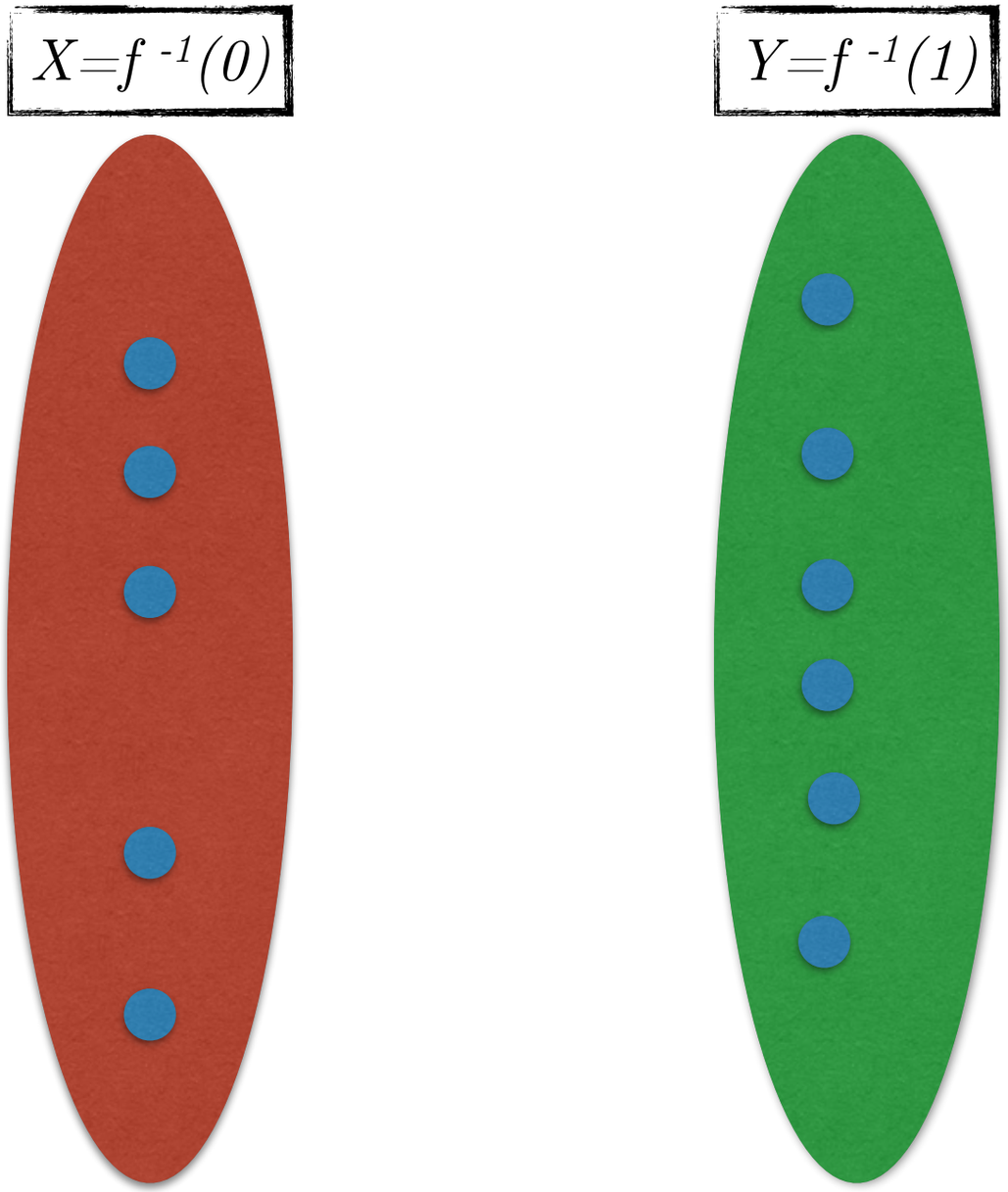
Lower bounds on quantum query complexity Part II

Marc Kaplan
Telecom ParisTech - University of Edinburgh

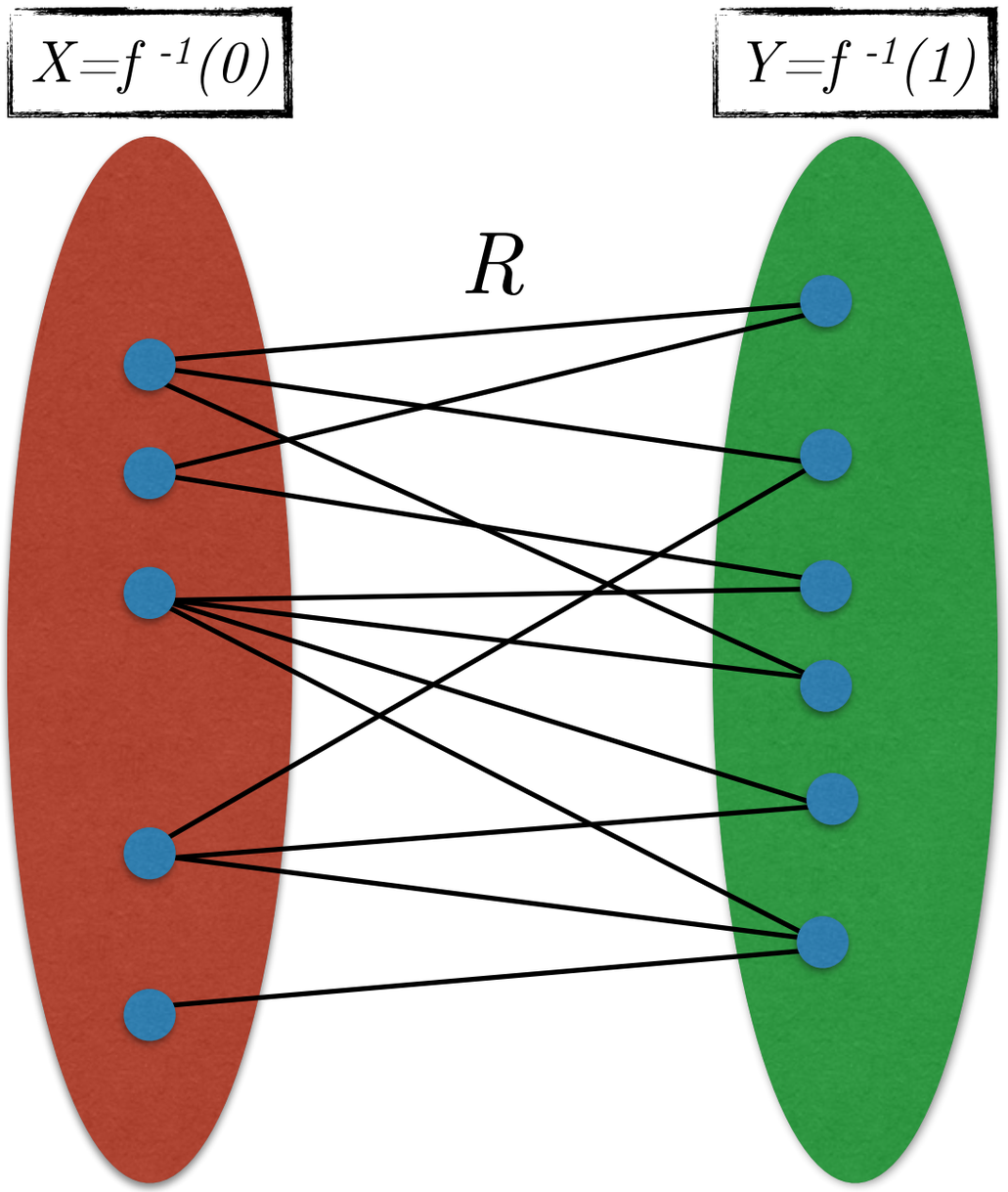
Adversary method(s)

- Original adversary method
- Weighted adversary method
- Spectral adversary method
- Generalized adversary method

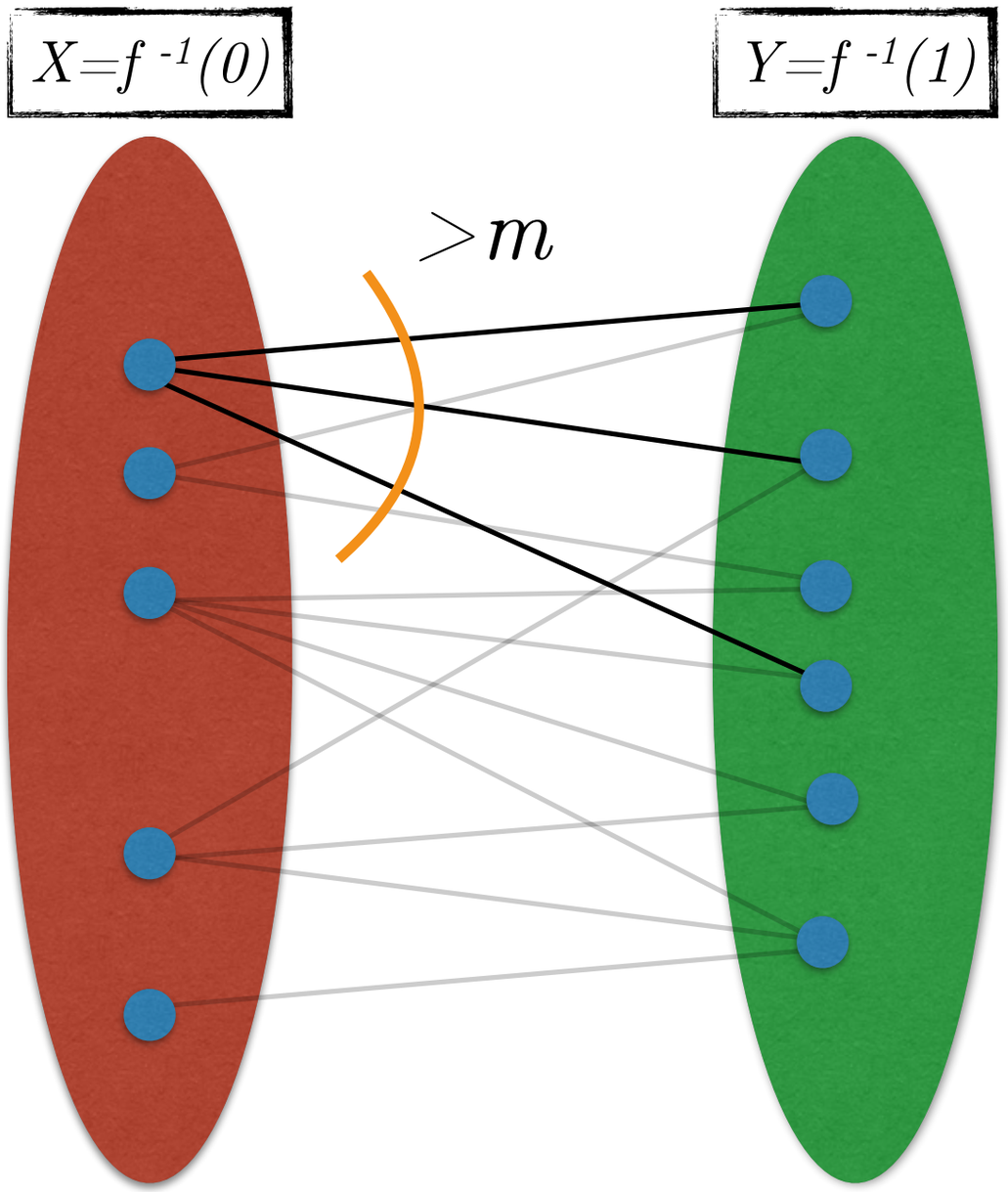
Adversary method: original version



Adversary method: original version

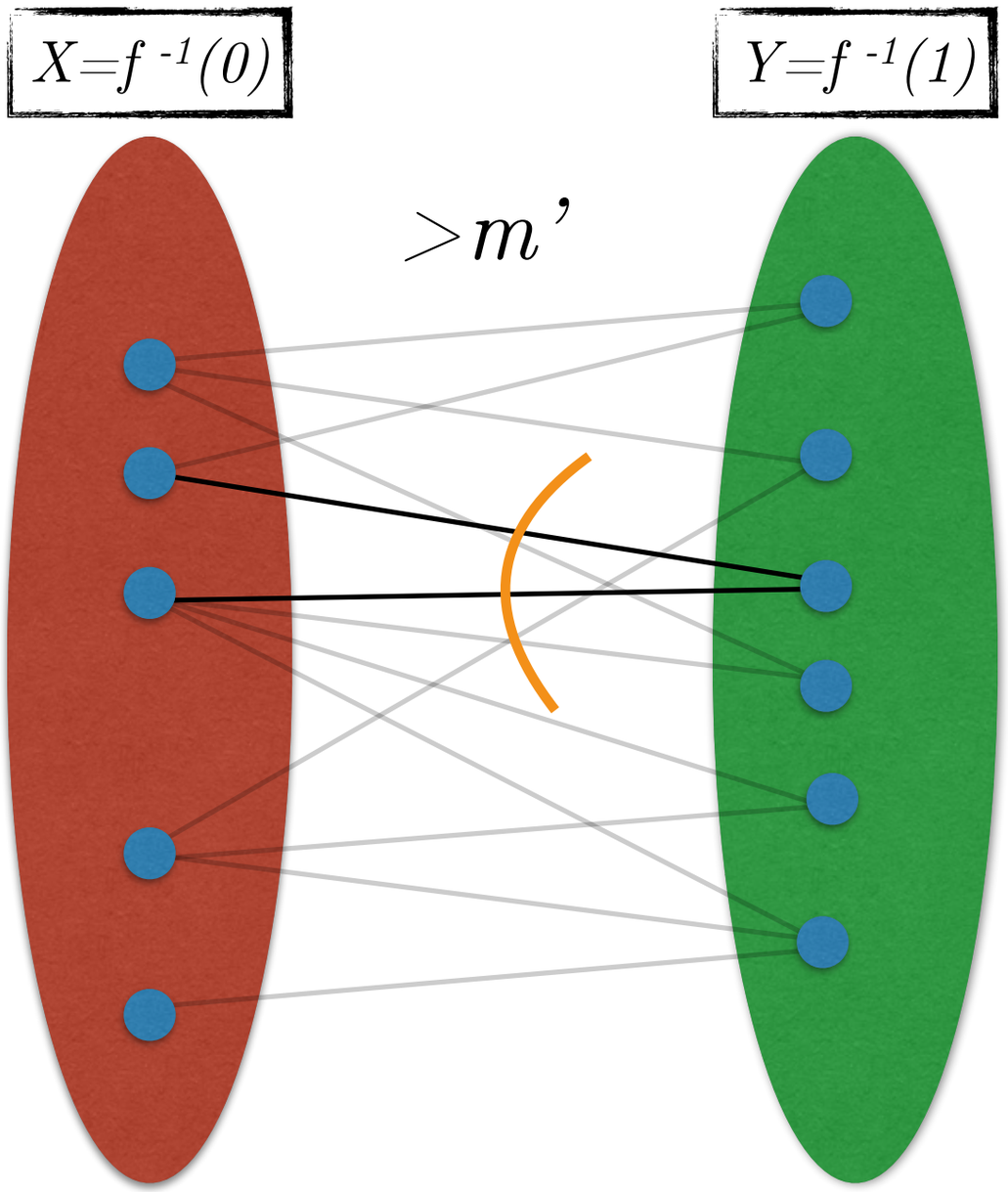


Adversary method: original version



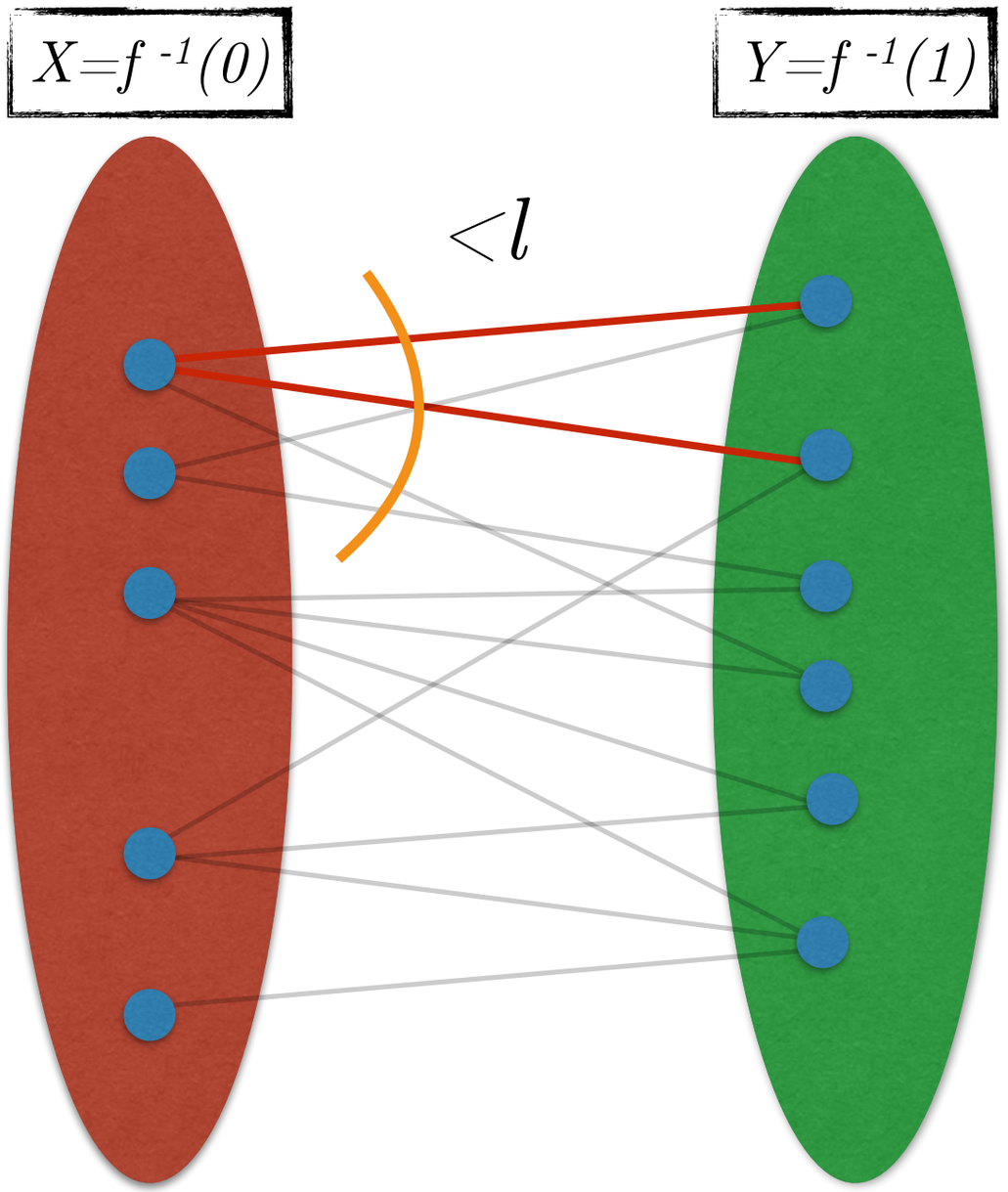
$$(x, y) \in R$$

Adversary method: original version



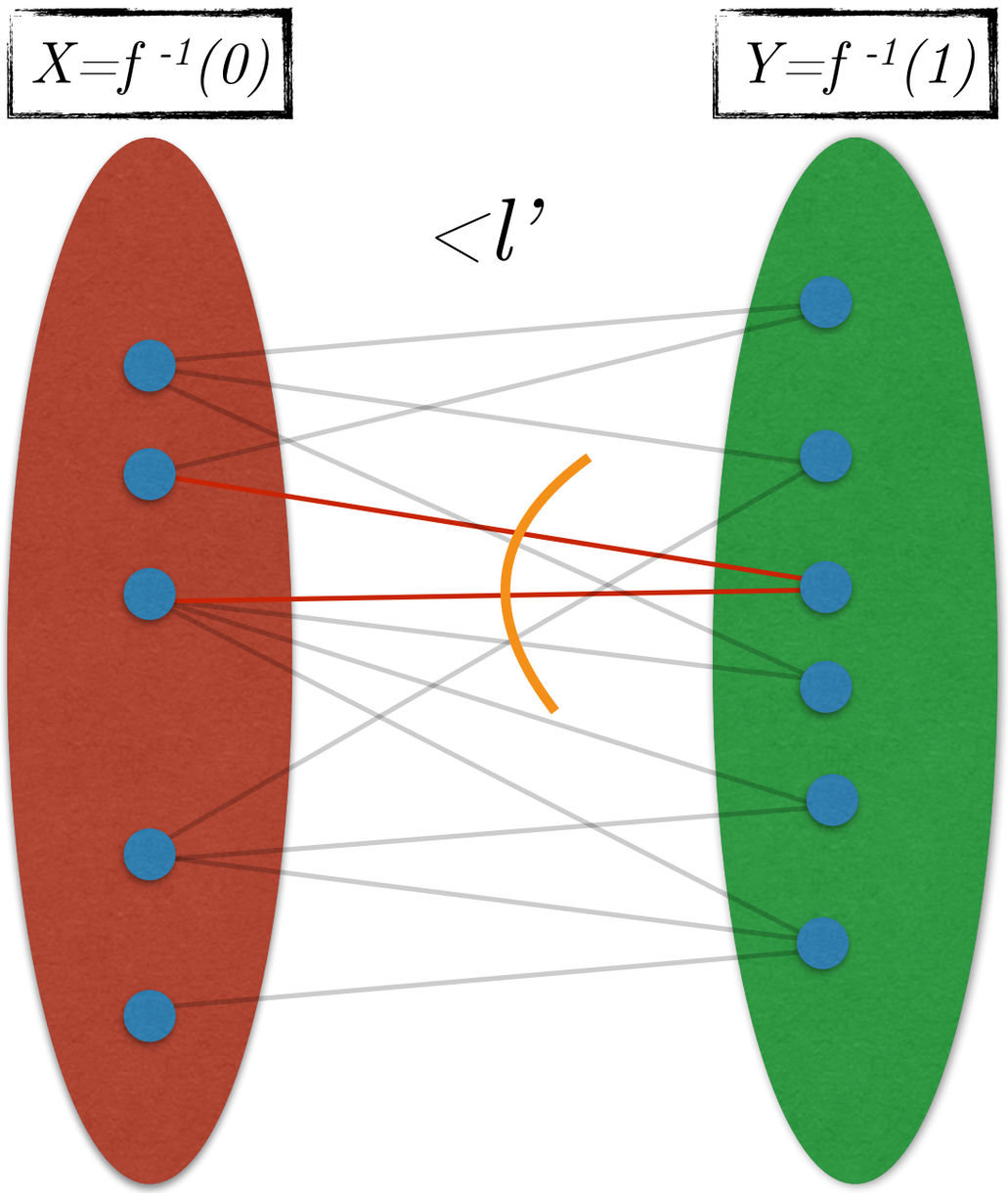
$(x, y) \in R$

Adversary method: original version



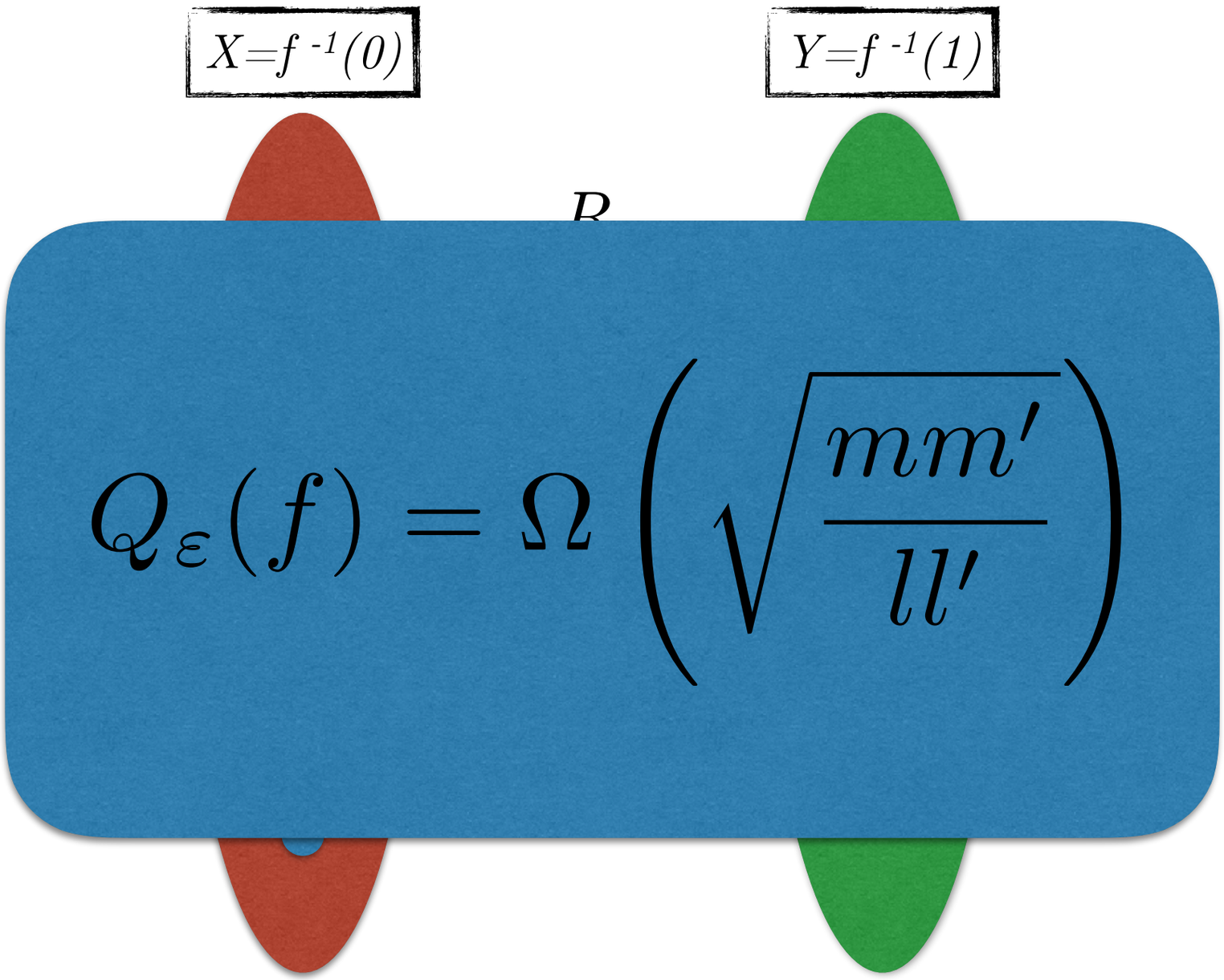
$(x, y) \in R$ and $x_i \neq y_i$

Adversary method: original version

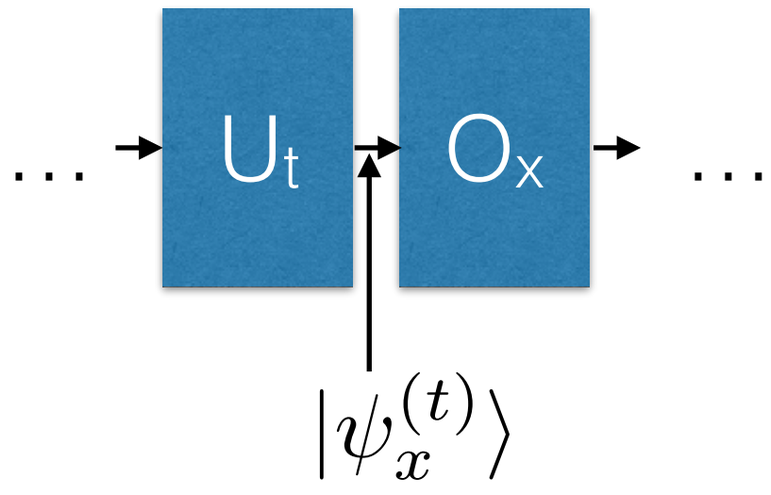


$(x, y) \in R$ and $x_i \neq y_i$

Adversary method: original version



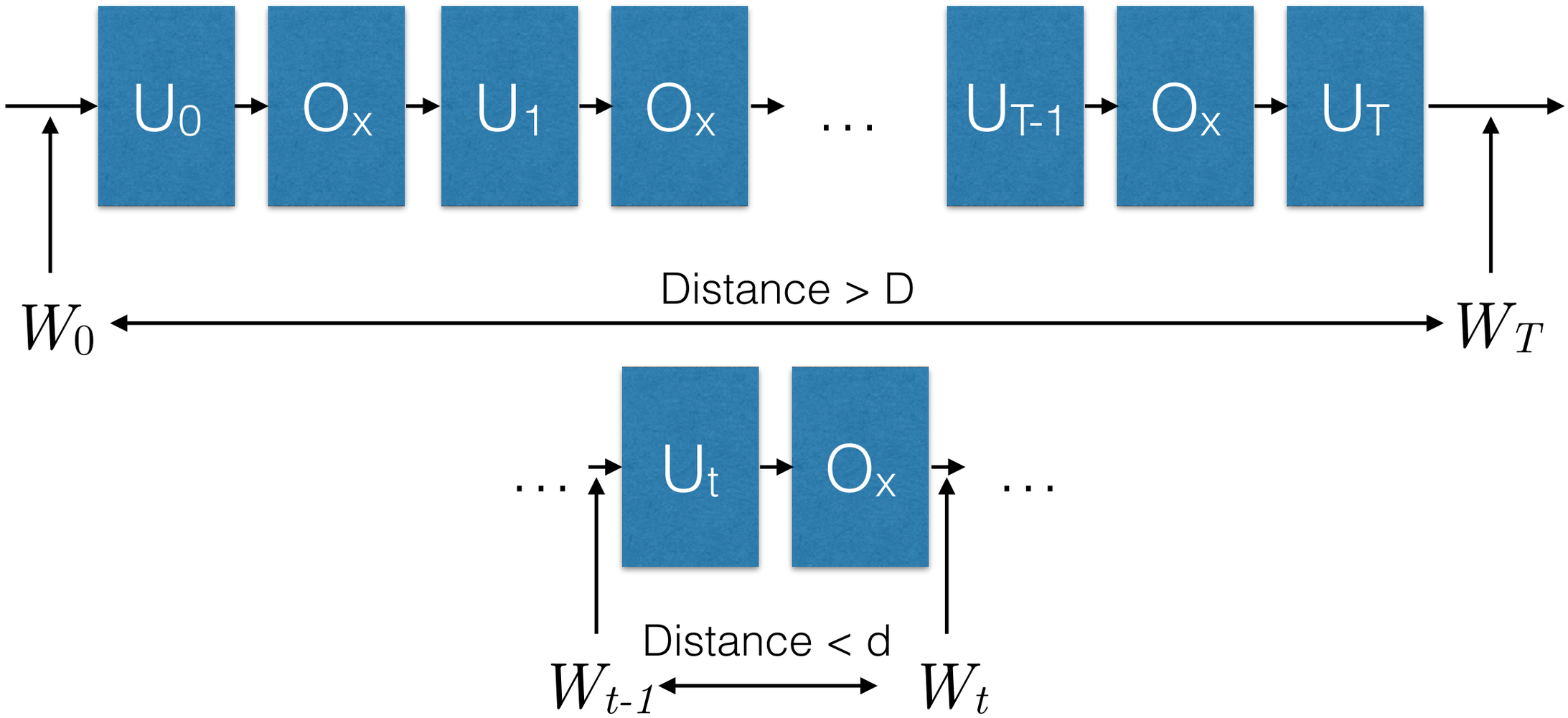
Proof sketch



Progress function:

$$W_t = \sum_{x,y \in R} \langle \psi_x^{(t)} | \psi_y^{(t)} \rangle$$

Proof sketch



1. $|W_T - W_0| = \Omega(\sqrt{|X||Y|mm'})$

2. $|W_t - W_{t-1}| = O(\sqrt{|X||Y|ll'})$

Proof sketch - Part 1

$$W_0 = \sum_{x,y \in R} \langle \Psi_x^{(0)} | \Psi_y^{(0)} \rangle$$

$$= \#\{(x,y) \in R\}$$

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

$$\geq \sqrt{|X||Y|mm'}$$

$$W_T \simeq 0$$

Proof sketch - Part 2

$$|W_t - W_{t-1}| \leq \sum_{x,y \in R} |\langle \psi_x^{(t)} | \psi_y^{(t)} \rangle - \langle \psi_x^{(t-1)} | \psi_y^{(t-1)} \rangle|$$

$$\leq \sum_{x,y \in R} |\langle O_x U_t \psi_x | O_y U_t \psi_y \rangle - \langle \psi_x | \psi_y \rangle|$$

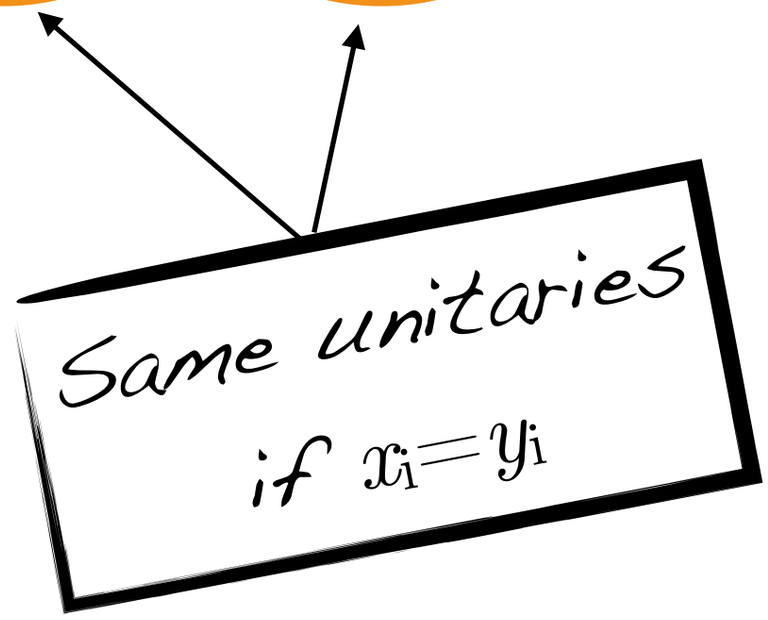
$$\leq \max_i \sum_{x,y \in R} |\langle O_{x,i} U_t \psi_x | O_{y,i} U_t \psi_y \rangle - \langle \psi_x | \psi_y \rangle|$$

Proof sketch - Part 2

$$|W_t - W_{t-1}| \leq \sum_{x,y \in R} |\langle \psi_x^{(t)} | \psi_y^{(t)} \rangle - \langle \psi_x^{(t-1)} | \psi_y^{(t-1)} \rangle|$$

$$\leq \sum_{x,y \in R} |\langle O_x U_t \psi_x | O_y U_t \psi_y \rangle - \langle \psi_x | \psi_y \rangle|$$

$$\leq \max_i \sum_{x,y \in R} |\langle O_{x,i} U_t \psi_x | O_{y,i} U_t \psi_y \rangle - \langle \psi_x | \psi_y \rangle|$$



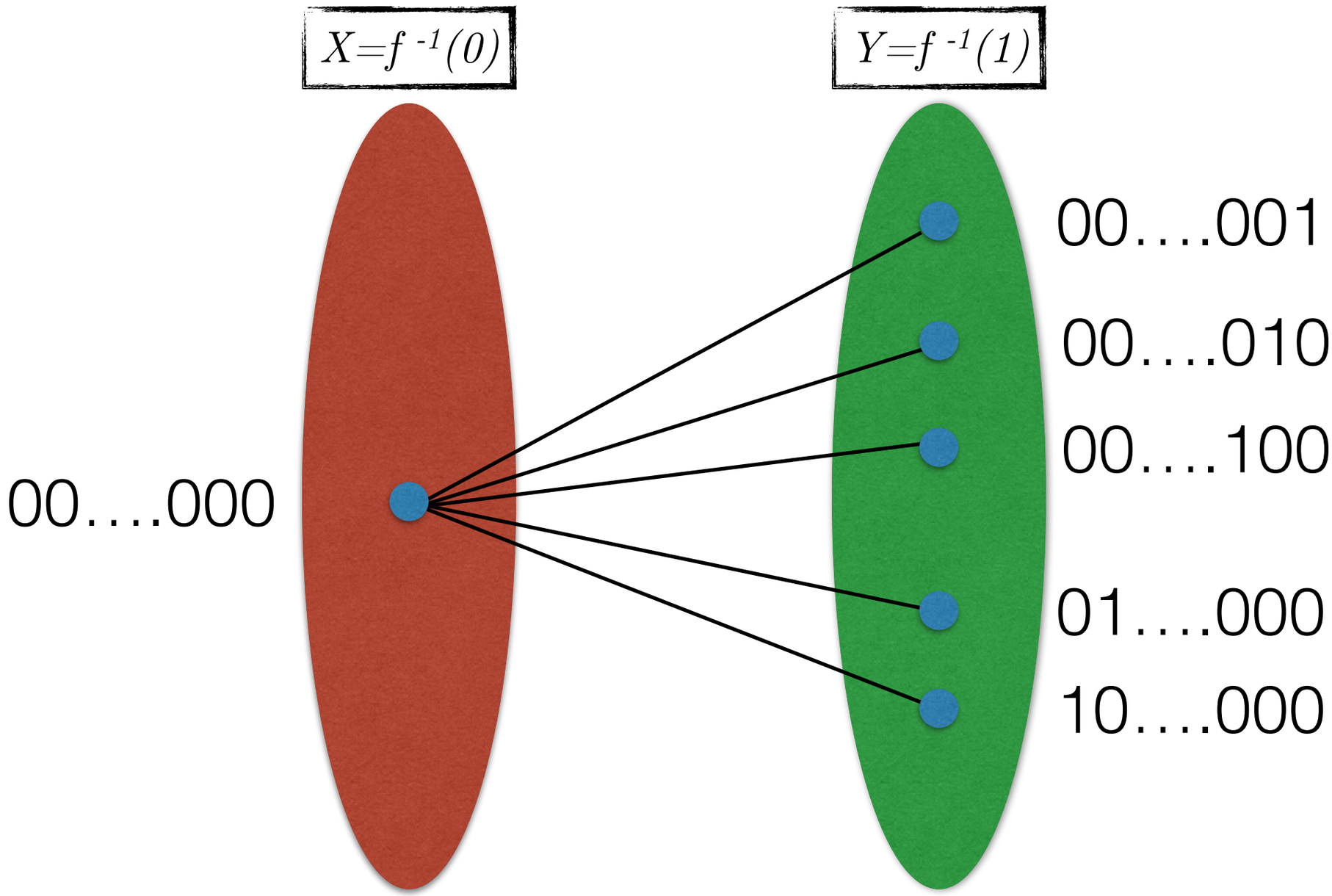
Proof sketch - Part 2

$$|W_t - W_{t-1}| \leq \max_i \sum_{x,y \in R} |\langle O_{x,i} U_t \psi_x | O_{y,i} U_t \psi_y \rangle - \langle \psi_x | \psi_y \rangle|$$

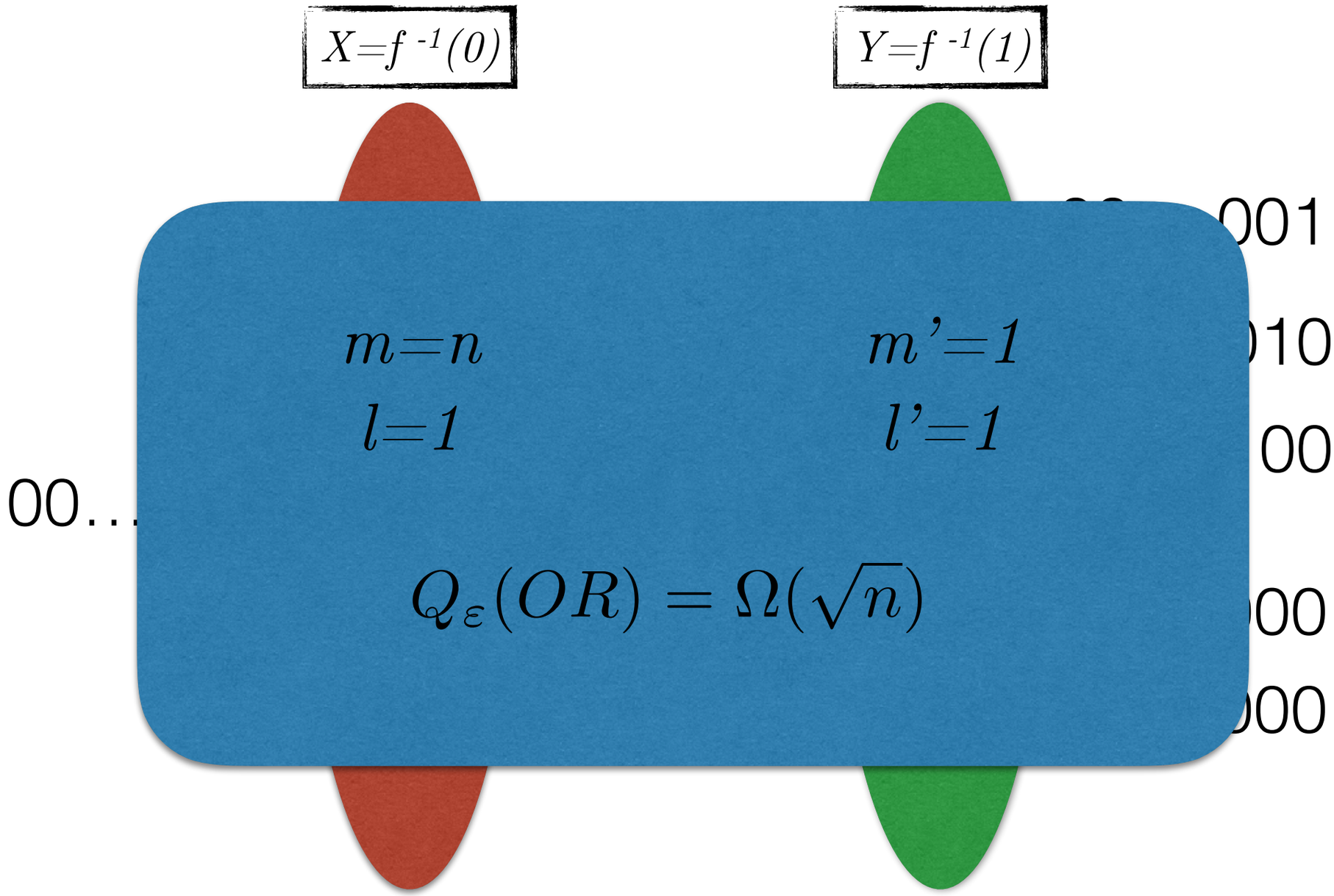
$$\leq \sqrt{|X||Y|ll'}$$

reduces to counting edges s.t. $x_i \neq y_i$

Application: the OR function



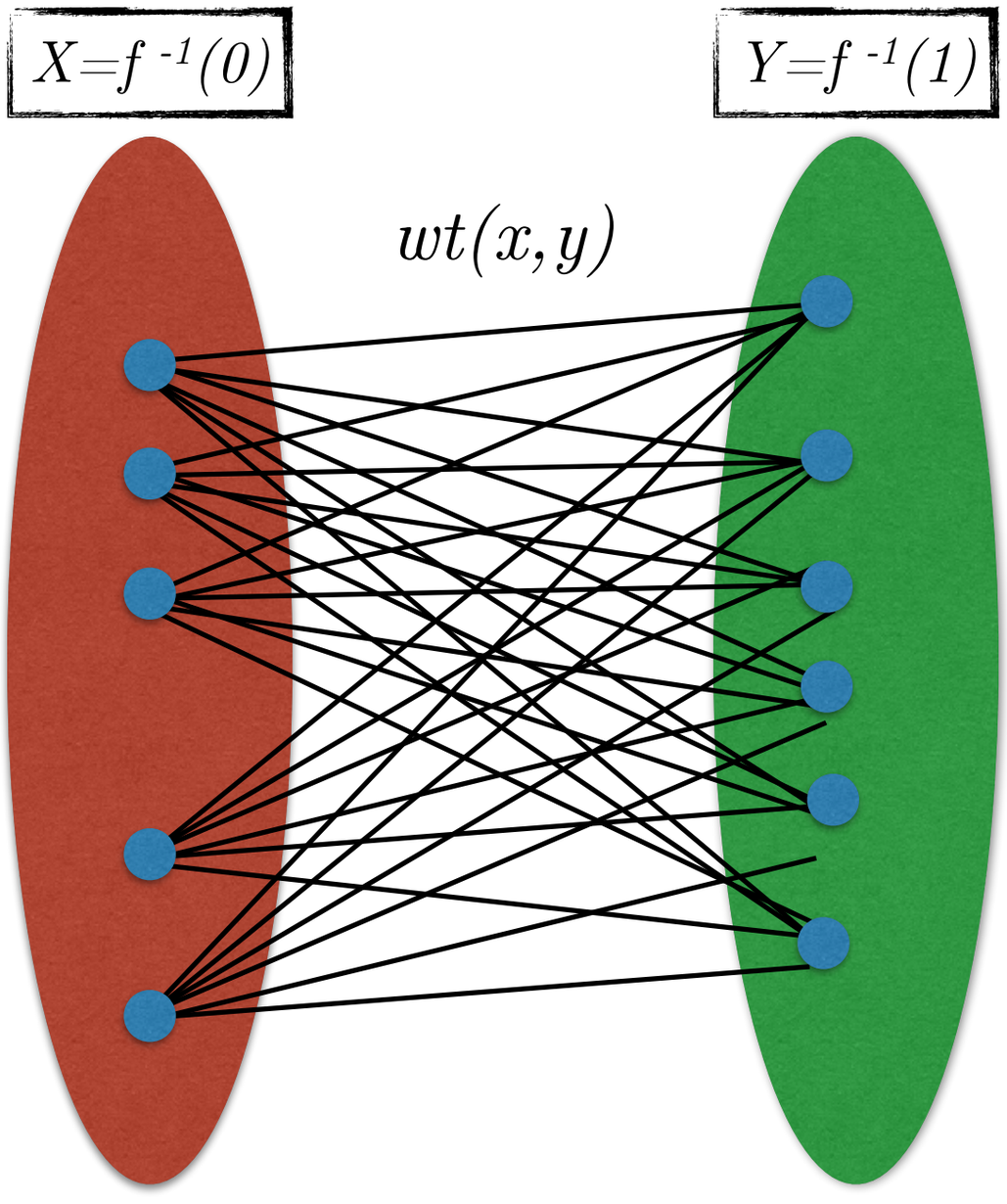
Application to the OR function



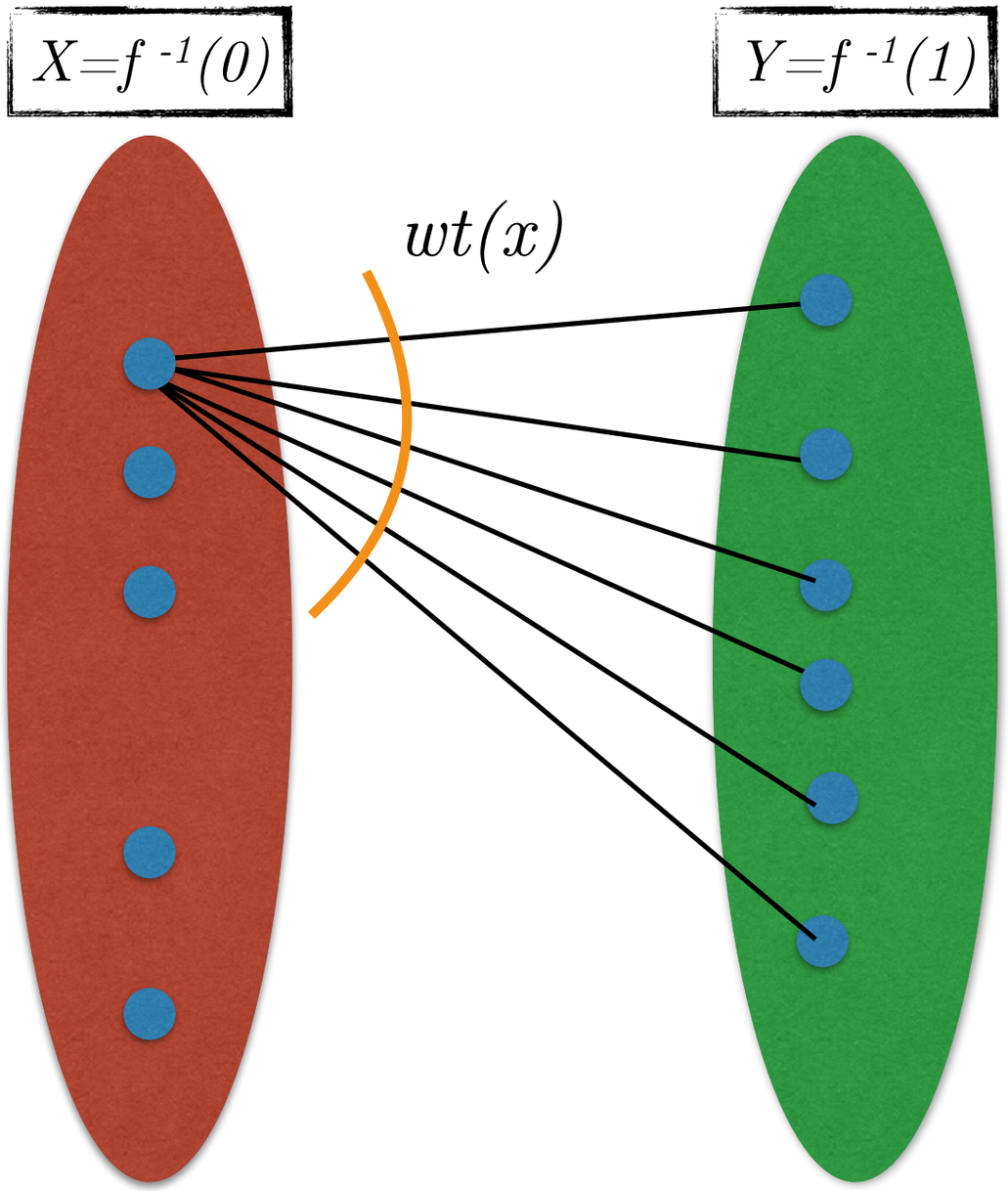
Adversary method(s)

- ✓ Original adversary method
- Weighted adversary method
- Spectral adversary method
- Generalized adversary method

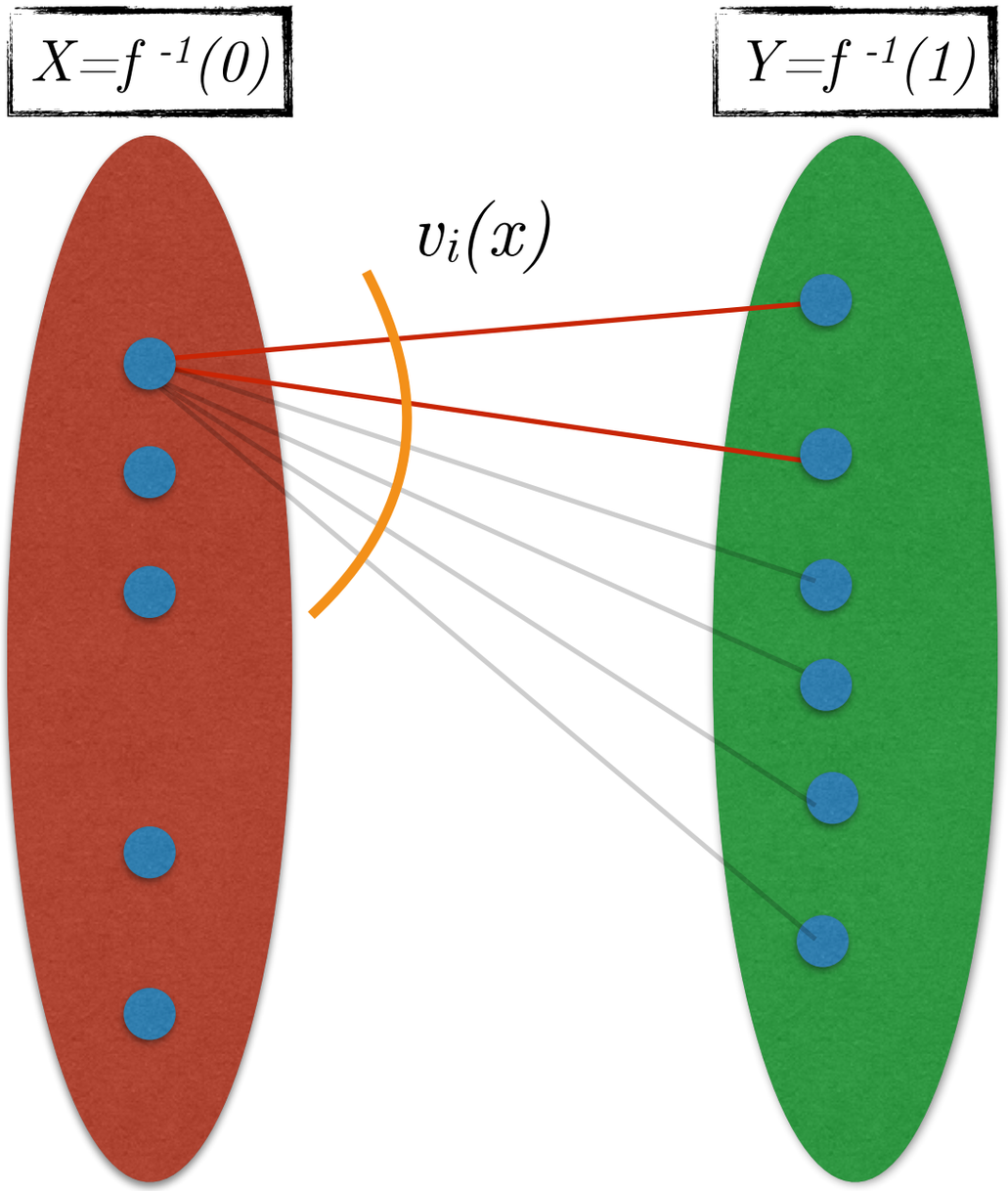
Weighted adversary method



Weighted adversary method

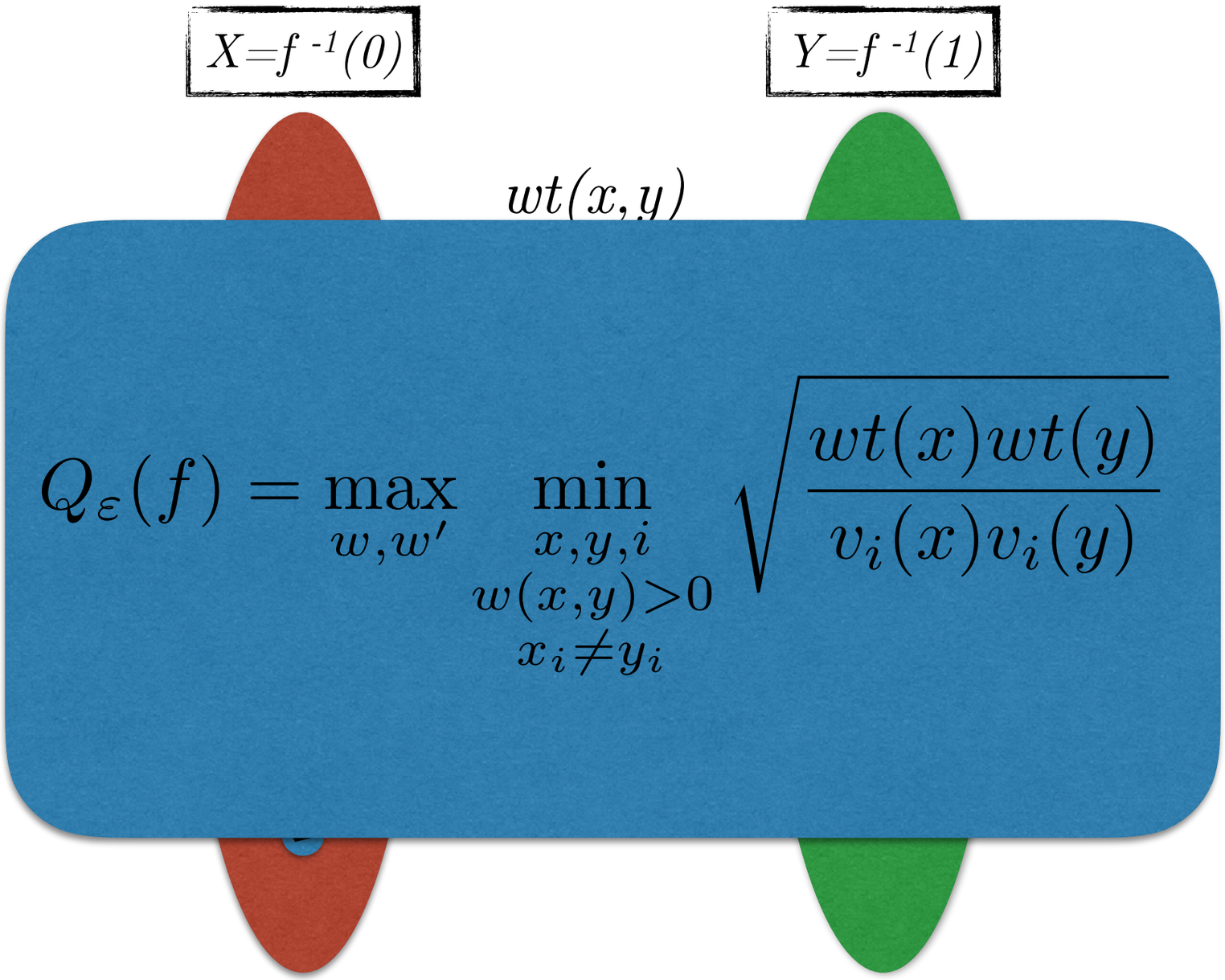


Weighted adversary method



$x_i \neq y_i$

Weighted adversary method



Adversary method(s)

- ✓ Original adversary method
- ✓ Weighted adversary method
- Spectral adversary method
- Generalized adversary method

Spectral adversary method

adversary matrix: $\Gamma \geq 0$

$\Gamma[x, y] = 0$ iff $f(x) = f(y)$

Masks : $D_i[x, y]{=}1$ iff $x_i \neq y_i$

$$Adv(f) = \max_{\Gamma \geq 0} \frac{\|\Gamma\|}{\max_i \|\Gamma \circ D_i\|}$$

Spectral adversary method

adversary matrix: $\Gamma \geq 0$

$\Gamma[x, y] = 0$ iff $f(x) = f(y)$

Masks : $D_i[x, y]{=}1$ iff $x_i \neq y_i$

$$Adv(f) = \max_{\Gamma \geq 0} \frac{\|\Gamma\|}{\max_i \|\Gamma \circ D_i\|}$$

Entry-wise product

Spectral adversary method

$$Adv(f) = \max_{\Gamma \geq 0} \frac{\|\Gamma\|}{\max_i \|\Gamma \circ D_i\|}$$

$$Q_\varepsilon(f) = \Omega(Adv(f))$$

Spectral adversary method

$$Adv(f) = \max_{\Gamma \geq 0} \frac{\|\Gamma\|}{\max_i \|\Gamma \circ D_i\|}$$

- Easy generalization
- semi-definite program
- Ambainis' function f :

$$Q_\varepsilon(f) = \Omega\left(deg(f)^{1.321}\right)$$

Limitation of the adversary method

$$Adv(f) = \max_{\Gamma \geq 0} \frac{\|\Gamma\|}{\max_i \|\Gamma \circ D_i\|}$$

$$Adv(ED) \leq \sqrt{n}$$

$$Q_\varepsilon(ED) = \Omega(n^{2/3})$$

Certificate complexity barrier:
A feasible solution to the dual SDP

Adversary method(s)

- ✓ Original adversary method
- ✓ Weighted adversary method
- ✓ Spectral adversary method
- • Generalized adversary method

Generalized adversary method

$$Adv(f) = \max_{\Gamma \geq 0} \frac{\|\Gamma\|}{\max_i \|\Gamma \circ D_i\|}$$

$$Adv^{\pm}(f) = \max_{\Gamma} \frac{\|\Gamma\|}{\max_i \|\Gamma \circ D_i\|}$$

$Adv^{\pm}$ breaks the certificate complexity barrier

« Negative weight makes adversary stronger »
Høyer, Lee, Špalek

Generalized adversary method

$$Adv^{\pm}(f) = \max_{\Gamma} \frac{\|\Gamma\|}{\max_i \|\Gamma \circ D_i\|}$$

$$Q_{\varepsilon}(f) = \Theta(Adv^{\pm}(f))$$

Lower bound: Høyer, Lee, Špalek [2006]

Upper bound: Reichardt [09]

Dual of $Adv^{\pm}$ can be interpreted as a span program

Generalized adversary method

$$Adv^{\pm}(f) = \max_{\Gamma} \frac{\|\Gamma\|}{\max_i \|\Gamma \circ D_i\|}$$

$$Adv^{\pm}(ED) = \Theta(n^{2/3})$$

Belovs [12]: explicit adversary matrix

Function composition

$$f{:}B^n \rightarrow C,\ g{:}\ A \rightarrow B$$

$$f{\circ}g^n{:}A^n \rightarrow C$$

$$f{\circ}g^n(x_1,\ldots,x_n) = f(g(x_1),\ldots,g(x_n))$$

$$Q_\varepsilon(f \circ g^n) = O(Q_\varepsilon(f)Q_\varepsilon(g))$$

Composition of algorithms: run an algorithm for f. For each query, run an algorithm for g.

Function composition

$$f{:}B^n \rightarrow C,\ g{:}\ A \rightarrow B$$

$$f{\circ}g^n{:}A^n \rightarrow C$$

$$f{\circ}g^n(x_1,\ldots,x_n) = f(g(x_1),\ldots,g(x_n))$$

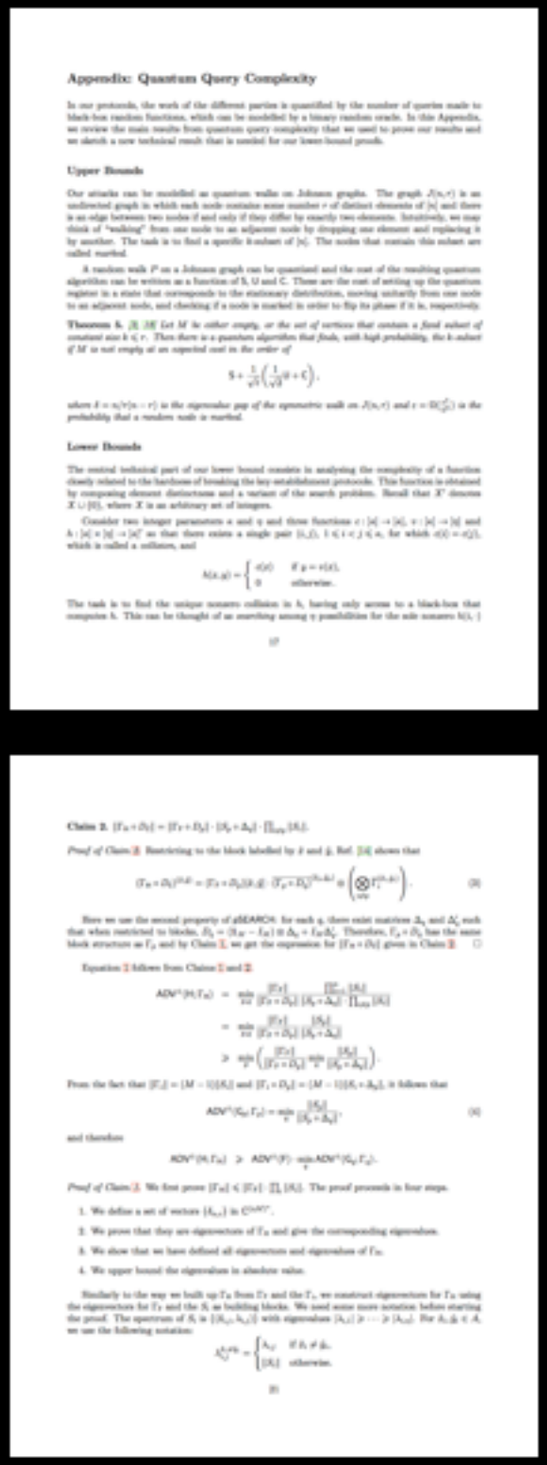
If $B{=}\{0,1\}$: $Q_\varepsilon(f \circ g^n) = \Omega(Q_\varepsilon(f)Q_\varepsilon(g))$

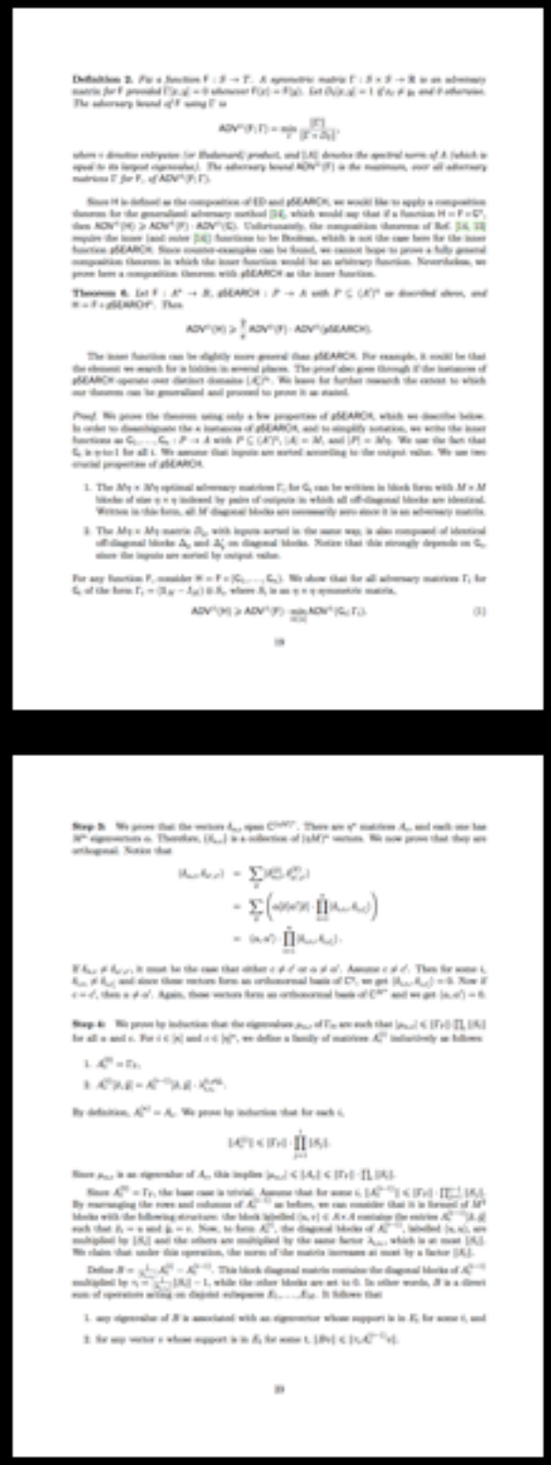
Easy counterexample to generalization:

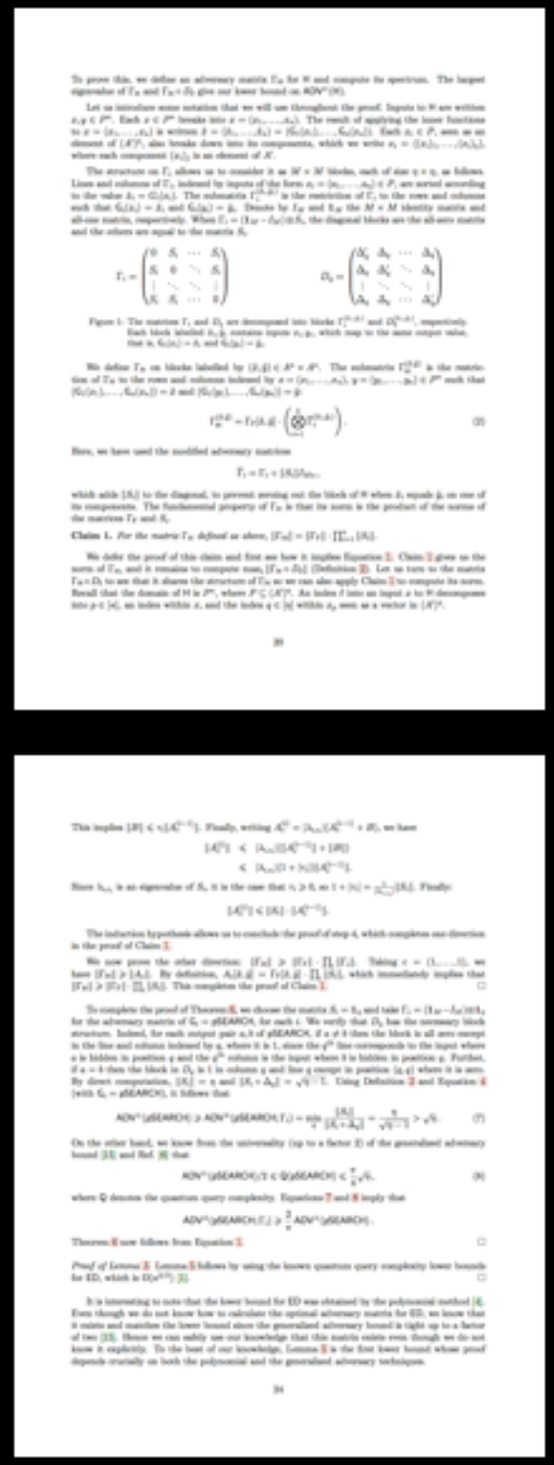
g always returns an odd number

f is constant if all inputs are odd, hard otherwise

Proof overview







Peter Høyer

Function composition

$$\begin{array}{ccccc} & & A^m & \xrightarrow{\qquad} & \{0,1\}^n & \xrightarrow{\qquad} & C \\ & & & \overset{g}{\longrightarrow} & & \overset{f}{\longrightarrow} & \\ x = (x_1, \ldots, x_n) & & & \tilde{x} = g^n(x) & & & f(\tilde{x}) = f \circ g^n(x) \end{array}$$

$$\Gamma_g = \left(\begin{array}{c|c} 0 & \Gamma_g^{1,0} \\ \hline \Gamma_g^{0,1} & 0 \end{array}\right) \qquad \Gamma_f = \left(\begin{array}{c} \\ \Gamma_f[\tilde{x}, \tilde{y}] \\ \\ \end{array}\right)$$

$$\Gamma_{f \circ g^n} = \left(\begin{array}{c|c|c} & & \\ \hline & \Gamma^{\tilde{x},\tilde{y}} & \\ \hline & & \end{array}\right)$$

Function composition

$$A^m \longrightarrow \{0,1\}^n \longrightarrow C$$

$$x = (x_1, \ldots, x_n) \xrightarrow{g} \tilde{x} = g^n(x) \xrightarrow{f} f(\tilde{x}) = f \circ g^n(x)$$

$$\tilde{x} = (g(x_1), g(x_2), \ldots g(x_n))$$

$$\Gamma^{\tilde{x},\tilde{y}} = \Gamma_f[\tilde{x}, \tilde{y}].$$

$$\Gamma_g = \left(\begin{array}{c|c} 0 & \Gamma_g^{1,0} \\ \hline \Gamma_g^{0,1} & 0 \end{array}\right)$$

$$\Gamma_f = \begin{pmatrix} \\ \Gamma_f[\tilde{x}, \tilde{y}] \\ \\ \end{pmatrix}$$

Function composition

$$A^m \longrightarrow \{0,1\}^n \longrightarrow C$$

$$x = (x_1, \ldots, x_n) \xrightarrow{g} \tilde{x} = g^n(x) \xrightarrow{f} f(\tilde{x}) = f \circ g^n(x)$$

$$\tilde{x} = (g(x_1), g(x_2), \ldots g(x_n))$$

$$\Gamma^{\tilde{x},\tilde{y}} = \Gamma_f[\tilde{x}, \tilde{y}] \cdot (\Gamma_g^{g(x_1),g(y_1)} \otimes$$

$$\Gamma_g = \left(\begin{array}{c|c} 0 & \Gamma_g^{1,0} \\ \hline \Gamma_g^{0,1} & 0 \end{array}\right)$$

$$\Gamma_f = \begin{pmatrix} \Gamma_f[\tilde{x}, \tilde{y}] \end{pmatrix}$$

Function composition

$$A^m \longrightarrow \{0,1\}^n \longrightarrow C$$

$$x = (x_1, \ldots, x_n) \xrightarrow{g} \tilde{x} = g^n(x) \xrightarrow{f} f(\tilde{x}) = f \circ g^n(x)$$

$$\tilde{x} = (g(x_1), g(x_2), \ldots g(x_n))$$

$$\Gamma^{\tilde{x},\tilde{y}} = \Gamma_f[\tilde{x}, \tilde{y}] \cdot (\Gamma_g^{g(x_1),g(y_1)} \otimes \Gamma_g^{g(x_2),g(y_2)}$$

$$\Gamma_g = \left(\begin{array}{c|c} 0 & \Gamma_g^{1,0} \\ \hline \Gamma_g^{0,1} & 0 \end{array}\right)$$

$$\Gamma_f = \begin{pmatrix} \Gamma_f[\tilde{x}, \tilde{y}] \end{pmatrix}$$

Function composition

$$A^m \longrightarrow \{0,1\}^n \longrightarrow C$$

$$x = (x_1, \ldots, x_n) \xrightarrow{g} \tilde{x} = g^n(x) \xrightarrow{f} f(\tilde{x}) = f \circ g^n(x)$$

$$\tilde{x} = (g(x_1), g(x_2), \ldots g(x_n))$$

$$\Gamma^{\tilde{x},\tilde{y}} = \Gamma_f[\tilde{x},\tilde{y}] \cdot (\Gamma_g^{g(x_1),g(y_1)} \otimes \Gamma_g^{g(x_2),g(y_2)} \otimes \ldots \otimes \Gamma_g^{g(x_n),g(y_n)})$$

$$\Gamma_g = \left(\begin{array}{c|c} 0 & \Gamma_g^{1,0} \\ \hline \Gamma_g^{0,1} & 0 \end{array}\right)$$

$$\Gamma_f = \begin{pmatrix} \Gamma_f[\tilde{x},\tilde{y}] \end{pmatrix}$$

Function composition

$$A^m \longrightarrow \{0,1\}^n \longrightarrow C$$

$$x = (x^1, \ldots, x^n) \xrightarrow[g]{} \tilde{x} = g^n(x) \xrightarrow[f]{} f(\tilde{x}) = f \circ g^n(x)$$

$$\Gamma_{f \circ g^n} = \left(\begin{array}{|c|c|c|} \hline & & \\ \hline & \Gamma^{\tilde{x},\tilde{y}} & \\ \hline & & \\ \hline \end{array} \right) \qquad \Gamma^{\tilde{x},\tilde{y}} = \Gamma_f[\tilde{x},\tilde{y}] \cdot \left(\bigotimes_{i=1}^{m} \overline{\Gamma}_g^{\tilde{x}_i,\tilde{y}_i} \right)$$

$$\|\Gamma_{f \circ g^m}\| = \|\Gamma_f\| \|\Gamma_g\|^m$$

And something similar for $\Gamma \circ D_i$...

Multiplicative adversary

- Better handling of the errors
- Used to prove direct product theorems (rather than direct sum)
- Also generalizes the polynomial method

Other applications

- Various functions: graph problems, Element Distinctness, etc…
- Cryptographic applications: Maximum gap is polynomial !
    - Merkle Puzzles
    - Symmetric cryptography