Quantum query complexity:

Adversaries, polynomials and direct product theorems

Jérémie Roland

Université Libre de Bruxelles

ULB

NEC Laboratories America

NEC

Based on joint work with

Andris Ambainis
Troy Lee
Loïck Magnin
Martin Rötteler

[AMRR, CCC'11, arxiv:1012.2112]
[LeeR, CCC'12, arxiv:1104.4468]
[MagninR, STACS'13, arXiv:1209.2713]

Introduction

Classical query complexity

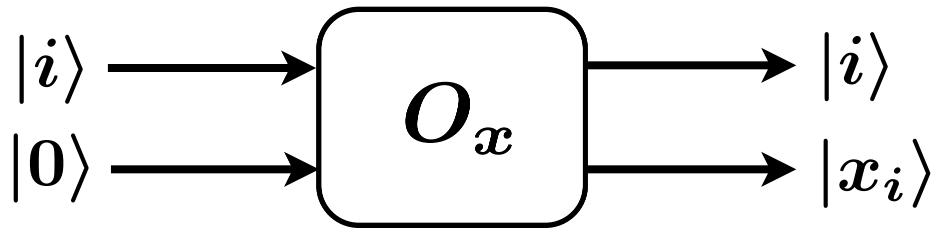
- Function $f(x)$, where $x = (x_1, \ldots, x_n)$
- Oracle $O_x : i \to x_i$
- Goal: Compute $f(x)$ given black-box access to O_x

Randomized query complexity $R_\varepsilon(f)$

Minimum # calls to O_x necessary to compute $f(x)$ with success probability $(1 - \varepsilon)$

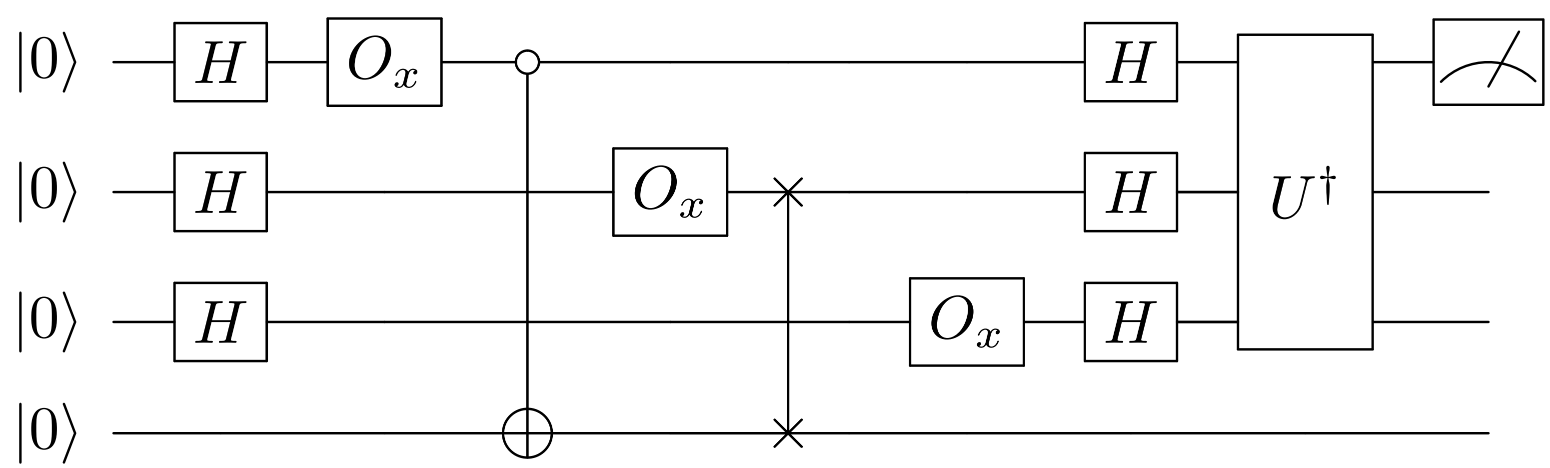
Quantum query complexity

* Quantum oracle:



* Extra power:

Can query O_x in superposition $\Rightarrow Q_\varepsilon(f) \leq R_\varepsilon(f)$



Quantum lower bounds

- Query complexity: Compute $f(x)$ given black-box access to $x = (x_1, \ldots, x_n)$
- Different lower bound methods for $Q_\varepsilon(f)$:
  - Adversary methods:
    - Idea: bound the change in a progress function for each query
    - Different variations: additive, negative weights, multiplicative
  - Polynomial method:
    - Idea: bound the degree of polynomials approximating the function

Question I

- The different methods have different advantages:
  - Additive adversary with negative weights:
    - Tight for bounded error
  - Multiplicative adversary and polynomial:
    - Better bounds for low success probability
  - Bounds for specific problems

Question I

Is there a method that combines all advantages?

Question II

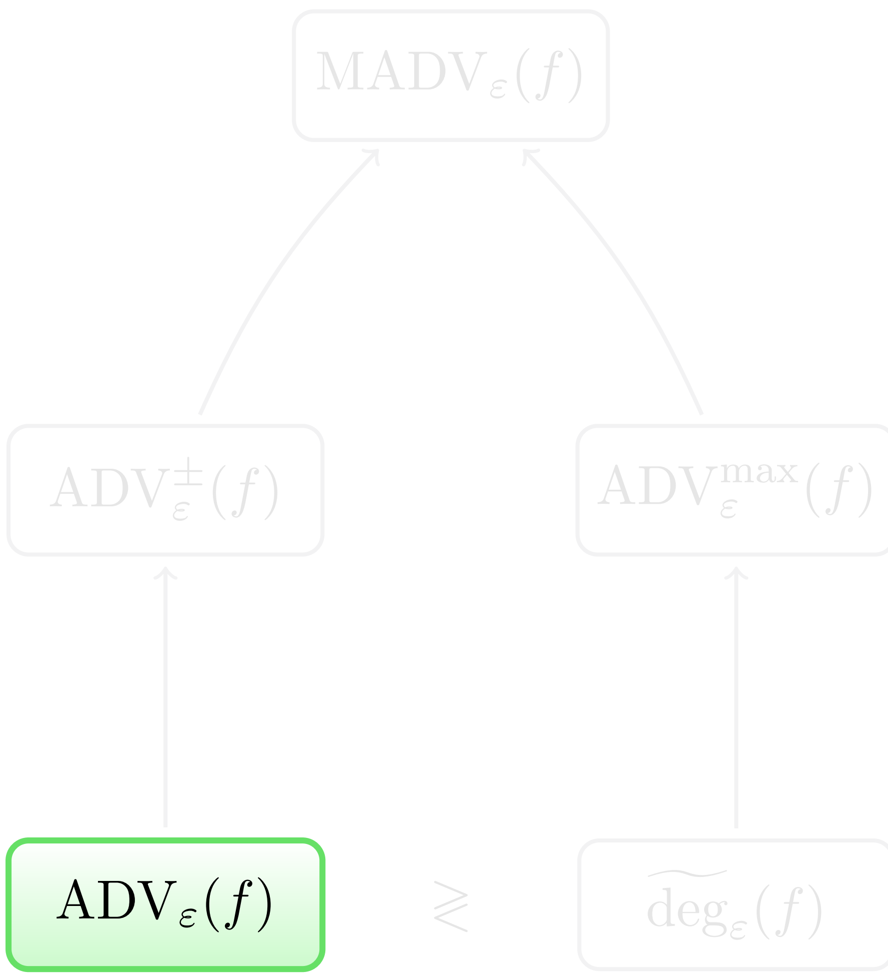
- Suppose we want to evaluate f on k different inputs $x^{(1)}, \ldots, x^{(k)}$

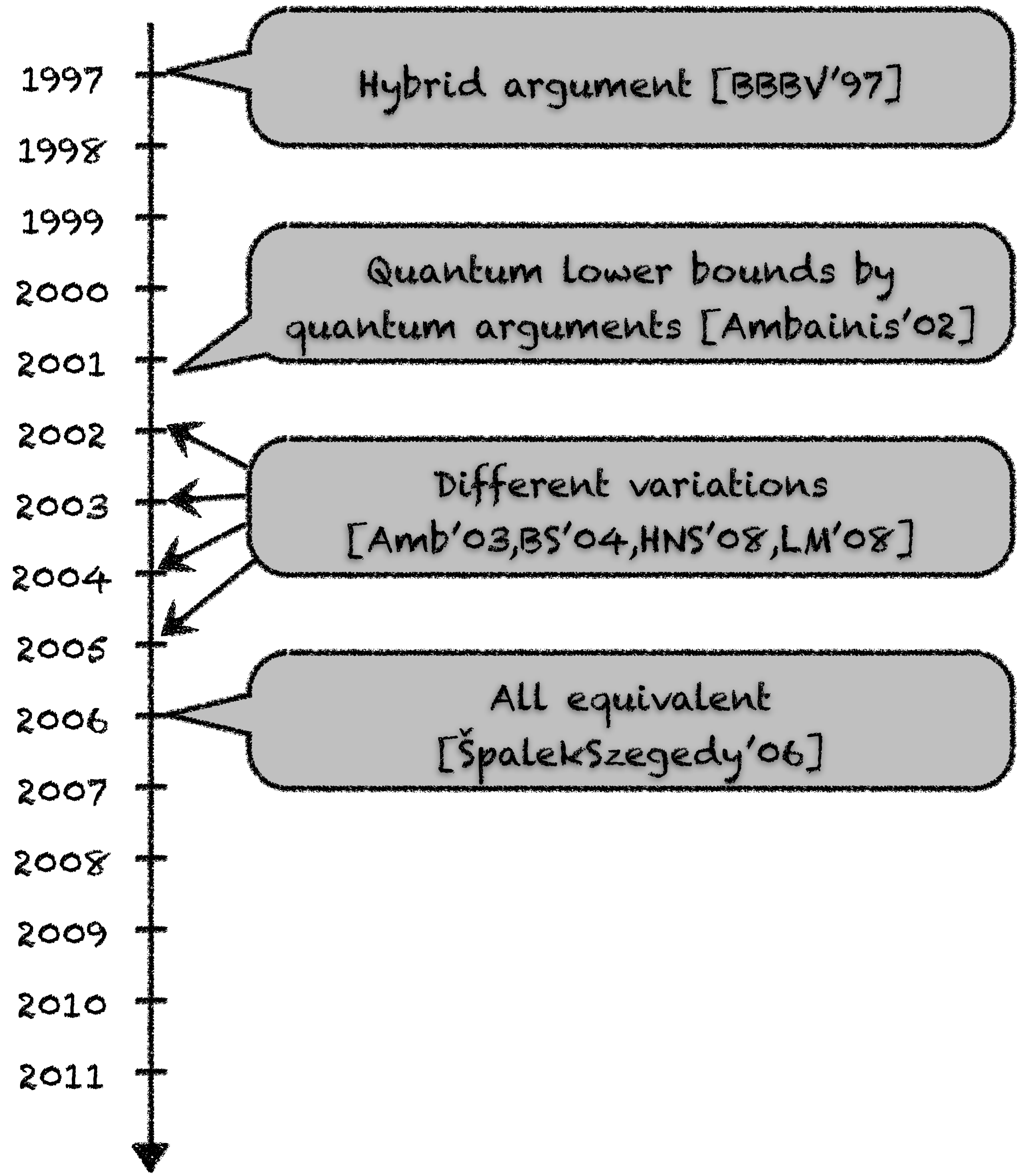
Question II
Can we do much better than just applying k times the algorithm for f ?

- If not :"Strong direct product theorem" (SDPT) for f
- Success p for 1 application $\Rightarrow$ success p^k for k applications
  - Requires to prove lower bound for exponentially small success probability
- SDPTs known for:
  - Classical query complexity [Drucker'11], one-way classical communication [Jain'10], parallel repetition theorem for games [Raz'98]

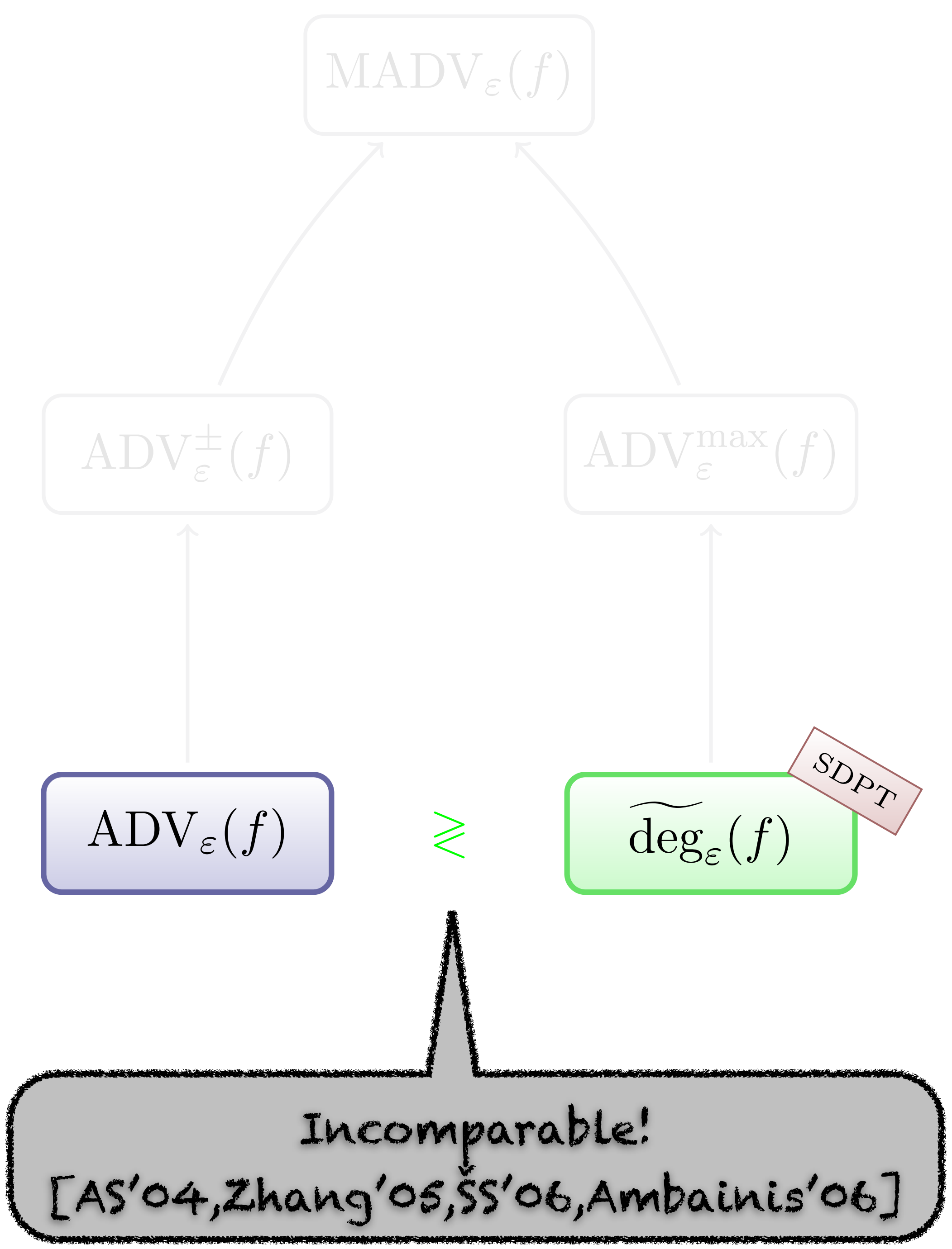
A brief history of lower bound methods

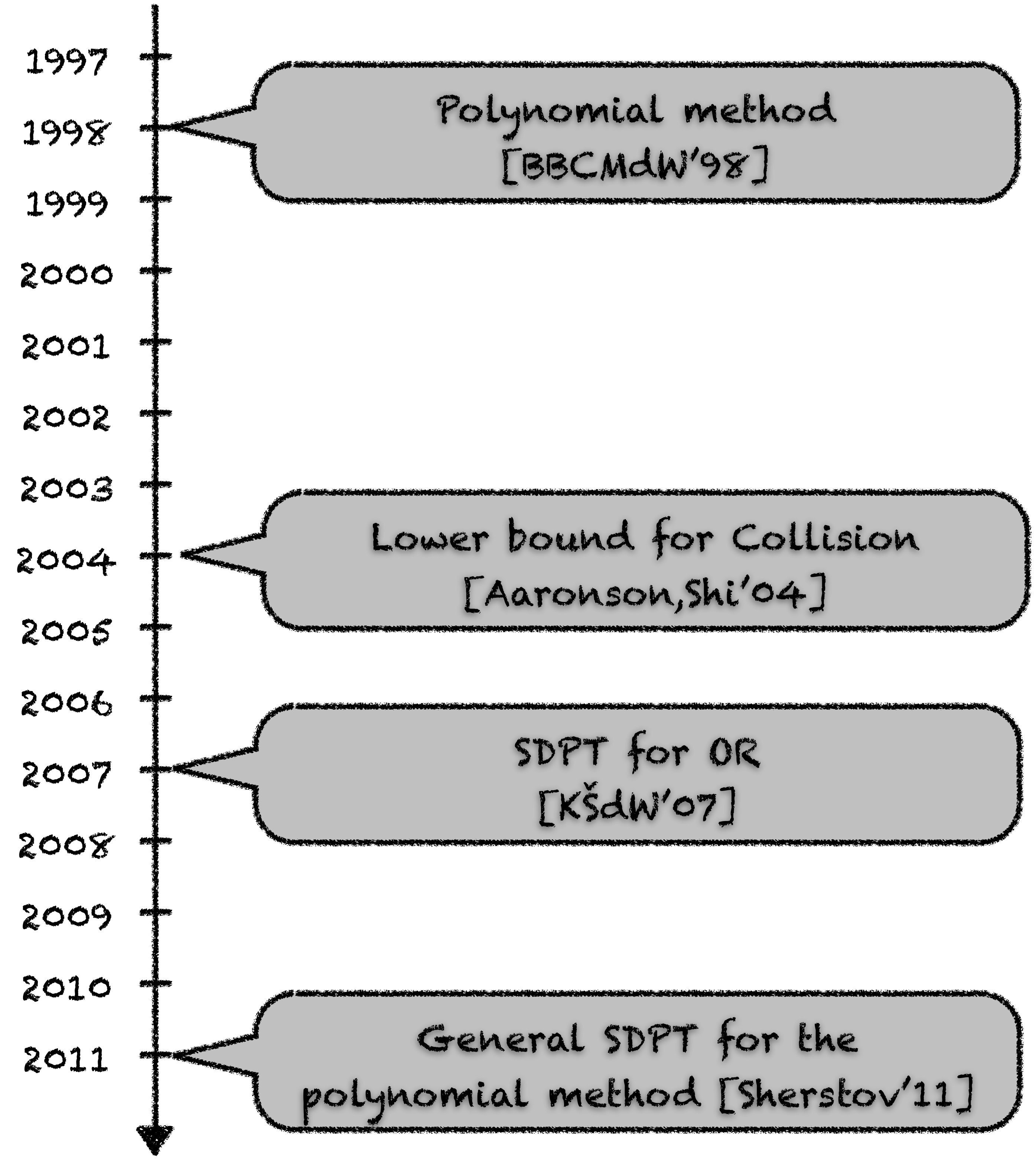
Adversary method



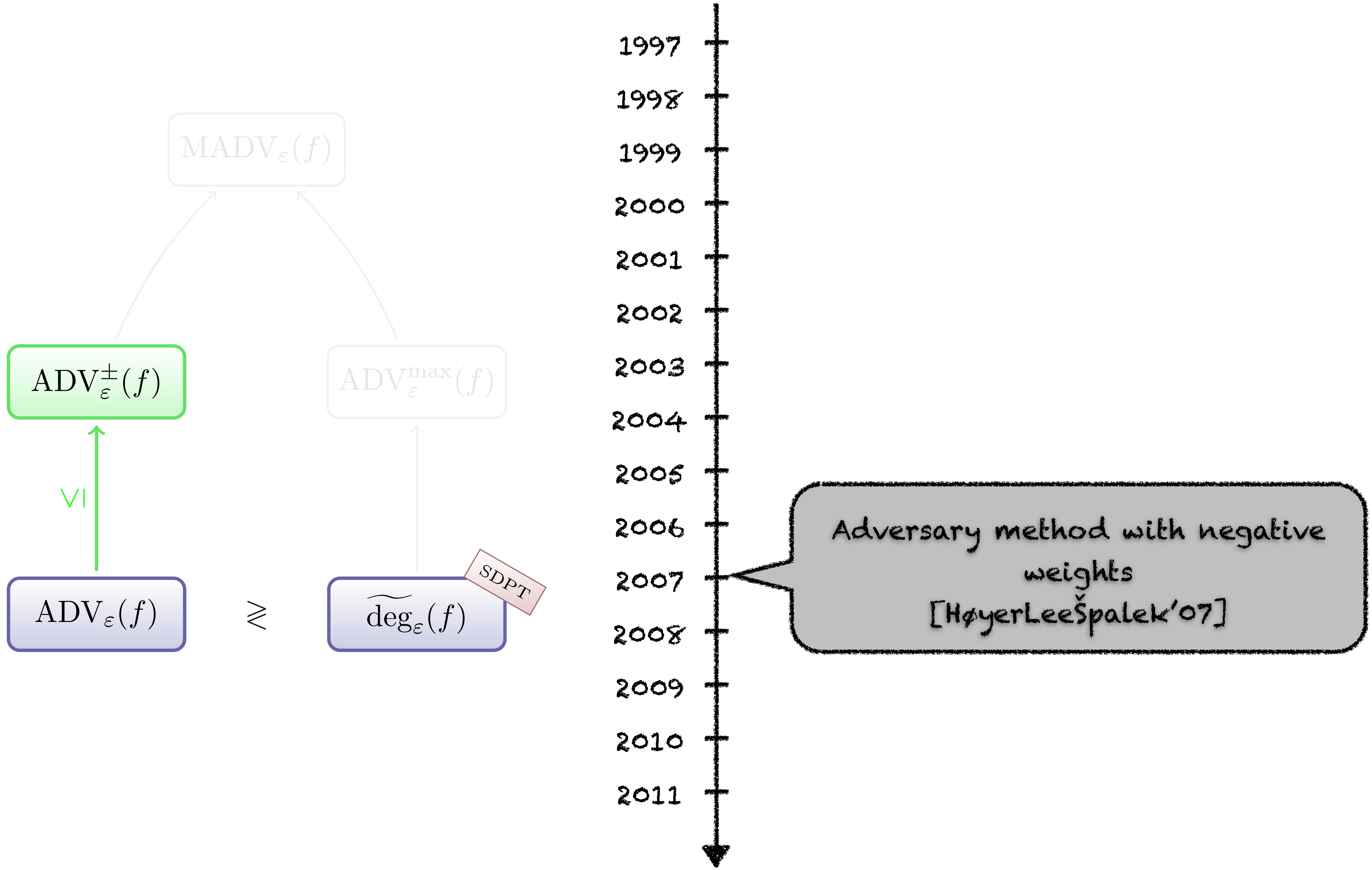


Polynomial method

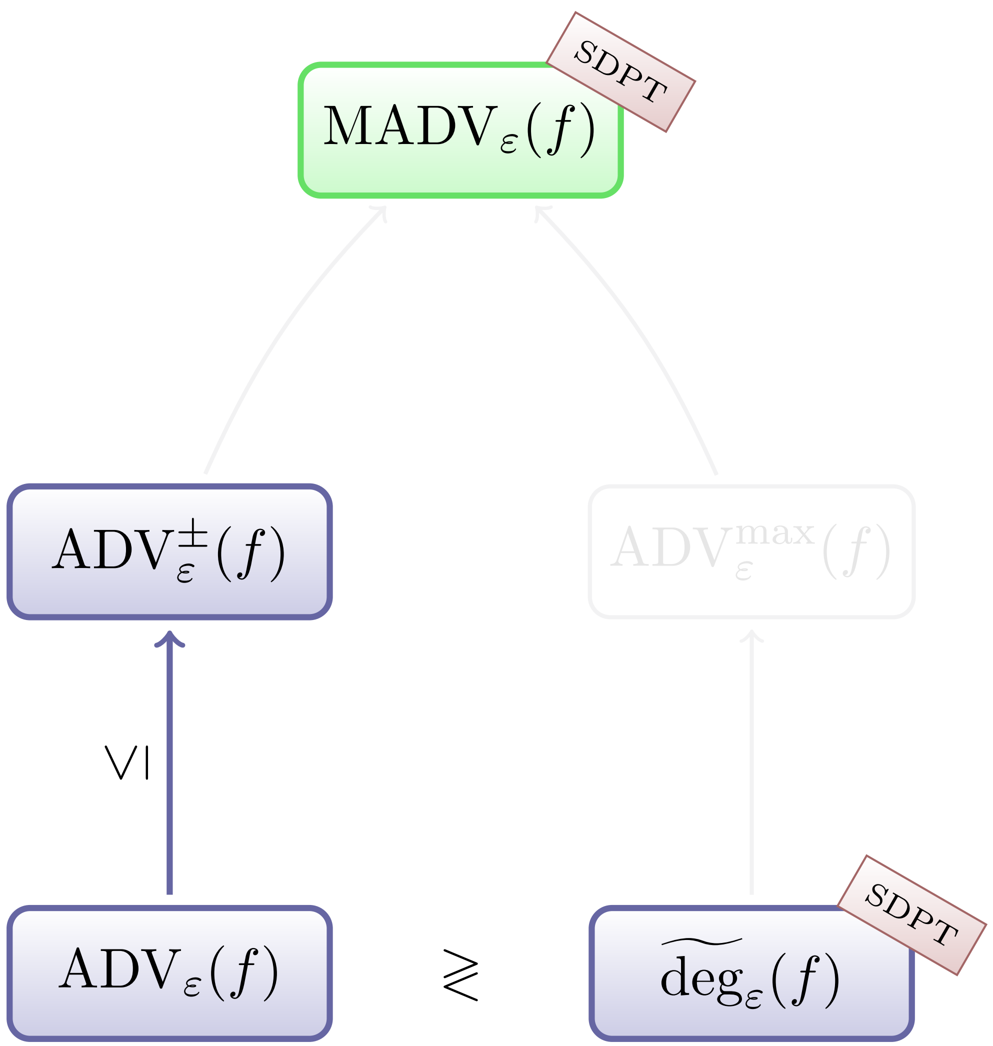


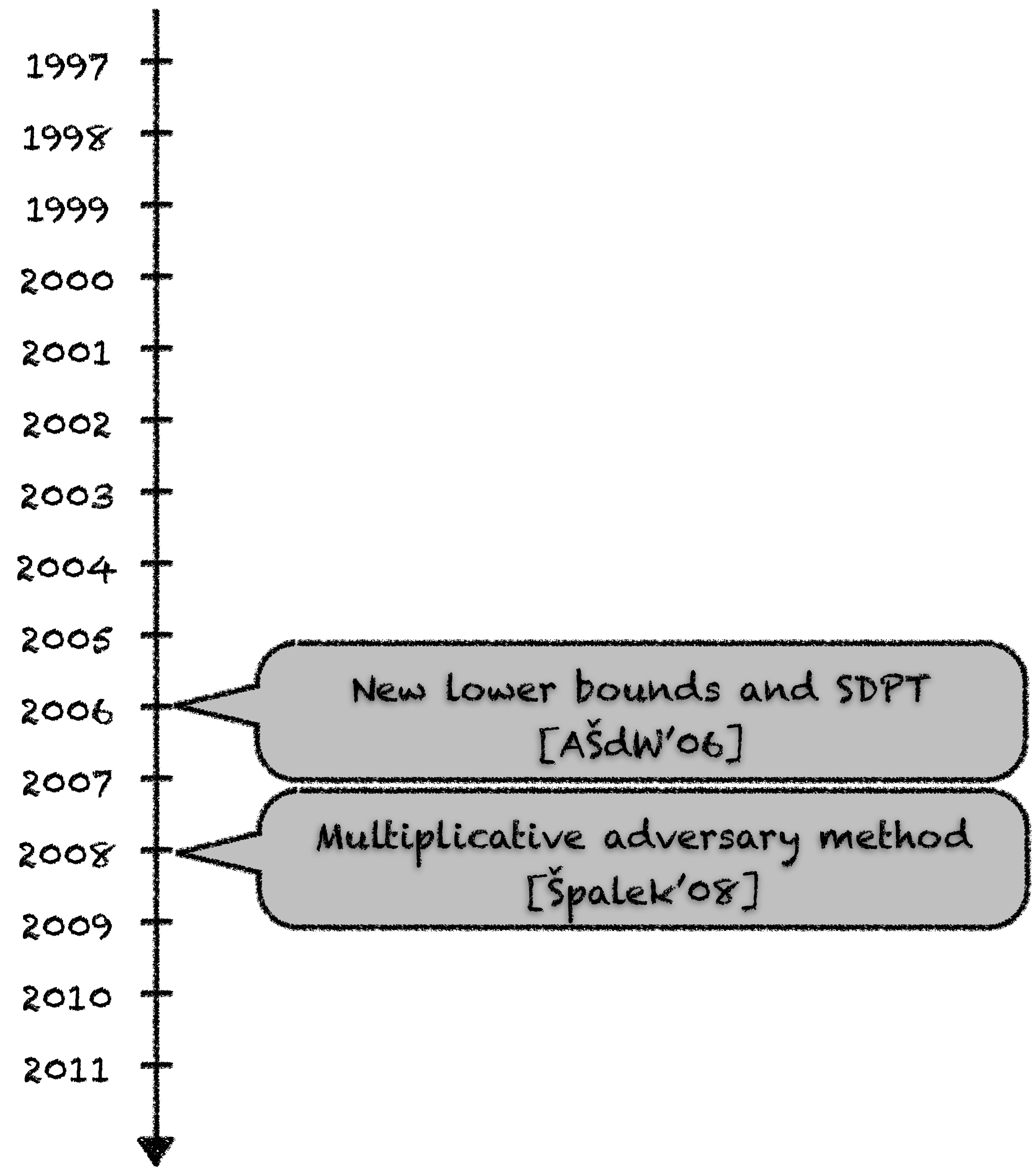


Generalized adversary method

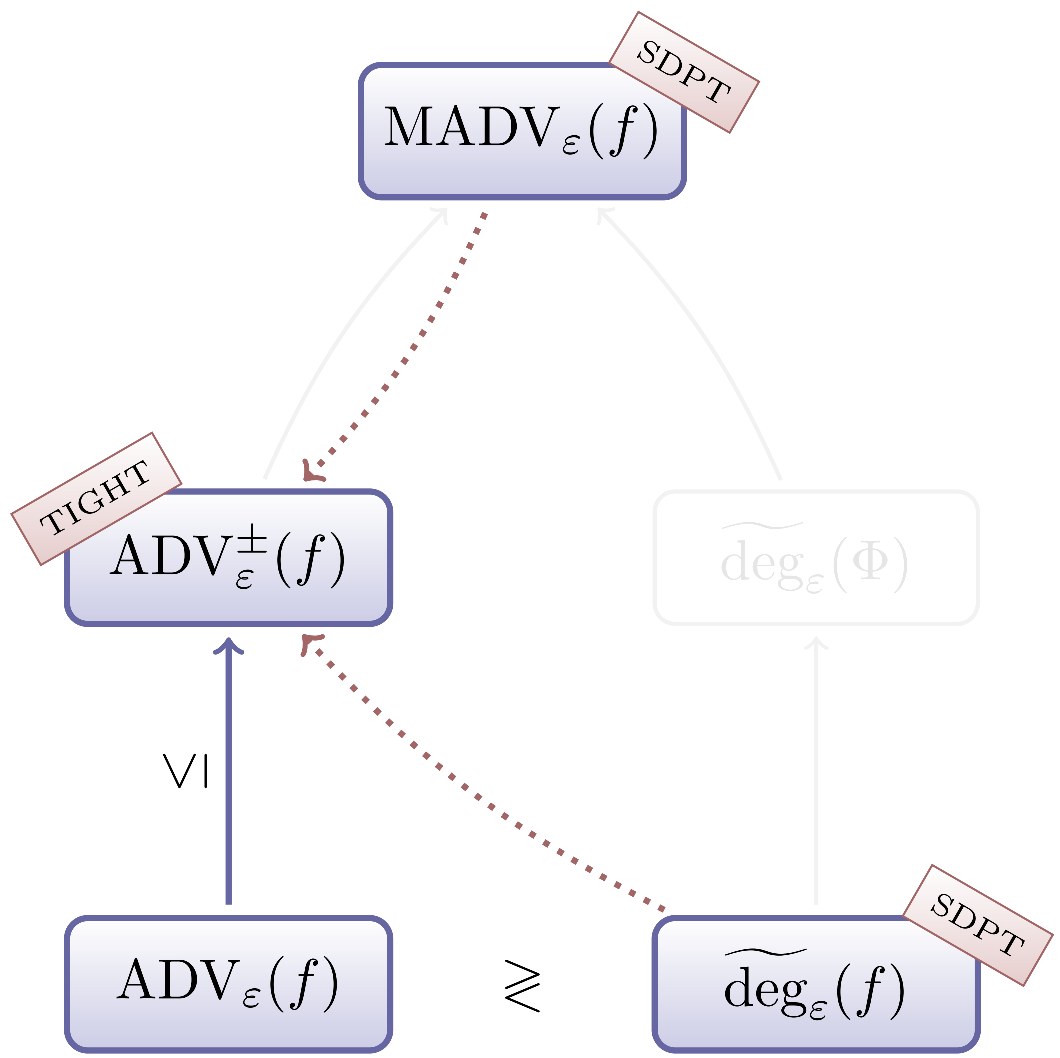


Multiplicative adversary method

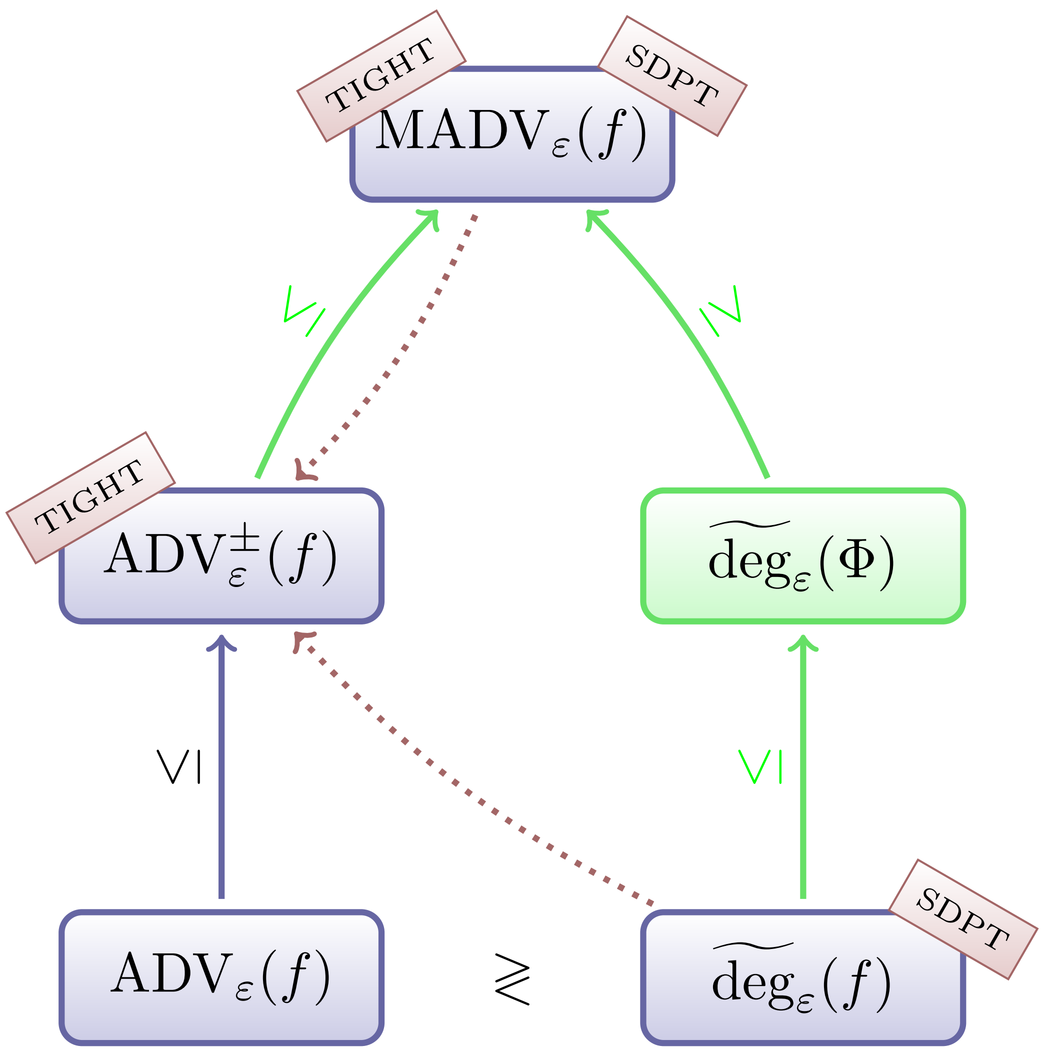




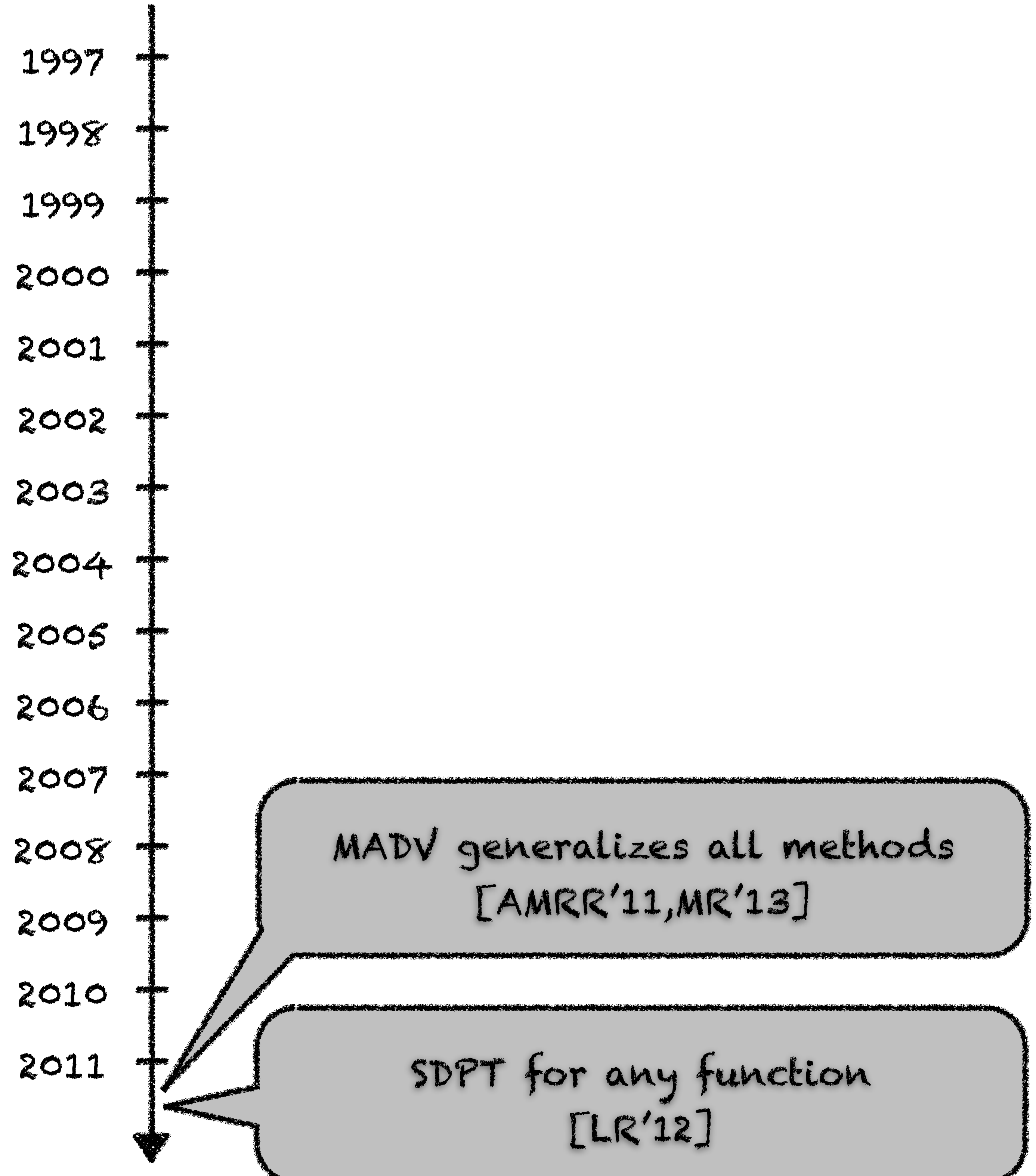
Optimality of adversary method



Our results



TIGHT
SDPT
$\mathrm{MADV}_\varepsilon(f)$
TIGHT
$\mathrm{ADV}^{\pm}_\varepsilon(f)$
$\widetilde{\deg}_\varepsilon(\Phi)$
$\mathrm{ADV}_\varepsilon(f)$
$\gtrless$
$\widetilde{\deg}_\varepsilon(f)$
SDPT



1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
MADV generalizes all methods
[AMRR'11,MR'13]
SDPT for any function
[LR'12]

Techniques

Quantum state generation

- Set of quantum states $\{|\psi_x\rangle : x \in \mathcal{D}^n\}$
- Oracle $O_x : |i\rangle|b\rangle \mapsto |i\rangle|b \oplus x_i\rangle$
- Goal: Generate $|\psi_x\rangle$ given black-box access to O_x
- Observation: Problem only depends on Gram matrix

$$M_{xy} = \langle\psi_x|\psi_y\rangle$$

Quantum query complexity $Q_\varepsilon(M)$

Minimum # calls to O_x necessary to generate a state $\sqrt{1-\varepsilon}|\psi_x\rangle|\bar{0}\rangle + \sqrt{\varepsilon}|\mathrm{error}_x\rangle$

work space

Reducing to zero-error case

- $|\psi_x^t\rangle$: state of the algorithm after t queries on input x
- Gram matrix $\quad M_{xy}^t = \langle \psi_x^t | \psi_y^t \rangle$
- Initially: $\quad |\psi_x^0\rangle = |\bar{0}\rangle \; \forall x \; \Rightarrow M^0 = J$
- At the end: $\quad |\psi_x^T\rangle \approx |\psi_x\rangle \; \Rightarrow M^T \approx M$

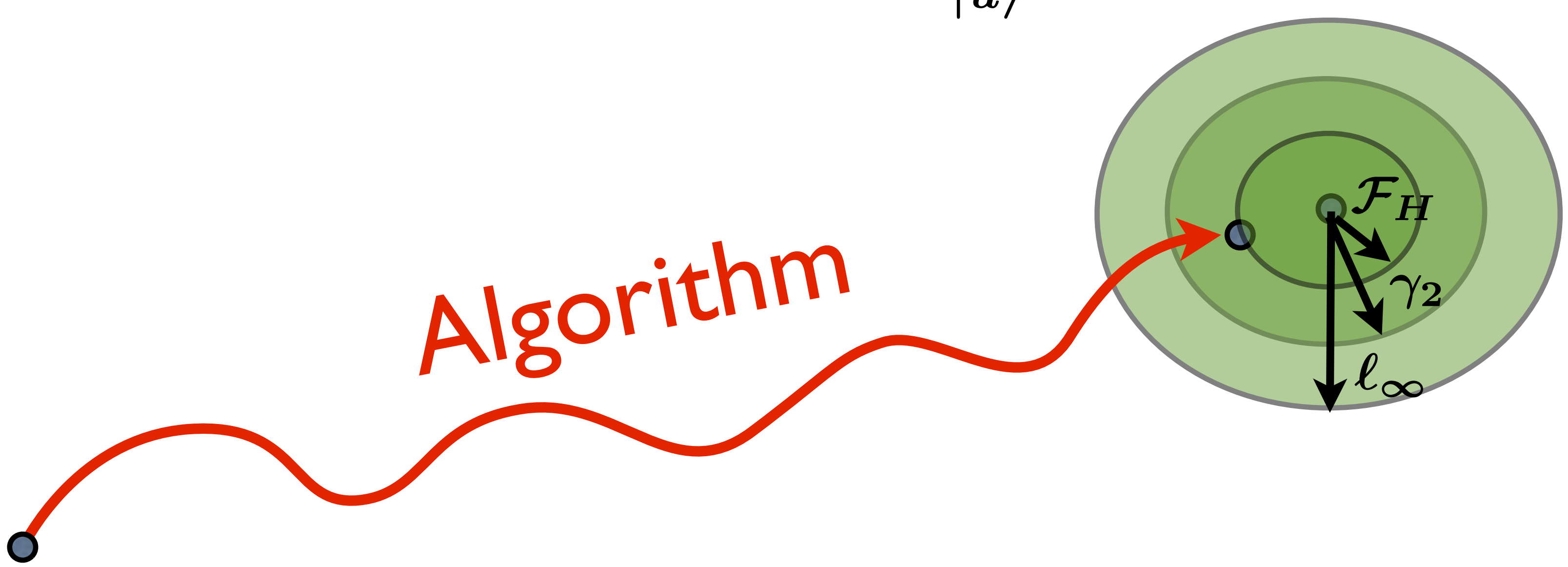
All-1 matrix

What distance?

Output conditions

- $\|M^T - M\|_\infty \le 2\sqrt{\varepsilon}$ [Ambainis02]
- $\gamma_2(M^T - M) \le 2\sqrt{\varepsilon}$ [HøyerLeeŠpalek07]
- $\mathcal{F}_H(M^T, M) \ge \sqrt{1-\varepsilon}$ [LeeR11]

where $\mathcal{F}_H(M^T, M) = \min_{|u\rangle} \mathcal{F}(M^T \circ |u\rangle\langle u|, M \circ |u\rangle\langle u|)$



- Theorem: The last condition is tight

$$\boxed{Q_\varepsilon(M) = \min_{\mathcal{F}_H(N,M) \ge \sqrt{1-\varepsilon}} Q_0(N)}$$

From adversaries to random variables

- Adversary methods involve a Hermitian matrix Γ called "adversary matrix".

- We can view Γ as an observable, and consider the random variable obtained by measuring this observable on a state.

Lemma

Let p, p' be the distribution of random variables obtained by measuring Γ on ρ, ρ'. Then, we have $\mathcal{F}(\rho, \rho') \leq \mathcal{F}(p, p')$

Classical fidelity: $\sum_i \sqrt{p_i p_i'}$.

From adversaries to random variables

- Using this idea, we can use properties of classical distributions to prove properties of adversary bounds.
- In particular, the following result is key to the proof of the strong direct product theorem.

Lemma

[LeeR12]

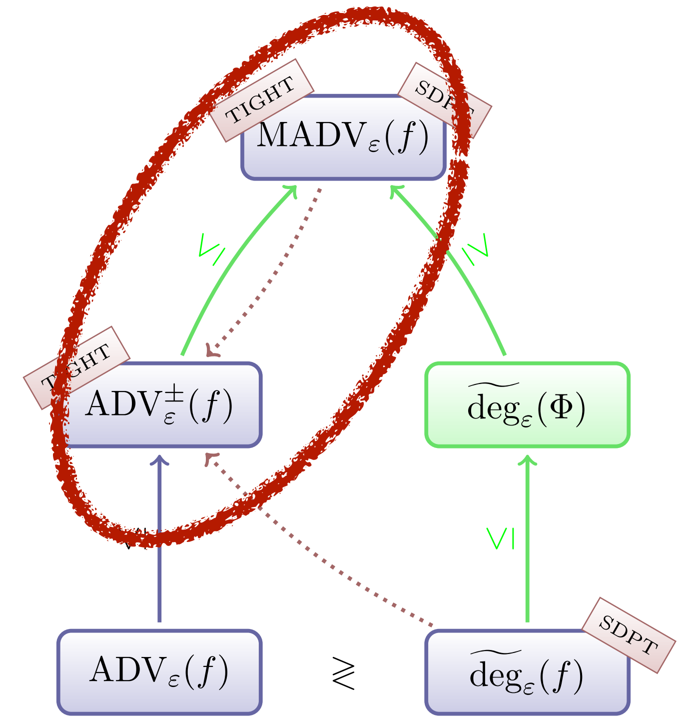
Let $A, A_1, \ldots, A_k$ be random variables on $[1, 3]$.
Let $A \sim p$ with $E_p[A] = 2$ and $(A_1, \ldots, A_k) \sim q$

Then

$$\mathcal{F}(p^{\otimes k}, q) \geq \sqrt{\delta^k} \quad \Rightarrow \quad E[\Pi_l A_l] \geq \left(\frac{3\delta}{2}\right)^k$$

- Note: this would be trivial if $A_1, \ldots, A_k$ were independent.

Multiplicative >= Additive



Additive adversary

[HøyerLeeŠpalek07]

- Progress function: $\mathcal{W}[M^t] = \mathbf{Tr}[(\boldsymbol{\Gamma} \circ M^t)vv^*]$
- Initial value: $\mathcal{W}[J] = \mathbf{Tr}[\boldsymbol{\Gamma} vv^*]$

Adversary matrix

- Additive change for one query:

$$\|\boldsymbol{\Gamma} \circ (J - \boldsymbol{\Delta}_i)\| \le 1 \quad \Rightarrow \quad |\mathcal{W}[M^{t+1}] - \mathcal{W}[M^t]| \le 1$$

- Final value after T queries: $|\mathcal{W}[M^T] - \mathcal{W}[M^0]| \le T$

Additive adversary bound

$$\mathrm{ADV}_0^{\pm}(M) = \max_{\boldsymbol{\Gamma}} \|\boldsymbol{\Gamma} \circ (J - M)\|$$

$$\text{subject to } \|\boldsymbol{\Gamma} \circ (J - \boldsymbol{\Delta}_i)\| \le 1 \quad \forall i$$

Multiplicative adversary [Špalek08]

- Progress function: $\mathcal{W}[M^t] = \mathbf{Tr}[(\mathbf{\Gamma}_m \circ M^t)vv^*]$
- Initial value: $\mathcal{W}[J] = \mathbf{Tr}[\mathbf{\Gamma}_m vv^*]$

Adversary matrix

- Multiplicative change for one query:

$$c^{-1} \cdot \mathbf{\Gamma} \preceq \mathbf{\Gamma} \circ \mathbf{\Delta}_i \preceq c \cdot \mathbf{\Gamma} \quad \Rightarrow \quad \mathcal{W}[M^{t+1}] \leq c \cdot \mathcal{W}[M^t]$$

- Maximum value after T queries: $\mathcal{W}[M^T] \leq c^T \cdot \mathcal{W}[J]$

Multiplicative adversary bound

$$\mathrm{MADV}_0^c(M) = \frac{1}{\log c} \max_{\Gamma_m \succeq 0} \log \frac{\mathbf{Tr}[(\mathbf{\Gamma}_m \circ M)vv^*]}{\mathbf{Tr}[\mathbf{\Gamma}_m vv^*]}$$

subject to $c^{-1} \cdot \mathbf{\Gamma} \preceq \mathbf{\Gamma} \circ \mathbf{\Delta}_i \preceq c \cdot \mathbf{\Gamma} \quad \forall i$

Multiplicative >= Additive

[AmbainisMagninRoettelerR11]

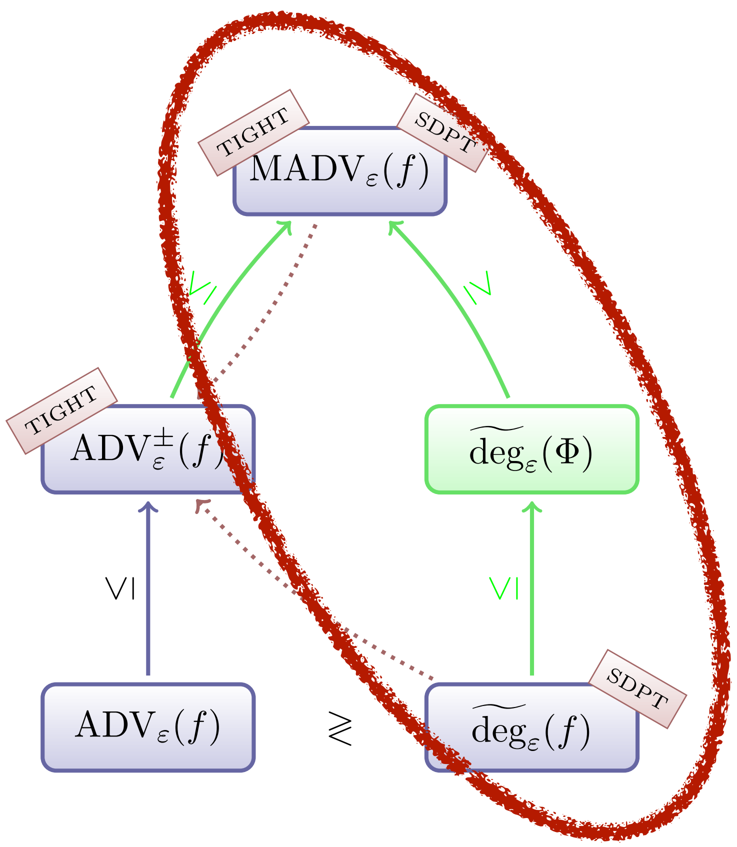
Theorem

$$\lim_{c\to 1} \mathrm{MADV}^c(M) \geq \mathrm{ADV}^{\pm}(M)$$

Proof idea:

- Use the adversary matrix: $\Gamma_m = I + \gamma \cdot (\|\Gamma\| I - \Gamma)$
- Show that it satisfies the conditions for $c = 1 + \gamma$
- Show the we get the same bound for $\gamma \to 0$

Multiplicative >= Polynomial



Polynomial method

[BBCMdW97]

- Let $f : \{0,1\}^n \to \{0,1\}$ be a Boolean function
- Approximate degree:

$$\widetilde{\deg}_\varepsilon(f) = \min_p \{\deg(p) : \forall x \in \{0,1\}^n,\ |f(x) - p(x)| \le \varepsilon\}$$

Polynomial method

$$Q_\varepsilon(f) \ge \frac{\widetilde{\deg}_\varepsilon(f)}{2}$$

- Proof idea:

After t queries, $|\psi_x^t\rangle = \sum_k \alpha_k^t(x)|k\rangle$

where $\alpha_k^t(x)$ are polynomials of degree at most k

Extended polynomial method

[MagninR13]

- Fourier basis: $|\chi_S\rangle = \frac{1}{\sqrt{2^n}} \sum_x (-1)^{x \cdot S} |x\rangle$
- Degree of a Gram matrix:

$$\deg(M) = \max_S \{|S| : \mathrm{tr}(|\chi_S\rangle\langle\chi_S| M) \neq 0\}$$

- Approximate degree:

$$\widetilde{\deg}(M) = \min_N \left\{ \deg(N) : \mathcal{F}_H(M, N) \geq \sqrt{1 - \varepsilon} \right\}$$

Extended polynomial method

$$\boxed{Q_\varepsilon(M) \geq \widetilde{\deg}_\varepsilon(M)}$$

- Proof idea:
  - Initially: $M_0 = 2^n |\chi_\varnothing\rangle\langle\chi_\varnothing|$
  - Querying bit x_i maps $|\chi_S\rangle$ to $|\chi_T\rangle$ with $T = S \cup \{x_i\}$

Max >= Polynomial

[MagninR13]

- Let Φ be the Gram matrix for computing f in the phase, i.e., for generating $(-1)^{f(x)}|\bar{0}\rangle$
- We have $Q_{(1-\sqrt{1-\varepsilon})/2+\varepsilon/4}(f) \le Q_\varepsilon(\Phi) \le 2Q_{(1-\sqrt{1-\varepsilon})/2}(f)$

[LeeR12]

Theorem

$$\lim_{c\to\infty} \mathrm{MADV}_\varepsilon^c(\Phi) = \widetilde{\deg}_\varepsilon(\Phi) \ge \widetilde{\deg}_{\varepsilon/2}(f)$$

Proof idea:

- Use the adversary matrix: $\Gamma = \sum_S c^{|S|} |\chi_S\rangle\langle\chi_S|$
- Final value of the progress function:

$$\mathcal{W}[\Phi] = \frac{1}{2^n} \sum_S c^{|S|} \mathrm{tr}(|\chi_S\rangle\langle\chi_S|\Phi) \xrightarrow[c\to\infty]{} \frac{1}{2^n} c^{\deg(\Phi)}$$

Strong direct product theorem

SDPT

[LeeR12]

Let $f^{(k)}(x^{(1)}, \ldots, x^{(k)}) = (f(x^{(1)}), \ldots, f(x^{(k)}))$

Theorem

$$Q_{1-\delta^{k/2}}(f^{(k)}) \geq \frac{k \cdot \ln(3\delta/2)}{C} \cdot Q_{1/4}(f)$$

Proof idea:

- Use optimality of $\mathrm{ADV}^{\pm}$: $Q_{1/4}(f) \leq C \cdot \mathrm{ADV}_0^{\pm}(F)$ [LMRŠS11]
- Use $\mathrm{MADV}_0^c(F) \geq \frac{\mathrm{ADV}_0^{\pm}(F)}{2}$ for $c = 1 + \frac{1}{\mathrm{ADV}_0^{\pm}(F)}$
- Using adversary matrix $\Gamma_m^{\otimes k}$, we have:

$$\mathrm{MADV}_0^c(F^{\otimes k}) \geq k \cdot \mathrm{MADV}_0^c(F)$$

- Almost there... but this is for zero error!

SDPT

[LeeR12]

Theorem

$$Q_{1-\delta^{k/2}}(f^{(k)}) \geq \frac{k \cdot \ln(3\delta/2)}{C} \cdot Q_{1/4}(f)$$

Proof idea (continued):

$$\mathrm{MADV}_0^c(F^{\otimes k}) \geq k \cdot \mathrm{MADV}_0^c(F)$$

- We have $\mathrm{MADV}_\varepsilon^c(F^{\otimes k}) = \min_M \mathrm{MADV}_0^c(M)$

  subject to $\mathcal{F}_H(F^{\otimes k}, M) \geq \sqrt{1-\varepsilon}$

- Using lemma about <u>classical fidelity</u>, we have

$$\mathcal{F}_H(F^{\otimes k}, M) \geq \delta^{k/2} \quad \Rightarrow \quad \mathrm{Tr}[(\Gamma_m^{\otimes k} \circ M)(vv^*)^{\otimes k}] \geq (3\delta/2)^k$$

- This implies: $\mathrm{MADV}_{1-\delta^{k/2}}^c(F^{\otimes k}) \geq k \cdot \ln(3\delta/2) \cdot \mathrm{MADV}_0^c(F)$

Conclusion

Conclusion and future work

* Multiplicative adversary $\mathrm{MADV}^c(f)$ generalizes all known methods:
  - Additive adversary $\mathrm{ADV}^{\pm}(f)$ for $c \to 1$
  - Polynomial method $\widetilde{\deg}_\varepsilon(f)$ for $c \to \infty$
* Polynomial method $\approx$ fixed adversary matrix (independent of f) $\Rightarrow$ insight for its limitations
* General SDPT for any function
* XOR lemma for Boolean functions
* Other applications? (new lower bounds, time-space tradeoffs,...)

Support: