# Quantum query complexity

## Lecture 5

### Algorithmic dual to the adversary method

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

# Focus of this lecture

- The adversary method can be formulated as a semidefinite program (SDP)
- The dual of that SDP can be transformed into an algorithm
- This implies that the adversary method is always optimal!

# Dual SDP

We saw in the last lecture that:

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

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

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

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

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

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

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:

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

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

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

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

$$\Leftrightarrow$$

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

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

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

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

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

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

Rewrite the optimization problem:

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

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

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

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

$\Leftrightarrow$

Semidefinite program

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

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

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

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

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

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

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

Strong duality $\longrightarrow$

**Primal SDP**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Alternative formulation

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

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

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

# Algorithm

## Dual SDP

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

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

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

**Theorem:** Any feasible solution $\{w^{(x,i)}\}_{x,i}$ can be converted into a quantum algorithm computing $f$ with $O\left(\max_x \sum_{1 \le i \le n} \|w^{(x,i)}\|^2\right)$ queries.

**Corollary:** $Q(f) = \Theta(\mathrm{Adv}(f))$

# Angle detection algorithm

Given an integer $T \geq 1$ and (controlled) "black-box" access to $U$ that is either

$$U = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \text{or} \qquad U = \begin{pmatrix} \cos(\pi/T) & -\sin(\pi/T) \\ \sin(\pi/T) & \cos(\pi/T) \end{pmatrix}$$

Identity

Rotation by an angle $\pi/T$

Then we can find which is the case by computing

$$(H \otimes \mathrm{Id})\text{c-}U^T(H \otimes \mathrm{Id})|0\rangle|0\rangle = \begin{cases} |0\rangle|0\rangle & \text{if identity} \\ |1\rangle|0\rangle & \text{if } \mathrm{Rot}(\pi/T) \end{cases}$$

# Angle detection algorithm

Given an integer $T \geq 1$ and (controlled) "black-box" access to $U$ that is either

$$U = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \text{or} \qquad U = \begin{pmatrix} \cos(\pi/T) & -\sin(\pi/T) \\ \sin(\pi/T) & \cos(\pi/T) \end{pmatrix}$$

$f(x) = 1$ $\qquad$ $f(x) = 0$

Then we can find which is the case by computing

$$(H \otimes \mathrm{Id})\text{c-}U^T(H \otimes \mathrm{Id})|0\rangle|0\rangle = \begin{cases} |0\rangle|0\rangle & \text{if identity} \\ |1\rangle|0\rangle & \text{if } \mathrm{Rot}(\pi/T) \end{cases}$$

$T$ quantum queries

# Angle detection algorithm

Given an integer $T \geq 1$ and (controlled) "black-box" access to $U$ that is either

$$U = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{or} \quad U = \begin{pmatrix} \cos(\varphi) & -\sin(\varphi) \\ \sin(\varphi) & \cos(\varphi) \end{pmatrix}$$

Identity

Rotation by an angle $\varphi \geq \pi/T$

Then we can find which is the case by time-$O(T)$ quantum phase estimation:

$$\text{QPE}_U |\text{ev}\rangle|0\rangle = \begin{cases} |\text{ev}\rangle|0\rangle & \text{if identity} \\ |\text{ev}\rangle|\varphi \pm 1/T\rangle & \text{if } \text{Rot}(\varphi) \end{cases}$$

$\neq 0$

# Jordan's lemma

We will apply the angle detection algorithm to a larger space and to a product

$$U = (2\Pi - \mathrm{Id})(2\Delta - \mathrm{Id})$$

for some projectors $\Pi, \Delta$ .

Jordan's lemma tells us that any such unitary can be block-diagonalized as:

Blocks of $\pm\mathrm{Id}$

Blocks of rotations

$$U = \begin{pmatrix} \boxed{\begin{matrix} \pm 1 & & \\ & \ddots & \\ & & \pm 1 \end{matrix}} & & & 0 \\ & \boxed{\begin{matrix} \cos(\theta_1) & -\sin(\theta_1) \\ \sin(\theta_1) & \cos(\theta_1) \end{matrix}} & & \\ & & \boxed{\begin{matrix} \cos(\theta_2) & -\sin(\theta_2) \\ \sin(\theta_2) & \cos(\theta_2) \end{matrix}} & \\ 0 & & & \ddots \end{pmatrix}$$

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

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

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

Fix any feasible solution $\{w^{(x,i)}\}_{x,i}$ and let its value be $T = \max_x \sum_i \|w^{(x,i)}\|^2$

Hilbert space: $H = |\star\rangle \cup \mathrm{span}\big\{ |i,b\rangle \otimes |w\rangle : 1 \le i \le n, b \in \{0,1\}, |w\rangle \in \mathbb{C}^{2^n}\big\}$

Vectors: $|t_x^+\rangle = |\star\rangle + \frac{1}{\sqrt{3T}} \sum_i |i,x_i\rangle \otimes |w^{(x,i)}\rangle$ and $|t_x^-\rangle = |\star\rangle - \sqrt{3T} \sum_i |i,\bar{x}_i\rangle \otimes |w^{(x,i)}\rangle$

Projectors: $\Pi_x = |\star\rangle\langle\star| + \sum_i |i,x_i\rangle\langle i,x_i| \otimes \mathrm{Id}$ and $\Delta = \mathrm{Proj}\big(\mathrm{span}_y\{|t_y^+\rangle : f(y)=1\}\big)$

Product of reflections: $U_x = (2\Pi_x - \mathrm{Id})(2\Delta - \mathrm{Id})$

---

Let $P_\theta$ be the projector onto the eigenspaces of $U_x$ with eigenvalues $e^{i\varphi}, |\varphi| \le \theta$

Lemma: If $f(x) = 1$ then $|\star\rangle = P_0|\star\rangle + |\mathrm{err}_1\rangle$ where $\|\mathrm{err}_1\|^2 \le 1/3$

Lemma: If $f(x) = 0$ then $|\star\rangle = (\mathrm{Id} - P_{1/(2T)})|\star\rangle + |\mathrm{err}_0\rangle$ where $\|\mathrm{err}_0\|^2 \le 1/3$

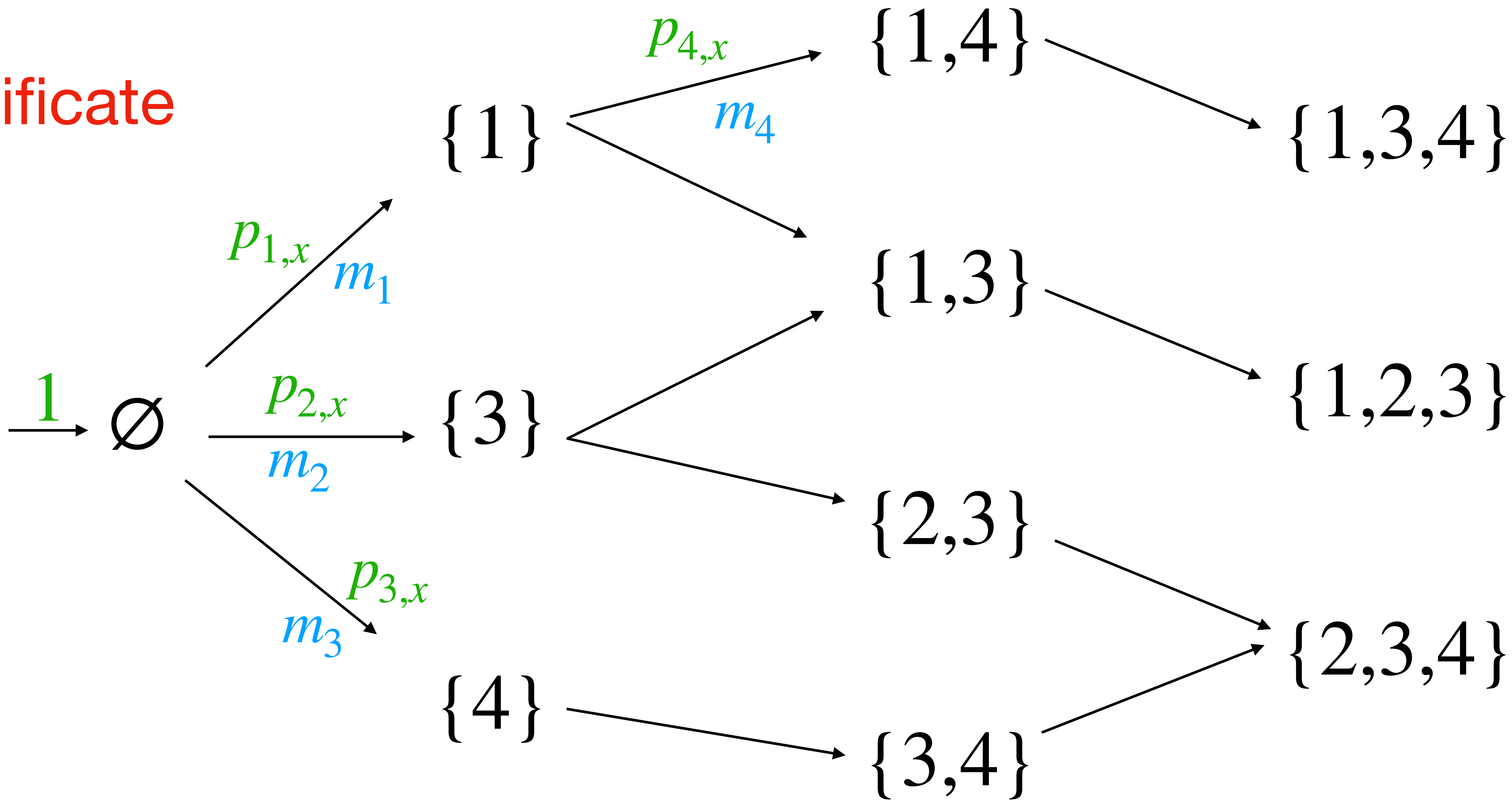
# Learning graphs

# Subgraph of the power set graph over $\{1, \ldots, n\}$

Weights $m_e > 0$

Each $x \in f^{-1}(1)$ has a 1-certificate contained in some node

Unit flow $p_{e,x}$ with source $\varnothing$ is valid for $x \in f^{-1}(1)$ if its sinks are 1-certificates for $x$




Complexity: $\sqrt{M_0 M_1}$

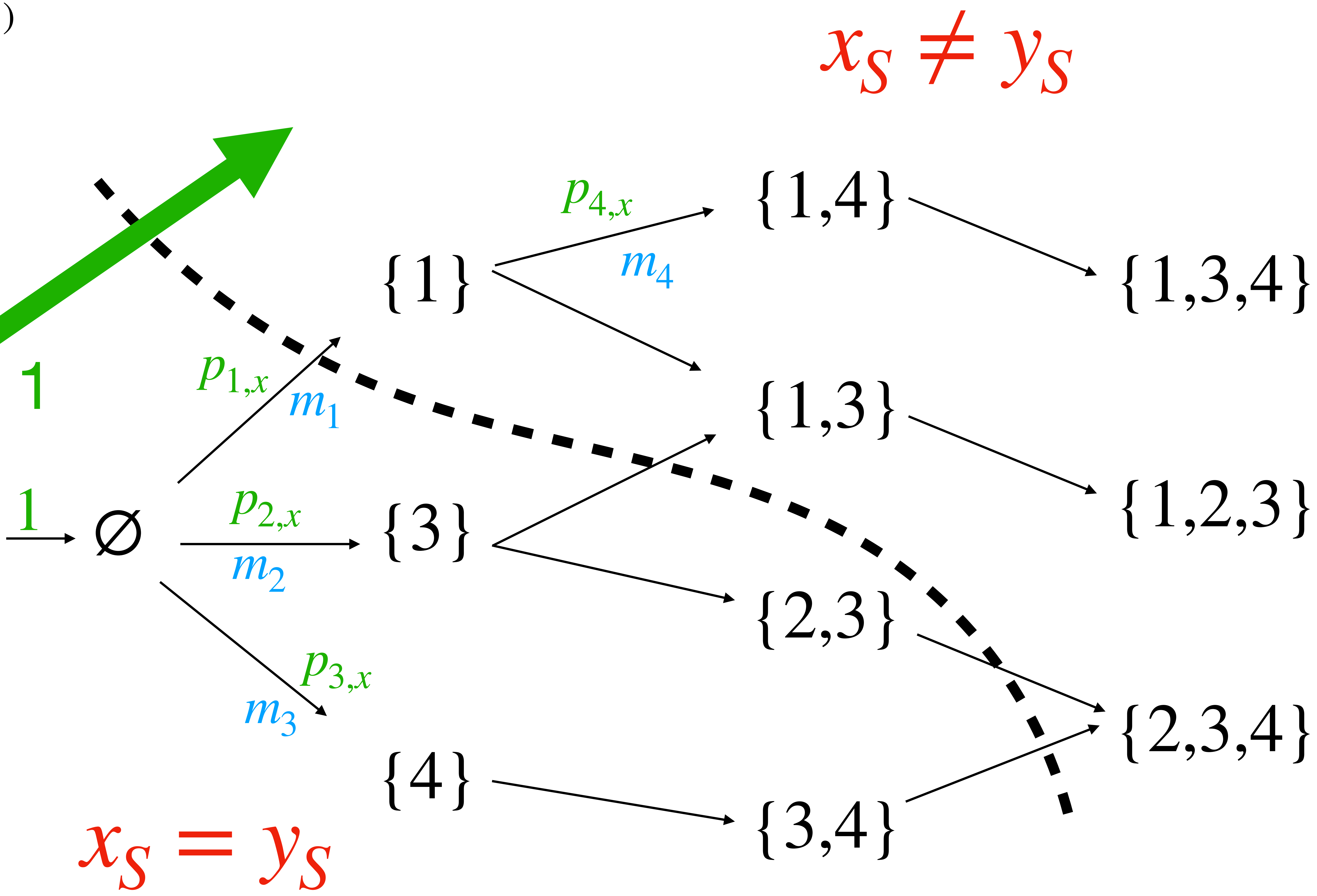
$\sum_e m_e$ $\qquad$ $\max\limits_{x \in f^{-1}(1)} \; \min\limits_{\text{valid flow}} \sum_e p_{e,x}^2 / m_e$

**Theorem:** $Q(f) = O(\sqrt{M_0 M_1})$

$$
|w^{(x,i)}\rangle = \begin{cases} \displaystyle\sum_{\text{edge } (S, S\cup\{i\})} \sqrt{m_{(S,S\cup\{i\})}}\,|S, x_S\rangle & \text{if } f(x) = 0 \\ \displaystyle\sum_{\text{edge } (S, S\cup\{i\})} \frac{p_{(S,S\cup\{i\})}}{\sqrt{m_{(S,S\cup\{i\})}}}\,|S, x_S\rangle & \text{if } f(x) = 1 \end{cases}
$$

If $f(x) \neq f(y)$:

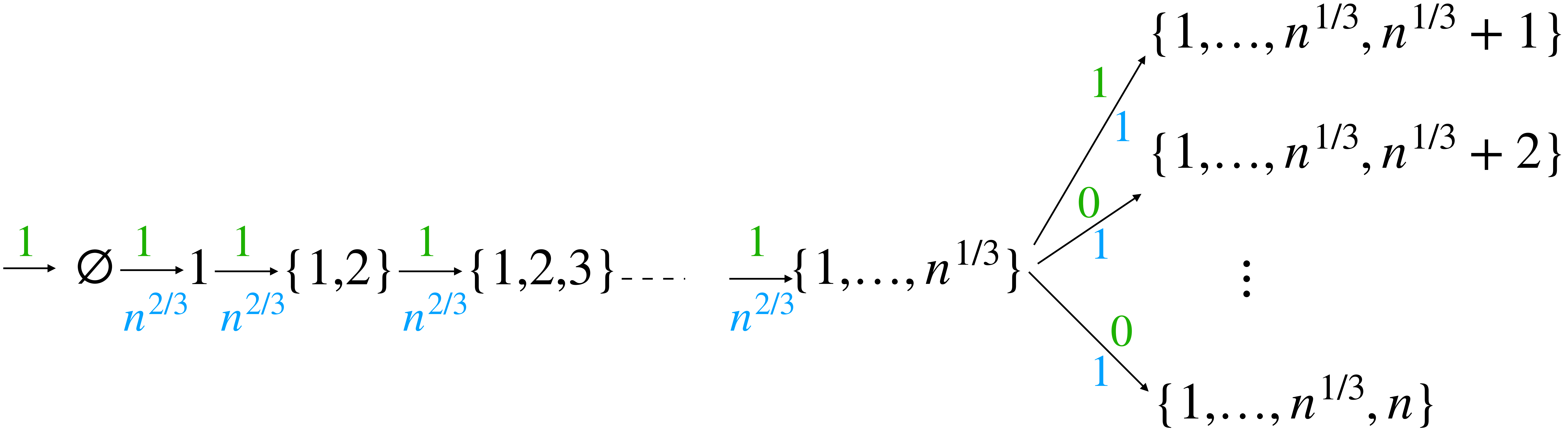
$$
\sum_{i:x_i \neq y_i} \langle w^{(x,i)} | w^{(y,i)} \rangle = \text{flow} = 1
$$



# Learning graph for collision finding

$x = (x_1, \ldots, x_n) \in [n]^n$ is 1-to-1 or 2-to-1

$M_0 \approx n$




Flow when $x$ is 2-to-1 (i.e. $f(x) = 1$):

- collision among $x_1, \ldots, x_{n^{1/3}}$ → flow $1$ on any last edge

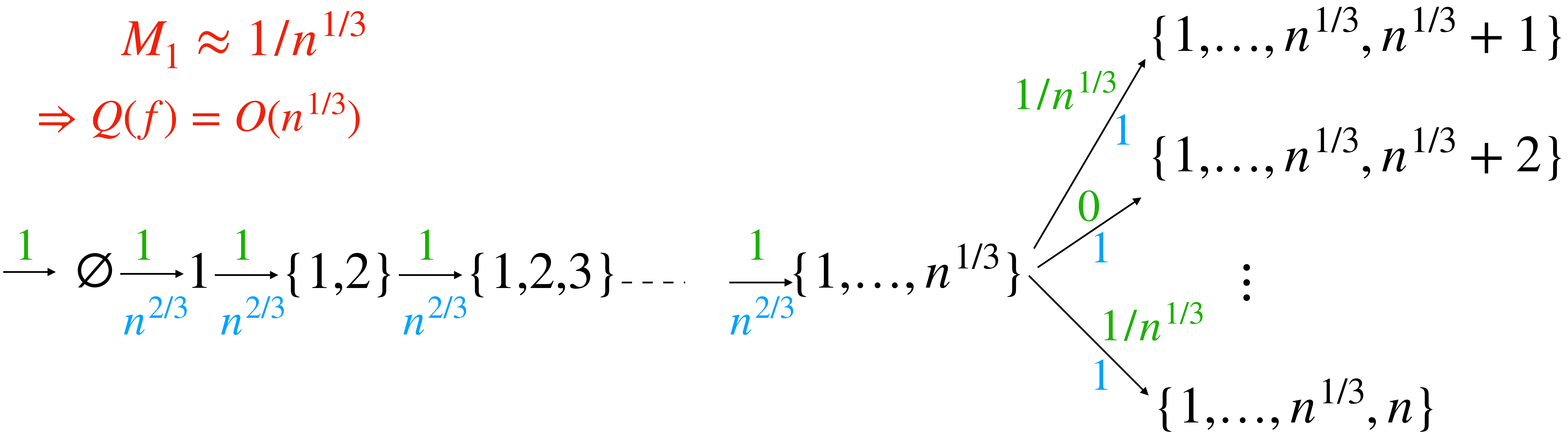
# Learning graph for collision finding

$x = (x_1, \ldots, x_n) \in [n]^n$ is 1-to-1 or 2-to-1

$M_0 \approx n$

$M_1 \approx 1/n^{1/3}$

$\Rightarrow Q(f) = O(n^{1/3})$




Flow when $x$ is 2-to-1 (i.e. $f(x) = 1$):

- collision among $x_1, \ldots, x_{n^{1/3}}$ → flow $1$ on any edge
- no collision among $x_1, \ldots, x_{n^{1/3}}$ → flow $1/n^{1/3}$ on edges with collision

# Simplifying the dual

$$\mathrm{Adv}(f) = \min_{\{w^{(x,i)}\}} \cancel{\max_{x\in\{0,1\}^n} \sum_{1\le i\le n} \|w^{(x,i)}\|^2} \quad \sqrt{\max_{x\in f^{-1}(0)} \sum_{1\le i\le n} \|w^{(x,i)}\|^2 \cdot \max_{x\in f^{-1}(1)} \sum_{1\le i\le n} \|w^{(x,i)}\|^2}$$

s.t.

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

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