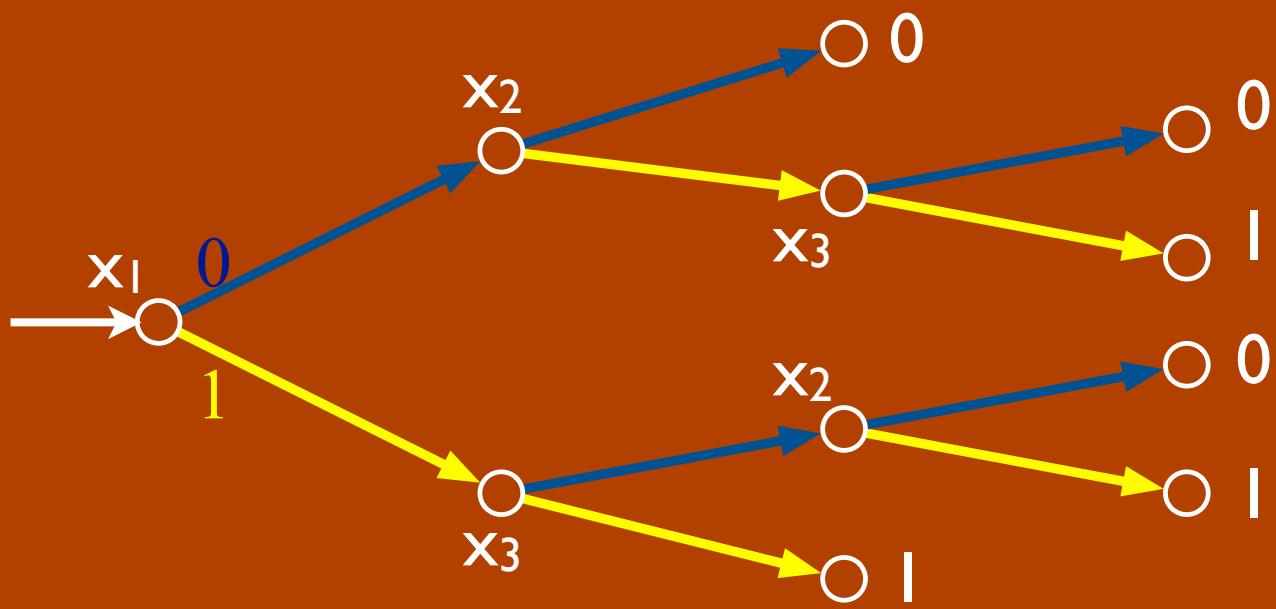
Quantum query complexity

Ben Reichardt

IQC, University of Waterloo

$$f:\mathcal{D}\rightarrow E$$

$$\mathcal{D} \subseteq \{0,1\}^n$$



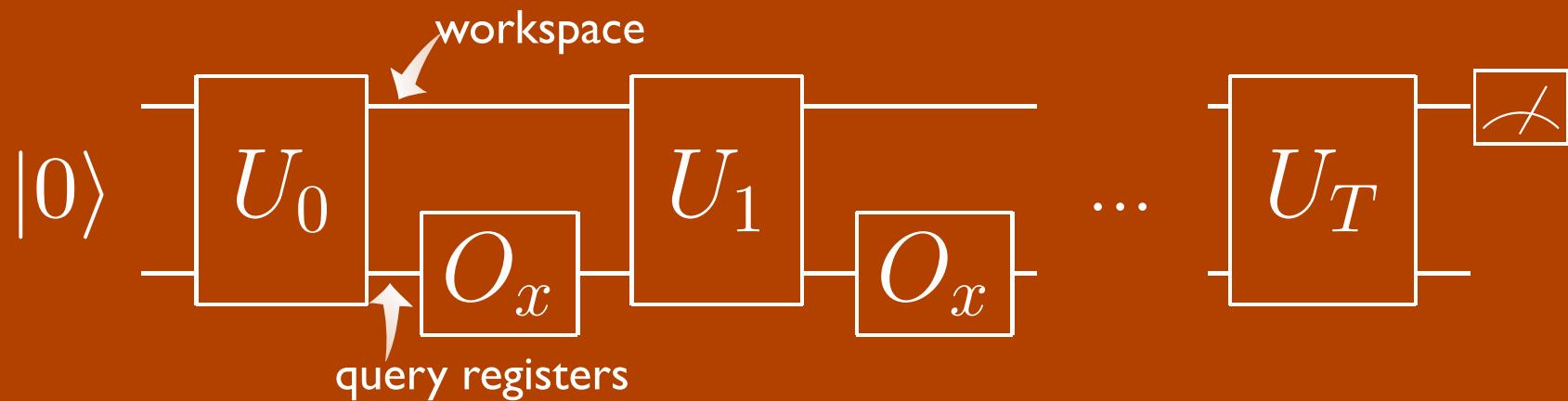
$x = 1 | 0$

- Models:
- Deterministic query/decision-tree complexity
 - Randomized query complexity
 - bounded-error/Monte Carlo (R_2), Zero-error/Las Vegas (R_0), one-sided error (R_1)
 - Certificate complexity
 - A.K.A. Nondeterministic query complexity
 - Quantum query complexity

For **total** functions (i.e., domain $D=\{0,1\}^n$), all are equivalent up to polynomials, e.g.,

$$D(f) \leq \min\{C^2, R_0^2, R_2^3, R_1 R_2, Q_2^6, Q_E, Q_1 Q_2^2\}$$

see [BBCMW 9802049]
also [AA 0911.0996]



$$O_x|j\rangle = (-1)^{x_j}|j\rangle \quad (\text{with } x_0 = 0)$$

A. Query complexity

B. Adversary lower bounds

Break

C. Spectra of reflections

D. Adversary upper bound

$$Q(f) = \Theta(\text{Adv}^\pm(f))$$

Examples

$$\text{OR} : \{0,1\}^n \rightarrow \{0,1\}$$

$$\text{OR}(x) = \begin{cases} 1 & \text{if } |x| := \sum_{j=1}^n x_j \geq 1 \\ 0 & \text{otherwise} \end{cases}$$

OR

\sqrt{n}

[G 9605043, BBBV 9701001]

$$A: \{0,1\}^* \rightarrow \{0,1\}^*$$

uniformly random length-preserving function

$$L_A = \text{Range}(A)$$

- $L_A \in \text{NP}^A$
- With probability one, $L_A \notin \text{BQTime}(o(\sqrt{2^n}))^A$

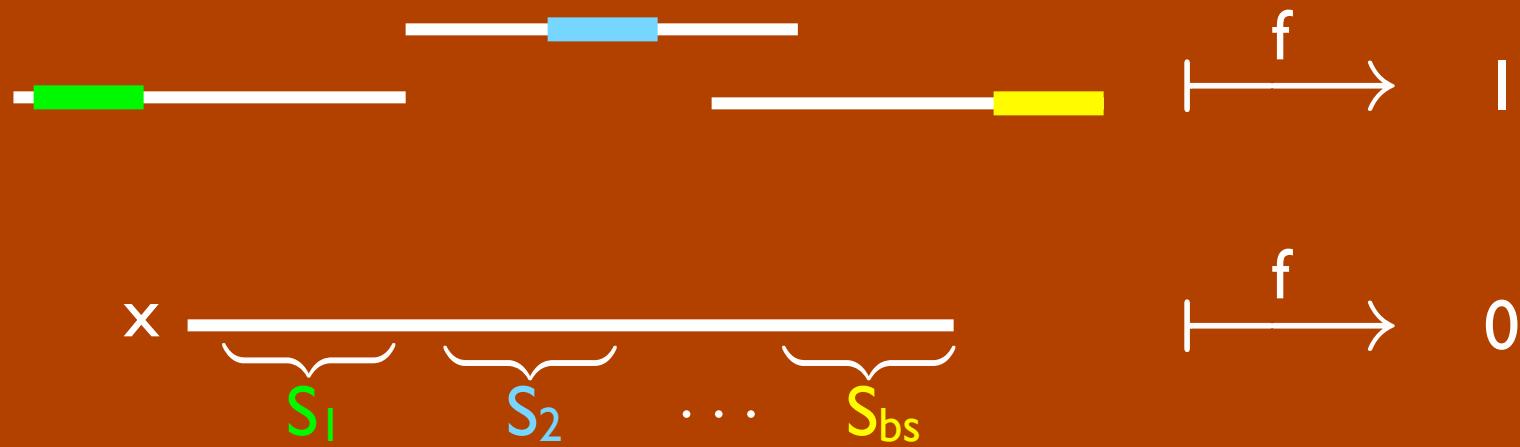
OR

\sqrt{n}

[G 9605043, BBBV 9701001]

Theorem: For $f: \{0,1\}^n \rightarrow \{0,1\}$, $D(f) = O(Q(f)^6)$

Proof: Block sensitivity of x = $\#$ of disjoint sets each of which can be flipped to flip f



Just like $OR_{bs}!$ $\Rightarrow \sqrt{bs} \leq Q(f|_{\{x \text{ and its neighbors}\}}) \leq Q(f)$

Rest of proof is classical: $D(f) \leq bs(f)C(f)$, $C(f) \leq bs(f)^2$

OR
Hidden subgroup \sqrt{n} $[G \text{ 9605043, BBBV 9701001}]$
 $\log |G|$ $[\text{EHK 9901034, KNP 0501060}]$

Input: $x = \text{[Sequence of colored squares]} \in \Sigma^G$
 $x_g = x_h \Leftrightarrow gh^{-1} \in H$

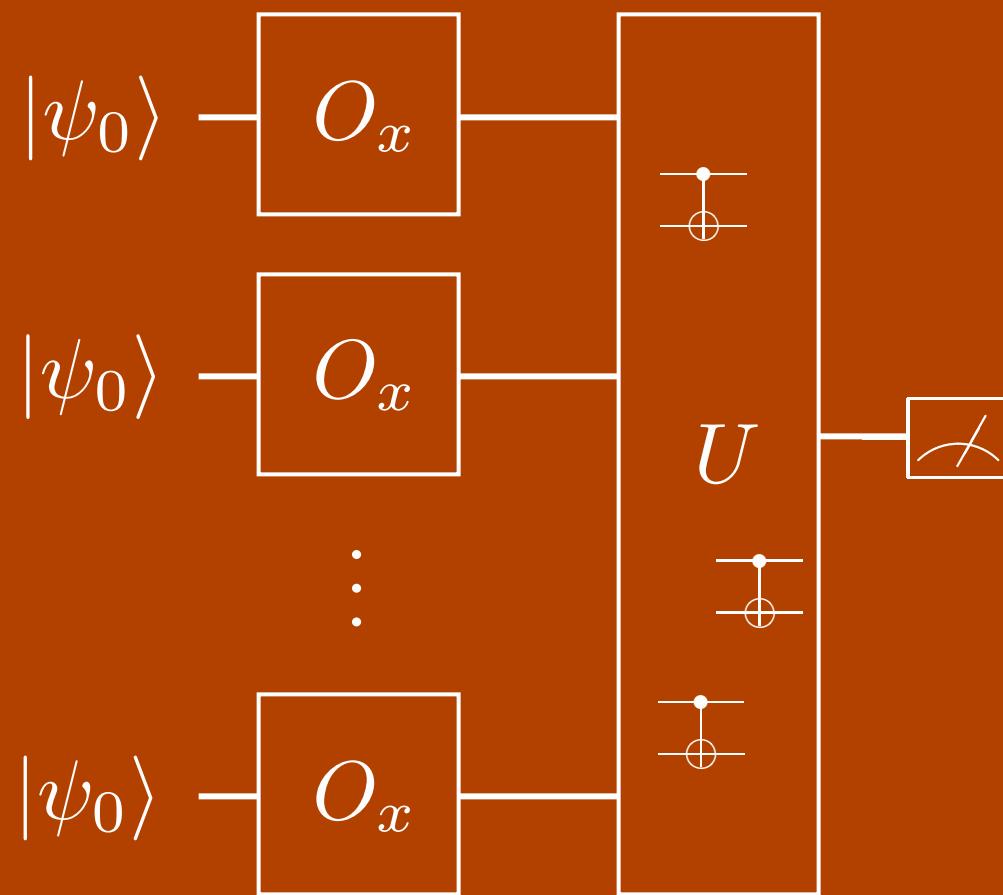
Output: H

OR
Hidden subgroup

\sqrt{n}
 $\log |G|$

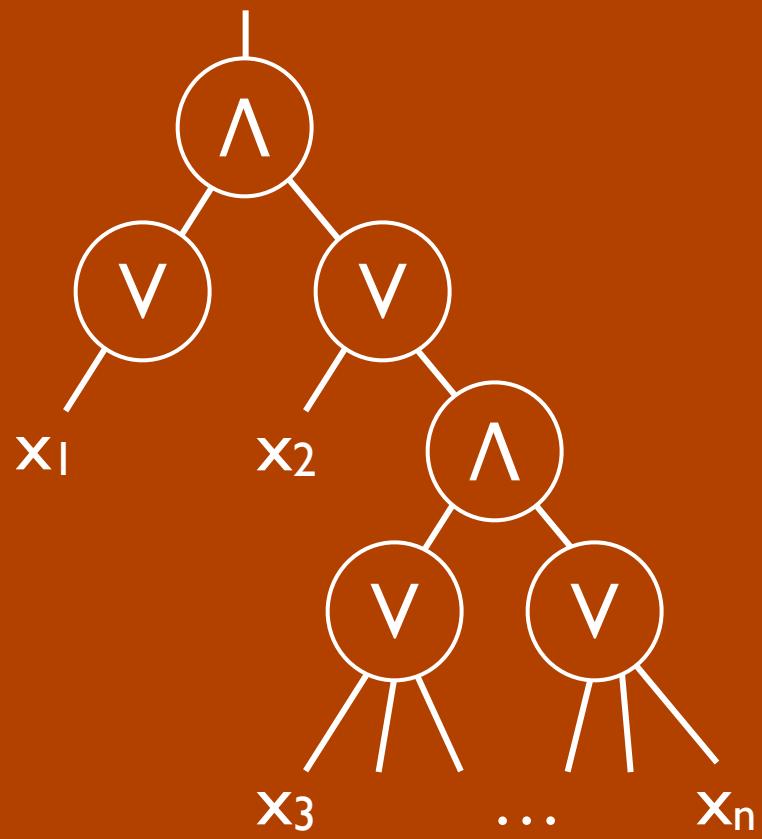
[G 9605043, BBBV 9701001]

[EHK 9901034, KNP 0501060]



Time complexity > Query complexity (can be $\gg!$)

OR	\sqrt{n}	[G 9605043, BBBV 9701001]
Hidden subgroup	$\log G $	[EHK 9901034, KNP 0501060]
Parity	$n/2$	[D 9805006]
Symmetric functions	$\sqrt{(n(n-\Gamma))}$	[BBCMW 9802049]
Most functions	$\Theta(n)$	[A 9811080]
Graph connectivity	$n^{3/2}$	[DHJM 0401091]
Ordered search	$\Theta(\log n)$	[BH 0703231, CLP 0608161]



OR	\sqrt{n}	[G 9605043, BBBV 9701001]
Hidden subgroup	$\log G $	[EHK 9901034, KNP 0501060]
Parity	$n/2$	[D 9805006]
Symmetric functions	$\sqrt{(n(n-\Gamma))}$	[BBCMW 9802049]
Most functions	$\Theta(n)$	[A 9811080]
Graph connectivity	$n^{3/2}$	[DHJM 0401091]
Ordered search	$\Theta(\log n)$	[BH 0703231, CLP 0608161]
AND-OR formula	\sqrt{n}	[FGG 0702144, ACRSZ 0703015, R 0907.1623]

Element distinctness

 $\in \Sigma^n$

OR	\sqrt{n}	[G 9605043, BBBV 9701001]
Hidden subgroup	$\log G $	[EHK 9901034, KNP 0501060]
Parity	$n/2$	[D 9805006]
Symmetric functions	$\sqrt{(n(n-\Gamma))}$	[BBCMW 9802049]
Most functions	$\Theta(n)$	[A 9811080]
Graph connectivity	$n^{3/2}$	[DHJM 0401091]
Ordered search	$\Theta(\log n)$	[BH 0703231, CLP 0608161]
AND-OR formula	\sqrt{n}	[FGG 0702144, ACRSZ 0703015, R 0907.1623]
Collision	$n^{1/3}$	[BHT 9705002, AS 04]
Element distinctness	$n^{2/3}$	[A 0311001, MSS 0310134, S 0401053]

a subset of size k of entries satisfying some property
Given $x \in \Sigma^n$, find ~~k equal~~ [✓] entries, if possible

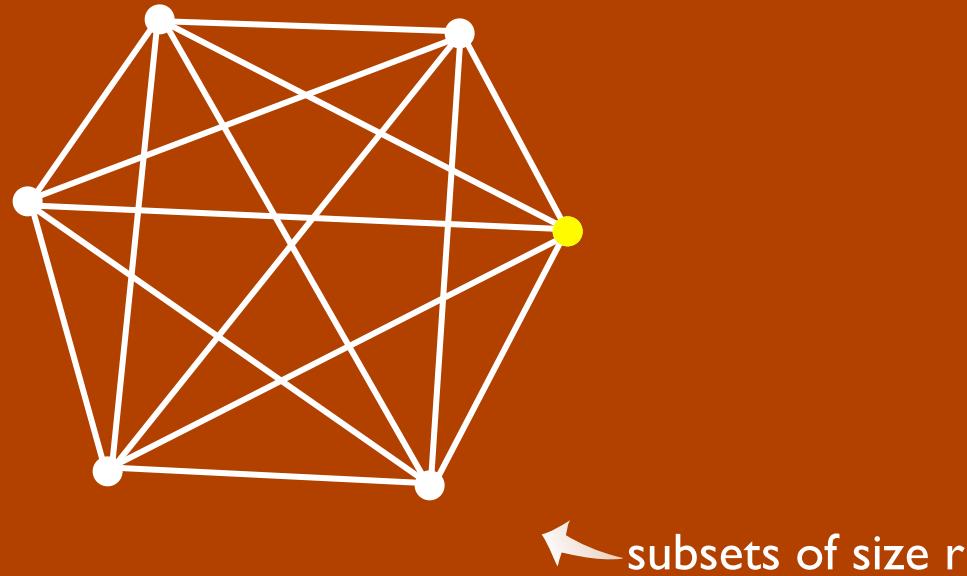
Algorithm:

1. Query, and remember, a random r positions of x
 - $r = "database\ size"$
 - Check for a good subset—probability $\binom{n-k}{r-k} / \binom{n}{r} \approx (r/n)^k$
2. Repeat $(n/r)^{k/2}$ times:
 - a. Add a -I phase if the database includes a good subset
 - b. \sqrt{r} times: Move to an adjacent subset by a quantum walk (one query to add & one to delete an element)
3. Measure the subset and check it

$$Q \leq r + (n/r)^{k/2} \times \sqrt{r} = n^{k/(k+1)} \text{ for } r = n^{k/(k+1)}$$

Algorithm:

1. Query, and remember, a random r positions of x
 - r = “database size”
 - Check for a good subset—probability $\binom{n-k}{r-k} / \binom{n}{r} \approx (r/n)^k$
2. Repeat $(n/r)^{k/2}$ times:
 - a. Add a -I phase if the database includes a good subset
 - b. \sqrt{r} times: Move to an adjacent subset by a quantum walk (one query to add & one to delete an element)



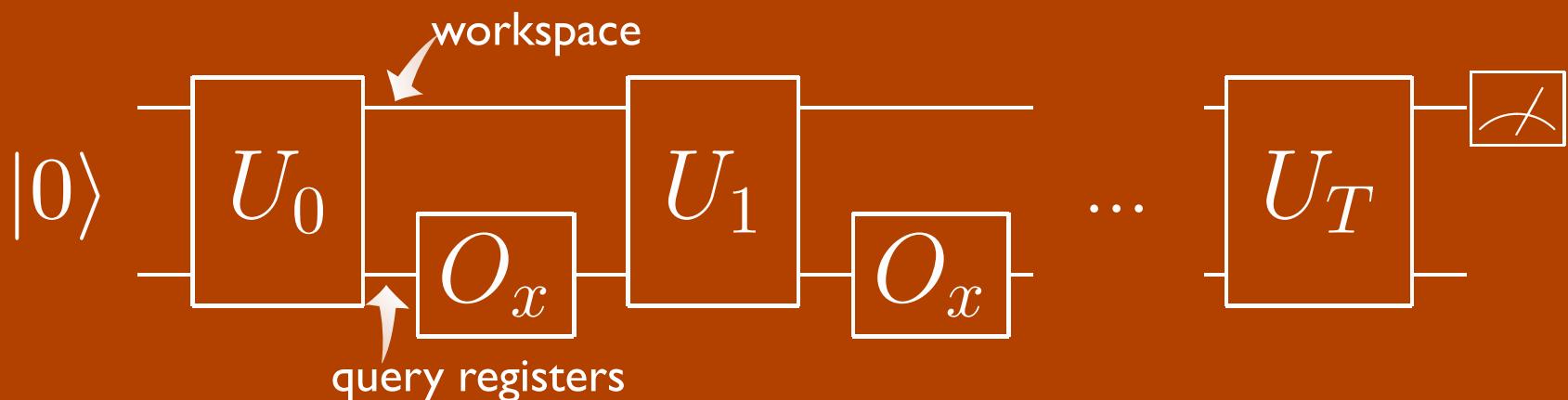
OR	\sqrt{n}	[G 9605043, BBBV 9701001]
Hidden subgroup	$\log G $	[EHK 9901034, KNP 0501060]
Parity	$n/2$	[D 9805006]
Symmetric functions	$\sqrt{(n(n-\Gamma))}$	[BBCMW 9802049]
Most functions	$\Theta(n)$	[A 9811080]
Graph connectivity	$n^{3/2}$	[DHJM 0401091]
Ordered search	$\Theta(\log n)$	[BH 0703231, CLP 0608161]
AND-OR formula	\sqrt{n}	[FGG 0702144, ACRSZ 0703015, R 0907.1623]
Collision	$n^{1/3}$	[BHT 9705002, AS 04]
Element distinctness	$n^{2/3}$	[A 0311001, MSS 0310134, S 0401053]
Triangle finding	$(n, n^{1.3})$	[MSS 0310134, CE 0311038, MNRS 0608026]
Matrix product verification	$\leq n^{5/3}$	[BS 0409035]
Hamiltonian simulation	$(\sqrt{n}, n^{2/3})$	[BC 0910.4157]
Bdd-degree bipartite property	$n^{1/3}$	[ACL 1012.3174]
Graph planarity	$n^{3/2}$	[CK 1011.1443 Tuesday]
State generation: Index erasure	\sqrt{n}	[AMRR 1012.2112 Tuesday]

Most of these algorithms are also time efficient

Quantum query complexity lower bounds:

- Polynomial method

$$Q_\epsilon(f) \geq \frac{1}{2} \deg_\epsilon(f)$$



$$\begin{aligned} O_x &= \sum_j (-1)^{x_j} |j\rangle\langle j| \\ &= \sum_j (1 - 2x_j) |j\rangle\langle j| \end{aligned}$$

Quantum query complexity lower bounds:

- Polynomial method

$$Q_\epsilon(f) \geq \frac{1}{2} \deg_\epsilon(f)$$

- Adversary method

$$Q_\epsilon(f) \geq \frac{1-2\sqrt{\epsilon(1-\epsilon)}}{2} \text{Adv}(f)$$

Can be very loose:

For OR on $\{0^n, 10^{n-1}, \dots, 0^{n-1}1\}$,

$f(x) = x_1 + x_2 + \dots + x_n$ so $\deg(f) = n$

but $Q(f) = \Theta(\sqrt{n})$

Also,

- General adversary bound
- Multiplicative adversary

For *total* functions on $\{0,1\}^n$:

$$Q_\epsilon(f) = O(\deg_\epsilon(f)^6)$$

largest known separation is

$$Q(f) = \Omega(\deg(f)^{1.3})$$

A **certificate** for input x is a set of positions whose values fix f .

For $f=OR$:	<u>Input</u>	<u>Minimal certificate</u>	
	00110	{3}	$\Rightarrow C(OR_n)=n$
	00000	{1,2,3,4,5}	

Given a certificate for the input, it suffices to read those bits

\therefore Certificate complexity = Nondeterministic query complexity

For $f : \{0, 1\}^n \rightarrow \{0, 1\}$,

$$f(x) = 0, f(y) = 1$$

$$\Rightarrow c_x \cap c_y \neq \emptyset$$



For $f : \{0, 1\}^n \rightarrow \{0, 1\}$,

$$f(x) = 0, f(y) = 1$$

$$\Rightarrow (c_x \cap c_y) \cap \{j : x_j \neq y_j\} \neq \emptyset$$

$$C(f) = \min_{\text{certificates } c_x} \max_x |c_x|$$

$$C(f) = \min_{\{\vec{p}_x \in \{0,1\}^n\}} \max_x \sum_j p_x[j] \\ \text{s.t. } \sum_{j: x_j \neq y_j} p_x[j] p_y[j] \geq 1 \quad \text{if } f(x) \neq f(y)$$

$$\text{Adv}(f) = \min_{\{\vec{p}_x \in \mathbb{R}^n\}} \max_x \sum_j p_x[j]^2 \\ \text{s.t. } \sum_{j: x_j \neq y_j} p_x[j] p_y[j] \geq 1 \text{ if } f(x) \neq f(y)$$

$$\text{Adv}(f) = \min_{\{\vec{p}_x \in \mathbb{R}^n\}} \max_x \|\vec{p}_x\|^2$$

s.t. $\sum_{j:x_j \neq y_j} p_x[j]p_y[j] \geq 1 \text{ if } f(x) \neq f(y)$

For OR on $\{0^n, |0^{n-1}, \dots, 0^{n-1}| \}$,

x	0^n	10^{n-1}	\dots	$0^{n-1}1$
\vec{p}_x	$(1, \dots, 1)$	$(1, 0, \dots, 0)$		$(0, \dots, 0, 1)$

$$\Rightarrow \text{Adv}(\text{OR}_n) = \sqrt{n}$$

$$\text{Adv}(f) \leq \sqrt{C_0(f)C_1(f)} \quad \text{for total functions}$$

$$\text{Adv}(f) \leq \sqrt{n \min\{C_0(f), C_1(f)\}} \quad \text{in general}$$

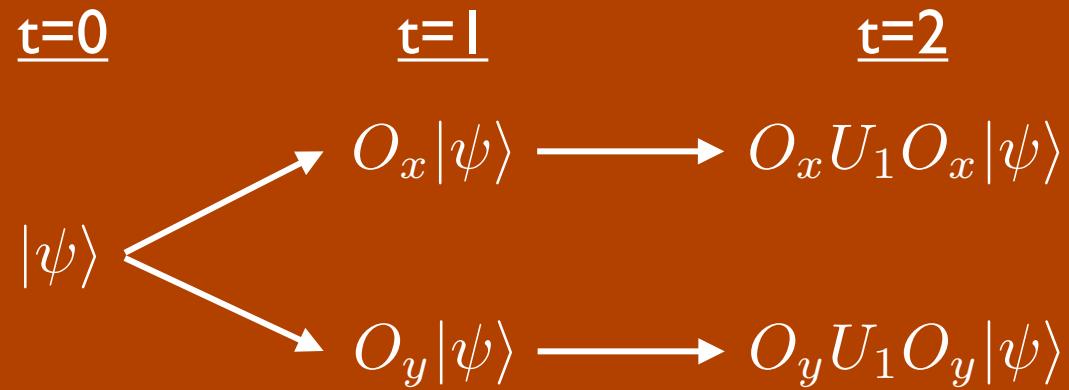
Problem 2. This is still a **minimization** problem

$$\begin{aligned} \text{Adv}(f) = & \min_{\{\vec{p}_x \in \mathbb{R}^n\}} \max_x \|\vec{p}_x\|^2 \\ \text{s.t. } & \sum_{j:x_j \neq y_j} p_x[j]p_y[j] \geq 1 \quad \text{when } f(x) \neq f(y) \end{aligned}$$

Take the dual:

$$\begin{aligned} \text{Adv}(f) = & \max_{\Gamma \in \mathbb{R}^{\mathcal{D} \times \mathcal{D}}} \|\Gamma\| \\ \text{s.t. } & \Gamma[x, y] \geq 0 \\ & \Gamma[x, y] = 0 \text{ if } f(x) = f(y) \\ & \forall j \left\| \Gamma \circ \sum_{x,y:x_j \neq y_j} |x\rangle\langle y| \right\| \leq 1 \end{aligned}$$

$$Q(f) = \Omega(\mathrm{Adv}(f))$$



Idea: Track the divergence of pairs (x, y) with $f(x) \neq f(y)$

All pairs can't diverge at once,
e.g., querying bit 1 only separates pairs with $x_1 \neq y_1$

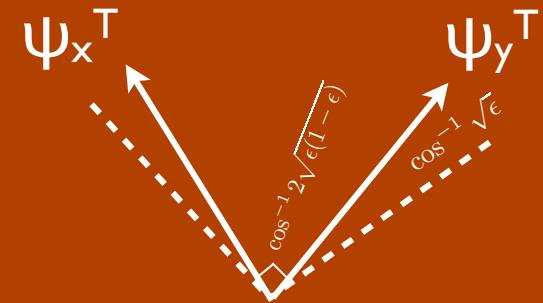
Gram matrix $\rho^t[x,y] = \langle \Psi_x^t, \Psi_y^t \rangle$

Initially

$\rho^0 = \text{all-ones matrix } (J)$

Finally

$|\rho^T[x,y]| \leq 2\sqrt{\epsilon(1-\epsilon)}$



Proof: For a $D \times D$ matrix M , let

$$A(M) = \min_{\{\vec{p}_x \in \mathbb{R}^n\}} \max_x \|\vec{p}_x\|^2$$

$$\sum_{j:x_j \neq y_j} p_x[j]p_y[j] \geq |M[x, y]|$$

- $A(M+N) \leq A(M) + A(N)$
- $A(M) \leq A(N)$ if $M \leq N$ entry-wise
- If J =all-ones matrix, $F[x, y] = \delta_{f(x), f(y)}$,
 $\text{Adv}(f) = A(J - F)$

$$f^{-1}(0) \left\{ \begin{array}{c} f^{-1}(0) \\ f^{-1}(1) \\ f^{-1}(2) \end{array} \right\} \left(\begin{array}{ccc} 0 & f^{-1}(1) & f^{-1}(2) \\ f^{-1}(1) & 0 & 1 \\ f^{-1}(2) & 1 & 0 \end{array} \right)$$

Proof: For a $D \times D$ matrix M , let

$$A(M) = \min_{\{\vec{p}_x \in \mathbb{R}^n\}} \max_x \|\vec{p}_x\|^2$$

$$\sum_{j:x_j \neq y_j} p_x[j]p_y[j] \geq |M[x, y]|$$

- $A(M+N) \leq A(M) + A(N)$
- $A(M) \leq A(N)$ if $M \leq N$ entry-wise
- If J =all-ones matrix, $F[x, y] = \delta_{f(x), f(y)}$,
 $\text{Adv}(f) = A(J - F)$
(a distance: $\rho^0 = J$, “ ρ^T almost lies under F ”)

$$\begin{aligned} \text{Adv}(f) &= A(J - F) = A(\rho^0 \circ (J - F)) \\ &= A\left(\left(\rho^T + \sum_{t=0}^{T-1} (\rho^t - \rho^{t+1})\right) \circ (J - F)\right) \\ &\leq A(\rho^T \circ (J - F)) + \sum_{t=0}^{T-1} A(\rho^t - \rho^{t+1}) \end{aligned}$$

Proof: For a $D \times D$ matrix M , let

$$A(M) = \min_{\{\vec{p}_x \in \mathbb{R}^n\}} \max_x \|\vec{p}_x\|^2$$

s.t. $\sum_{j:x_j \neq y_j} p_x[j]p_y[j] \geq |M[x, y]|$

- $A(M+N) \leq A(M) + A(N)$
- $A(M) \leq A(N)$ if $M \leq N$ entry-wise
- If J =all-ones matrix, $F[x, y] = \delta_{f(x), f(y)}$,
 $\text{Adv}(f) = A(J - F)$
(a distance: $\rho^0 = J$, “ ρ^T almost lies under F ”)

$$\text{Adv}(f) = A(J - F) \leq \underbrace{A(\rho^T \circ (J - F))}_{\| \wedge \|} + \sum_{t=0}^{T-1} \underbrace{A(\rho^t - \rho^{t+1})}_{\| \wedge \|} + 2\sqrt{\epsilon(1-\epsilon)}A(J - F)$$

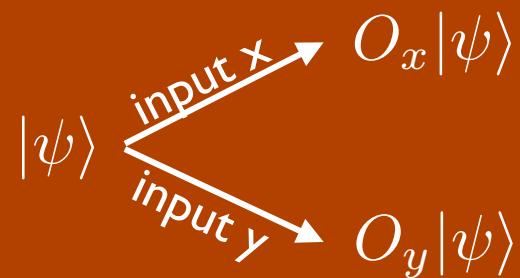
1. Ψ_x^T ($1-\epsilon$)-distinguishable from $\Psi_y^T \Rightarrow |\langle \psi_x^T | \psi_y^T \rangle| \leq 2\sqrt{\epsilon(1-\epsilon)}$
2. Each step is small...

$$\Rightarrow T \text{ is large: } \text{Adv}(f) \leq 2\sqrt{\epsilon(1-\epsilon)}\text{Adv}(f) + 2T$$

□

Each step is small: $A(\rho^t - \rho^{t+1}) \leq 2$

t=0 t=1



$$(\rho^0 - \rho^1)[x, y] = \langle \psi | \psi \rangle - \langle \psi | O_x^\dagger O_y | \psi \rangle = 2 \sum_{j: x_j \neq y_j} \langle \psi | j \rangle \langle j | \psi \rangle$$

$$O_x^\dagger O_y = \sum_j (-1)^{x_j + y_j} |j\rangle\langle j| = I - 2 \sum_{j: x_j \neq y_j} |j\rangle\langle j|$$

General adversary bound
 Adv^\pm

$$C(f) = \min_{\{\vec{p}_x \in \{0,1\}^{\textcolor{blue}{n}}\}} \max_x \left\| \vec{p}_x \right\|^2$$

$$\text{s.t. } \sum_{j: x_j \neq y_j} p_x[j] p_y[j] \geq 1 \quad \text{if } f(x) \neq f(y)$$

$$\mathrm{Adv}(f) = \min_{\{\vec{p}_x \in \mathbb{R}^{\textcolor{blue}{n}}\}} \max_x \left\| \vec{p}_x \right\|^2$$

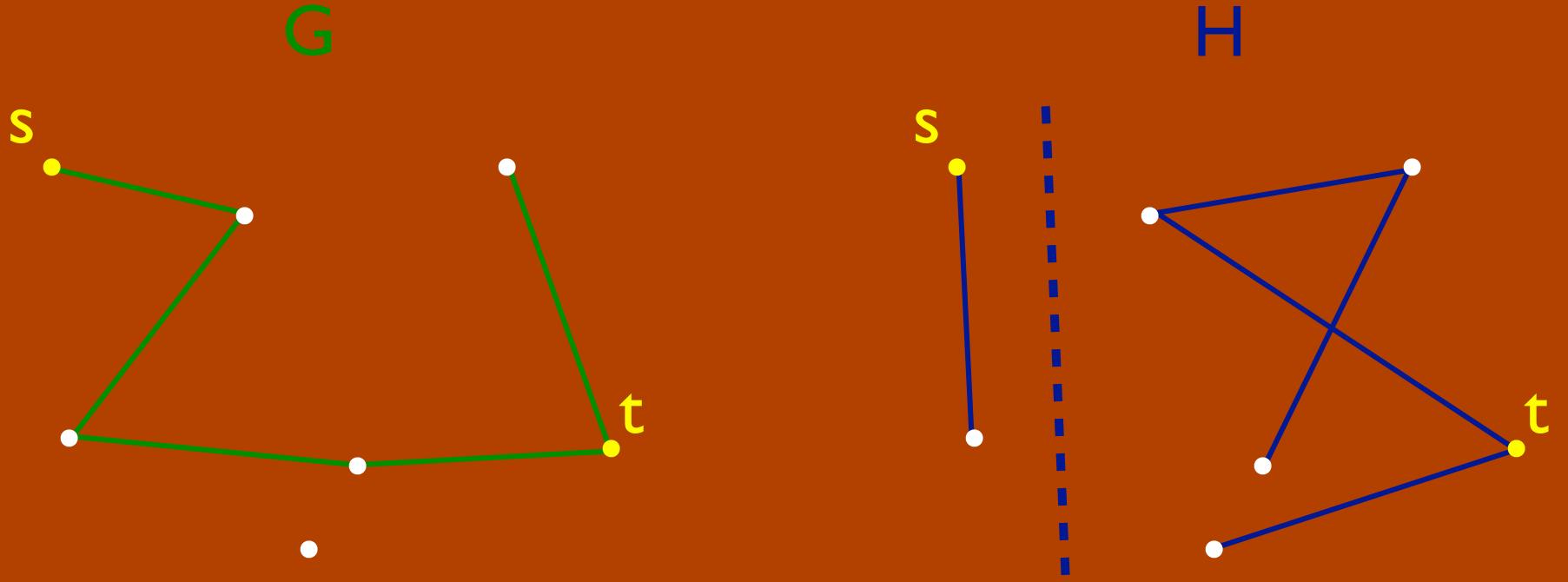
$$\text{s.t. } \sum_{j: x_j \neq y_j} p_x[j] p_y[j] \geq 1 \quad \text{if } f(x) \neq f(y)$$

$$C(f) = \min_{\{p_{xj} \in \{0,1\}\}} \max_x \sum_j p_{xj}^2 \\ \text{s.t. } \sum_{j:x_j=y_j} p_{xj}p_{yj} \geq 1 \quad \text{if } f(x) \neq f(y)$$

$$\mathrm{Adv}(f) = \min_{\{p_{xj} \in \mathbb{R}\}} \max_x \sum_j p_{xj}^2 \\ \text{s.t. } \sum_{j:x_j=y_j} p_{xj}p_{yj} \geq 1 \quad \text{if } f(x) \neq f(y)$$

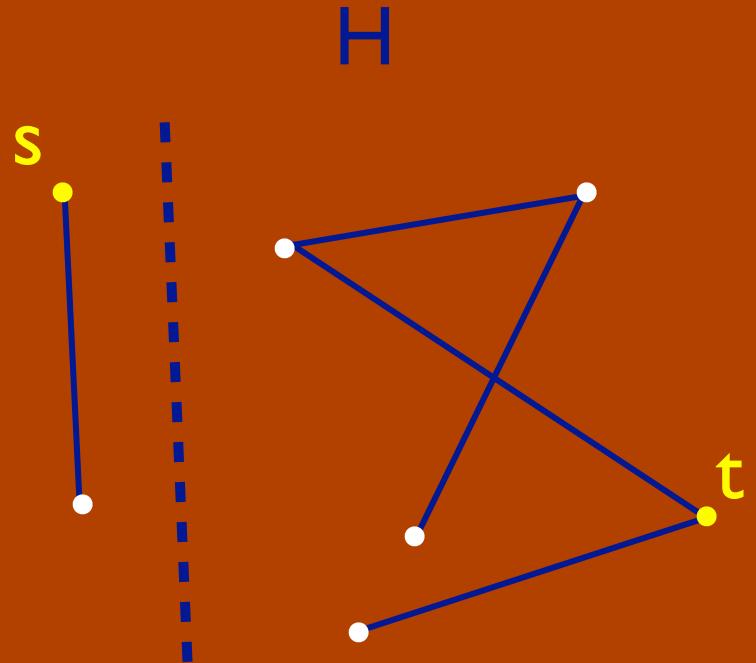
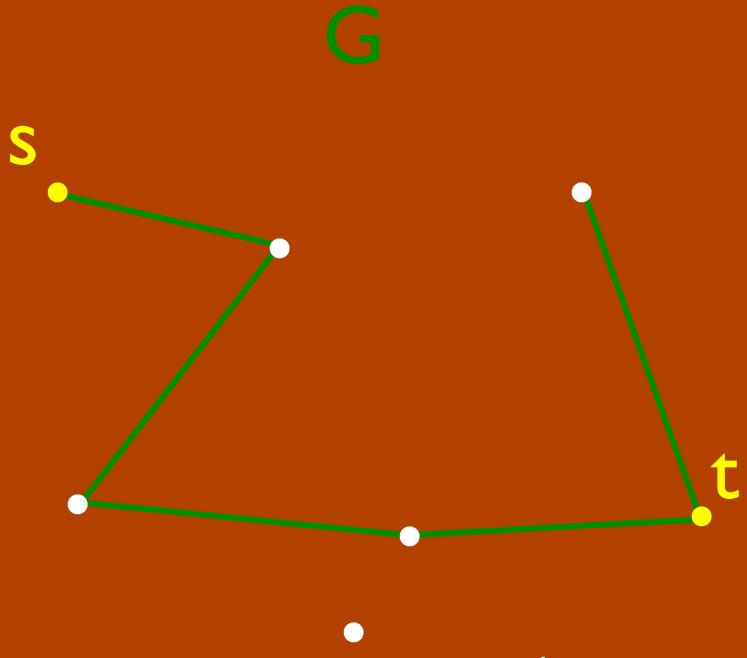
$$\mathrm{Adv}^\pm(f) = \min_{\{|u_{xj}\rangle \in \mathbb{R}^{\textcolor{violet}{m}}\}} \max_x \sum_j \|u_{xj}\|^2 \\ \text{s.t. } \sum_{j:x_j \neq y_j} \langle u_{xj}|u_{yj}\rangle \textcolor{blue}{=} 1 \quad \text{if } f(x) \neq f(y)$$

Example: s-t Connectivity



$p_{Ge} = 1$ along the path, $p_{He} = 1$ across the cut

$$\Rightarrow \sum_{e: e \in G, e \notin H} p_{Ge} p_{He} \geq 1 \quad \Rightarrow \text{Adv}(f) \leq \sqrt{dn^2} \leq n^{3/2}$$



$$u_{Ge} = \begin{cases} 1 & \text{path crosses } e \text{ to the right} \\ -1 & \text{path crosses } e \text{ to the left} \end{cases}$$

$$u_{He} = 1 \text{ across the cut}$$

$$\Rightarrow \sum_{e: e \in G, e \notin H} \langle u_{Ge} | u_{He} \rangle = (\# \text{ right crossings}) - (\# \text{ left crossings}) = 1$$

$$\Rightarrow \text{Adv}^\pm(f) \leq n^{3/2}$$

Why is Adv^\pm a semi-definite program (SDP)?

$$\begin{aligned} \min_{X \succcurlyeq 0} \quad & \text{Tr}(C^T X) \\ \text{s.t.} \quad & \text{Tr}(A_i^T X) = a_i \end{aligned}$$

$$\begin{aligned} \max_{\{b_i\}} \quad & \sum_i a_i b_i \\ \text{s.t.} \quad & C - \sum_i b_i A_i \succcurlyeq 0 \end{aligned}$$

$$\begin{aligned} \text{Adv}^\pm(f) = \min_{\{u_{xj} \in \mathbb{R}^m\}} \quad & \max_x \sum_j \|u_{xj}\|^2 \\ \text{s.t.} \quad & \sum_{j: x_j \neq y_j} \langle u_{xj} | u_{yj} \rangle = 1 \quad \text{if } f(x) \neq f(y) \end{aligned}$$

$$X_j[x, y] = \langle u_{xj} | u_{yj} \rangle$$

$$\begin{aligned} \text{Adv}^\pm(f) = \min_{\{X_j \succcurlyeq 0\}} \quad & \max_x \sum_j \langle x | X_j | x \rangle \\ \text{s.t.} \quad & \sum_{j: x_j \neq y_j} \langle x | X_j | y \rangle = 1 \quad \text{if } f(x) \neq f(y) \end{aligned}$$

$$\text{Adv}^{\pm}(f) = \max_{\Gamma \in \mathbb{R}^{\mathcal{D} \times \mathcal{D}}} \|\Gamma\|$$

subject to:

$$\Gamma[x, y] \geq 0$$

$$\Gamma[x, y] = 0 \text{ if } f(x) = f(y)$$

$$\forall j \left\| \Gamma \circ \sum_{x,y: x_j \neq y_j} |x\rangle\langle y| \right\| \leq 1$$

General adversary bound:

For $f: D \rightarrow \{0, 1\}$:

$$\begin{aligned} \text{Adv}^{\pm}(f) = & \min_{\{u_{xj} \in \mathbb{R}^m\}} \max_x \sum_j \|u_{xj}\|^2 \\ \text{s.t. } & \sum_{j: x_j \neq y_j} \langle u_{xj} | u_{yj} \rangle = 1 \quad \text{if } f(x) \neq f(y) \end{aligned}$$

For $f: D \rightarrow E$:

$$\begin{aligned} \text{Adv}^{\pm}(f) = & \min_{\{u_{xj}, v_{xj} \in \mathbb{R}^m\}} \max_x \max \left\{ \sum_j \|u_{xj}\|^2, \sum_j \|v_{xj}\|^2 \right\} \\ \text{s.t. } & \sum_{j: x_j \neq y_j} \langle u_{xj} | v_{yj} \rangle = 1 \quad \text{if } f(x) \neq f(y) \end{aligned}$$

$$Q(f) = \Omega(\mathrm{Adv}^\pm(f))$$

$$\begin{aligned} A^\pm(M) = & \min_{\{\vec{u}_{xj} \in \mathbb{R}^m\}} \max_x \sum_j \|u_{xj}\|^2 \\ \text{s.t. } & \sum_{j:x_j \neq y_j} \langle u_{xj} | u_{yj} \rangle = M[x, y] \end{aligned}$$

- Same initial condition
- Same single-step factorization
- More involved final case

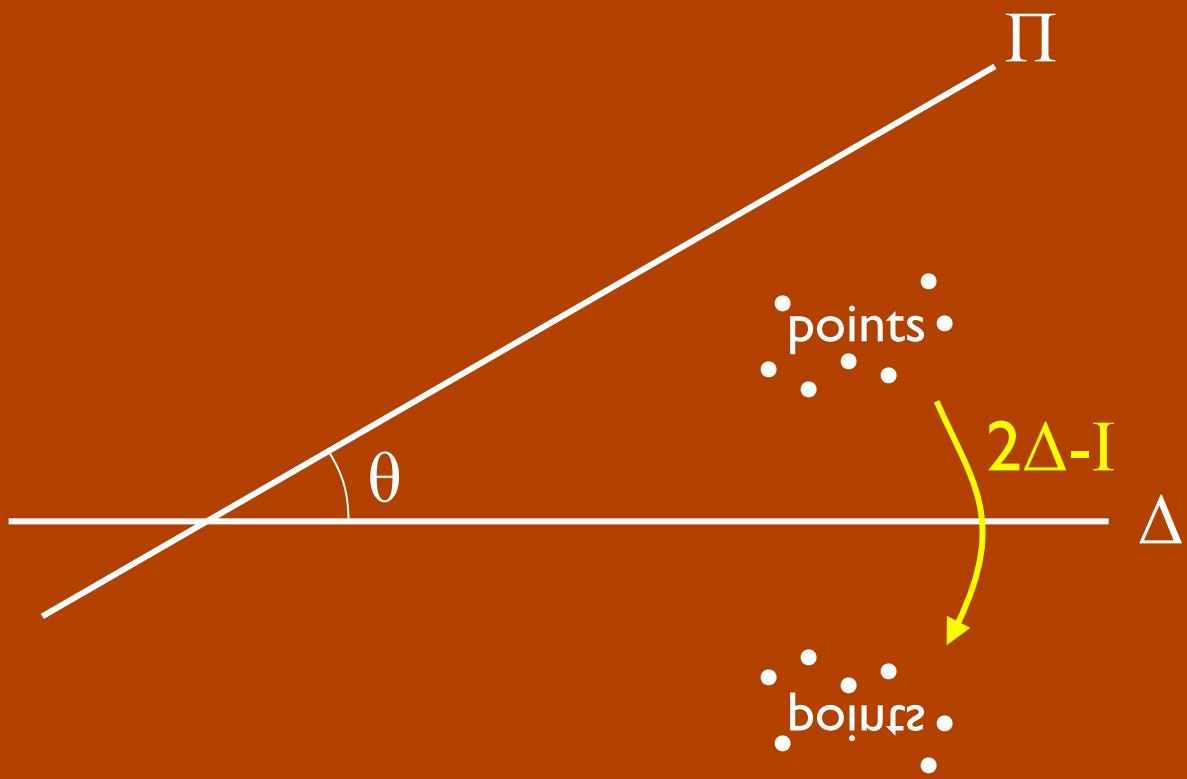
- A. Query complexity
- B. Adversary lower bounds
- C. Spectra of reflections
- D. Adversary upper bound
$$Q(f) = \Theta(\text{Adv}^\pm(f))$$

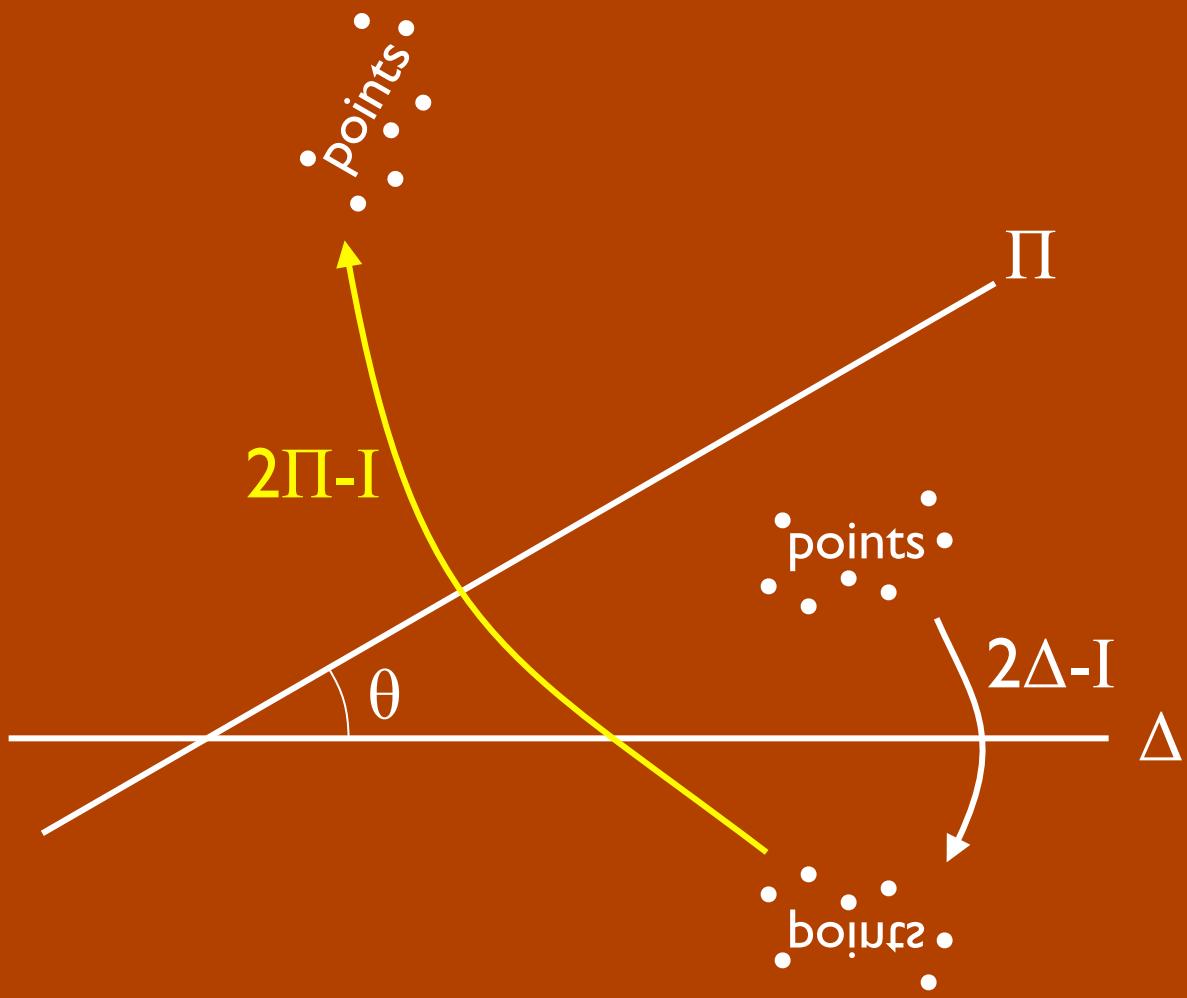
A reflection is an operator that squares to the identity.

A reflection is a unitary with eigenvalues ± 1 .

$$R = \Pi - (I - \Pi) = 2\Pi - I$$

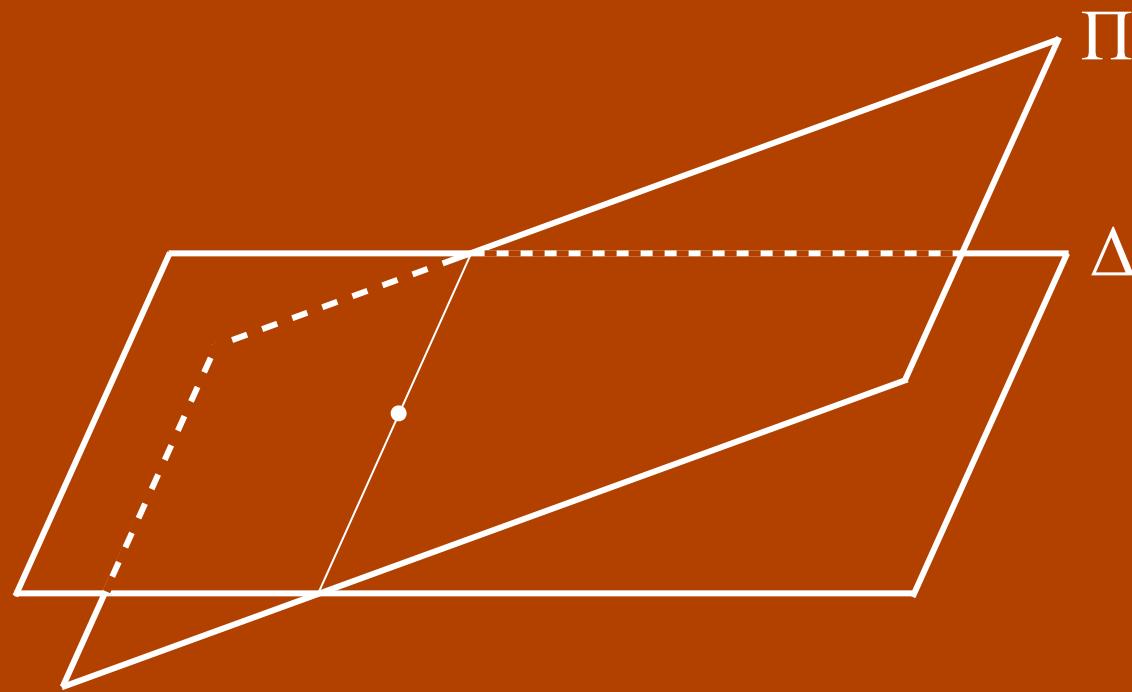
Π = projection onto the $+1$ -eigenvalue eigenspace of R

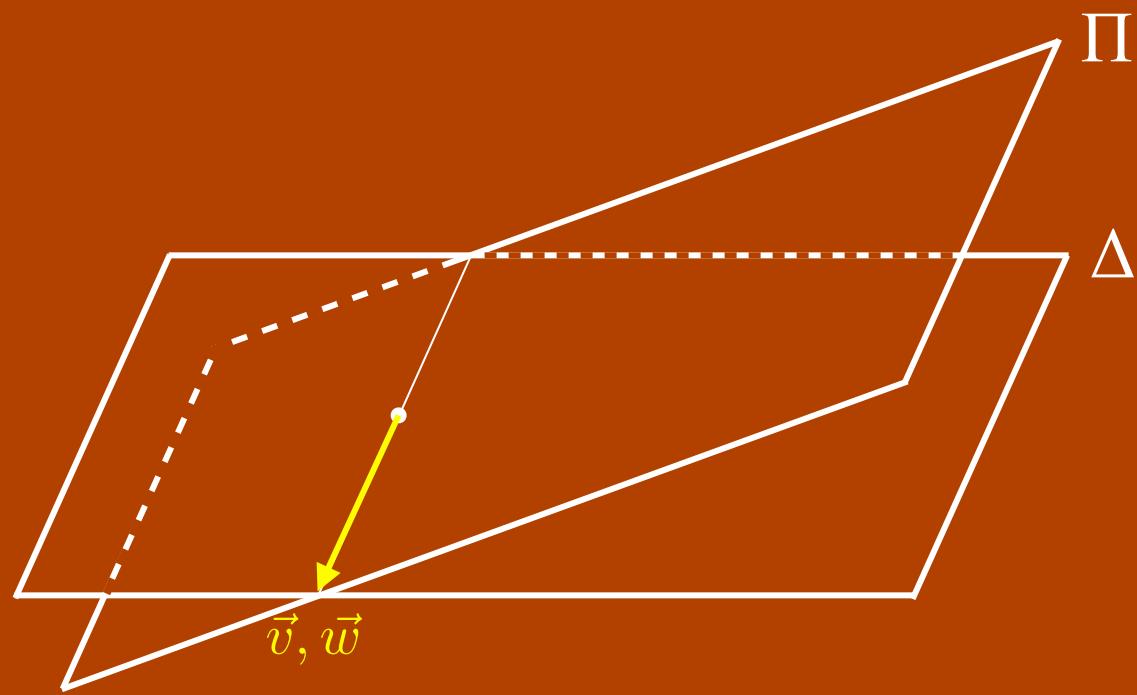




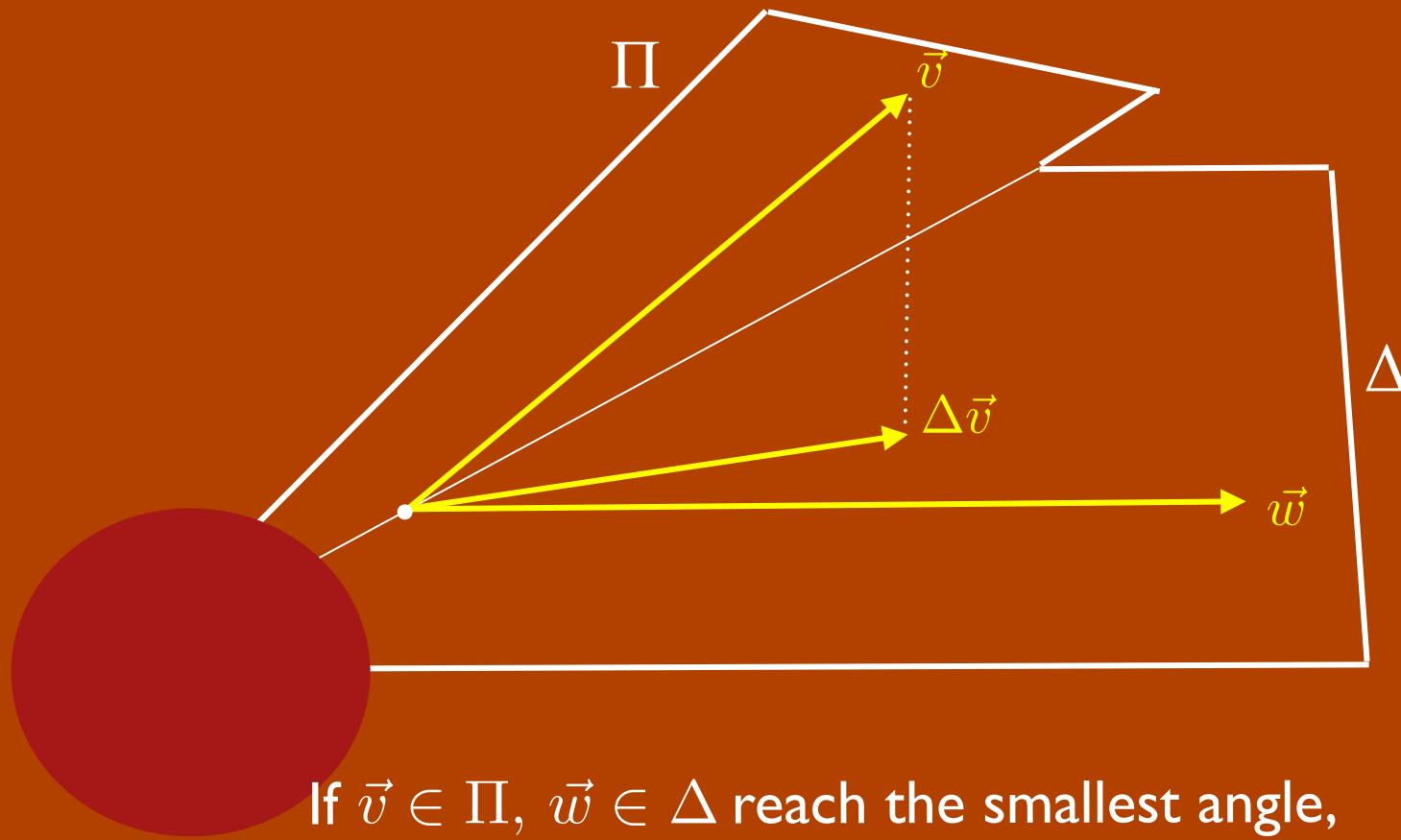
$(2\Pi-I)(2\Delta-I)$ is a rotation by angle 2θ ,
eigenvalues $e^{\pm 2i\theta}$, eigenvectors $(1, \pm i)$

Two subspaces will not generally lie at a fixed angle

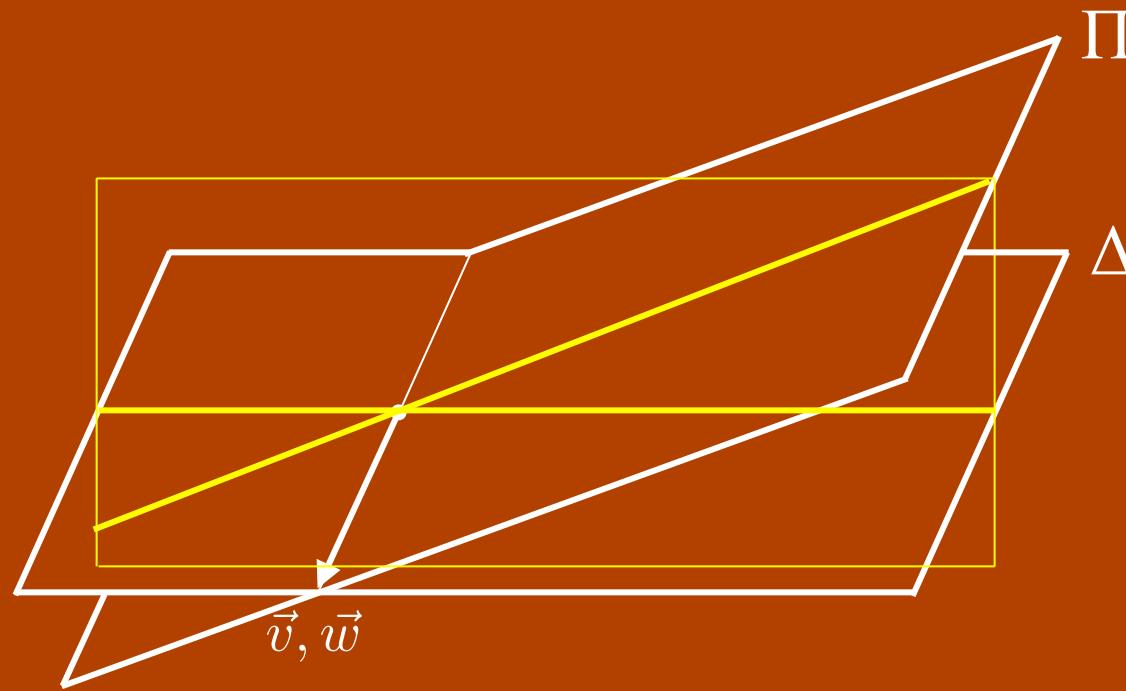




If $\vec{v} \in \Pi$, $\vec{w} \in \Delta$ reach the smallest angle,
then $\Delta\vec{v} \propto \vec{w}$, $\Pi\vec{w} \propto \vec{v}$



$$\begin{aligned}\Delta\vec{v} &= \lambda\vec{w} + \mu\vec{w}^\perp \\ \Rightarrow \frac{1}{\sqrt{1+\epsilon^2}}\langle v, w + \epsilon w^\perp \rangle &= \frac{\langle v, w \rangle + \epsilon\mu}{\sqrt{1+\epsilon^2}} > \langle v, w \rangle\end{aligned}$$



If $\vec{v} \in \Pi$, $\vec{w} \in \Delta$ reach the smallest angle,
then $\Delta\vec{v} \propto \vec{w}$, $\Pi\vec{w} \propto \vec{v}$

$\therefore \text{Span}\{\vec{v}, \vec{w}\}$ is fixed by Π and Δ

$\therefore \text{Span}\{\vec{v}, \vec{w}\}^\perp$ is fixed by Π and Δ

Jordan's Lemma (1875)

Two reflections acting on a Hilbert space decompose it into irreducible one- and two-dimensional subspaces

Any two projections can be simultaneously block-diagonalized with blocks of dimension at most two

$$U\Pi U^\dagger = \begin{pmatrix} & & 0 & 0 \\ & \ddots & & \\ 0 & & \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} & 0 \\ & & & \ddots \\ 0 & 0 & & \end{pmatrix}$$

$$U\Delta U^\dagger = \begin{pmatrix} & & 0 & 0 \\ & \ddots & & \\ 0 & \begin{pmatrix} \cos^2 \theta & \cos \theta \sin \theta \\ \cos \theta \sin \theta & \sin^2 \theta \end{pmatrix} & 0 \\ & & & \ddots \\ 0 & 0 & & \end{pmatrix}$$

Up to an isometry,

$$(2\Pi - I)(2\Delta - I) = \sum_{\beta} |\beta\rangle\langle\beta| \otimes \begin{pmatrix} \cos 2\theta_{\beta} & -\sin 2\theta_{\beta} \\ \sin 2\theta_{\beta} & \cos 2\theta_{\beta} \end{pmatrix}$$

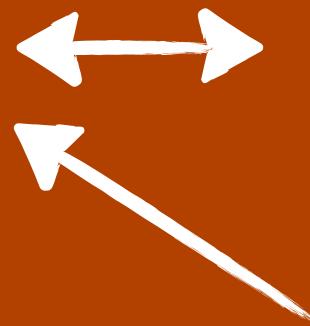
In-place amplification of QMA

Quantum zero knowledge

Szegedy correspondence

Discrete-time
quantum walks
(unitary)

Continuous-time
quantum walks
(Hamiltonian)



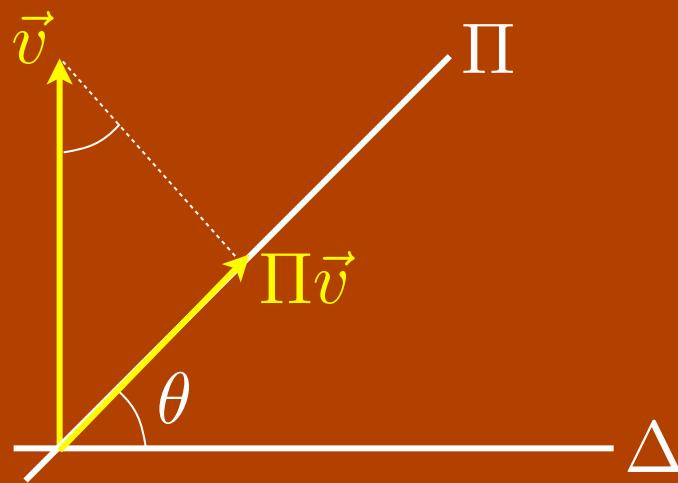
Random walks

1. [MW cs/0506068, NWZ 0904.1549]
2. [W 0511020]
3. [S 0401053, MNRS 0608026, RS 0710.2630, C 0810.0312]

Effective Spectral Gap Lemma:

- Let Π, Δ be two projections
- Let P_Θ be the projection onto eigenvectors of $(2\Pi-1)(2\Delta-1)$ with phase less than 2Θ in magnitude
- Then for any \vec{v} with $\Delta\vec{v} = 0$,

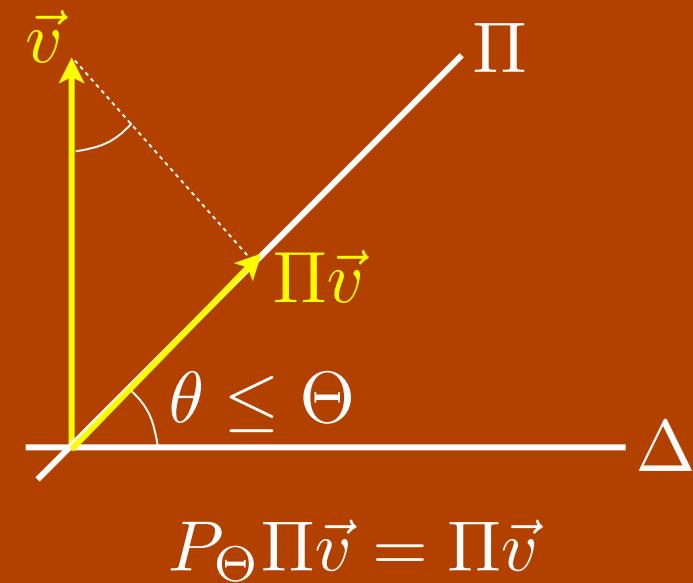
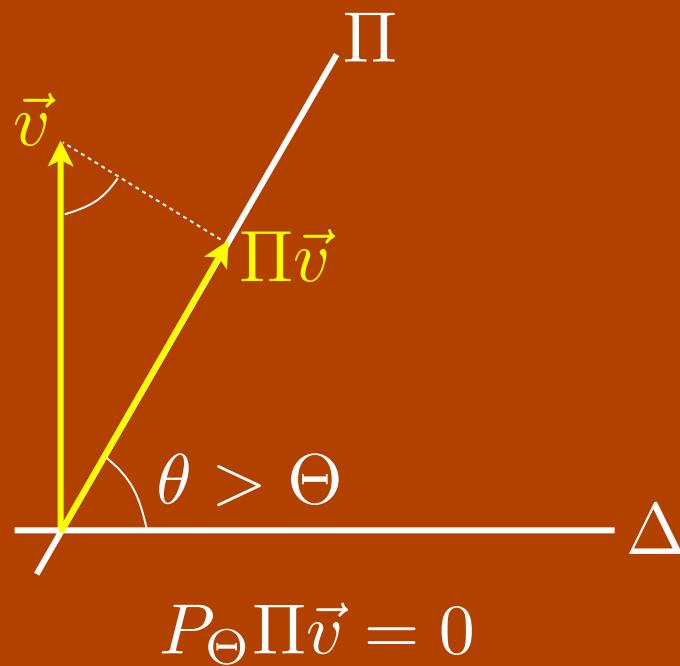
$$\|P_\Theta \Pi \vec{v}\| \leq \Theta \|\vec{v}\|$$



Effective Spectral Gap Lemma:

- Let Π, Δ be two projections
- Let P_Θ be the projection onto eigenvectors of $(2\Pi-1)(2\Delta-1)$ with phase less than 2Θ in magnitude
- Then for any \vec{v} with $\Delta\vec{v} = 0$,

$$\|P_\Theta \Pi \vec{v}\| \leq \Theta \|\vec{v}\|$$

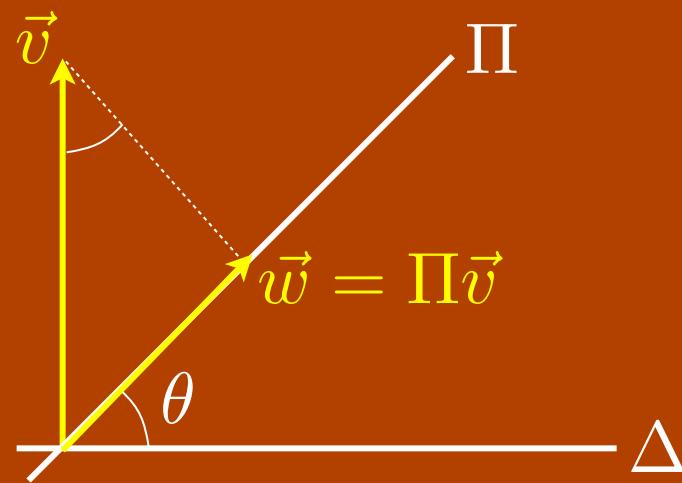


Effective Spectral Gap Lemma:

- Let Π, Δ be two projections
- Let P_Θ be the projection onto eigenvectors of $(2\Pi-1)(2\Delta-1)$ with phase less than 2Θ in magnitude
- Then for any \vec{v} with $\Delta\vec{v} = 0$,

$$\|P_\Theta \Pi \vec{v}\| \leq \Theta \|\vec{v}\|$$

Application:



Effective Spectral Gap Lemma:

- Let Π, Δ be two projections
- Let P_Θ be the projection onto eigenvectors of $(2\Pi-1)(2\Delta-1)$ with phase less than 2Θ in magnitude
- Then for any \vec{v} with $\Delta\vec{v} = 0$,

$$\|P_\Theta \Pi \vec{v}\| \leq \Theta \|\vec{v}\|$$

Proof: Jordan's Lemma \Rightarrow Up to a change in basis,

$$\Delta = \sum_{\beta} |\beta\rangle\langle\beta| \otimes \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

$$\Pi = \sum_{\beta} |\beta\rangle\langle\beta| \otimes \begin{pmatrix} \cos^2 \theta_{\beta} & \sin \theta_{\beta} \cos \theta_{\beta} \\ \sin \theta_{\beta} \cos \theta_{\beta} & \sin^2 \theta_{\beta} \end{pmatrix}$$

$$\Delta|v\rangle = 0 \Rightarrow |v\rangle = \sum_{\beta} d_{\beta} |\beta\rangle \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$\Rightarrow P_\Theta \Pi |v\rangle = \sum_{\beta: |\theta_{\beta}| \leq \Theta} d_{\beta} |\beta\rangle \otimes \sin \theta_{\beta} \begin{pmatrix} \cos \theta_{\beta} \\ \sin \theta_{\beta} \end{pmatrix}$$

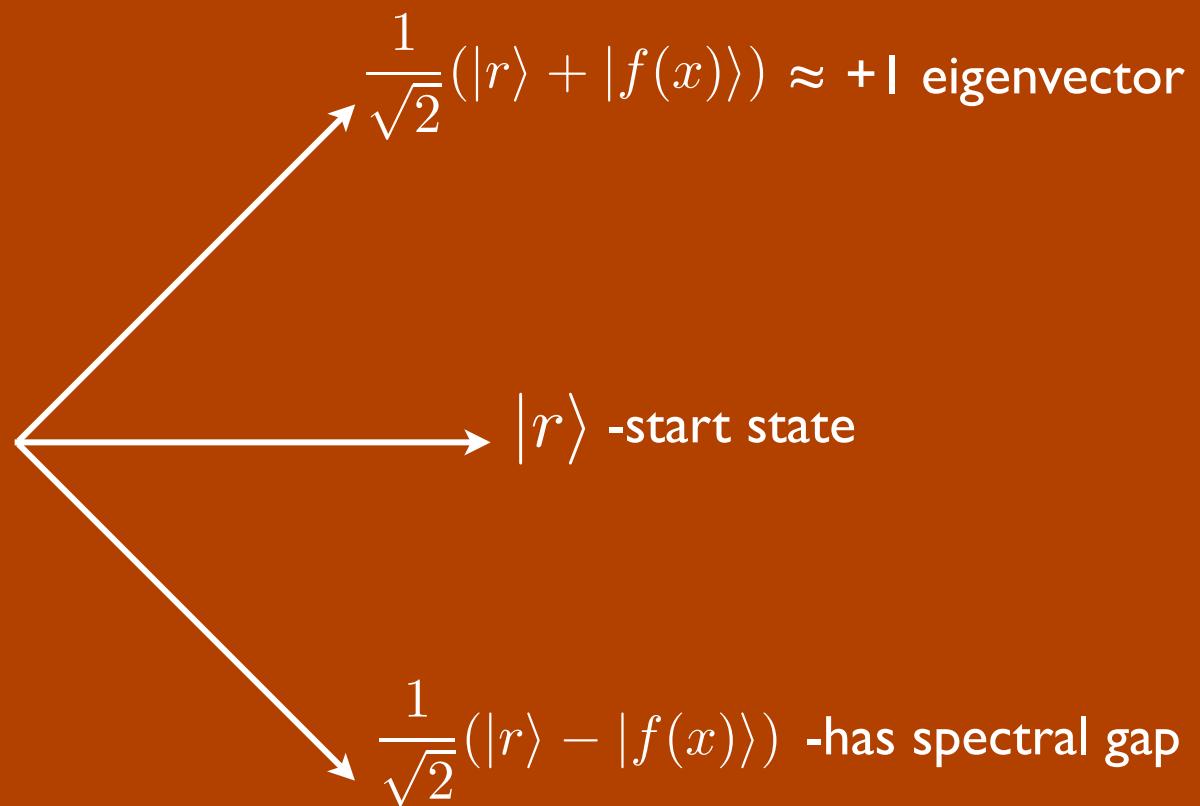
□

- A. Query model
- B. Adversary lower bounds
- C. Spectra of reflections
- D. Adversary upper bound

$$Q(f) = \Theta(\text{Adv}^\pm(f))$$

For $f : \mathcal{D} \rightarrow E$

let $\mathcal{H} = \mathbb{C}^{\{r\}} \oplus \mathbb{C}^E$, i.e., $\mathbb{C}^{1+|E|}$ with basis $|r\rangle, |e\rangle : e \in E$



The algorithm: Let $f : \{0, 1\}^n \rightarrow E$

I. Begin with a vector solution to the SDP:

$$\begin{aligned} \min_{\{u_{xj}, v_{xj} \in \mathbb{C}^m\}} \quad & \max_x \max \left\{ \sum_j \|u_{xj}\|^2, \sum_j \|v_{xj}\|^2 \right\} \\ \text{s.t. } \forall x, y \quad & \sum_{j: x_j \neq y_j} \langle u_{xj} | v_{xj} \rangle = 1 - \delta_{f(x), f(y)} \\ & \| \end{aligned}$$

$$\begin{aligned} \min \quad & \max_x \max \left\{ \|\tilde{u}_x\|^2, \|\tilde{v}_x\|^2 \right\} \\ |\tilde{u}_x\rangle = \sum_j & |j, x_j\rangle \otimes |u_{xj}\rangle \\ |\tilde{v}_y\rangle = \sum_j & |j, \bar{y}_j\rangle \otimes |v_{yj}\rangle \quad \text{s.t. } \forall x, y \quad \langle \tilde{u}_x | \tilde{v}_y \rangle = 1 - \delta_{f(x), f(y)} \end{aligned}$$

The algorithm: Let $f : \{0, 1\}^n \rightarrow E$

I. Begin with a vector solution to the SDP:

$$W = \min_{\substack{|\tilde{u}_x\rangle = \sum_j |j, x_j\rangle \otimes |u_{xj}\rangle \\ |\tilde{v}_x\rangle = \sum_j |j, \bar{x}_j\rangle \otimes |v_{xj}\rangle}} \max_x \max \left\{ \|\tilde{u}_x\|^2, \|\tilde{v}_x\|^2 \right\}$$

s.t. $\forall x, y \quad \langle \tilde{u}_x | \tilde{v}_y \rangle = 1 - \delta_{f(x), f(y)}$

2. Let $\mathcal{H} = \mathbb{C}^{\{r\}} \oplus \mathbb{C}^E \oplus (\mathbb{C}^n \otimes \mathbb{C}^2 \otimes \mathbb{C}^m)$

$$|\psi_y\rangle = |r\rangle + |f(y)\rangle + \frac{1}{10\sqrt{W}} |\tilde{u}_y\rangle \in \mathcal{H}$$

Δ = projection onto $\text{span}\{\psi_y\}$

$$\Pi_x = I - \sum_j |j\rangle\langle j| \otimes |\bar{x}_j\rangle\langle\bar{x}_j| \otimes I_m$$

3. Starting at r , alternate reflections about Δ and Π_x ...

$$\begin{aligned} |\tilde{u}_x\rangle &= \sum_j |j, x_j\rangle \otimes |u_{xj}\rangle \\ |\tilde{v}_x\rangle &= \sum_j |j, \bar{x}_j\rangle \otimes |v_{xj}\rangle \end{aligned}$$

$$|\psi_y\rangle = |r\rangle + |f(y)\rangle + \tfrac{1}{10\sqrt{W}}|\tilde{u}_y\rangle$$

Δ = proj. onto $\text{span}\{\psi_y\}$

$$\Pi_x = I - \sum_j |j, \bar{x}_j\rangle \langle j, \bar{x}_j| \otimes I_m$$

$$\sqrt{W} = \max_x \max \{ \|\tilde{u}_x\|, \|\tilde{v}_x\| \}$$

$$\langle \tilde{u}_x | \tilde{v}_y \rangle = 1 - \delta_{f(x), f(y)}$$

Lemma:

$$\vec{v} \in \Delta^\perp \Rightarrow \|P_\Theta \Pi \vec{v}\| \leq \Theta \|\vec{v}\|$$

The analysis:

$$|r\rangle = \frac{1}{2}(|r\rangle + |f(x)\rangle) + \frac{1}{2}(|r\rangle - |f(x)\rangle)$$

$$\begin{aligned} |\tilde{u}_x\rangle &= \sum_j |j, x_j\rangle \otimes |u_{xj}\rangle \\ |\tilde{v}_x\rangle &= \sum_j |j, \bar{x}_j\rangle \otimes |v_{xj}\rangle \end{aligned}$$

$$|\psi_y\rangle = |r\rangle + |f(y)\rangle + \tfrac{1}{10\sqrt{W}}|\tilde{u}_y\rangle$$

Δ = proj. onto $\text{span}\{\psi_y\}$

$$\Pi_x = I - \sum_j |j, \bar{x}_j\rangle \langle j, \bar{x}_j| \otimes I_m$$

$$\sqrt{W} = \max_x \max \{ \|\tilde{u}_x\|, \|\tilde{v}_x\| \}$$

$$\langle \tilde{u}_x | \tilde{v}_y \rangle = 1 - \delta_{f(x), f(y)}$$

Lemma:

$$\vec{v} \in \Delta^\perp \Rightarrow \|P_\Theta \Pi \vec{v}\| \leq \Theta \|\vec{v}\|$$

The analysis:

$$|r\rangle = \underbrace{\frac{1}{2}(|r\rangle + |f(x)\rangle)}_{\text{close to } |\psi_x\rangle} + \frac{1}{2}(|r\rangle - |f(x)\rangle)$$

–doesn't move

$$\begin{aligned} |\tilde{u}_x\rangle &= \sum_j |j, x_j\rangle \otimes |u_{xj}\rangle \\ |\tilde{v}_x\rangle &= \sum_j |j, \bar{x}_j\rangle \otimes |v_{xj}\rangle \end{aligned}$$

$$|\psi_y\rangle = |r\rangle + |f(y)\rangle + \frac{1}{10\sqrt{W}}|\tilde{u}_y\rangle$$

Δ = proj. onto $\text{span}\{\psi_y\}$

$$\Pi_x = I - \sum_j |j, \bar{x}_j\rangle \langle j, \bar{x}_j| \otimes I_m$$

$$\sqrt{W} = \max_x \max \{ \|\tilde{u}_x\|, \|\tilde{v}_x\| \}$$

$$\langle \tilde{u}_x | \tilde{v}_y \rangle = 1 - \delta_{f(x), f(y)}$$

Lemma:

$$\vec{v} \in \Delta^\perp \Rightarrow \|P_\Theta \Pi \vec{v}\| \leq \Theta \|\vec{v}\|$$

The analysis:

$$\begin{aligned} |r\rangle &= \underbrace{\frac{1}{2}(|r\rangle + |f(x)\rangle)}_{\substack{\text{close to } |\psi_x\rangle \\ \text{--doesn't move}}} + \underbrace{\frac{1}{2}(|r\rangle - |f(x)\rangle)}_{\substack{} \\ = \Pi_x(|r\rangle - |f(x)\rangle - 10\sqrt{W}|\tilde{v}_x\rangle)} \end{aligned}$$

$$\begin{aligned} |\tilde{u}_x\rangle &= \sum_j |j, x_j\rangle \otimes |u_{xj}\rangle \\ |\tilde{v}_x\rangle &= \sum_j |j, \bar{x}_j\rangle \otimes |v_{xj}\rangle \end{aligned}$$

$$|\psi_y\rangle = |r\rangle + |f(y)\rangle + \frac{1}{10\sqrt{W}}|\tilde{u}_y\rangle$$

Δ = proj. onto $\text{span}\{\psi_y\}$

$$\Pi_x = I - \sum_j |j, \bar{x}_j\rangle \langle j, \bar{x}_j| \otimes I_m$$

$$\sqrt{W} = \max_x \max \{ \|\tilde{u}_x\|, \|\tilde{v}_x\| \}$$

$$\langle \tilde{u}_x | \tilde{v}_y \rangle = 1 - \delta_{f(x), f(y)}$$

Lemma:

$$\vec{v} \in \Delta^\perp \Rightarrow \|P_\Theta \Pi \vec{v}\| \leq \Theta \|\vec{v}\|$$

The analysis:

$$\begin{aligned} |r\rangle &= \underbrace{\frac{1}{2}(|r\rangle + |f(x)\rangle)}_{\substack{\text{close to } |\psi_x\rangle \\ \text{--- doesn't move}}} + \underbrace{\frac{1}{2}(|r\rangle - |f(x)\rangle)}_{\substack{} \\ = \Pi_x(|r\rangle - |f(x)\rangle - 10\sqrt{W}|\tilde{v}_x\rangle)} \\ &\quad \nparallel \vec{v} \in \Delta^\perp \end{aligned}$$

$$\begin{aligned} |\tilde{u}_x\rangle &= \sum_j |j, x_j\rangle \otimes |u_{xj}\rangle \\ |\tilde{v}_x\rangle &= \sum_j |j, \bar{x}_j\rangle \otimes |v_{xj}\rangle \end{aligned}$$

$$|\psi_y\rangle = |r\rangle + |f(y)\rangle + \frac{1}{10\sqrt{W}}|\tilde{u}_y\rangle$$

Δ = proj. onto $\text{span}\{\psi_y\}$

$$\Pi_x = I - \sum_j |j, \bar{x}_j\rangle \langle j, \bar{x}_j| \otimes I_m$$

$$\sqrt{W} = \max_x \max \{ \|\tilde{u}_x\|, \|\tilde{v}_x\| \}$$

$$\langle \tilde{u}_x | \tilde{v}_y \rangle = 1 - \delta_{f(x), f(y)}$$

Lemma:

$$\vec{v} \in \Delta^\perp \Rightarrow \|P_\Theta \Pi \vec{v}\| \leq \Theta \|\vec{v}\|$$

The analysis:

$$\begin{aligned} |r\rangle &= \underbrace{\frac{1}{2}(|r\rangle + |f(x)\rangle)}_{\substack{\text{close to } |\psi_x\rangle \\ \text{--- doesn't move}}} + \underbrace{\frac{1}{2}(|r\rangle - |f(x)\rangle)}_{\substack{} \\ = \Pi_x(|r\rangle - |f(x)\rangle - 10\sqrt{W}|\tilde{v}_x\rangle)} \\ &\quad \nparallel \vec{v} \in \Delta^\perp \\ &\Rightarrow \Omega(1/W) \text{ effective spectral gap} \end{aligned}$$

$$\begin{aligned} |\tilde{u}_x\rangle &= \sum_j |j, x_j\rangle \otimes |u_{xj}\rangle \\ |\tilde{v}_x\rangle &= \sum_j |j, \bar{x}_j\rangle \otimes |v_{xj}\rangle \end{aligned}$$

$$|\psi_y\rangle = |r\rangle + |f(y)\rangle + \frac{1}{10\sqrt{W}}|\tilde{u}_y\rangle$$

Δ = proj. onto $\text{span}\{\psi_y\}$

$$\Pi_x = I - \sum_j |j, \bar{x}_j\rangle \langle j, \bar{x}_j| \otimes I_m$$

$$\sqrt{W} = \max_x \max \{ \|\tilde{u}_x\|, \|\tilde{v}_x\| \}$$

$$\langle \tilde{u}_x | \tilde{v}_y \rangle = 1 - \delta_{f(x), f(y)}$$

Lemma:

$$\vec{v} \in \Delta^\perp \Rightarrow \|P_\Theta \Pi \vec{v}\| \leq \Theta \|\vec{v}\|$$

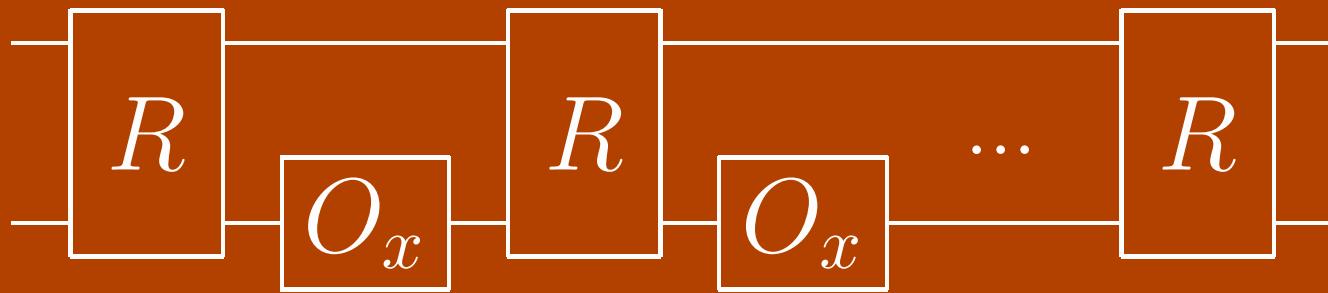
The analysis:

$$\begin{aligned} |r\rangle &= \underbrace{\frac{1}{2}(|r\rangle + |f(x)\rangle)}_{\substack{\text{close to } |\psi_x\rangle \\ \text{--- doesn't move}}} + \underbrace{\frac{1}{2}(|r\rangle - |f(x)\rangle)}_{\substack{} \\ = \Pi_x(|r\rangle - |f(x)\rangle - 10\sqrt{W}|\tilde{v}_x\rangle)} \\ &\quad \Rightarrow \vec{v} \in \Delta^\perp \\ &\quad \Rightarrow \Omega(1/W) \text{ effective spectral gap} \end{aligned}$$

\Rightarrow Running phase estimation with precision $1/100W$,

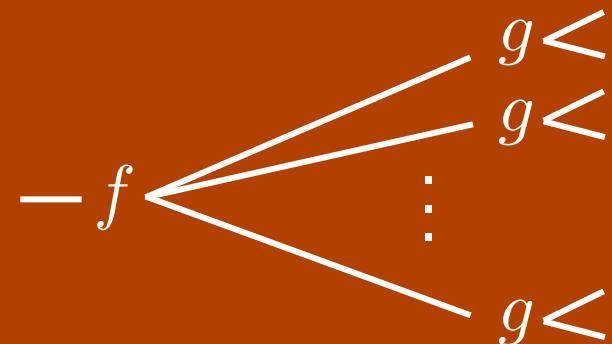
with prob. $\approx 1/2$ measure eigenvalue 1 , leaving $\frac{1}{\sqrt{2}}(|r\rangle + |f(x)\rangle)$!

Corollaries



How does query complexity change under composition?

Model: For $f : \{0, 1\}^n \rightarrow \{0, 1\}$, $g : \{0, 1\}^m \rightarrow \{0, 1\}$
let $f \bullet g$ be the function $f \circ (g, g, \dots, g)$



- Deterministic query complexity $D(f \bullet g) = D(f)D(g)$
- Randomized $R(f \bullet g) \leq R(f)R(g) \cdot O(\log n)$
- Certificate complexity $C(f \bullet g) \leq C(f)C(g)$
(can be \ll)

Model: For $f : \{0, 1\}^n \rightarrow \{0, 1\}$, $g : \{0, 1\}^m \rightarrow \{0, 1\}$
let $f \bullet g$ be the function $f \circ (g, g, \dots, g)$

- Deterministic query complexity • Certificate complexity

$$D(f \bullet g) = D(f)D(g)$$
 - Randomized

$$R(f \bullet g) \leq R(f)R(g) \cdot O(\log n)$$

- Quantum query complexity

Claim: $\text{Adv}^\pm(f \bullet g) = \text{Adv}^\pm(f)\text{Adv}^\pm(g)$

$$\Rightarrow Q(f \bullet g) = \Theta(Q(f)Q(g))$$

$$\Rightarrow Q(f_1 \bullet f_2 \bullet \dots \bullet f_d) = \Theta(\text{Adv}^\pm(f_1) \dots \text{Adv}^\pm(f_d))$$

Proof idea for \leq direction:

Let u, v and μ, ν be vector Adv^\pm solutions for f and for g

Then “ $u \otimes \mu$ ”, “ $v \otimes v$ ” is a solution for $f \bullet g$

if domain $D \subseteq \{0, 1\}^n$:

$$\begin{aligned} |\tilde{u}_x\rangle &= \sum_j |j, x_j\rangle \otimes |u_{xj}\rangle & \Rightarrow \quad \langle \tilde{u}_x | \tilde{v}_y \rangle &= \sum_{j: x_j \neq y_j} \langle u_{xj} | v_{xj} \rangle \\ |\tilde{v}_y\rangle &= \sum_j |j, \bar{y}_j\rangle \otimes |v_{xj}\rangle \end{aligned}$$

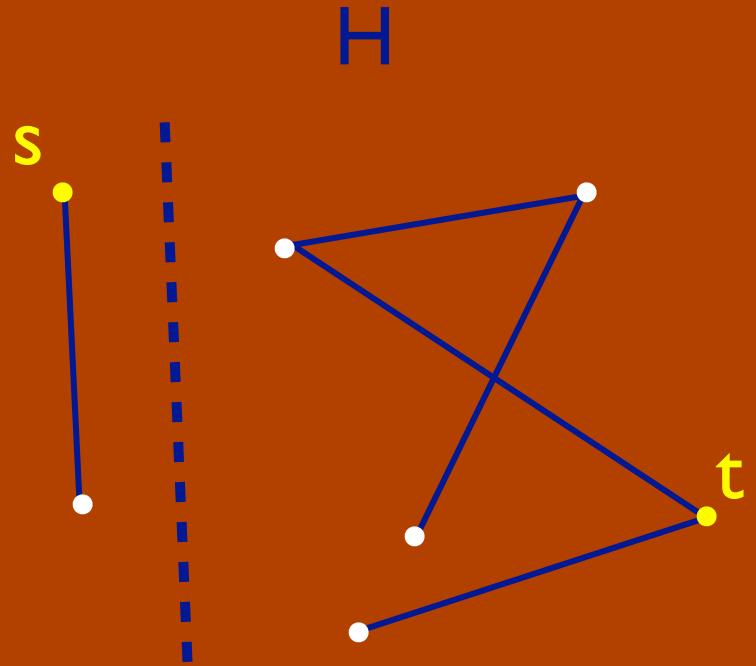
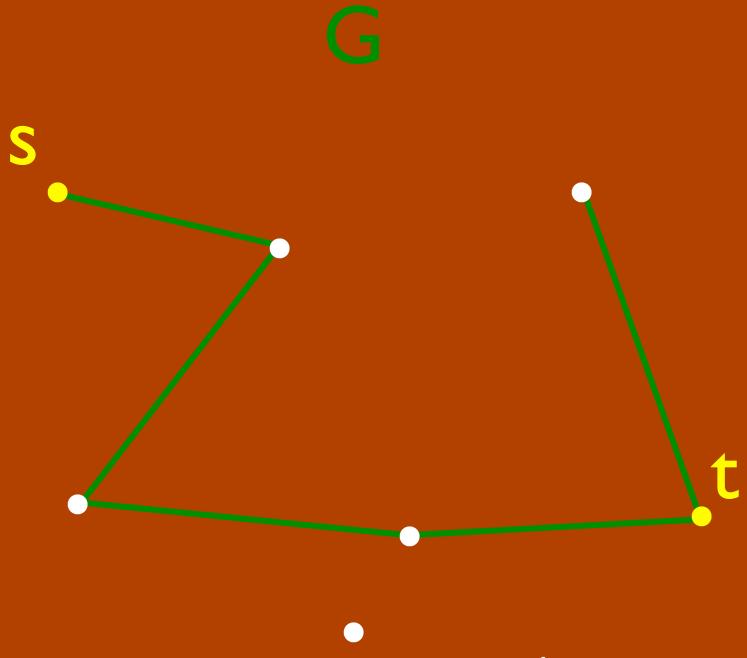
if $D \subseteq \{1, 2, \dots, k\}^n$:

let $|\mu_b\rangle = |0\rangle + |b\rangle$, $|\nu_b\rangle = |0\rangle - |b\rangle$

so $\langle \mu_b | \nu_{b'} \rangle = 1 - \delta_{b,b'}$

$$|\tilde{u}_x\rangle = \sum_j |j, \mu_{x_j}\rangle \otimes |u_{xj}\rangle \quad |\tilde{v}_y\rangle = \sum_j |j, \nu_{y_j}\rangle \otimes |v_{yj}\rangle$$

Time complexity:
s-t Connectivity

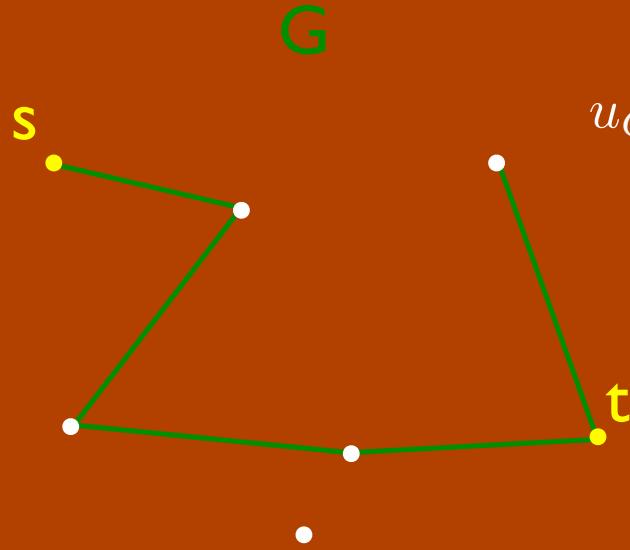


$$u_{Ge} = \begin{cases} 1 & \text{path crosses } e \text{ to the right} \\ -1 & \text{path crosses } e \text{ to the left} \end{cases}$$

$$u_{He} = 1 \text{ across the cut}$$

$$\Rightarrow \sum_{e: e \in G, e \notin H} \langle u_{Ge} | u_{He} \rangle = (\# \text{ right crossings}) - (\# \text{ left crossings}) = 1$$

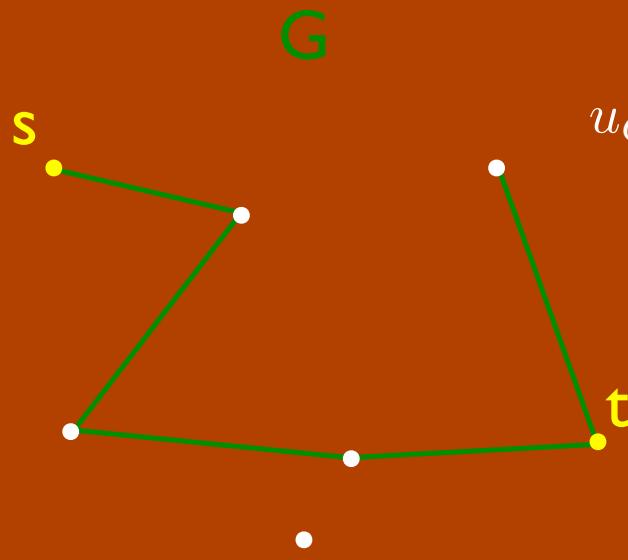
$$\Rightarrow \text{Adv}^\pm(f) \leq n^{3/2}$$



$$u_{Ge} = \begin{cases} 1 & e \in \text{path} \\ -1 & -e \in \text{path} \end{cases}$$

Δ = projection onto $\text{span}\{\psi_x\}$

$$\begin{aligned} |\psi_x\rangle &= |r\rangle + |f(x)\rangle + \frac{1}{10\sqrt{W}}|\tilde{u}_x\rangle \\ |\tilde{u}_x\rangle &= \sum_j |j, x_j\rangle \otimes |u_{xj}\rangle \end{aligned}$$

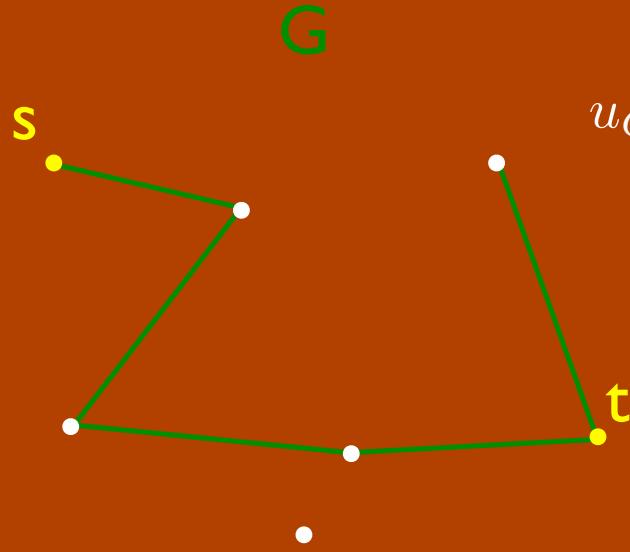


$$u_{Ge} = \begin{cases} 1 & e \in \text{path} \\ -1 & -e \in \text{path} \end{cases}$$

$\Delta = \text{projection onto } \text{span}\{\psi_G\}$

$$|\psi_G\rangle = |r\rangle + |f(G)\rangle + \frac{1}{10\sqrt{W}}|\tilde{u}_G\rangle$$

$$|\tilde{u}_G\rangle = \sum_e |e, G_e\rangle \otimes |u_{Ge}\rangle$$



$$u_{Ge} = \begin{cases} 1 & e \in \text{path} \\ -1 & -e \in \text{path} \end{cases}$$

$\Delta = \text{projection onto } \text{span}\{\psi_G : f(G) = 1\}$

$$|\psi_G\rangle = |r\rangle + |f(G)\rangle + \frac{1}{10\sqrt{W}}|\tilde{u}_G\rangle$$

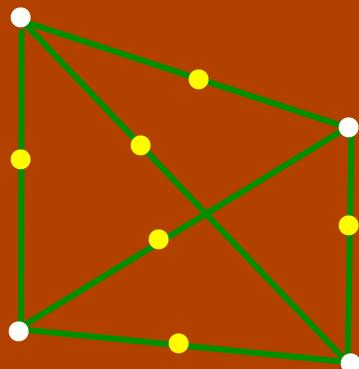
$$|\tilde{u}_G\rangle = \sum_e |c, G_e\rangle \otimes |u_{Ge}\rangle$$

$$|\tilde{u}_G\rangle = \sum_e u_{Ge}|e\rangle$$

$\Rightarrow \Delta \sim \text{proj. onto balanced } s-t \text{ flows in } K_n$

Implementing the reflection about the set of balanced flows in K_n

Flow = $|\psi\rangle \in \mathbb{C}^E$ s.t. $\forall v, |\psi\rangle \perp \sum_w |(v, w)\rangle$

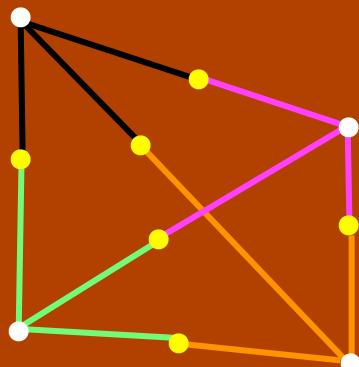


I. Factor the solution

- into constraints on original vertices & on edge vertices—now commuting

Implementing the reflection about the set of balanced flows in K_n

Flow = $|\psi\rangle \in \mathbb{C}^E$ s.t. $\forall v, |\psi\rangle \perp \sum_w |(v, w)\rangle$

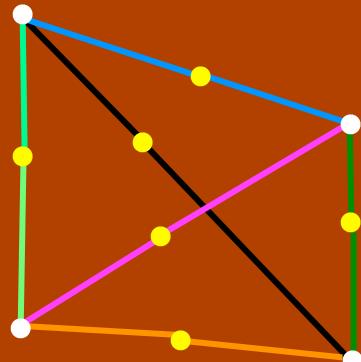


I. Factor the solution

- into constraints on original vertices & on edge vertices—now commuting

Implementing the reflection about the set of balanced flows in K_n

Flow = $|\psi\rangle \in \mathbb{C}^E$ s.t. $\forall v, |\psi\rangle \perp \sum_w |(v, w)\rangle$

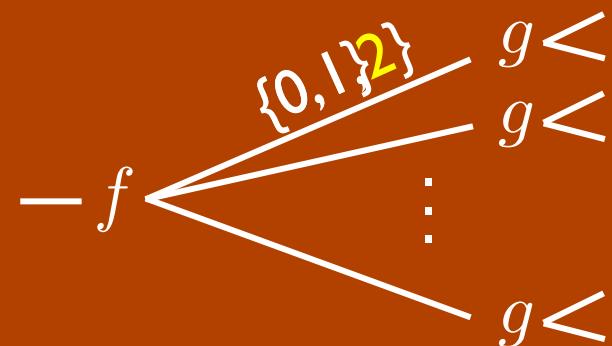


1. Factor the solution
 - into constraints on original vertices & on edge vertices—now commuting
2. Apply Jordan's lemma (Szegedy)
3. Use phase estimation to isolate the $+1$ eigenspace, reflect, uncompute

Open problems

- More quantum algorithms

- Composition lower bounds with a non-boolean intermediate space



e.g., if f only depends on the input parities & g outputs even numbers

$$Q(f \bullet g) = 0 \ll Q(f)Q(g)$$

- Strong direct-product thms. for evaluating multiple indep. functions?

$$Q((g, g, \dots, g)) = Q(\mathbf{1}_n \bullet g) = \Theta(nQ(g))$$

- Largest possible classical/quantum gap on total functions
or sufficiently symmetrical functions

- Other query questions:
 - Evaluating relations
 - State generation
- Query complexity with a bounded-error oracle

References

- Lower bound survey: Høyer & Špalek 0509153
- Adversary bound
 - Bennett, Bernstein, Brassard, Vazirani 9701001
 - Ambainis '00
 - Høyer, Neerbek, Shi '02
 - Ambainis 0305028
 - Barnum, Saks & Szegedy '03
 - Laplante & Magniez 0311189
 - Zhang 0311060
 - Špalek & Szegedy 0409116
 - Barnum, Saks '04
- Multiplicative adversary: Ambainis 0508200; Ambainis, Špalek, de Wolf '06; Špalek 0703237; Ambainis, Magnin, Roetteler, Roland 1012.2112
- General adversary bound: Høyer, Lee, Špalek 0611054
- Today's proofs: Lee, Mittal, Reichardt, Špalek '10?

Blank slide