Quantum query complexity:
Adversaries, polynomials and direct product theorems

Jérémie Roland

Université Libre de Bruxelles

NEC Laboratories America

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]

Introduction

Introduction

- 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

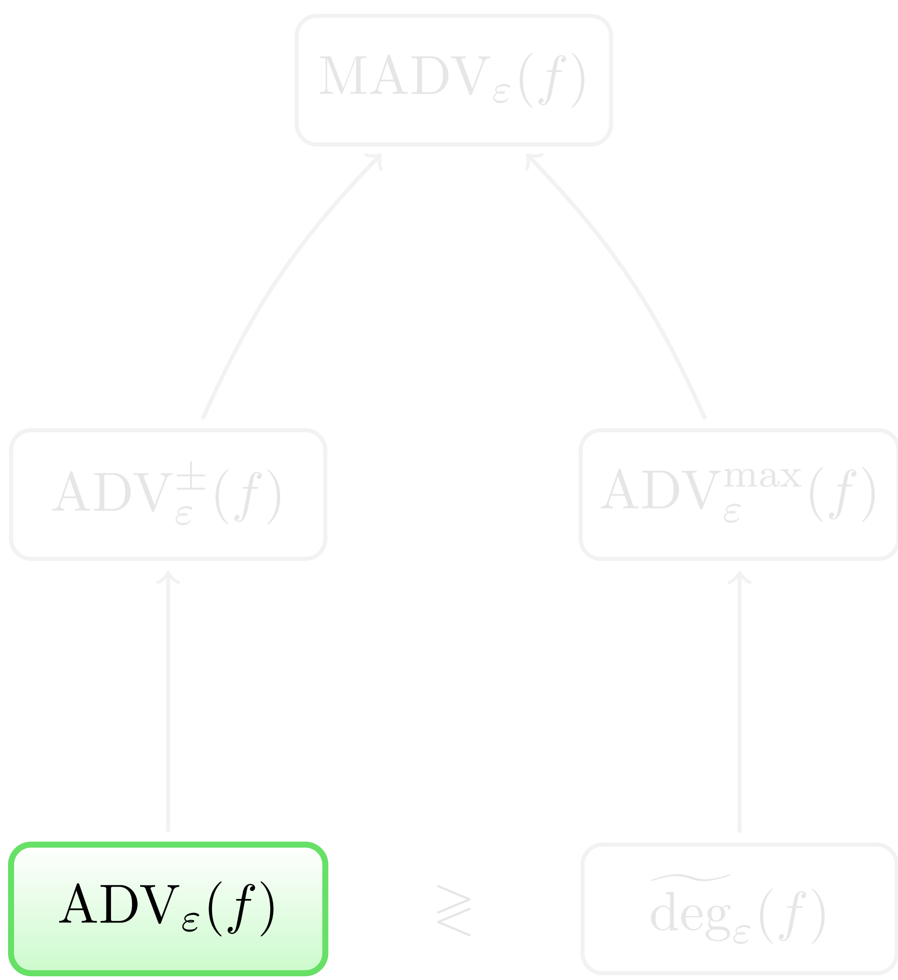
* Suppose we want to evaluate f on k different inputs $x^{(1)}, \ldots, x^{(k)}$

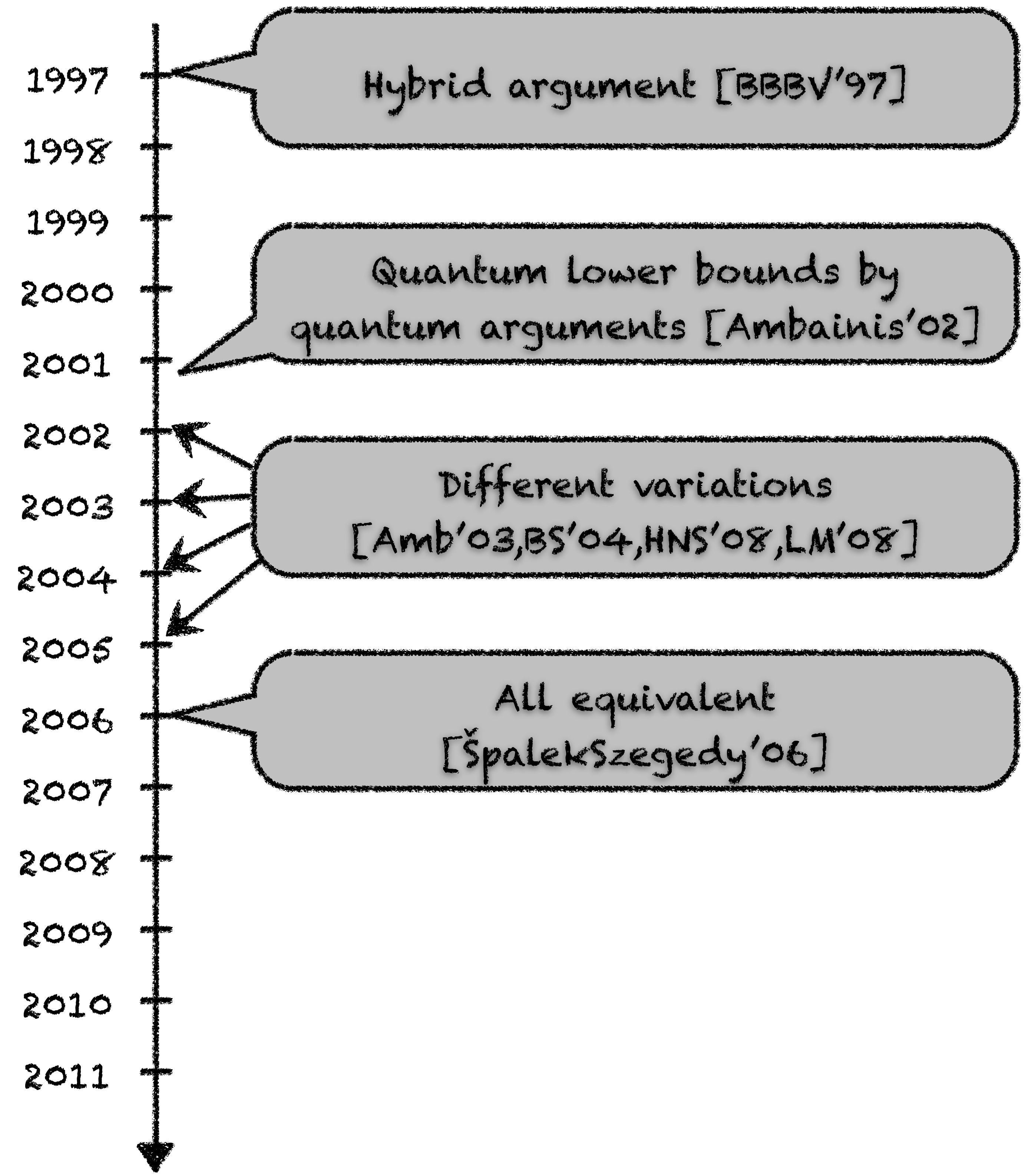
> **Question II**
> Can we do much better than just applying k times the algorithm for f ?

* 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]

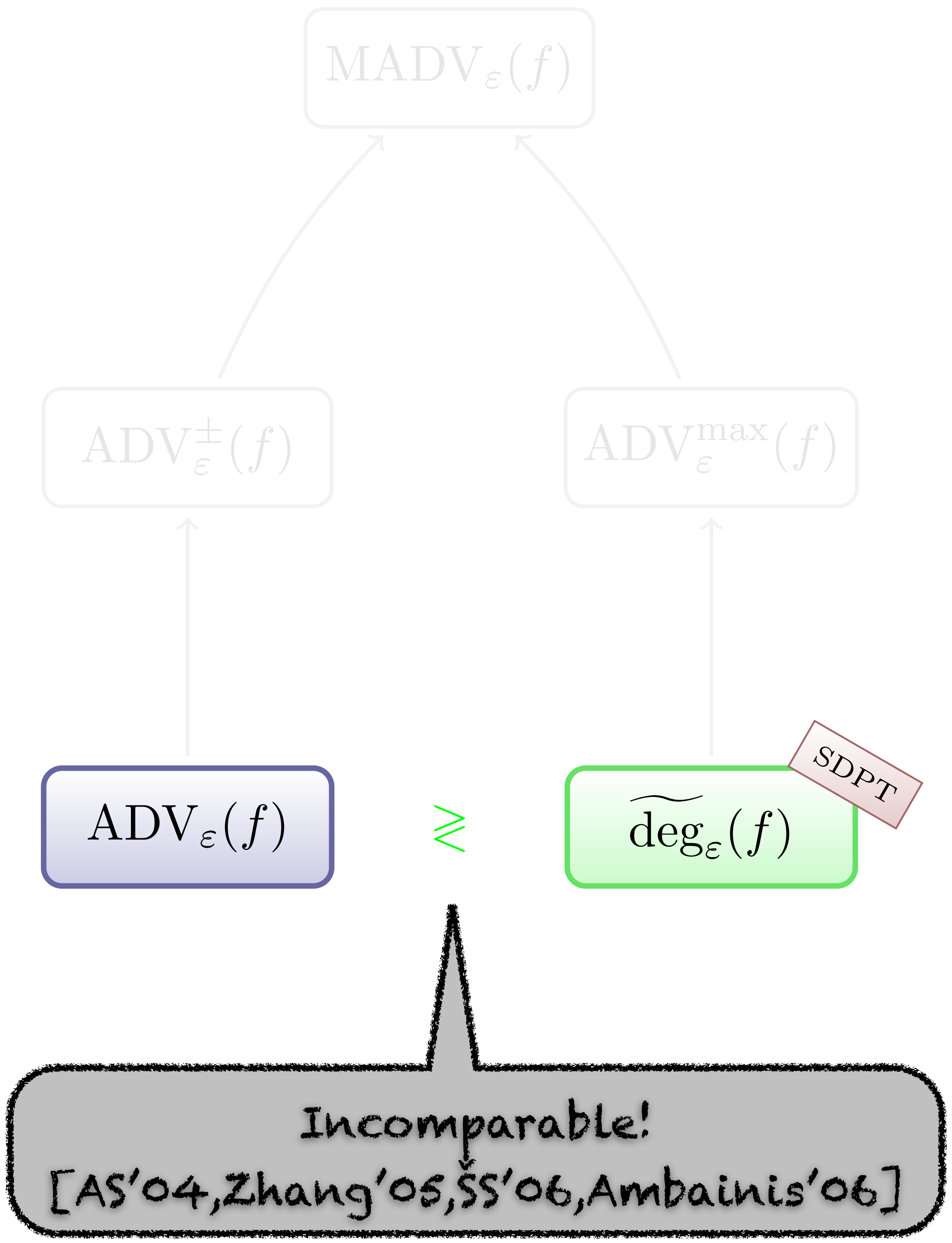
A brief history of lower bound methods

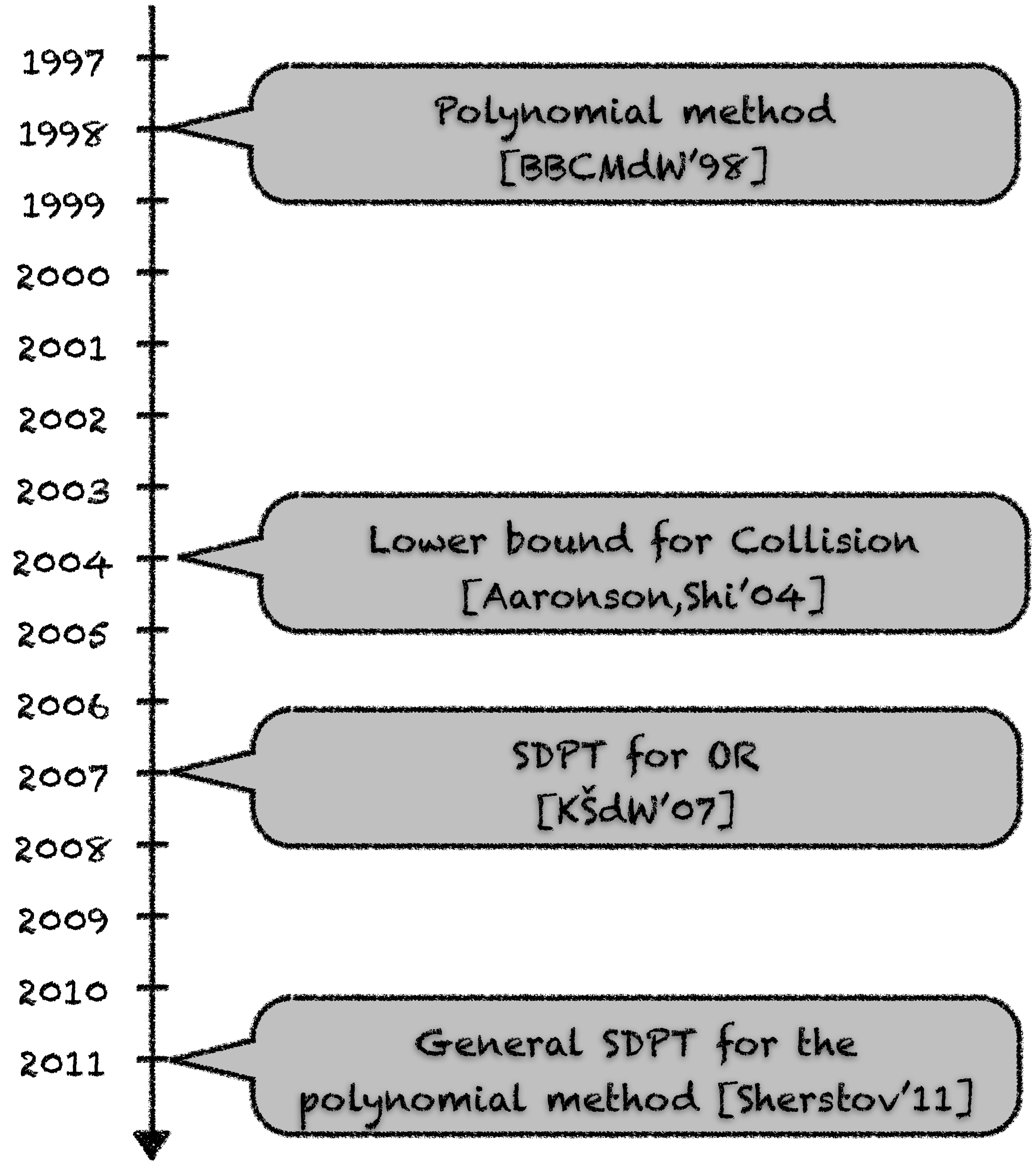
Adversary method



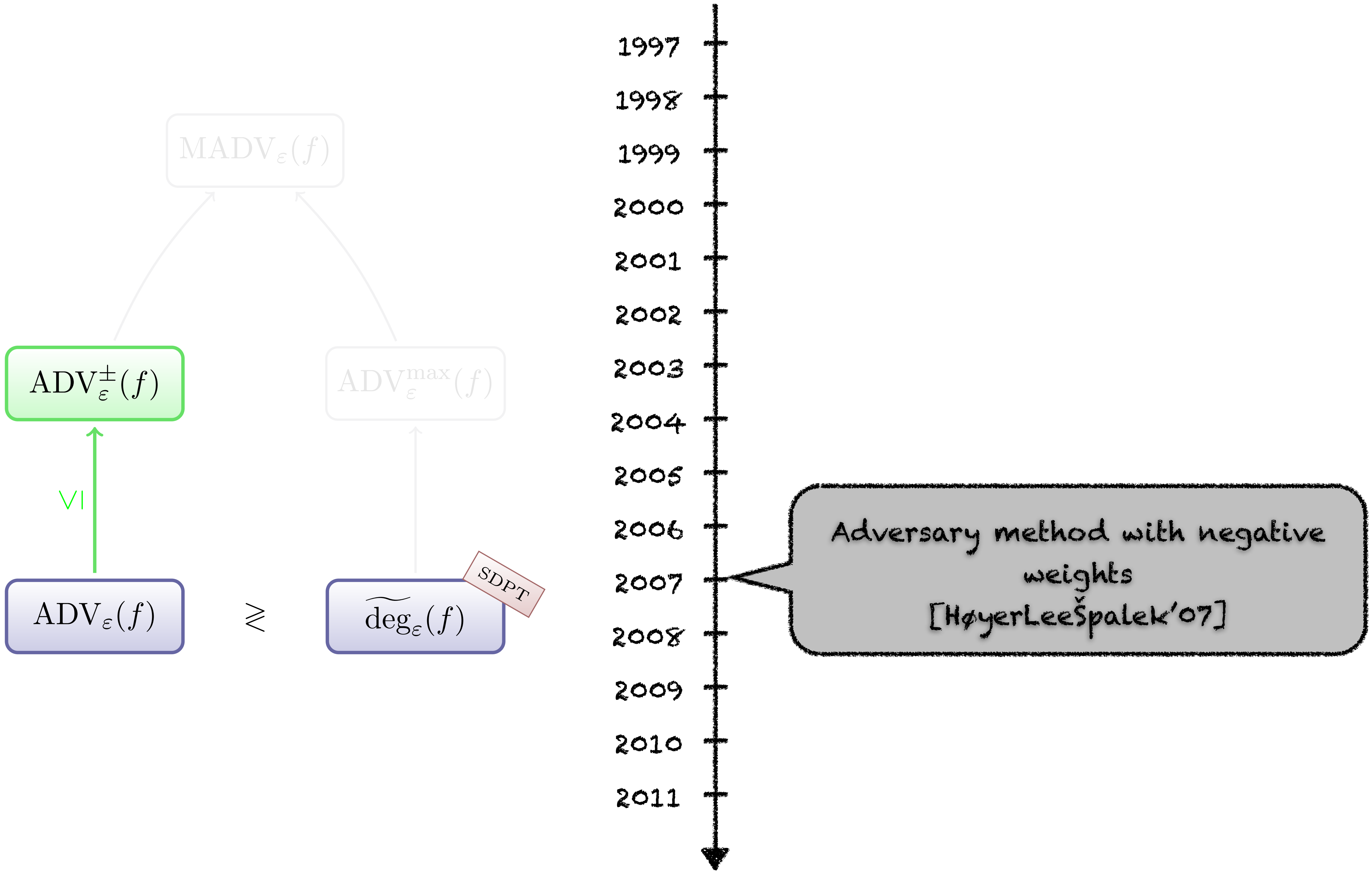


Polynomial method



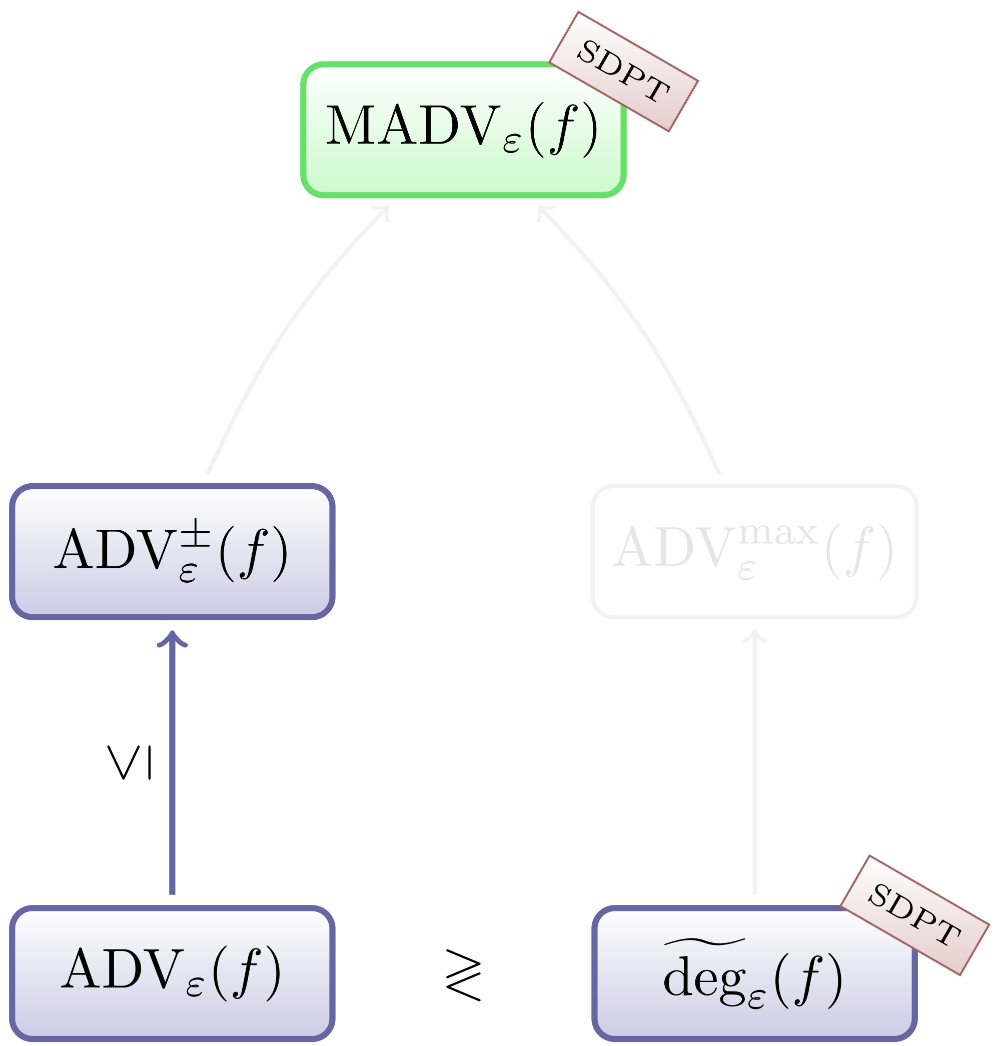


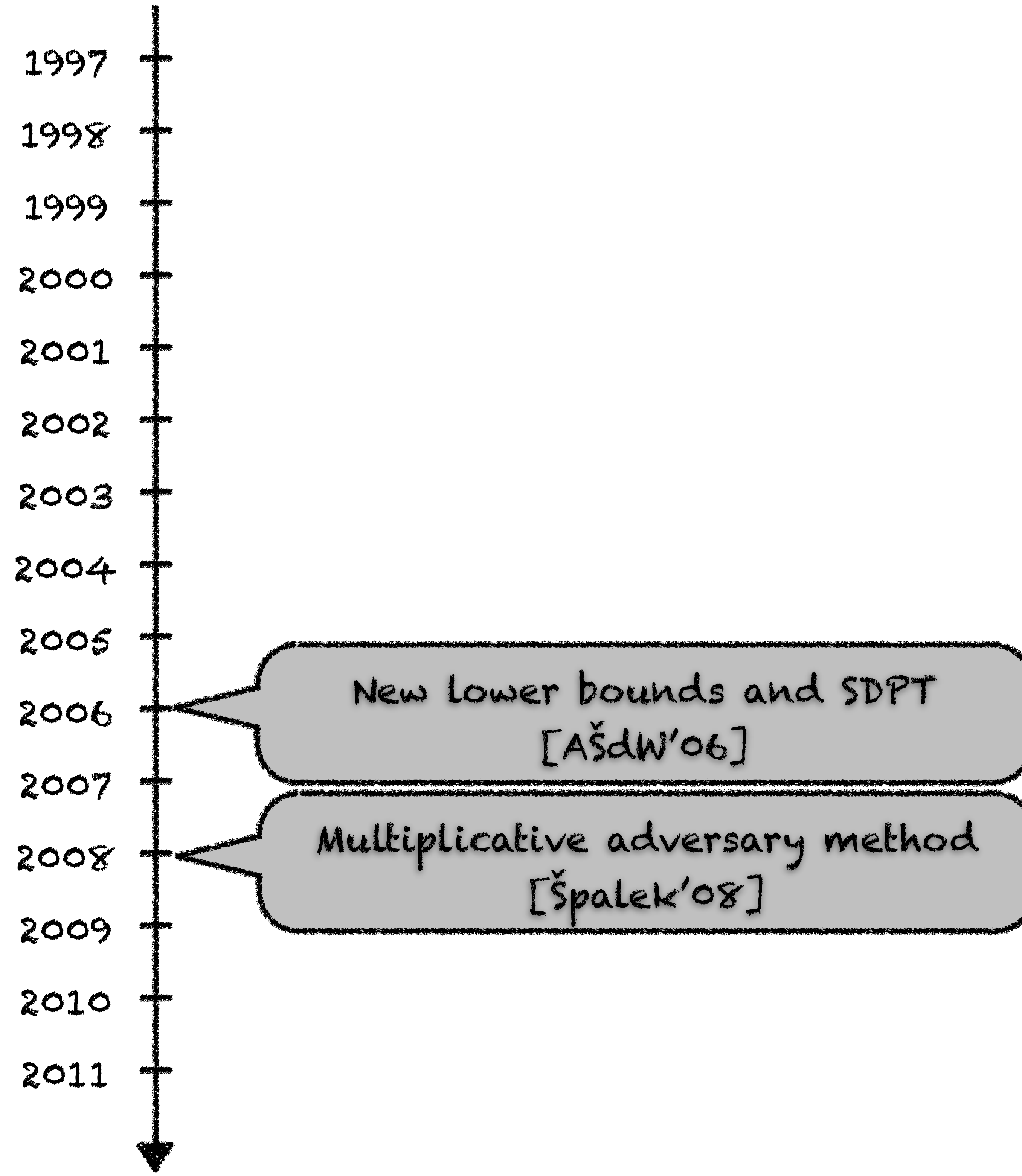
Generalized adversary method



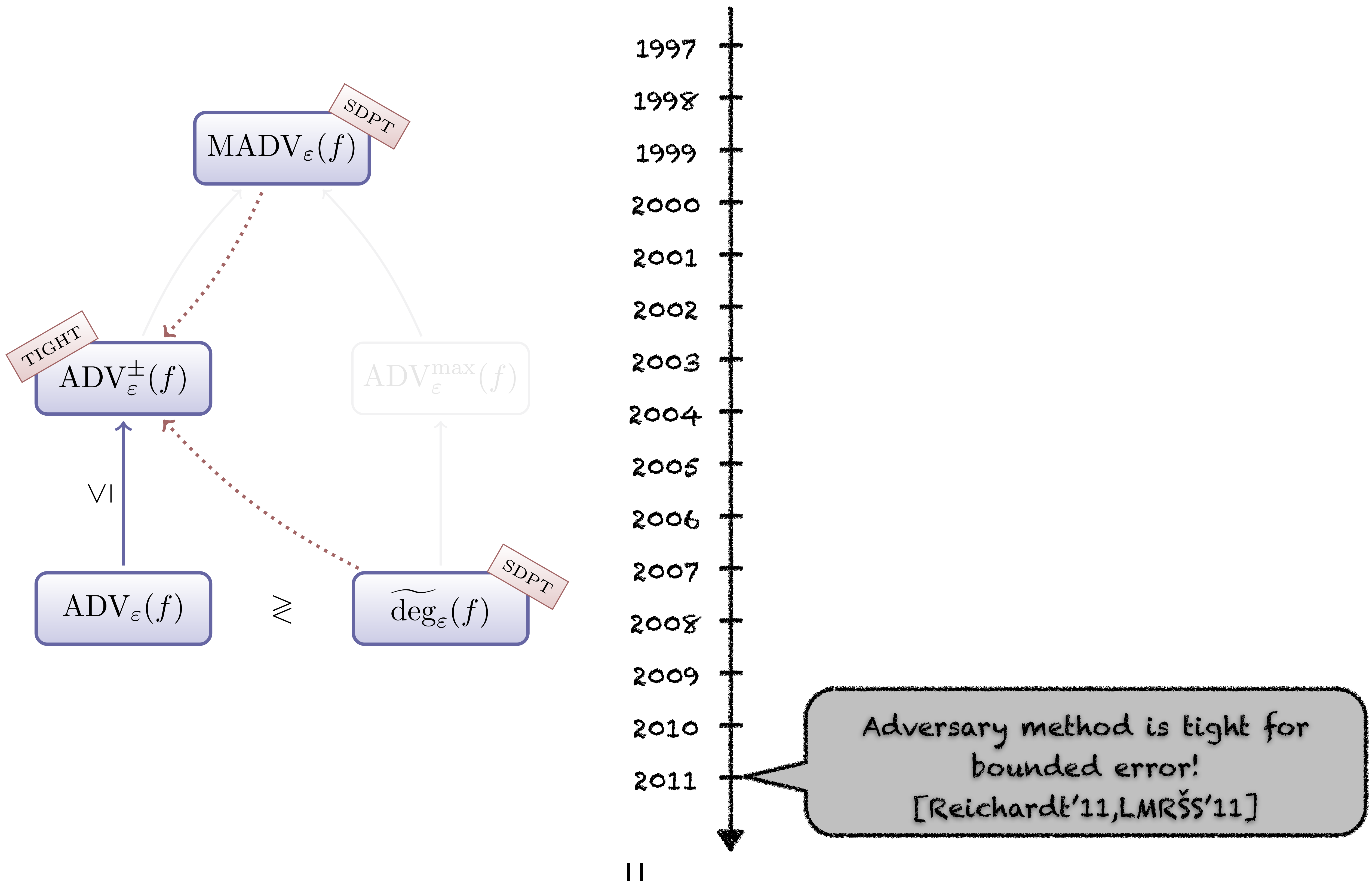
9

Multiplicative adversary method

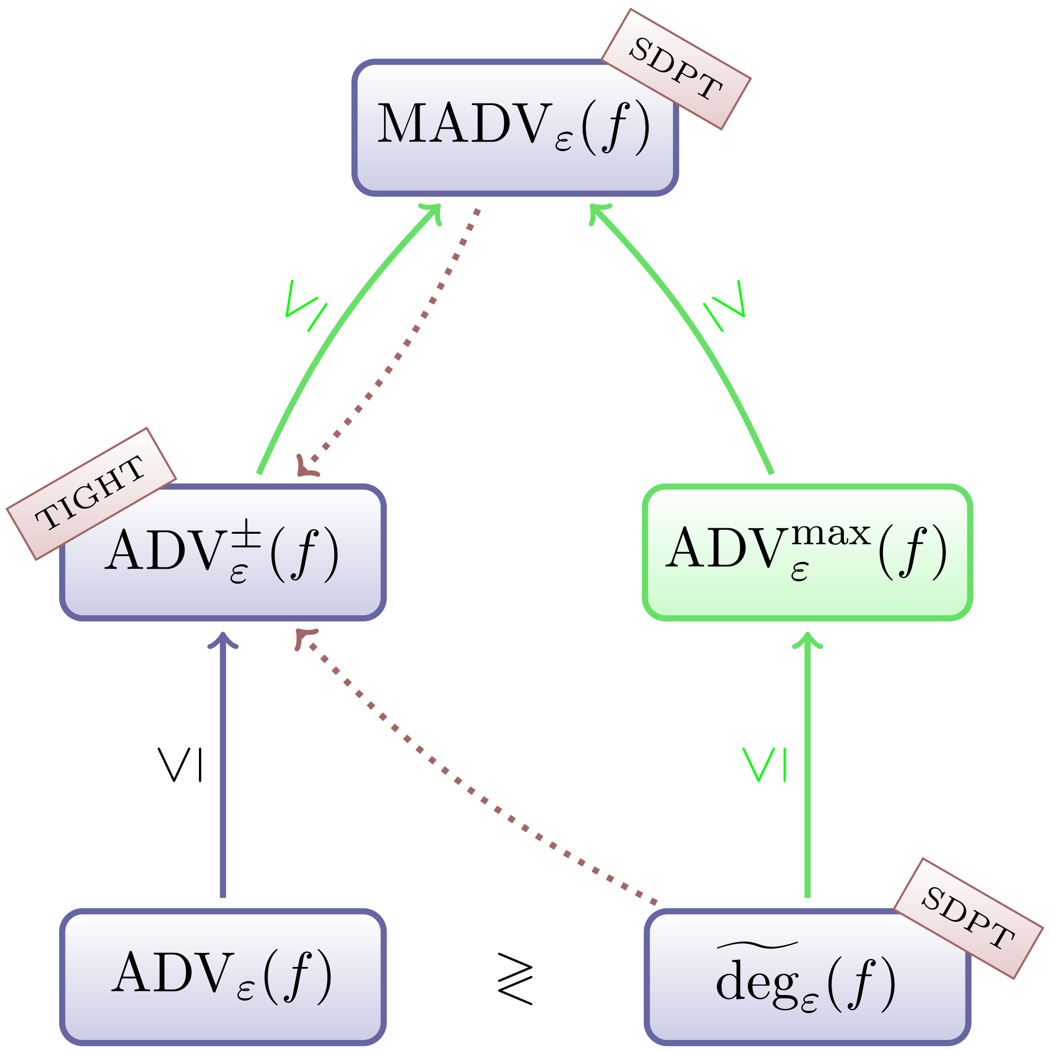




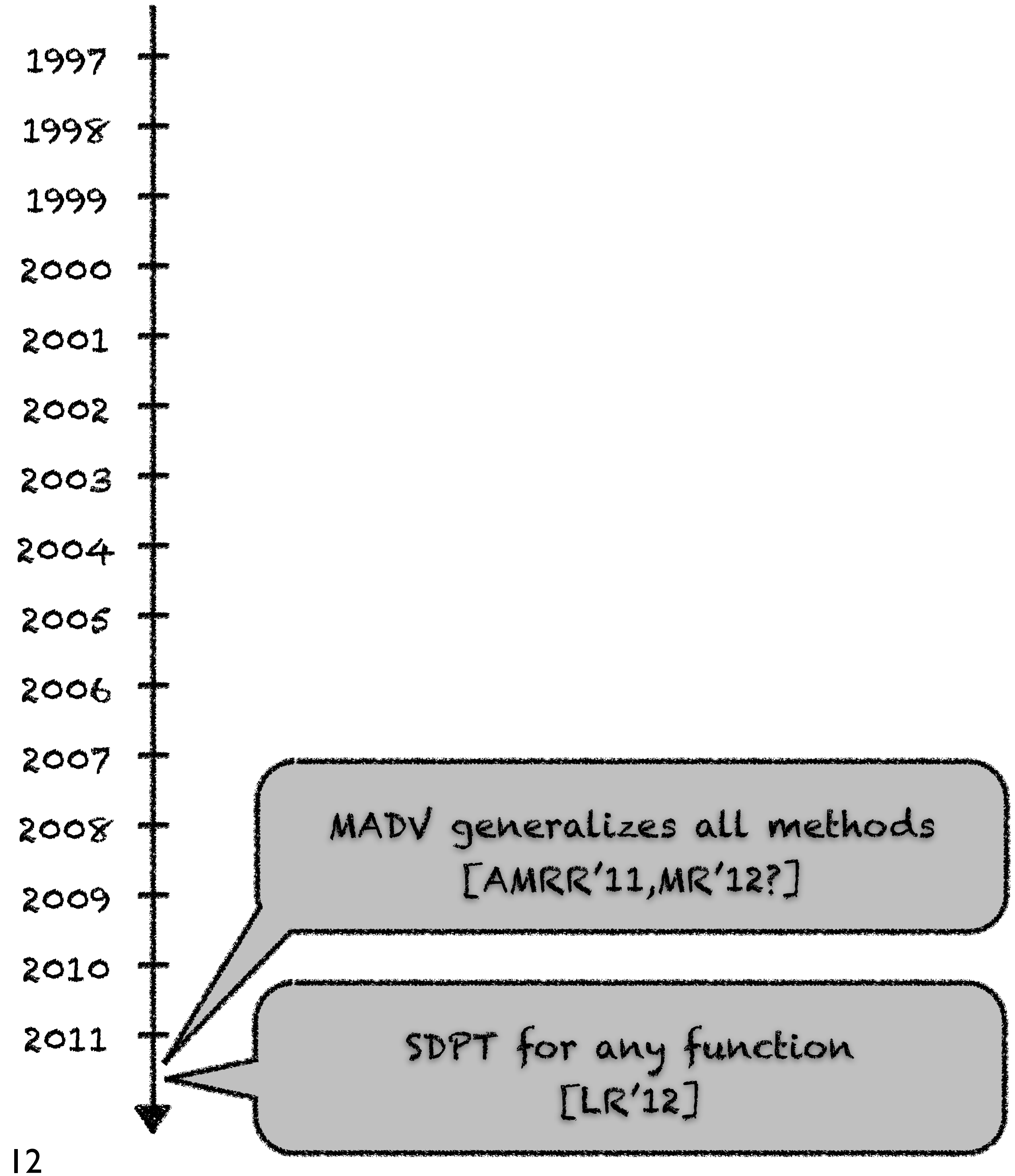
Optimality of adversary method



Our results



SDPT
$\mathrm{MADV}_\varepsilon(f)$
$\leq$
$\geq$
TIGHT
$\mathrm{ADV}^{\pm}_\varepsilon(f)$
$\mathrm{ADV}^{\max}_\varepsilon(f)$
$\leq$
$\leq$
$\mathrm{ADV}_\varepsilon(f)$
$\gtrsim$
$\widetilde{\deg}_\varepsilon(f)$
SDPT



1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
12
MADV generalizes all methods
[AMRR'11,MR'12?]
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 $M_{xy}^t = \langle \psi_x^t | \psi_y^t \rangle$
- Initially: $|\psi_x^0\rangle = |\bar{0}\rangle \ \forall x \ \Rightarrow M^0 = J$

All-1 matrix

- At the end: $|\psi_x^T\rangle \approx |\psi_x\rangle \ \Rightarrow M^T \approx M$

What distance?

Output conditions

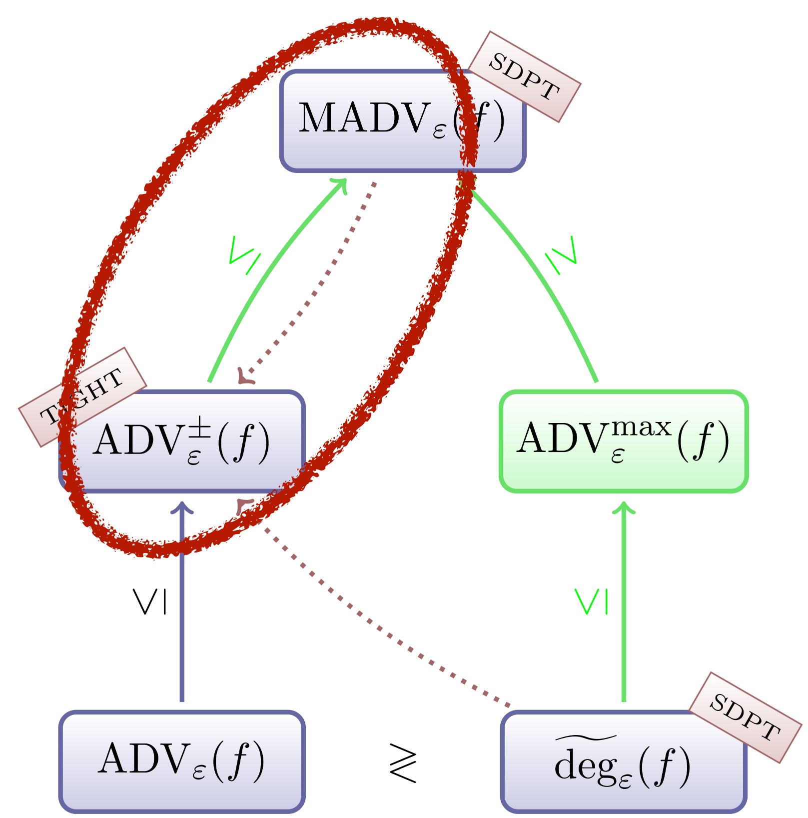
- $\|M^T - M\|_\infty \leq 2\sqrt{\varepsilon}$ [Ambainis02]
- $\gamma_2(M^T - M) \leq 2\sqrt{\varepsilon}$ [HøyerLeeŠpalek07]
- $\mathcal{F}_H(M^T, M) \geq \sqrt{1-\varepsilon}$ [LeeR11]

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

- Theorem: The last condition is tight

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

Multiplicative >= Additive



Additive adversary

[HøyerLeeŠpalek07]

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

Adversary matrix

- Additive change for one query:

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

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

Additive adversary bound

$$\mathbf{ADV}_{\mathbf{0}}^{\pm}(M) = \max_{\boldsymbol{\Gamma}} \|\boldsymbol{\Gamma} \circ (\boldsymbol{J} - \boldsymbol{M})\|$$

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

Multiplicative adversary [Špalek08]

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

Adversary matrix

- Multiplicative change for one query:

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

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

Multiplicative adversary bound

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

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

Multiplicative >= Additive

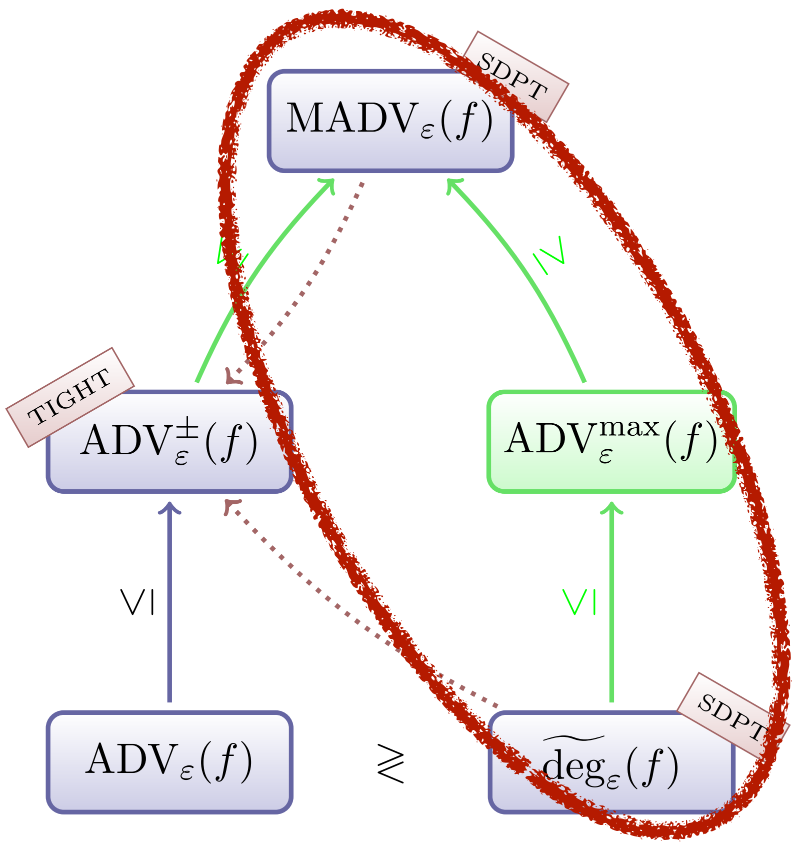
Theorem

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

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

New adversary method

- Let us partition the Hilbert space into subspaces $(S_k : 0 \leq k \leq K)$ such that:

1. Initialization: $\mathrm{Tr}(\Pi_{S_0} J) = \mathrm{Tr}(J)$
2. Change due to 1 query:

$$\Pi_{S_{k'}}(\Pi_{S_k} \circ \Delta_i)\Pi_{S_{k''}} = 0 \quad \text{if } |k - k'| > 1 \text{ or } |k - k''| > 1$$

- Therefore: $\mathrm{Tr}(\Pi_{S_k} M^t) = 0 \; \forall k > t$

Max-adversary method

$$\mathrm{ADV}^{\max}(M) = \max_{(S_k), k_0} \{k_0 : \mathrm{Tr}(\Pi_{S_{k_0}} M) \neq 0\}$$

Multiplicative >= Max

Theorem

$$\lim_{c\to\infty} \mathrm{MADV}^c(M) \geq \mathrm{ADV}^{\max}(M)$$

Proof idea:

- Use the adversary matrix: $\Gamma_m = \sum_k \lambda^k \Pi_{S_k}$
- Show that it satisfies the conditions for $c = 3\lambda$
- Show the we get the same bound for $\lambda \to \infty$

Max >= Polynomial

- Let Φ be the Gram matrix for computing f in the phase, i.e., for generating $(-1)^{f(x)}|\bar{0}\rangle$
- We have $Q_{(1-\sqrt{1-\varepsilon})/2+\varepsilon/4}(f) \leq Q_\varepsilon(\Phi) \leq 2Q_{(1-\sqrt{1-\varepsilon})/2}(f)$ [LeeR11]

Theorem

$$\mathrm{ADV}_\varepsilon^{\max}(\Phi) \geq \widetilde{\deg}_\varepsilon(f)$$

Proof idea:

- We use the Fourier basis: $|\chi_w\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{w\cdot x}|x\rangle$
- Subspaces are defined as $S_k = \mathrm{Span}\{|\chi_w\rangle : |w| = k\}$
- We show that if $\widetilde{\deg}_\varepsilon(f) \geq t$, every Gram matrix M ε-approximating Φ has overlap on some $|\chi_w\rangle$ with $|w| \geq t$

Strong direct product theorem

SDPT

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 $\mathrm{ADV}^{\pm}$: $Q_{1/4}(f) \leq C\cdot \mathrm{ADV}^{\pm}_{0}(F)$ [LMRŠS11]
- Use $\mathrm{MADV}^{c}_{0}(F) \geq \frac{\mathrm{ADV}^{\pm}_{0}(F)}{2}$ for $c = 1+\frac{1}{\mathrm{ADV}^{\pm}_{0}(F)}$
- Using adversary matrix $\Gamma_m^{\otimes k}$, we have:

$$\mathrm{MADV}^{c}_{0}(F^{\otimes k}) \geq k\cdot \mathrm{MADV}^{c}_{0}(F)$$

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

SDPT

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

- We show that if $\mathcal{F}_H(F^{\otimes k}, M) \geq \delta^{k/2}$,
- then $\mathrm{Tr}[(\Gamma_m^{\otimes k} \circ M)(vv^*)^{\otimes k}] \geq (3\delta/2)^k \cdot \mathrm{Tr}[(\Gamma_m \circ F)vv^*]^k$
- Therefore: $\mathrm{MADV}_0^c(M) \geq k \cdot \ln(3\delta/2) \cdot \mathrm{MADV}_0^c(F)$

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: