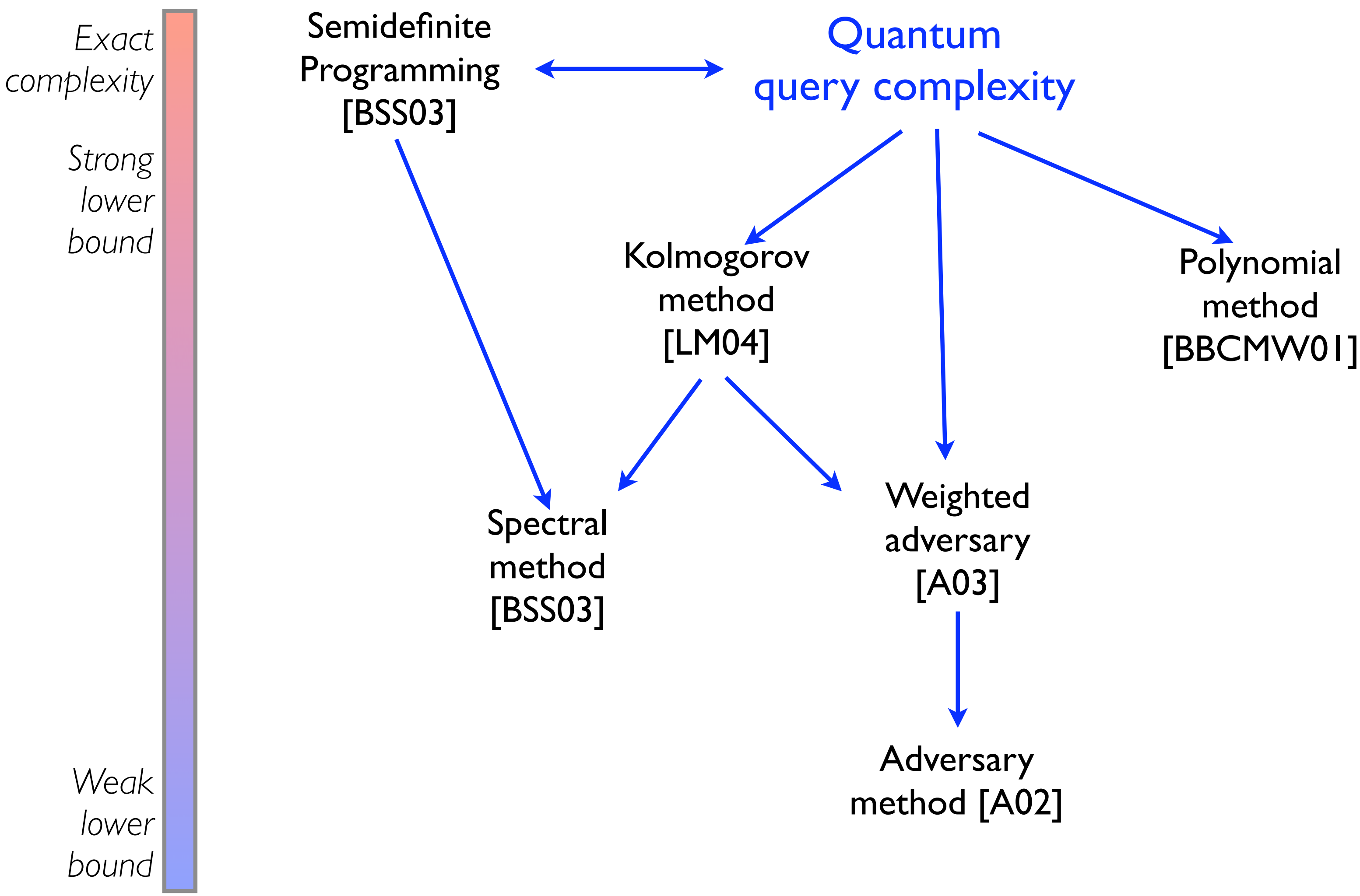
# Tutorial on the adversary method for quantum and classical lower bounds

Sophie Laplante
LRI, Université Paris-Sud Orsay

# Adversary method lower bounds



# Summary of this talk

| | |
|---|---|
| **Deterministic method**<br><br>- General statement<br><br>- Combinatorial bound | $DT(f) \geq \frac{\lvert R\rvert}{\max_i \lvert R_i\rvert}$<br><br>$\geq \max\{\frac{m}{l}, \frac{m'}{l'}\}$ |
| **Quantum method**<br><br>- General statement<br><br>- Combinatorial bound [A02] | $Q_\varepsilon(f) \geq \frac{c_\varepsilon \lvert R\rvert}{\sum_i Progress_t(i)}$<br><br>$\geq \frac{c_\varepsilon}{2}\sqrt{\frac{mm'}{ll'}}$ |
| **Weighted method [A03, LM04]** | $Q_\varepsilon(f) \geq \frac{c_\varepsilon}{2} \min_{x,y,i} \frac{\sqrt{p(x)p(y)p'_{x,i}(y)p'_{y,i}(x)}}{q(x,y)}$ |
| **Spectral method [BSS03]** | $Q_\varepsilon(f) \geq \frac{c_\varepsilon}{2} \frac{\lVert\Gamma\rVert}{max_i \lVert\Gamma_i\rVert}$ |

# Classical decision tree model

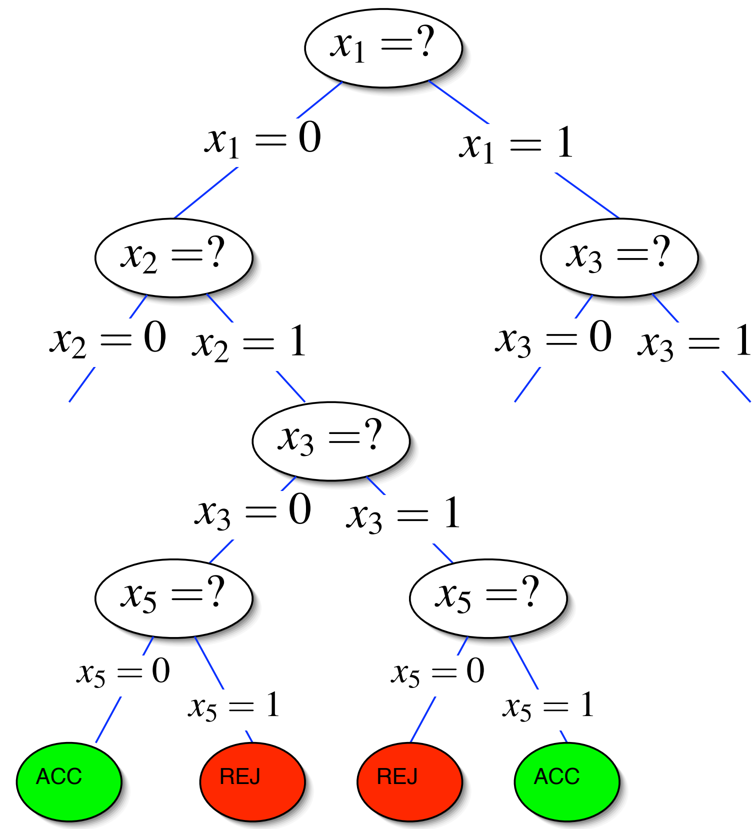
To compute a boolean function $f : \{0,1\}^n \rightarrow \{0,1\}$,

Model : decision tree

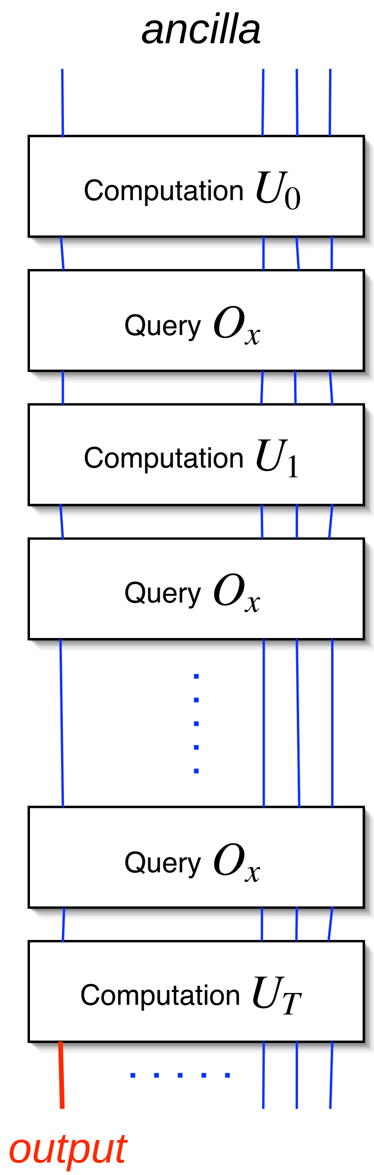
Cost : Number of queries to input

Query complexity of $f$:

depth of shallowest decision tree for $f$

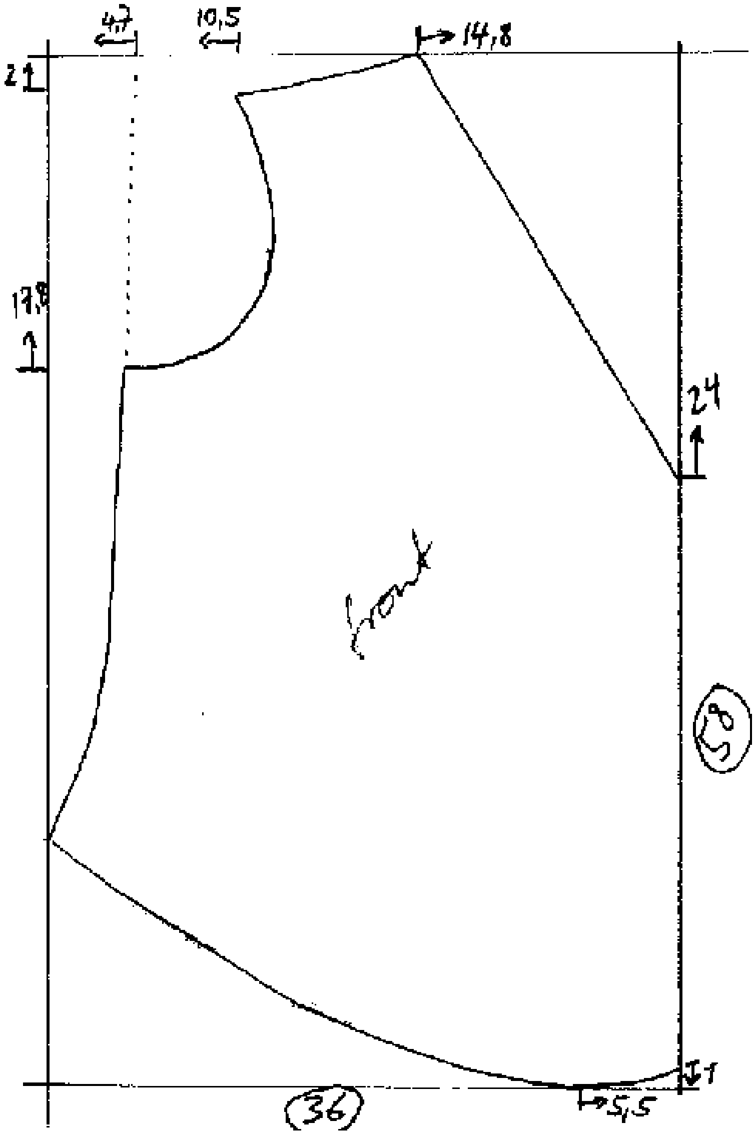


# Quantum query model




- Query: Unitary transformation $O_x$ that maps $|i,b\rangle$ to $|i, b\oplus x_i\rangle$
- Computation :
$$|\psi_T\rangle = U_T O_x \cdots O_x U_0 |0\rangle$$
- Output: Measure 1st qubit of $|\psi_T\rangle$
- Error probability at most *1/3*
- Same model with stochastic matrices for randomized query complexity

# Estimating number of pieces by their size

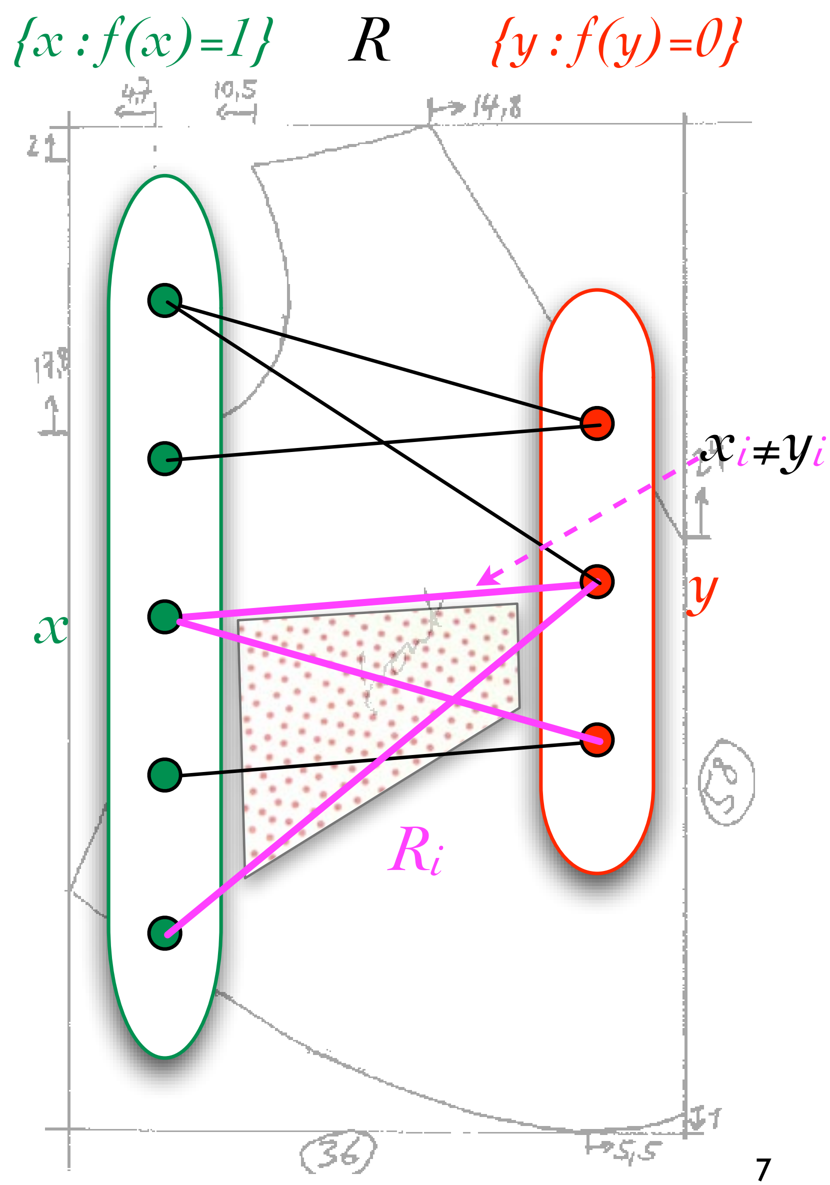



# Adversary method, deterministic setting

Goal: separate $\{x : f(x)=1\}$ from $\{y : f(y)=0\}$ with minimum queries to input bits

- Subrelation $R_i$ : pairs for which query $i$ is useful
- Queries $\geq$ number of $R_i$ needed to cover $R$.

$$DT(f) \geq \frac{|R|}{\max_i |R_i|}$$



# Deterministic lower bound

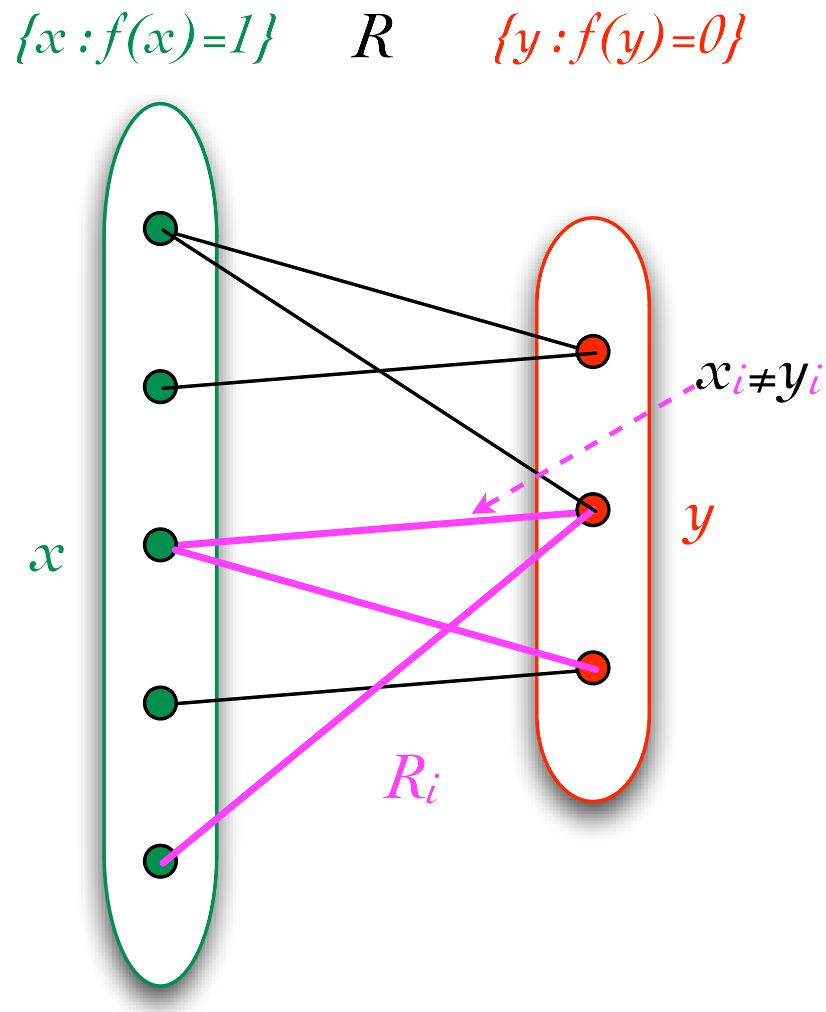
- left degree of $R \geq m$

  right degree $\geq m'$
- left degree of all $R_i \leq l$

  right degree $\leq l'$
- $|R| \geq m|X|, m'|Y|$
- $|R_i| \leq l|X|, l'|Y|$

$$DT(f) \geq \frac{|R|}{\max_i |R_i|}$$

$$\geq \max\{\frac{m}{l}, \frac{m'}{l'}\}$$



# Progress on $x, y, i$ after a query

At time $t$, progress towards distinguishing $(x,y) \in R_i$ by making one query :

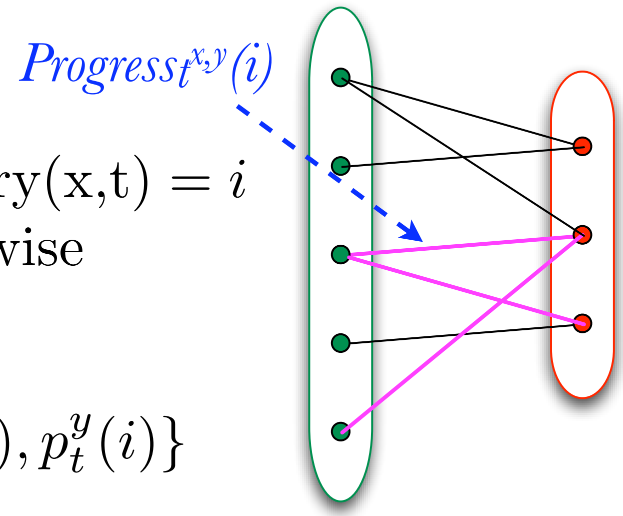
- Deterministic case

$$DProgress_t^{x,y}(i) = \begin{cases} 1 & \text{if query(x,t)} = i \\ 0 & \text{otherwise} \end{cases}$$

- Randomized case

$$RProgress_t^{x,y}(i) = 2\min\{p_t^x(i), p_t^y(i)\}$$

- Quantum case ? (next slide)

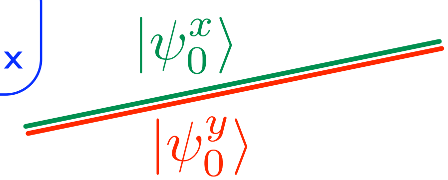


# Quantum progress

State of the system after query $t$, on input $x$ is written $|\psi_t^x\rangle$

Fix $(x,y) \in R$.

Amplitude$^2$ of $|i\rangle$ in query t, input x




- At beginning, $\langle \psi_0^x | \psi_0^y \rangle = 1$
- At each time step,

$$|\langle \psi_t^x | \psi_t^y \rangle - \langle \psi_{t+1}^x | \psi_{t+1}^y \rangle| \le 2 \sum_{i : x_i \neq y_i} \sqrt{p_t^x(i) p_t^y(i)}$$

- At the end, $|\langle \psi_T^x | \psi_T^y \rangle| \le 2\sqrt{\varepsilon(1-\varepsilon)}$

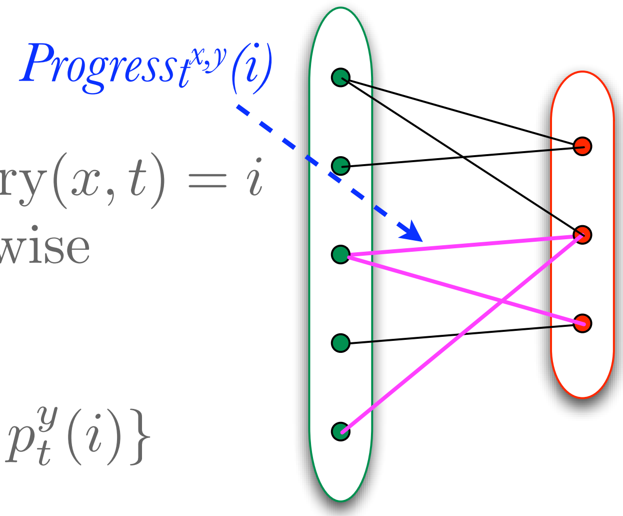
$$T \cdot \sum_i 2\sqrt{p_t^x(i) p_t^y(i)} \ge 1 - 2\sqrt{\varepsilon(1-\varepsilon)}$$

$c_\varepsilon$

*Progress$^t_{x,y}(i)$*

# Quantum progress on $x$, $y$, $i$ after a query

At time $t$, progress towards distinguishing $(x,y) \in R_i$ by making one query :




- Deterministic case

$$DProgress_t^{x,y}(i) = \begin{cases} 1 & \text{if query}(x,t) = i \\ 0 & \text{otherwise} \end{cases}$$

- Randomized case

$$RProgress_t^{x,y}(i) = 2\min\{p_t^x(i), p_t^y(i)\}$$

- Quantum case

$$QProgress_t^{x,y}(i) = 2\sqrt{p_t^x(i)p_t^y(i)}$$

# Ambainis' unweighted method

**Claim:** $\sum_i Progress_t(i) \leq 2\sqrt{l|X| \cdot l'|Y|}$

**Proof:** $\sum_i Progress_t(i)$

$$= \sum_{x,y,i} Progress_t^{x,y}(i)$$

$$= 2\sum_{x,y,i} \sqrt{p_t^x(i) p_t^y(i)}$$

$$\leq 2\sqrt{\sum_x \sum_i \sum_y p_t^x(i)} \sqrt{\sum_y \sum_i \sum_x p_t^y(i)}$$

Cauchy Schwarz

$\leq |X|$ terms

$\sum_i p_t^x(i) = 1$

$\leq l$ terms

$$\leq 2\sqrt{l|X| \cdot l'|Y|}$$

# Ambainis' unweighted method

**Claim:** $\sum_i Progress_t(i) \leq 2\sqrt{l|X| \cdot l'|Y|}$

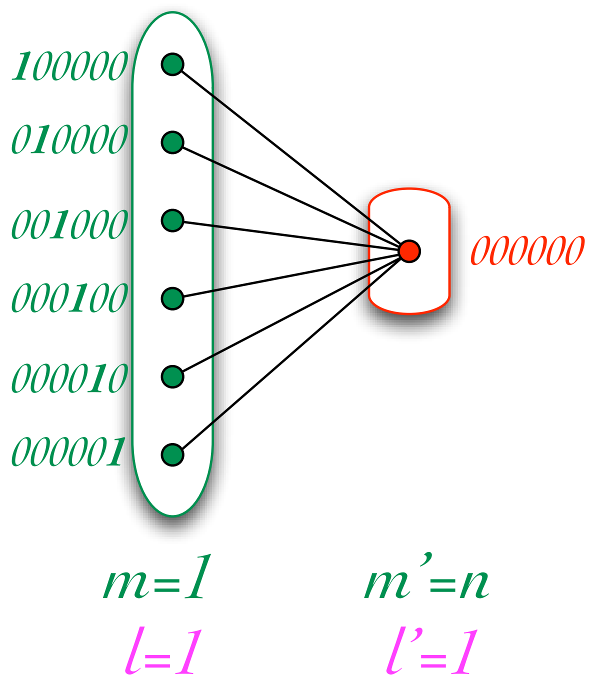
**Corollary:**

$$Q_\varepsilon(f) \geq \frac{c_\varepsilon |R|}{\sum_i Progress_t(i)} \geq \frac{c_\varepsilon \sqrt{m|X| \cdot m'|Y|}}{2\sqrt{lX| \cdot l'|Y|}}$$

$$|R| \geq \max\{m|X|, m'|Y|\} \geq \sqrt{m|X| \cdot m'|Y|}$$

$$Q_\varepsilon(f) \geq \frac{c_\varepsilon}{2}\sqrt{\frac{mm'}{ll'}}$$

# Example: OR function




- Deterministic queries
  $\geq max\{m/l,\ m'/l'\}$
  $= n$

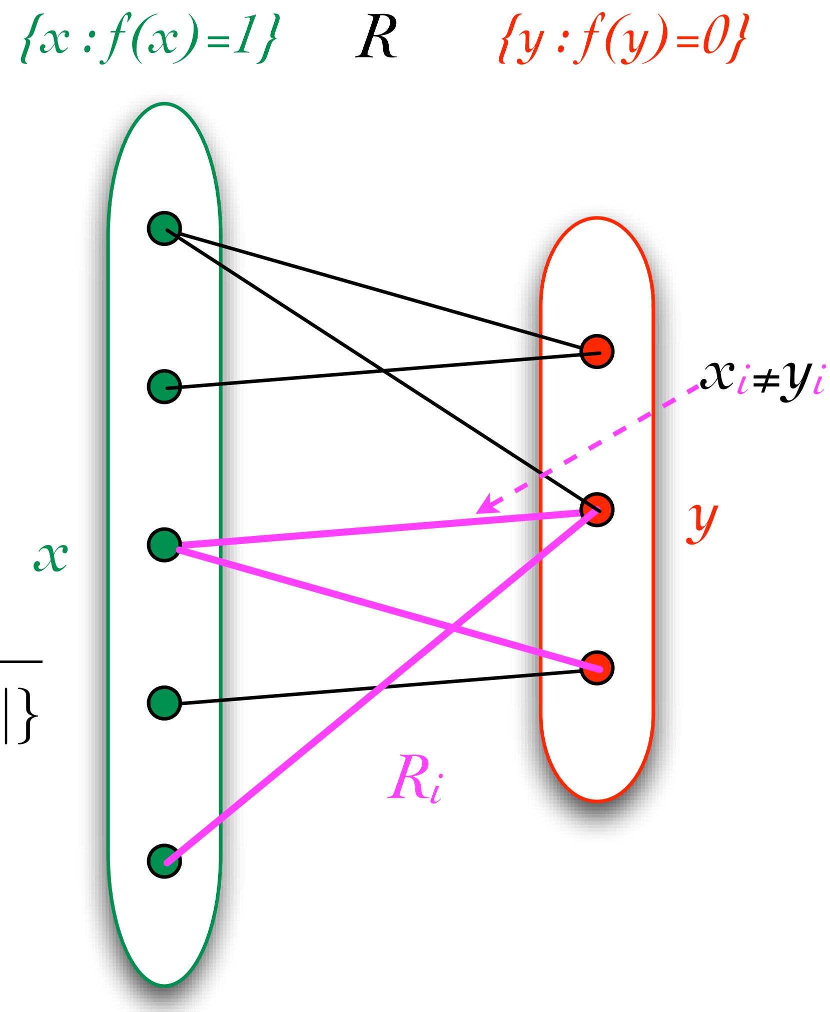
- Quantum queries
  $$\geq \sqrt{\frac{mm'}{ll'}}$$
  $$= \sqrt{n}$$

# Unweighted "$l_{max}$" lower bound

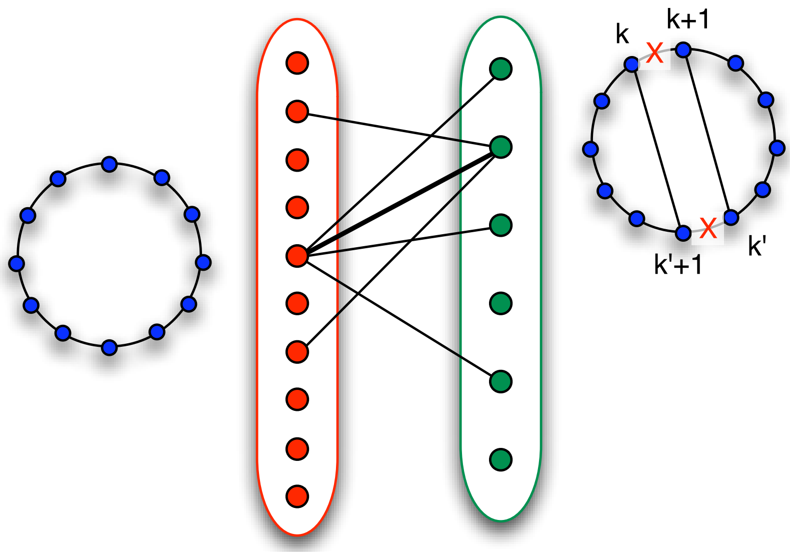
- left degree of $R \geq m$
  right degree $\geq m'$
- left degree of $R_i \leq l_i$
  right degree $\leq l_i'$
- $|R| \geq m|X|, m'|Y|$

$$\sum_i Progress_t(i) \leq 2\sqrt{max_i\{l_i|X| \cdot l_i'|Y|\}}$$

$$Q_\varepsilon(f) \geq \frac{c_\varepsilon}{2}\sqrt{\frac{mm'}{max_i\{l_i l_i'\}}}$$



# Example: Connectivity



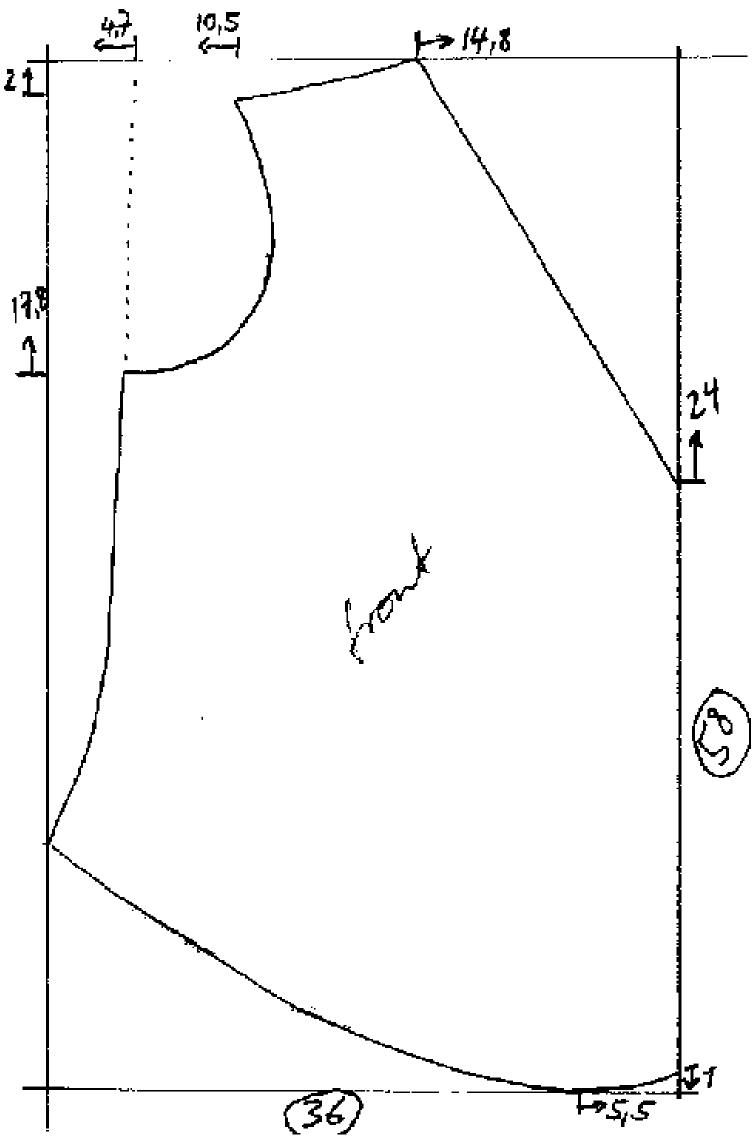

$m \approx n^2$ $m' \approx n^2$

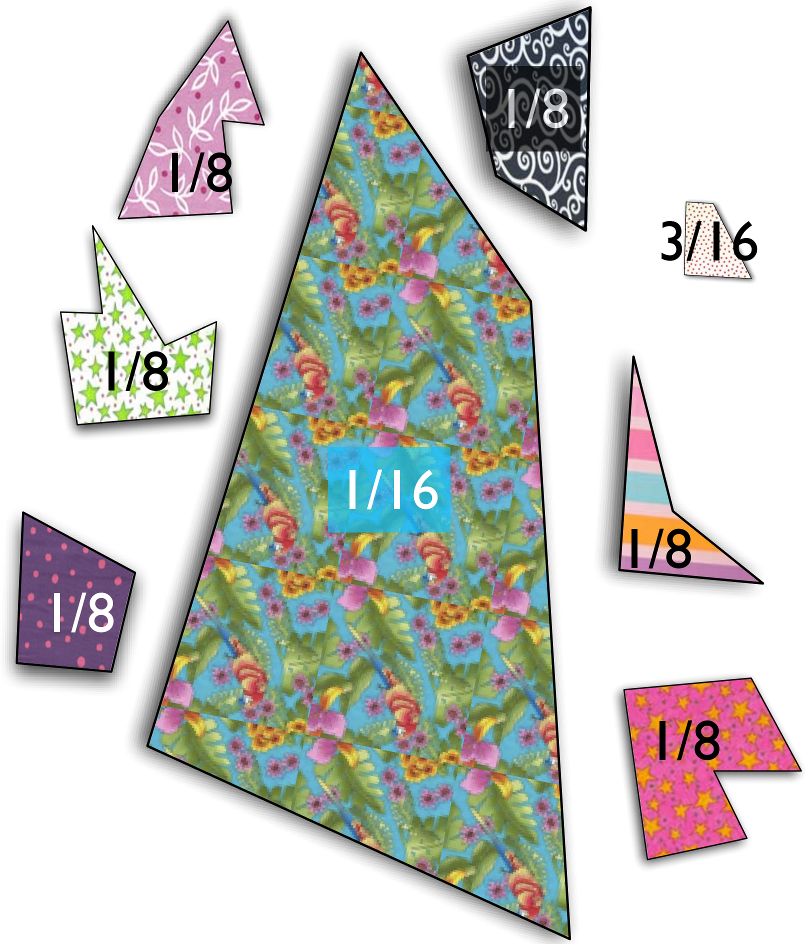
(x) $l_i \approx n$ $l_i' = 1$

(|) $l_i \approx 1$ $l_i' = n$

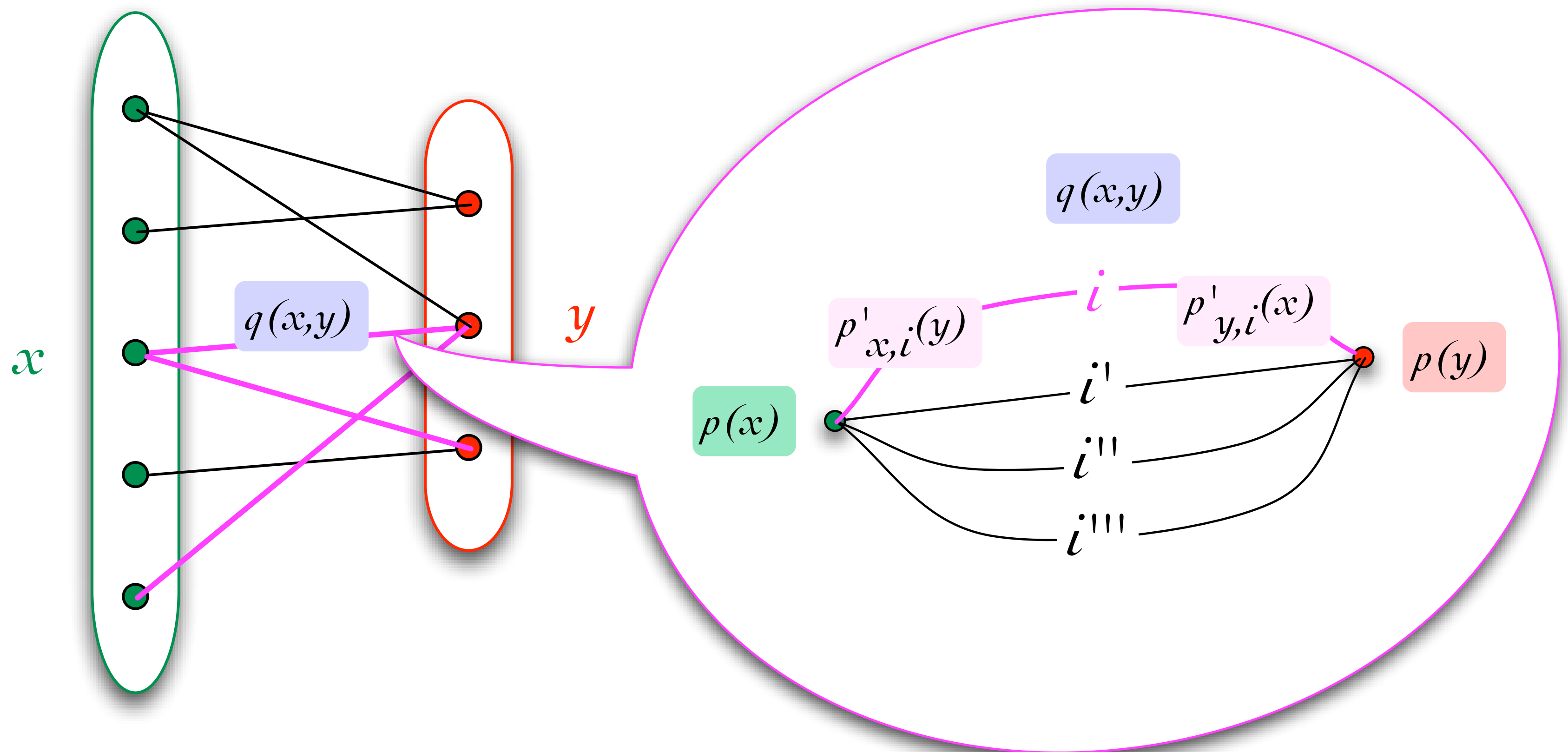
- Deterministic queries
  $\geq max\{m/l, m'/l'\}$
  $= n^2$
- Quantum queries
  $$\geq \sqrt{\frac{mm'}{ll'}}$$
  $$= n^{3/2}$$

# Weighted method



# Weight scheme for adversary method




$$\sum_{x,y \in R} q(x,y) = 1, \sum_{x \in X} p(x) = 1, \sum_{y \in Y} p'_{x,i}(y) = 1$$

# Weighted adversary method

Consider three distributions over pairs $(x,y) \in R$

$$\begin{aligned} P(x,y) &= \sum_i p(x) p_t^x(i) p'_{x,i}(y), \\ P'(x,y) &= \sum_i p(y) p_t^y(i) p'_{y,i}(x), \\ Q(x,y) &= q(x,y) \end{aligned}$$

Claim: $\exists (x,y) \in R \ \sum_i Progress_t^{x,y}(i)$

$$\leq \quad 2max_i \frac{q(x,y)}{\sqrt{p(x)p'_{x,i}(y)p(y)p'_{y,i}(x)}}$$

$$\begin{aligned} \sum_{x,y} \sqrt{P(x,y)P'(x,y)} &\leq \sqrt{\sum_{x,y} P(x,y) \sum_{x,y} P'(x,y)} \\ &\leq 1 = \sum_{x,y} Q(x,y) \end{aligned}$$

Proof: $\exists x,y \ \sqrt{P(x,y)P'(x,y)} \quad \leq \quad Q(x,y)$

$$\exists x,y \ \sum_i \sqrt{p_t^x(i) p_t^y(i)} \quad \leq \quad \frac{q(x,y)}{\min_i \sqrt{p(x)p(y)p'_{x,i}(y)p'_{y,i}(x)}}$$

# Weighted adversary method

Consider three distributions over pairs $(x,y) \in R$

$$
\begin{aligned}
P(x,y) &= \sum_i p(x) p_t^x(i) p'_{x,i}(y), \\
P'(x,y) &= \sum_i p(y) p_t^y(i) p'_{y,i}(x), \\
Q(x,y) &= q(x,y)
\end{aligned}
$$

Claim: $\exists (x,y) \in R \ \sum_i Progress_t^{x,y}(i)$

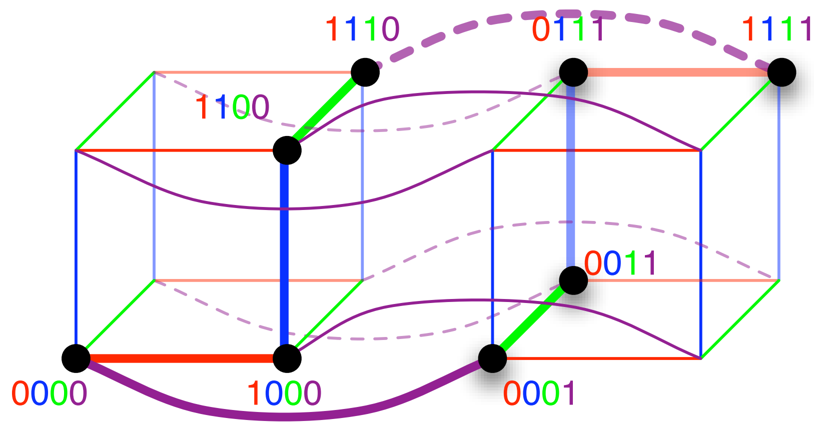
$$\leq \quad 2max_i \frac{q(x,y)}{\sqrt{p(x)p'_{x,i}(y)p(y)p'_{y,i}(x)}}$$

Corollary:

Recall that $\forall (x,y) \in R \ \ Q_\varepsilon(f) \quad \geq \quad \frac{c_\varepsilon}{\sum_i Progress_t^{x,y}(i)}$

$$Q_\varepsilon(f) \quad \geq \quad \frac{c_\varepsilon}{2} \min_{x,y,i} \frac{\sqrt{p(x)p(y)p'_{x,i}(y)p'_{y,i}(x)}}{q(x,y)}$$

# Example: Ambainis' function




$$f(x_1x_2x_3x_4) = \begin{cases} 1 & \text{if } x_1 \le x_2 \le x_3 \le x_4 \\ 1 & \text{if } x_1 \ge x_2 \ge x_3 \ge x_4 \\ 0 & \text{otherwise} \end{cases}$$

*q(x,y)*

0 0 0 1

! ! ✓ ✓

*3/80* — 1 0 0 1

*3/80* — 0 1 0 1

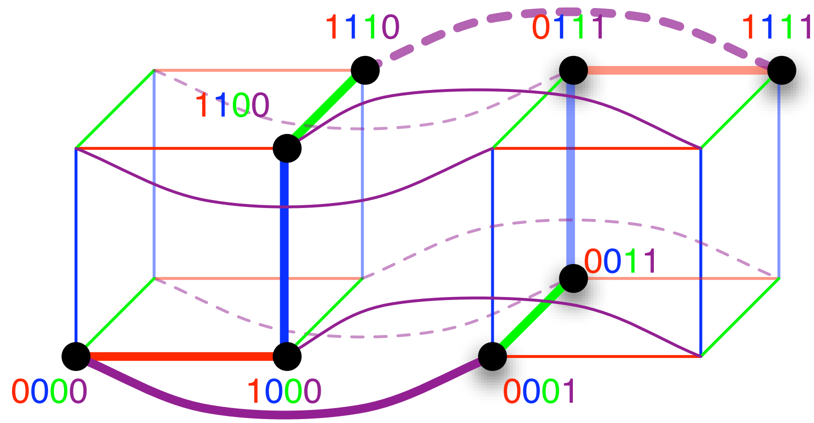
*1/40* — 1 1 0 1

*1/40* — 0 0 1 0

*p(x)* = *p(y)* = *1/8*

$$Q_\varepsilon(f) \quad \ge \quad \frac{c_\varepsilon}{2} \min_{x,y,i} \frac{\sqrt{p(x)p(y)p'_{x,i}(y)p'_{y,i}(x)}}{q(x,y)}$$

# Example: Ambainis' function

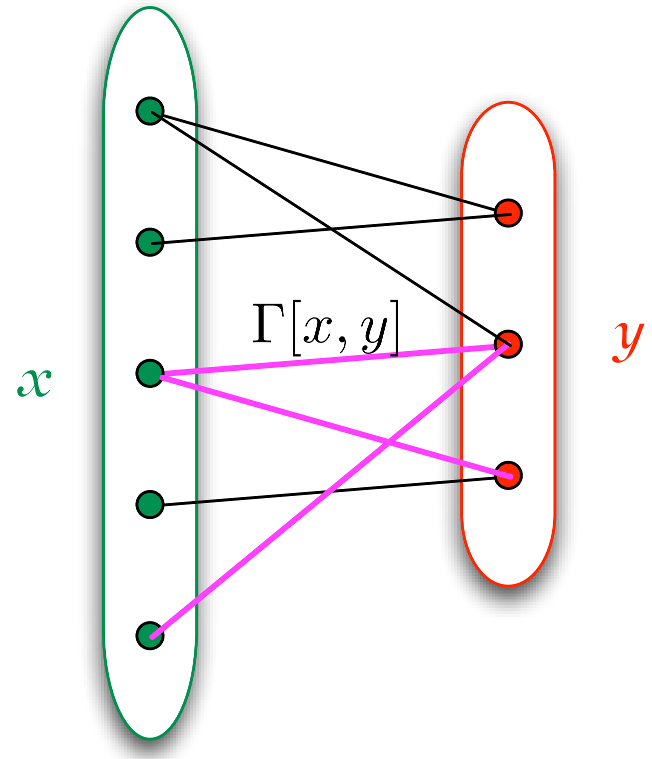



$$f(x_1x_2x_3x_4) = \begin{cases} 1 & \text{if } x_1 \le x_2 \le x_3 \le x_4 \\ 1 & \text{if } x_1 \ge x_2 \ge x_3 \ge x_4 \\ 0 & \text{otherwise} \end{cases}$$

| | $p'_{x,i}(y)$ | $p'_{y,i}(x)$ | | $q(x,y)$ | $\frac{\sqrt{p'_{x,i}(y)p'_{y,i}(x)}}{q(x,y)}$ | $\sqrt{p(x)p(y)}$ |
|---|---|---|---|---|---|---|
| 0 0 0 1 | 3/4 | 3/4 | 0 1 0 1 | 3/80 | 20 | 1/8 |
| 0 0 0 1 | 1/4 | 1 | 1 1 0 1 | 1/40 | 20 | 1/8 |
| 0 0 0 1 | 1 | 1/4 | 0 0 1 0 | 1/40 | 20 | 1/8 |

$$Q_\varepsilon(f) \ge \frac{c_\varepsilon}{2} \min_{x,y,i} \frac{\sqrt{p(x)p(y)p'_{x,i}(y)p'_{y,i}(x)}}{q(x,y)} = 20/8 = 5/2$$

# Spectral method




Nonnegative weights matrix

$$\Gamma[x,y]$$

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

$$\Gamma_i[x,y] = \begin{cases} 0 & \text{if } x_i = y_i \\ \Gamma[x,y] & \text{otherwise} \end{cases}$$

$$\|\Gamma\| = \max_{\substack{u,v \\ |u|=|v|=1}} |u^* \Gamma v|$$

$$Q_\varepsilon(f) \geq \frac{c_\varepsilon}{2} \frac{\|\Gamma\|}{max_i \|\Gamma_i\|}$$

Idea: $q(x,y)$ derived from

$p(x)$, $p(y)$ derived from $u$, $v$ maximizing $|u^*Tv|$

$p'_{y,i}(x)$, $p'_{x,i}(y)$ derived from $u_i$, $v_i$ maximizing $|u_i^*T_iv_i|$