Quantum query complexity

Lecture 4

The adversary method

Materials: https://yassine-hamoudi.github.io/pcmi2023/

Last lecture (end of the proof)

SEARCH problem: Find i such that $x_i = 1$

$$\Pi = \left(\sum_{1 \in x} |x\rangle\langle x|\right) \otimes \mathrm{Id} \qquad \Delta_t = \|\Pi|\psi^t_{\mathrm{rec}}\rangle\|^2$$

Lemma 1: $\Delta_0 = 0$

Lemma 2: $\sqrt{\Delta_{t+1}} \leq \sqrt{\Delta_t} + \sqrt{10/n}$

Proof: We showed that $\sqrt{\Delta_{t+1}} \leq \sqrt{\Delta_t} + \|\Pi R(\mathrm{Id} - \Pi)|\psi^t_{\mathrm{rec}}\rangle\|$

Claim: For all $|\psi\rangle \in \ker(\Pi)$ we have $\|\Pi R|\psi\rangle\| \leq \sqrt{10/n}\ \||\psi\rangle\|$

Last lecture (end of the proof)

<u>Proposition:</u> When $b \neq 0$, the recording query operator R acts as:

$$R\,|\ldots, x_{i-1}, \emptyset, x_{i+1}, \ldots\rangle \otimes |i, b\rangle \;=\; |\ldots, x_{i-1}\rangle \left(\frac{1}{\sqrt{n}} \sum_{0 \leq y < n} \omega^{by} |y\rangle \right) |x_{i+1}, \ldots\rangle \otimes |i, b\rangle$$

$$R\,|\ldots, x_{i-1}, y, x_{i+1}, \ldots\rangle \otimes |i, b\rangle \;=\; |\ldots, x_{i-1}\rangle \left(\omega^{by} |y\rangle + |\mathrm{error}_y\rangle \right) |x_{i+1}, \ldots\rangle \otimes |i, b\rangle$$

where $|\mathrm{error}_y\rangle = \frac{\omega^{by}}{\sqrt{n}} |\emptyset\rangle + \sum_{0 \leq z < n} \frac{1 - \omega^{by} - \omega^{bz}}{n} |z\rangle$

Focus of this lecture

The (generalized) adversary method

- A lower bound method that is always optimal

  > We'll show in lecture 5 how to turn it into an algorithm

  > Counterpart: often harder to use

- It shares some ideas with the hybrid method (lecture 1) and the recording method (lecture 3)

  (in fact: these can be seen as particular cases of it)

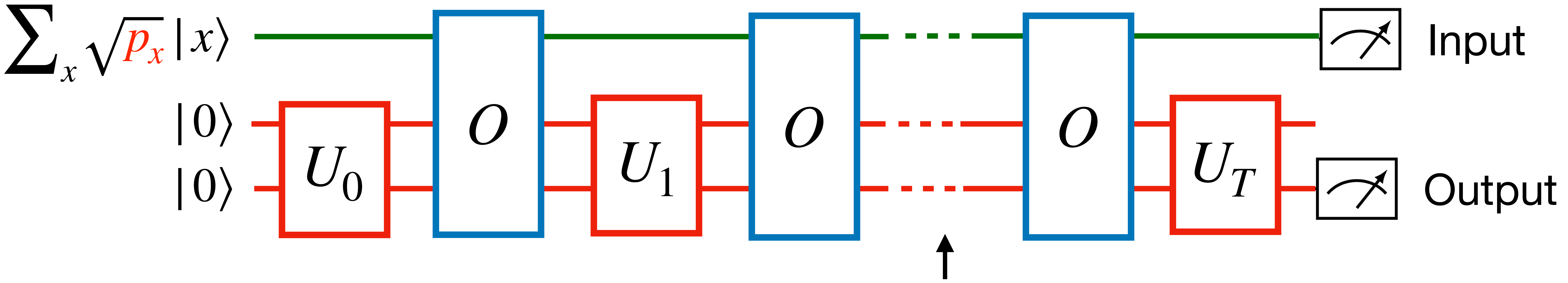
Reminders

The distinguishing lemma (lecture 1)

The states $|\psi_x^T\rangle$ and $|\psi_y^T\rangle$ can be distinguished with probability $\geq 2/3$ if an only if there are "sufficiently orthogonal" $|\langle\psi_x^T|\psi_y^T\rangle| \leq 2\sqrt{2}/3$

The purification viewpoint (lecture 3)

We can set a distribution $(p_x)_x$ on the input by adding a purification register

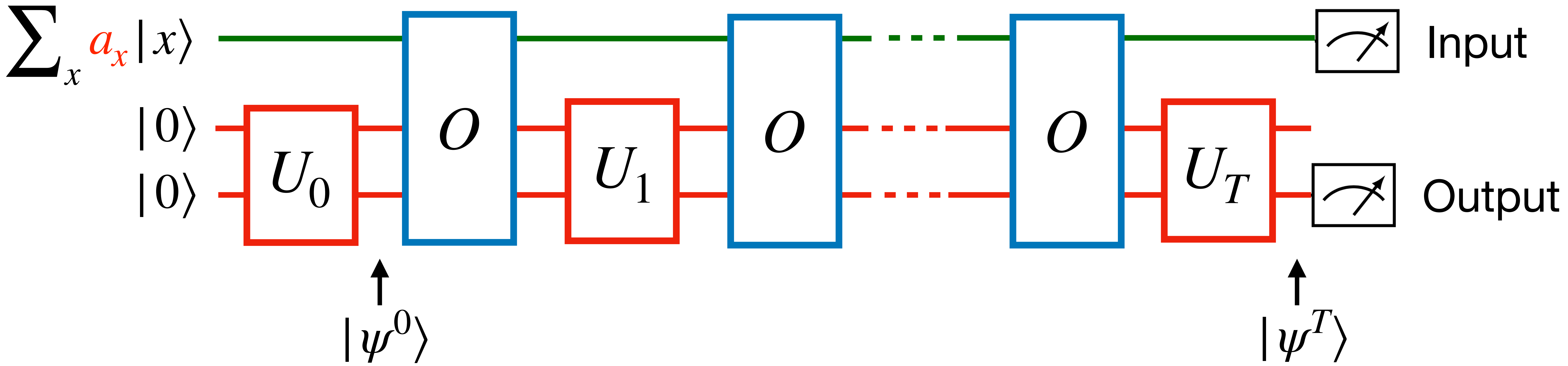


$|\psi^t\rangle = \sum_x \sqrt{p_x}|x\rangle \otimes |\psi_x^t\rangle$

Quantum adversary

First step: replace $(p_x)_x$ with complex numbers $(a_x)_x$ s.t. $\sum_x |a_x|^2 = 1$

$$|\psi^t\rangle = \sum_x a_x |x\rangle \otimes |\psi_x^t\rangle$$

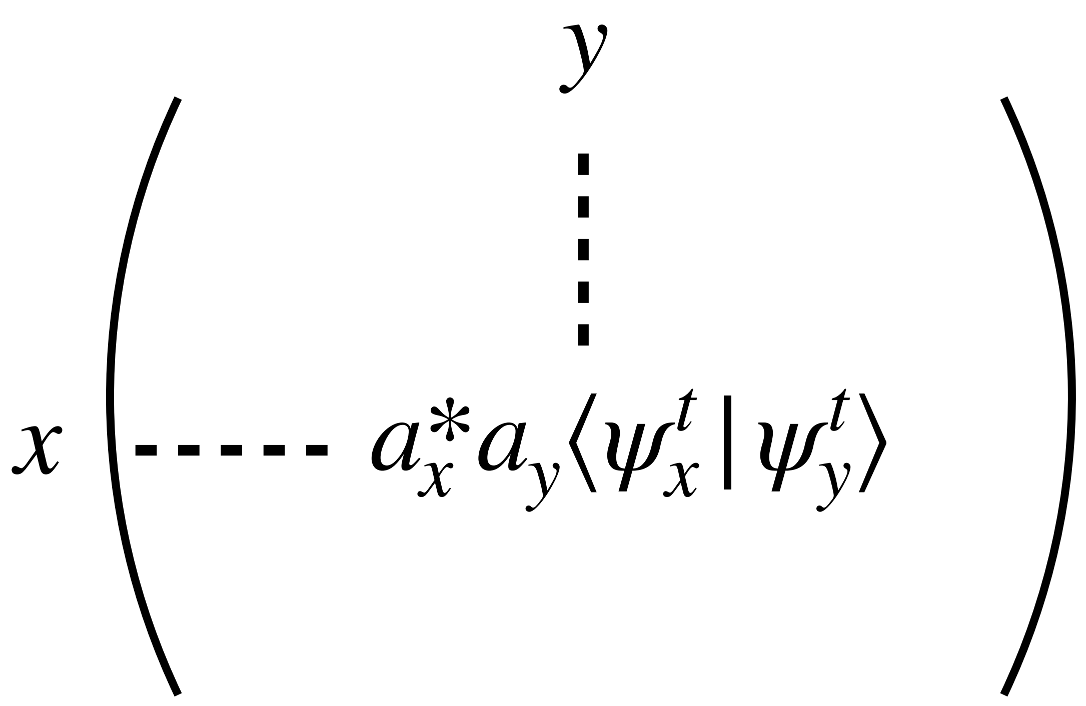


First step: replace $(p_x)_x$ with complex numbers $(a_x)_x$ s.t. $\sum_x |a_x|^2 = 1$

$$|\psi^t\rangle = \sum_x a_x |x\rangle \otimes |\psi_x^t\rangle$$

Second step: consider the Gram matrix:

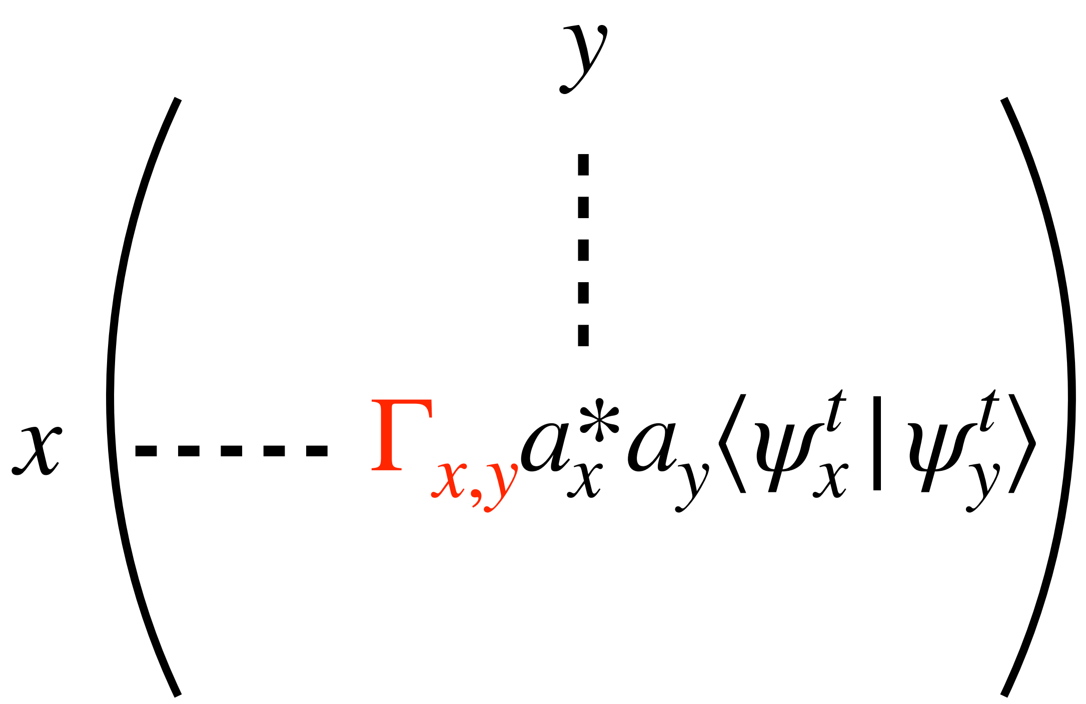
$$\sum_{x,y} a_x^* a_y \langle \psi_x^t | \psi_y^t \rangle |x\rangle\langle y|$$



Third step: place some weights $\Gamma_{x,y}$ on the "hard" pairs of inputs

(symmetric) $\Gamma_{x,y} = \Gamma_{y,x}$

(consistent) if $f(x) = f(y)$ then $\Gamma_{x,y} = 0$



Adversary matrix: $\Gamma \in \mathbb{R}^{2^n \times 2^n}$ symmetric and $f(x) = f(y) \Rightarrow \Gamma_{x,y} = 0$

Adversary distribution: $a \in \mathbb{C}^{2^n}$ principal (unit) eigenvector of Γ

"Punctured" matrices: $\Gamma_i \in \mathbb{R}^{2^n \times 2^n}$ such that $(\Gamma_i)_{x,y} = \Gamma_{x,y} \cdot \mathbf{1}_{x_i \neq y_i}$

Progress measure: $\Delta_t = |\langle \psi^t | (\Gamma \otimes \mathrm{Id}) | \psi^t \rangle| = \left| \sum_{x,y} \Gamma_{x,y} a_x^* a_y \langle \psi_x^t | \psi_y^t \rangle \right|$

Lemma 1: $\Delta_0 = \|\Gamma\|$ *(initial condition)*

Lemma 2: $\Delta_T < 0.95\|\Gamma\|$ if the algorithm succeeds wp $\geq 2/3$ *(final condition)*

Lemma 3: $\Delta_{t+1} \geq \Delta_t - 2 \max_{1 \leq i \leq n} \|\Gamma_i\|$ *(evolution)*

Theorem: $Q(f) \geq \max_{\Gamma} \frac{\|\Gamma\|}{40 \cdot \max_{1 \leq i \leq n} \|\Gamma_i\|}$

- Positive-weight adversary: $\forall x, y, \Gamma_{x,y} \geq 0$
  - Has a nice combinatorial interpretation (see problem session)
  - Sub-optimal (the "certificate" and "property testing" barriers)

- Negative-weight adversary: $\forall x, y, \Gamma_{x,y} \in \mathbb{R}$
  - Optimal! (see next lecture) $Q(f) = \Theta\left(\max_{\Gamma} \frac{\|\Gamma\|}{\max_{1 \leq i \leq n} \|\Gamma_i\|}\right)$

Applications

<u>OR function:</u> $f(x) = 0$ if and only if $x = (0,0,\ldots,0)$

We (again) only focus on the $n+1$ "hardest" inputs denoted by:

$\vec{0} = (0,0,\ldots,0)$ $\quad \vec{1} = (1,0,\ldots,0)$ $\quad \vec{2} = (0,1,0,\ldots,0)$ $\quad \ldots \quad$ $\vec{n} = (0,0,\ldots,1)$

$$\Gamma = \begin{array}{c} \begin{array}{cccc} \vec{0} & \vec{1} & \ldots & \vec{n} \end{array} \\ \begin{pmatrix} 0 & 1 & \ldots & 1 \\ 1 & 0 & \ldots & 0 \\ \vdots & \vdots & & \vdots \\ 1 & 0 & \ldots & 0 \end{pmatrix} \end{array} \begin{array}{c} \vec{0} \\ \vec{1} \\ \vdots \\ \vec{n} \end{array} \qquad \Gamma_i = \begin{array}{c} \vec{i} \\ \begin{pmatrix} 0 & \ldots & 0 & 1 & 0 & \ldots & 0 \\ \vdots & 0 & \ldots & \ldots & \ldots & \ldots & 0 \\ 0 & \vdots & & & & & \vdots \\ 1 & \vdots & & & & & \vdots \\ 0 & \vdots & & & & & \vdots \\ \vdots & \vdots & & & & & \vdots \\ 0 & 0 & \ldots & \ldots & \ldots & \ldots & 0 \end{pmatrix} \end{array} \vec{i}$$

(omitting the other 0-entries)

$\|\Gamma\| = \sqrt{n}$

$\|\Gamma_i\| = 1$

$\Rightarrow Q(\mathrm{OR}) \geq \sqrt{n}/40$

Dual SDP

$$Q(f) \geq \mathrm{Adv}(f)/40$$

Rewrite the optimization problem:

$$\mathrm{Adv}(f) = \max_{\Gamma} \frac{\|\Gamma\|}{\max_{1\leq i\leq n} \|\Gamma_i\|}$$

s.t. $\Gamma_{x,y} = \Gamma_{y,x} \ \ \forall x, y$

$\Gamma_{x,y} = 0 \ \ \forall x, y, f(x) = f(y)$

$\Gamma \in \mathbb{R}^{2^n \times 2^n}$

$\Leftrightarrow$

$$\mathrm{Adv}(f) = \max_{\Gamma} \|\Gamma\|$$

s.t. $\|\Gamma_i\| \leq 1 \ \ \forall i$

$\Gamma_{x,y} = \Gamma_{y,x} \ \ \forall x, y$

$\Gamma_{x,y} = 0 \ \ \forall x, y, f(x) = f(y)$

$\Gamma \in \mathbb{R}^{2^n \times 2^n}$

$$Q(f) \geq \mathrm{Adv}(f)/40$$

Rewrite the optimization problem:

$$\mathrm{Adv}(f) = \max_{\Gamma} \frac{\|\Gamma\|}{\max_{1\leq i\leq n} \|\Gamma_i\|}$$

$$\text{s.t.}\quad \Gamma_{x,y} = \Gamma_{y,x} \quad \forall x, y$$

$$\Gamma_{x,y} = 0 \quad \forall x, y, f(x) = f(y)$$

$$\Gamma \in \mathbb{R}^{2^n \times 2^n}$$

$$\Leftrightarrow$$

$$\mathrm{Adv}(f) = \max_{\Gamma,\epsilon} \epsilon$$

$$\text{s.t.}\quad \|\Gamma\| \leq \epsilon, \quad \|\Gamma_i\| \leq 1 \quad \forall i$$

$$\Gamma_{x,y} = \Gamma_{y,x} \quad \forall x, y$$

$$\Gamma_{x,y} = 0 \quad \forall x, y, f(x) = f(y)$$

$$\Gamma \in \mathbb{R}^{2^n \times 2^n}, \epsilon \in \mathbb{R}$$

$$Q(f) \geq \mathrm{Adv}(f)/40$$

Rewrite the optimization problem:

$$\mathrm{Adv}(f) = \max_{\Gamma} \frac{\|\Gamma\|}{\max_{1 \leq i \leq n} \|\Gamma_i\|}$$

s.t. $\Gamma_{x,y} = \Gamma_{y,x} \ \ \forall x, y$

$\Gamma_{x,y} = 0 \ \ \forall x, y, f(x) = f(y)$

$\Gamma \in \mathbb{R}^{2^n \times 2^n}$

$\Leftrightarrow$

Semidefinite program

$$\mathrm{Adv}(f) = \max_{\Gamma, \epsilon} \epsilon$$

s.t. $-\epsilon \mathrm{Id} \preceq \Gamma \preceq \epsilon \mathrm{Id}$

$-\mathrm{Id} \preceq \Gamma_i \preceq \mathrm{Id} \ \ \forall i$

$\Gamma_{x,y} = \Gamma_{y,x} \ \ \forall x, y$

$\Gamma_{x,y} = 0 \ \ \forall x, y, f(x) = f(y)$

$\Gamma \in \mathbb{R}^{2^n \times 2^n}, \epsilon \in \mathbb{R}$

$$Q(f) \geq \mathrm{Adv}(f)/40$$

Primal SDP

Strong duality →

Dual SDP

$$\mathrm{Adv}(f) = \max_{\Gamma} \frac{\|\Gamma\|}{\max_{1\leq i\leq n} \|\Gamma_i\|}$$

s.t. $\Gamma_{x,y} = \Gamma_{y,x} \ \forall x, y$

$\Gamma_{x,y} = 0 \ \ \forall x, y, f(x) = f(y)$

$\Gamma \in \mathbb{R}^{2^n \times 2^n}$

$$\mathrm{Adv}(f) = \min_{V^{(1)},\ldots,V^{(n)}} \ \max_{x\in\{0,1\}^n} \sum_{1\leq i\leq n} V^{(i)}_{x,x}$$

s.t. $\sum_{i:x_i\neq y_i} V^{(i)}_{x,y} = \mathbf{1}_{f(x)\neq f(y)} \ \ \forall x, y$

$V^{(i)} \succeq 0 \ \ \forall 1 \leq i \leq n$

$V^{(i)} \in \mathbb{C}^{2^n \times 2^n} \ \ \forall 1 \leq i \leq n$

$$Q(f) \geq \mathrm{Adv}(f)/40$$

Dual SDP

$$\mathrm{Adv}(f) = \min_{V^{(1)},\ldots,V^{(n)}} \max_{x\in\{0,1\}^n} \sum_{1\leq i\leq n} V^{(i)}_{x,x}$$

s.t. $\sum_{i:x_i\neq y_i} V^{(i)}_{x,y} = \mathbf{1}_{f(x)\neq f(y)} \ \forall x, y,$

$V^{(i)} \succeq 0 \ \forall 1 \leq i \leq n$

$V^{(i)} \in \mathbb{C}^{2^n\times 2^n} \ \forall 1 \leq i \leq n$

PSD (positive semidefinite) constraint

$V \succeq 0 \Leftrightarrow \langle w | V | w \rangle \geq 0 \ \forall w \in \mathbb{C}^{2^n}$

$\Leftrightarrow \exists w^{(1)}, \ldots, w^{(2^n)} \in \mathbb{C}^{2^n}$ such that

$V_{x,y} = (\langle w^{(x)} | w^{(y)} \rangle)_{x,y} \ \forall x, y$

(Gram matrix)

$$Q(f) \geq \mathrm{Adv}(f)/40$$

Dual SDP

$$\mathrm{Adv}(f) = \min_{V^{(1)},\ldots,V^{(n)}} \max_{x \in \{0,1\}^n} \sum_{1 \leq i \leq n} V^{(i)}_{x,x}$$

$$\text{s.t.} \sum_{i: x_i \neq y_i} V^{(i)}_{x,y} = \mathbf{1}_{f(x) \neq f(y)} \quad \forall x, y,$$

$$V^{(i)} \succeq 0 \quad \forall 1 \leq i \leq n$$

$$V^{(i)} \in \mathbb{C}^{2^n \times 2^n} \quad \forall 1 \leq i \leq n$$

Alternative formulation

$$\mathrm{Adv}(f) = \min_{\{w^{(x,i)}\}} \max_{x \in \{0,1\}^n} \sum_{1 \leq i \leq n} \| w^{(x,i)} \|^2$$

$$\text{s.t.} \sum_{i: x_i \neq y_i} \langle w^{(x,i)} | w^{(y,i)} \rangle = \mathbf{1}_{f(x) \neq f(y)} \quad \forall x, y$$

$$w^{(x,i)} \in \mathbb{C}^{2^n} \quad \forall x \in \{0,1\}^n, 1 \leq i \leq n$$