# Reflections for quantum query algorithms

Ben Reichardt
Institute for Quantum Computing
University of Waterloo

# Reflections for quantum query algorithms

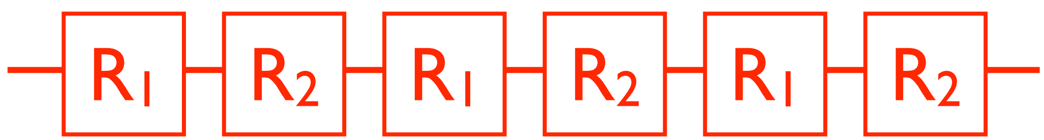
Ben Reichardt

Institute for Quantum Computing

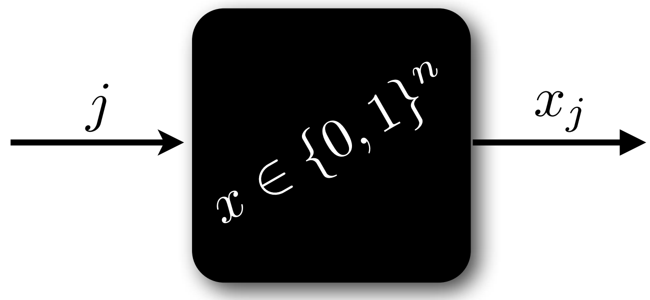
University of Waterloo

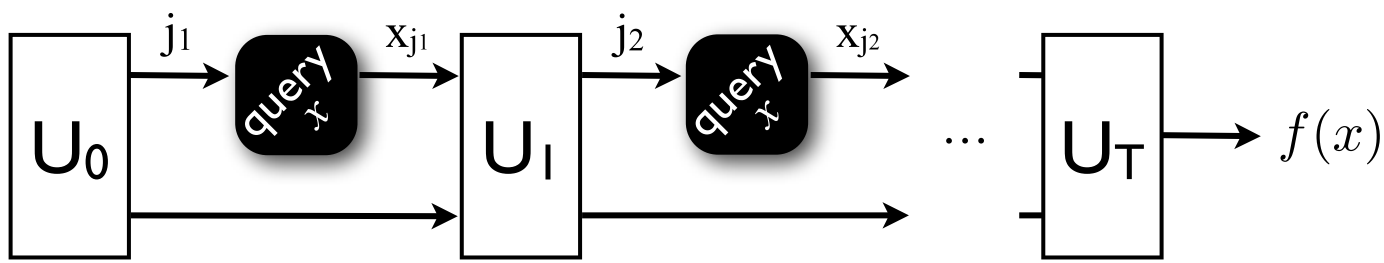
# Reflections for quantum query algorithms

Theorem: An optimal quantum query algorithm for evaluating any boolean function can be built out of two fixed reflections



Goal: Evaluate f: $\{0,1\}^n \rightarrow \{0,1\}$ using



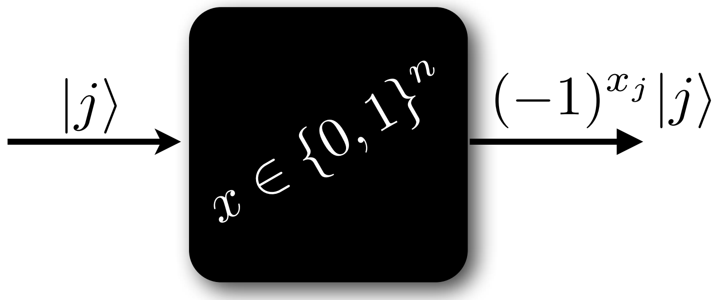


j1
xj1
j2
xj2
query x
query x
U0
UI
UT
...
f(x)

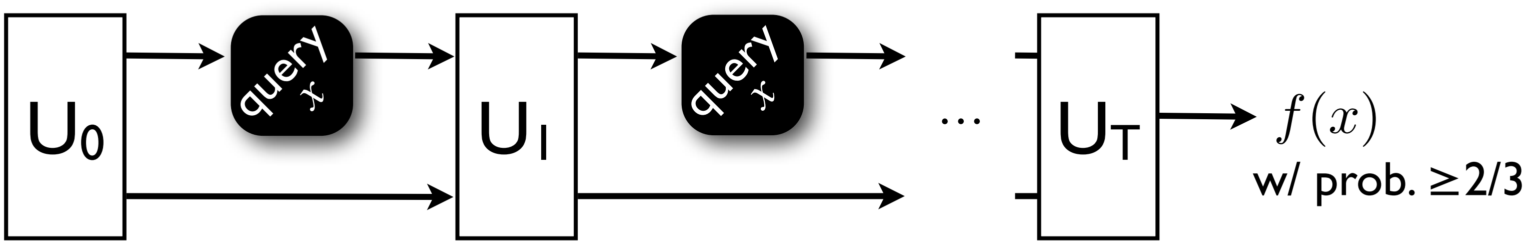
Query complexity models:

- Deterministic
- Randomized
  - bounded-, zero- or one-sided error
- Nondeterministic (Certificate complexity)
- Quantum

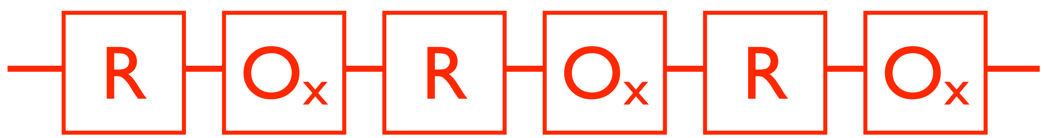
# Quantum query complexity

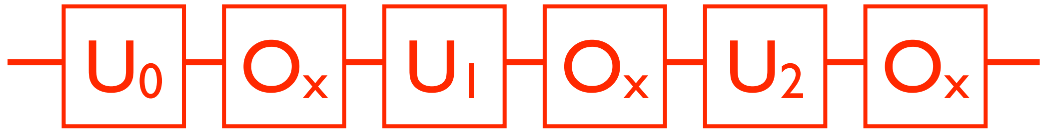



$$|1\rangle + |2\rangle \mapsto (-1)^{x_1}|1\rangle + (-1)^{x_2}|2\rangle$$



Theorem: An optimal quantum query algorithm for evaluating any boolean function can be built out of two fixed reflections






Clearly, w.l.o.g.,

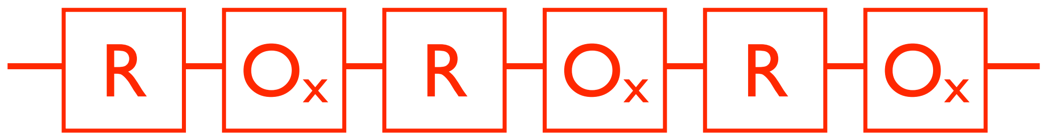
- may assume $U_t$ is independent of t

$$U = \sum_{t=0}^{T} |t+1\rangle\langle t| \otimes U_t + c.c.$$

- or, may assume $U_t$ is a reflection $\forall t$

$$R_t = |1\rangle\langle 0| \otimes U_t + |0\rangle\langle 1| \otimes U_t^\dagger$$

__Theorem:__ An optimal quantum query algorithm for evaluating any boolean function can be built out of two fixed reflections




__Theorem:__ The general adversary lower bound on quantum query complexity is also an upper bound

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

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

For f=OR:

| Input | Minimal certificate |
|---|---|
| 00110 | {3} |
| 00000 | {1,2,3,4,5} |

$$C(f) = \min_{\{\vec{p}_x \in \{0,1\}^n\}} \max_x \sum_j p_x[j]$$

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

$$\mathrm{Adv}(f) = \min_{\{\vec{p}_x \in \mathbb{R}^n\}} \max_x \sum_j p_x[j]^2$$

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

$\mathrm{Adv}(f)$ is a semi-definite program (SDP)

- Adversary method

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

  - Bennett, Bernstein, Brassard, Vazirani 9701001
  - Ambainis ’00
  - Høyer, Neerbek, Shi ’02
  - Ambainis 0305028
  - Barnum, Saks & Szegedy ’03
  - Laplante & Magniez 0311189
  - Zhang 0311060
  - Barnum, Saks ’04
  - Špalek & Szegedy 0409116

# General adversary bound

$$\mathrm{Adv}^{\pm}(f) = \min_{\{\vec{p}_x \in \mathbb{R}^n\}} \quad \max_x \sum_j p_x[j]^2$$

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

[Høyer, Lee, Špalek 0611054]

# General adversary bound

$$\mathrm{Adv}^{\pm}(f) = \min_{\{\vec{u}_{xj} \in \mathbb{R}^m\}} \max_x \sum_j \|\vec{u}_{xj}\|^2$$

$$\text{s.t.} \sum_{j : x_j \neq y_j} \langle u_{xj}, u_{yj} \rangle = 1 \quad \text{if } f(x) \neq f(y)$$

[Høyer, Lee, Špalek 0611054]

## Theorem: The general adversary lower bound on quantum query complexity is also an upper bound

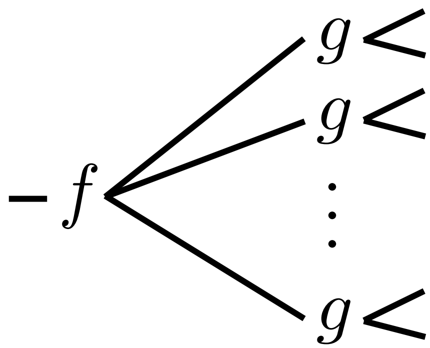
$$\mathrm{Adv}^{\pm}(f) = \min_{\{\vec{u}_{xj} \in \mathbb{R}^m\}} \max_x \sum_j \|\vec{u}_{xj}\|^2$$
$$\text{s.t.} \sum_{j : x_j \neq y_j} \langle u_{xj}, u_{yj} \rangle = 1 \quad \text{if } f(x) \neq f(y)$$

1. Simple understanding of quantum query complexity:
   - No unitaries, measurements, or time dependence
   - Equivalent to span programs [Karchmer, Wigderson '93]

| Quantum algorithms / query complexity | $\approx$ | Span programs / witness size |
|---|---|---|

(up to a constant factor, for boolean functions)

# Query complexity under composition



- Deterministic $= D(f)D(g)$
- Certificate $\leq C(f)C(g)$
- Randomized $\leq R(f)R(g)\, O(\log n)$

<u>Theorem:</u> $\mathrm{Adv}^{\pm}(f \circ \vec{g}) = \mathrm{Adv}^{\pm}(f)\mathrm{Adv}^{\pm}(g)$

[HLŠ '06, R'09]

$\Rightarrow Q(f \circ \vec{g}) = \Theta\big(Q(f)Q(g)\big)$

"Composition" of optimal algorithms for f and for g via tensor product of SDP vector solutions

<u>Characterizes</u> query complexity for read-once formulas

$$Q(f_1 \circ \cdots \circ \vec{f}_d) = \Theta\big(\mathrm{Adv}^{\pm}(f_1) \cdots \mathrm{Adv}^{\pm}(f_d)\big)$$

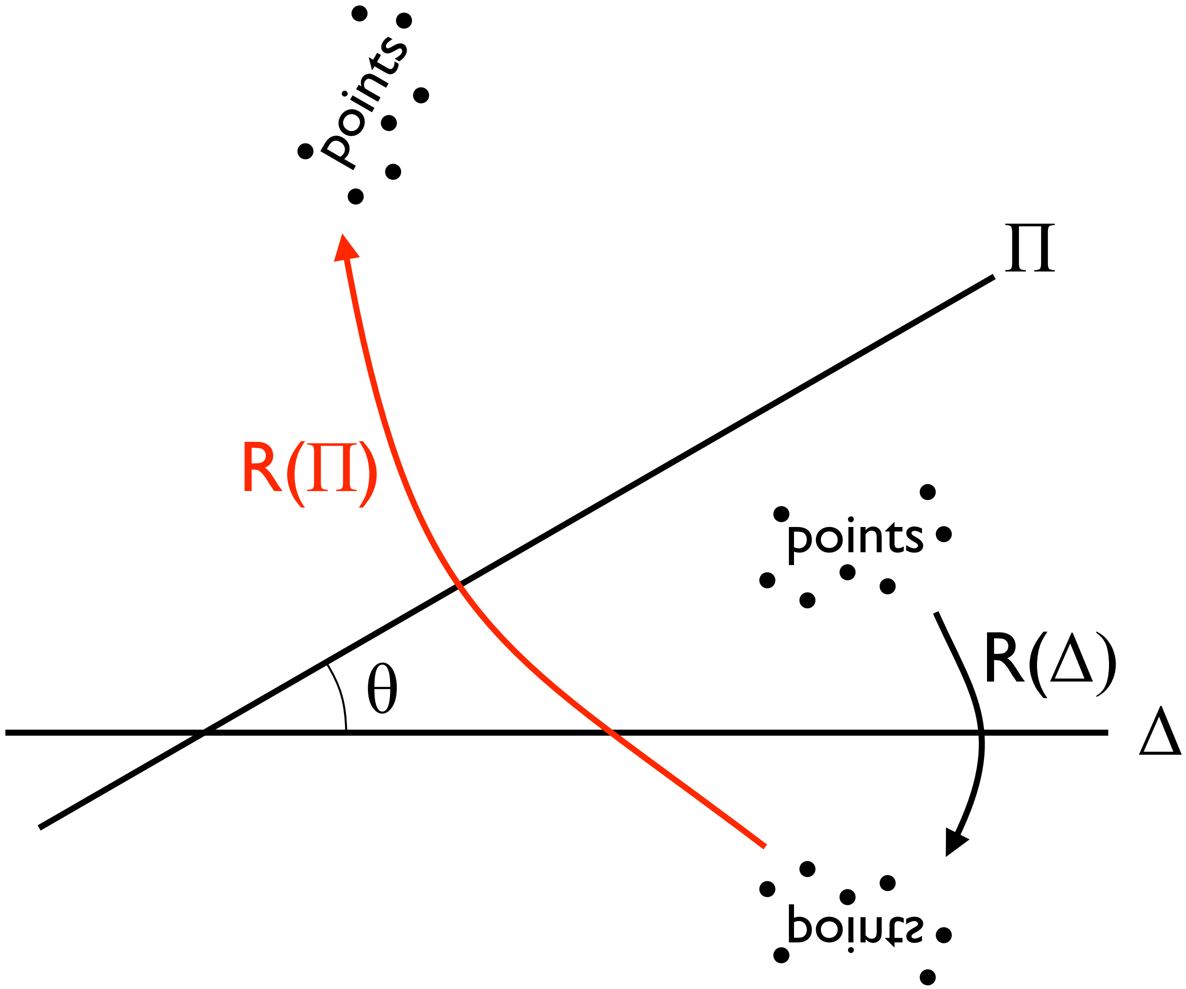
A. Query model

B. Adversary lower bounds

C. Spectra of reflections

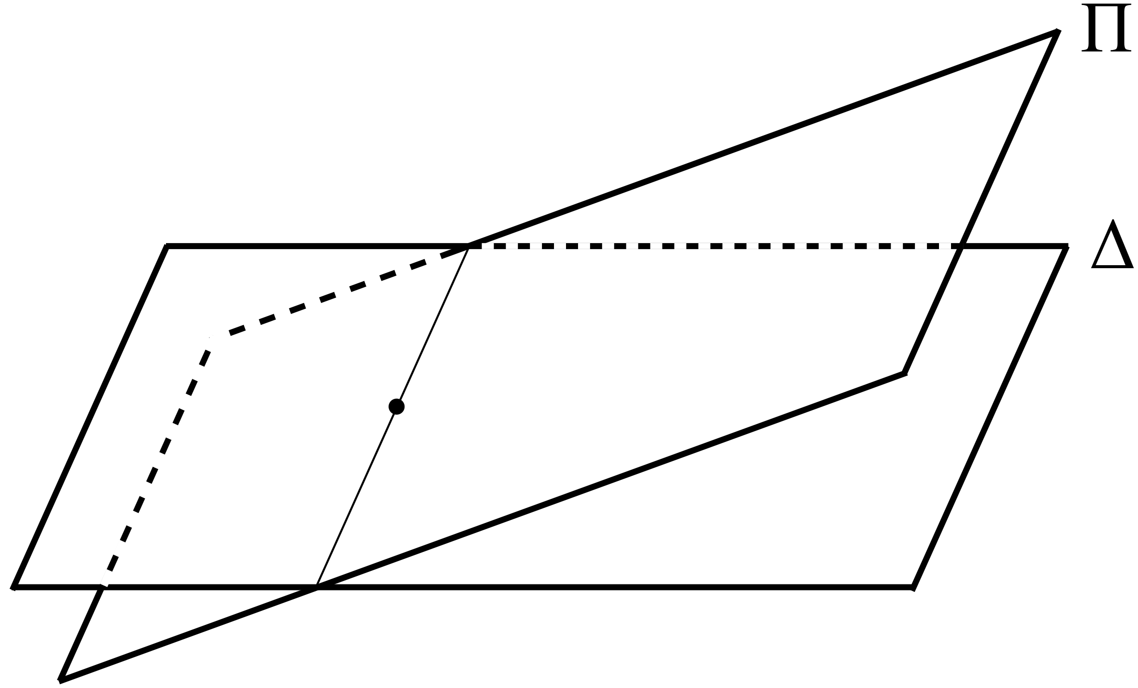
D. Adversary upper bound

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

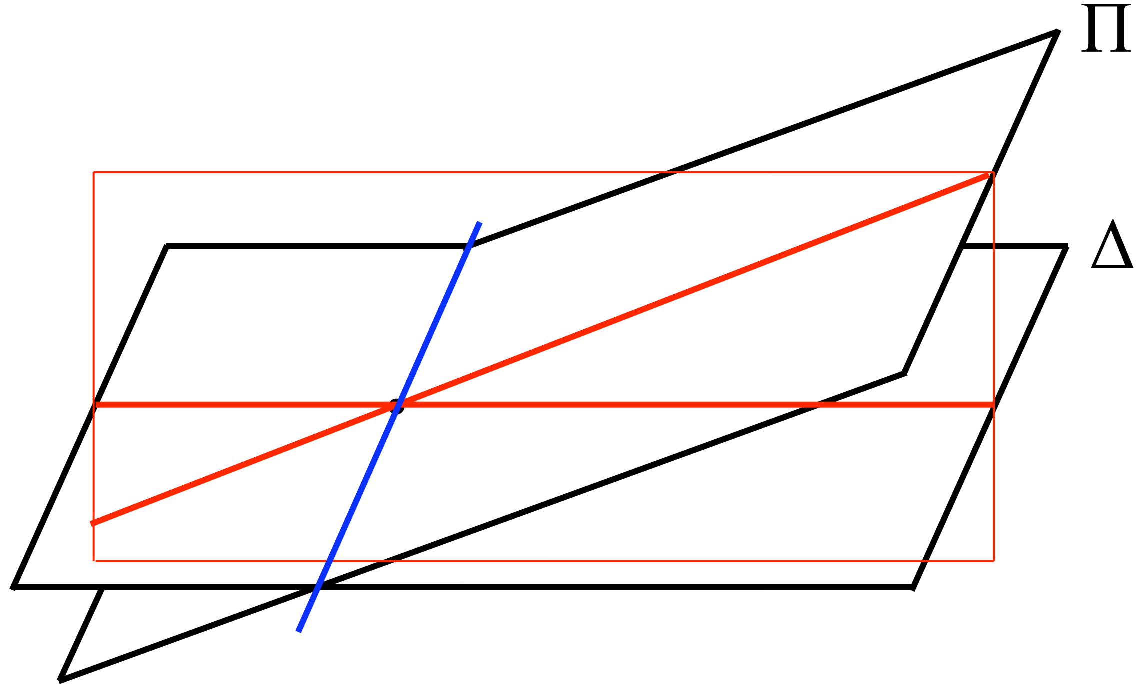



R(Π)R(Δ) is a rotation by angle 2θ, eigenvalues $e^{\pm 2i\theta}$

# Two subspaces will not generally lie at a fixed angle



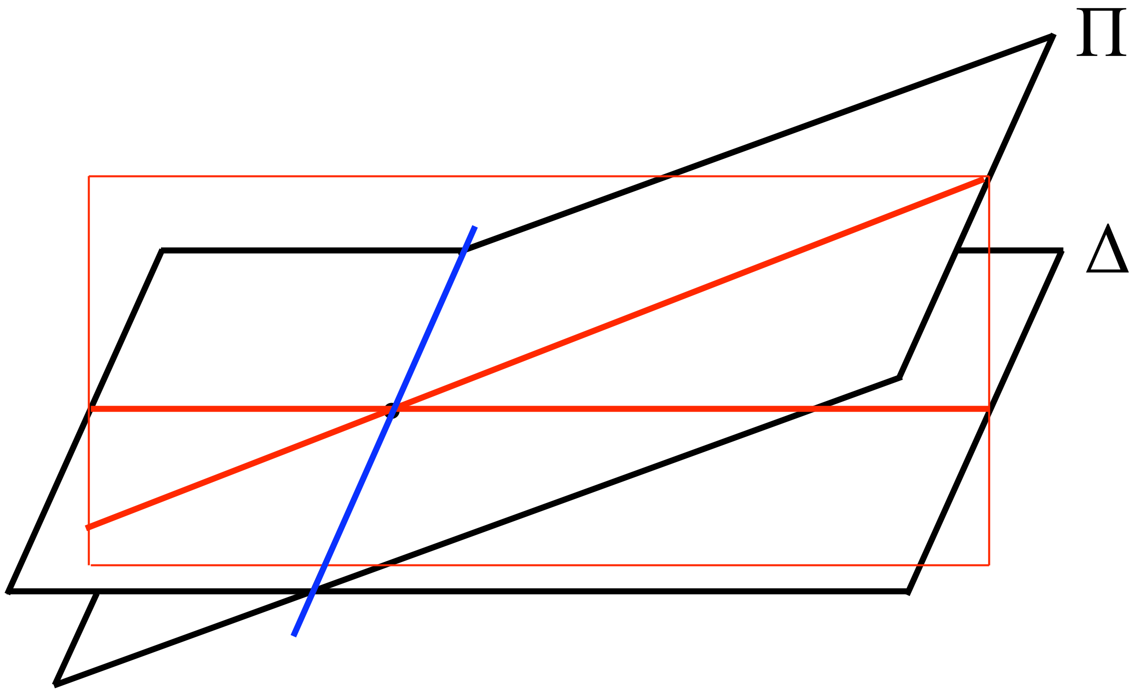
# Two subspaces will not generally lie at a fixed angle




Jordan's Lemma (1875)

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

# Two subspaces will not generally lie at a fixed angle



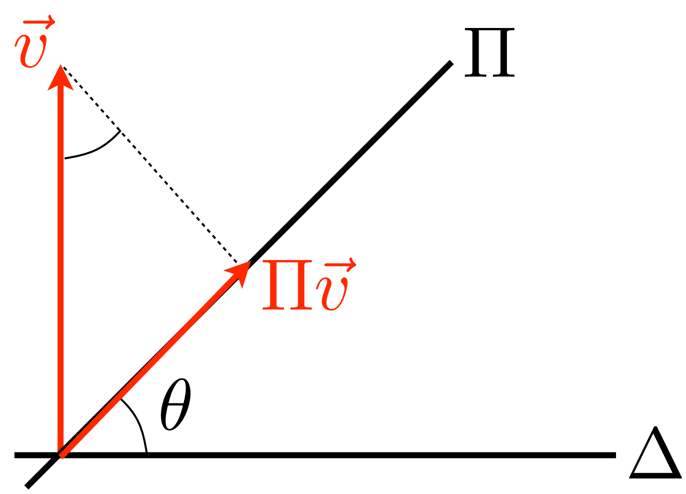

Jordan's Lemma (1875)

$$R(\Pi)R(\Delta) = \left(\begin{array}{c:c:c} \ddots & 0 & 0 \\ \hdashline 0 & \begin{matrix} \cos 2\theta & -\sin 2\theta \\ \sin 2\theta & \cos 2\theta \end{matrix} & 0 \\ \hdashline 0 & 0 & \ddots \end{array}\right)$$

## Effective Spectral Gap Lemma:

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

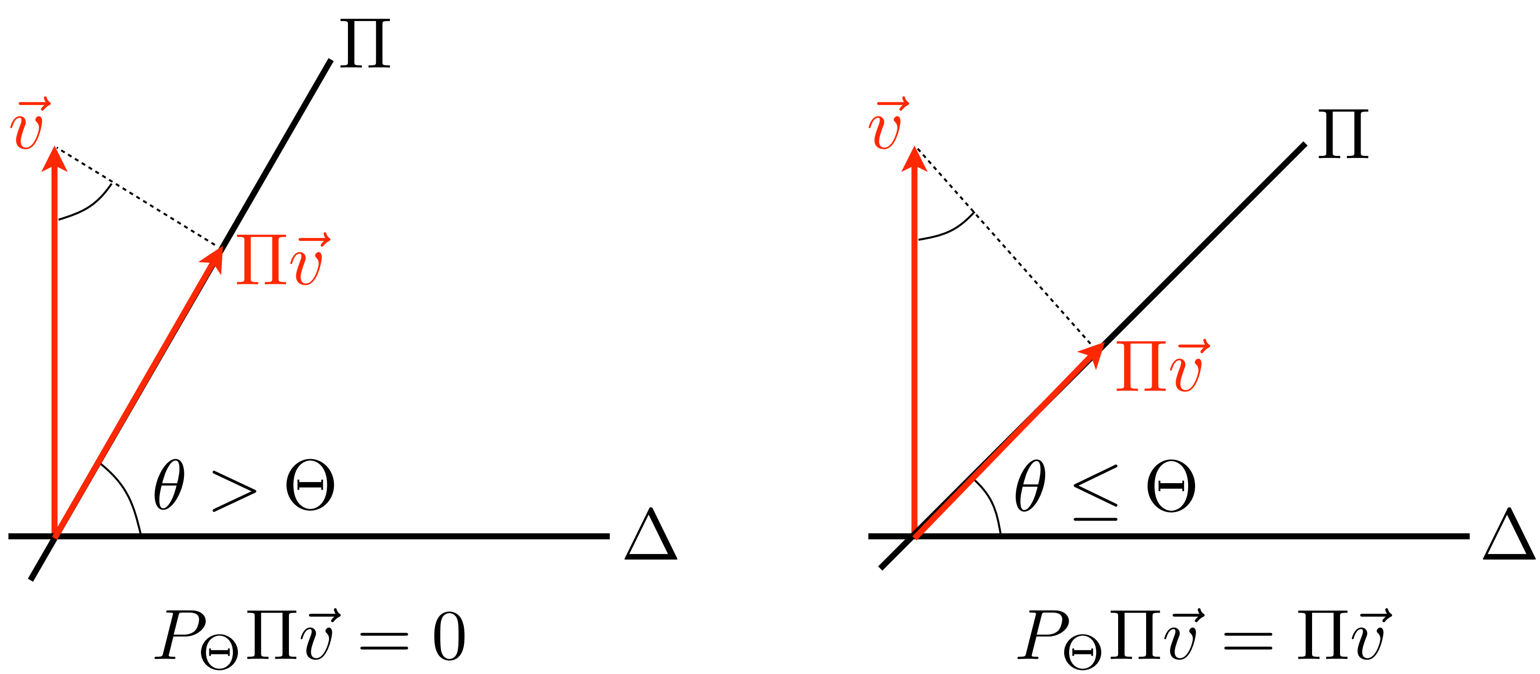
$$\|P_\Theta \Pi \vec{v}\| \leq \Theta \|\vec{v}\|$$



Effective Spectral Gap Lemma:

- Let $P_\Theta$ be the projection onto eigenvectors of R(Π)R(Δ) 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 $P_\Theta$ be the projection onto eigenvectors of R(Π)R(Δ) 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 ⇒ Up to a change in basis,

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

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

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

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

A. Query model

B. Adversary lower bounds

C. Spectra of reflections

D. Adversary upper bound

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

The algorithm:

1. Begin with an SDP solution:

$$\sum_{j:x_j \neq y_j} \langle u_{xj}, u_{yj} \rangle = 1 \quad \text{if } f(x) \neq f(y)$$

2. Let $\Delta$ = projection to the span of the vectors

$$|0\rangle + \frac{1}{10\sqrt{A^{\pm}}} \sum_j |j\rangle |u_{yj}\rangle |y_j\rangle$$

with f(y)=1

3. Starting at $|0\rangle$, alternate R($\Delta$) with the input oracle

$$\Delta = \text{Proj}\left\{ \begin{array}{r} |0\rangle + \frac{1}{10\sqrt{A^{\pm}}}\sum_j |j, u_{yj}, y_j\rangle \\ : f(y) = 1 \end{array} \right\}$$

$$\sum_{j: x_j \neq y_j} \langle u_{xj}, u_{yj}\rangle = 1 \text{ if } f(x) \neq f(y)$$

$$\Pi_x = |0\rangle\langle 0| + \sum_j |j\rangle\langle j| \otimes I \otimes |x_j\rangle\langle x_j|$$

Lemma:

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

---

## The analysis:

### Case f(x)=1:

$$\underbrace{|0\rangle}_{\text{close to}}$$

$$|0\rangle + \frac{1}{10\sqrt{A^{\pm}}}\sum_j |j\rangle|u_{xj}\rangle|x_j\rangle$$

$\Rightarrow$ doesn't move!

$$\Delta = \mathrm{Proj}\left\{ |0\rangle + \frac{1}{10\sqrt{A^{\pm}}} \sum_j |j, u_{yj}, y_j\rangle \;:\; f(y) = 1 \right\}$$

$$\sum_{j : x_j \neq y_j} \langle u_{xj}, u_{yj} \rangle = 1 \text{ if } f(x) \neq f(y)$$

Lemma:

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

$$\Pi_x = |0\rangle\langle 0| + \sum_j |j\rangle\langle j| \otimes I \otimes |x_j\rangle\langle x_j|$$

---

## The analysis:

### Case f(x)=1:

$$\underbrace{|0\rangle}_{\text{close to}}$$

$$|0\rangle + \frac{1}{10\sqrt{A^{\pm}}} \sum_j |j\rangle |u_{xj}\rangle |x_j\rangle$$

⇒ doesn't move!

### Case f(x)=0:

$$\underbrace{|0\rangle}$$

$$= \Pi_x \left( |0\rangle - 10\sqrt{A^{\pm}} \sum_j |j, u_{xj}, \bar{x}_j\rangle \right)$$

$$= \vec{v} \in \Delta^{\perp}$$

⇒ $\Omega(1/\mathrm{Adv}^{\pm})$ effective spectral gap

## Summary

Theorem: Optimal quantum query algorithms can be built out of two alternating reflections


Corollary: Characterization of quantum query complexity for read-once boolean formulas.

Theorem: The general adversary bound on quantum query complexity is tight

Corollary: Quantum query algorithms are equivalent to span programs.

## Open problems

Strong direct-product theorems?

Query complexity for non-boolean functions and state generation? ✓

Composition for non-boolean functions?

Upper and lower bounds for zero-error quantum query complexity?

Tight characterizations for communication complexity?