Privacy-Preserving Perturbation of Convex Optimization Programs

Vladimir Dvorkin, MIT Energy Initiative

August 4, 2022

MARIE CURIE **ACTIONS**

Fundación IBERDROLA ESPAÑA

I owe a lot of inspiration and joy to my co-authors

Pascal Van Hentenryck
GeorgiaTech

Nando Fioretto
Syracuse University

Jalal Kazempour
Technical Univ. of Denmark

Pierre Pinson
Imperial College London

Convex optimization solves real-world problems

$$\begin{aligned} \min_{x} \quad & c^\top x \\ \text{s.t.} \quad & b - Ax \in \mathcal{K} \end{aligned}$$

- Conic optimization program
- Optimization dataset $\mathcal{D} = \{c, b, A\}$
- Optimal solution $x^\star$ is dataset-specific
- Often, $x^\star(\mathcal{D}) \neq x^\star(\mathcal{D}')$ for different datasets $\mathcal{D}$ and $\mathcal{D}'$

Healthcare

Logistics

Credit scoring

eCommerce

Energy forecasting

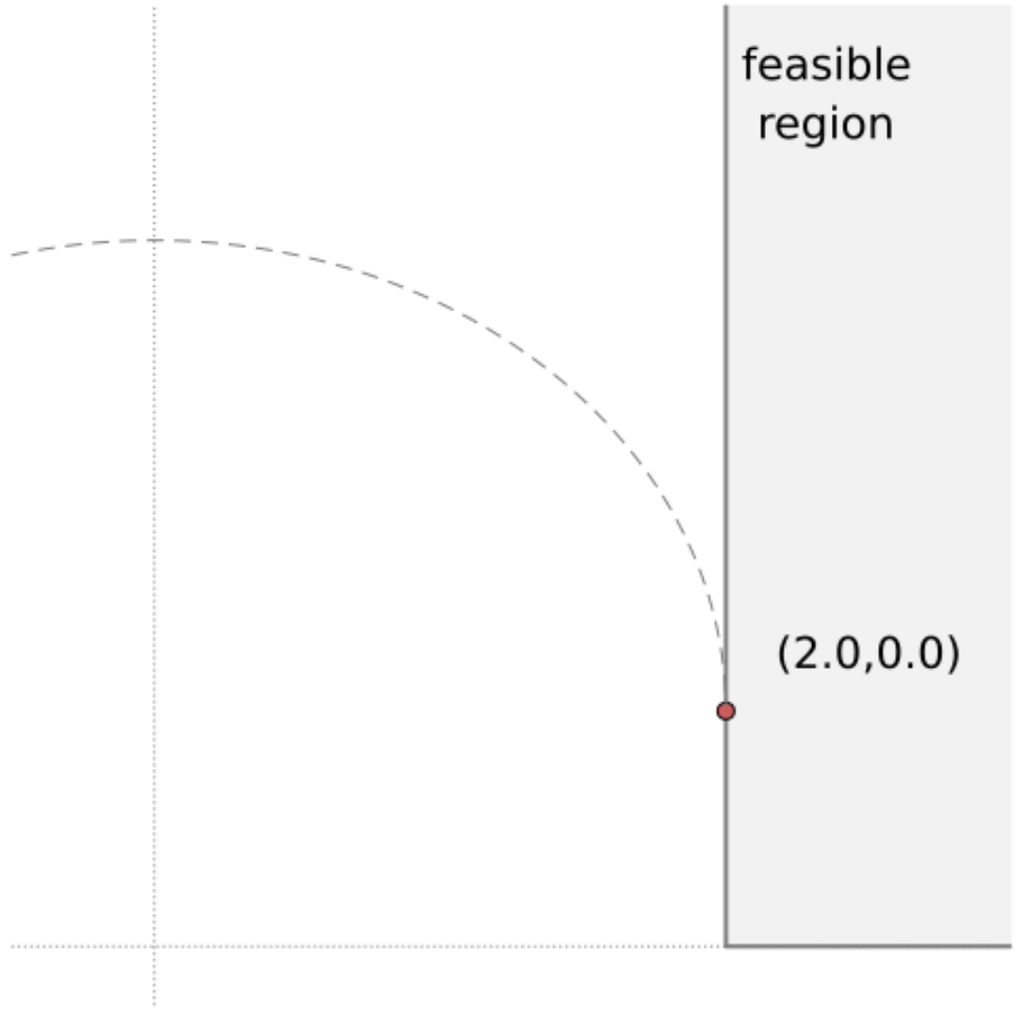
Distribution grids

Convex optimization solves real-world problems

$$\begin{aligned} \min_{x} \quad & c^\top x \\ \text{s.t.} \quad & b - Ax \in \mathcal{K} \end{aligned}$$

- Conic optimization program
- Optimization dataset $\mathcal{D} = \{c, b, A\}$
- Optimal solution $x^\star$ is dataset-specific
- Often, $x^\star(\mathcal{D}) \neq x^\star(\mathcal{D}')$ for different datasets $\mathcal{D}$ and $\mathcal{D}'$

- Quadratic programming
- Regression analysis
- Classification tasks
- Geometric problems

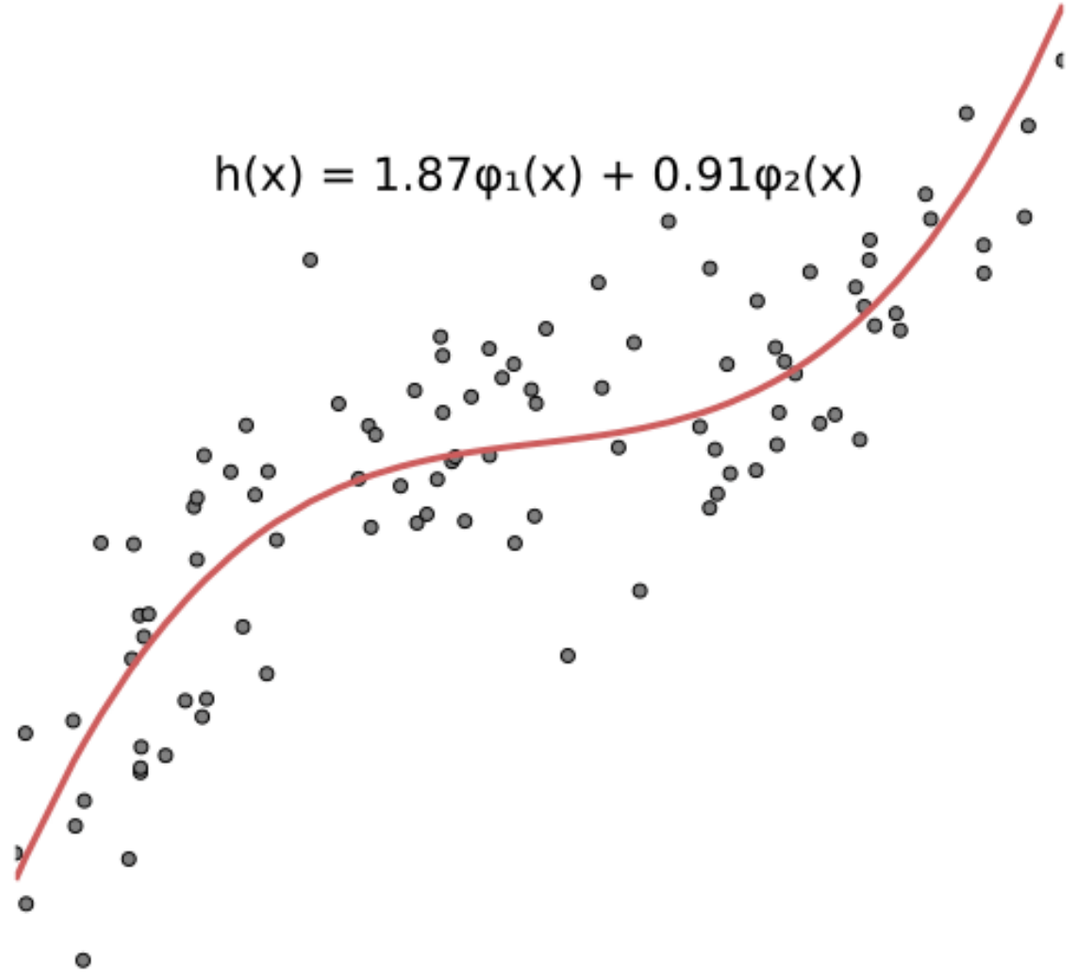


Convex optimization solves real-world problems

$$\begin{aligned} \min_{x} \quad & c^\top x \\ \text{s.t.} \quad & b - Ax \in \mathcal{K} \end{aligned}$$

- Conic optimization program
- Optimization dataset $\mathcal{D} = \{c, b, A\}$
- Optimal solution $x^\star$ is dataset-specific
- Often, $x^\star(\mathcal{D}) \neq x^\star(\mathcal{D}')$ for different datasets $\mathcal{D}$ and $\mathcal{D}'$

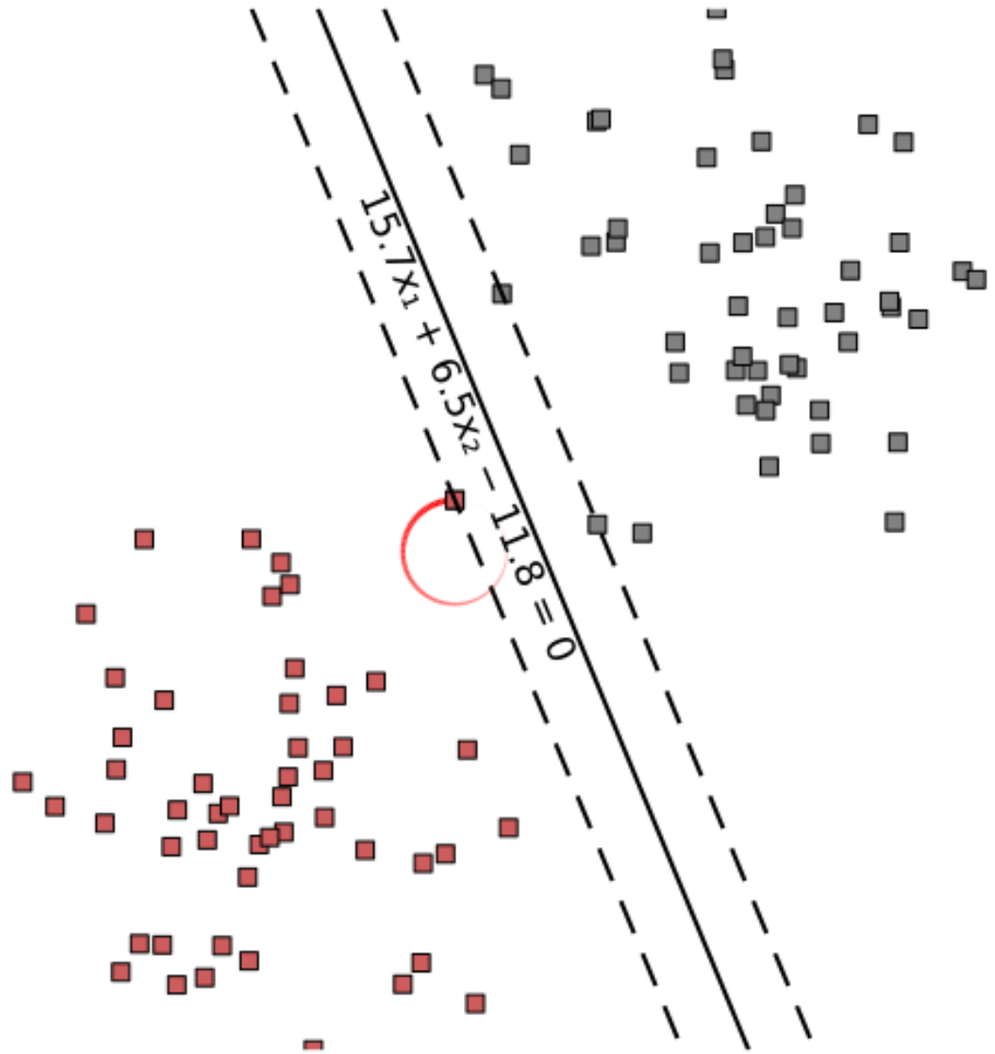
- Quadratic programming
- Regression analysis
- Classification tasks
- Geometric problems



Convex optimization solves real-world problems

$$\begin{aligned} \min_{x} \quad & c^\top x \\ \text{s.t.} \quad & b - Ax \in \mathcal{K} \end{aligned}$$

- Conic optimization program
- Optimization dataset $\mathcal{D} = \{c, b, A\}$
- Optimal solution $x^\star$ is dataset-specific
- Often, $x^\star(\mathcal{D}) \neq x^\star(\mathcal{D}')$ for different datasets $\mathcal{D}$ and $\mathcal{D}'$



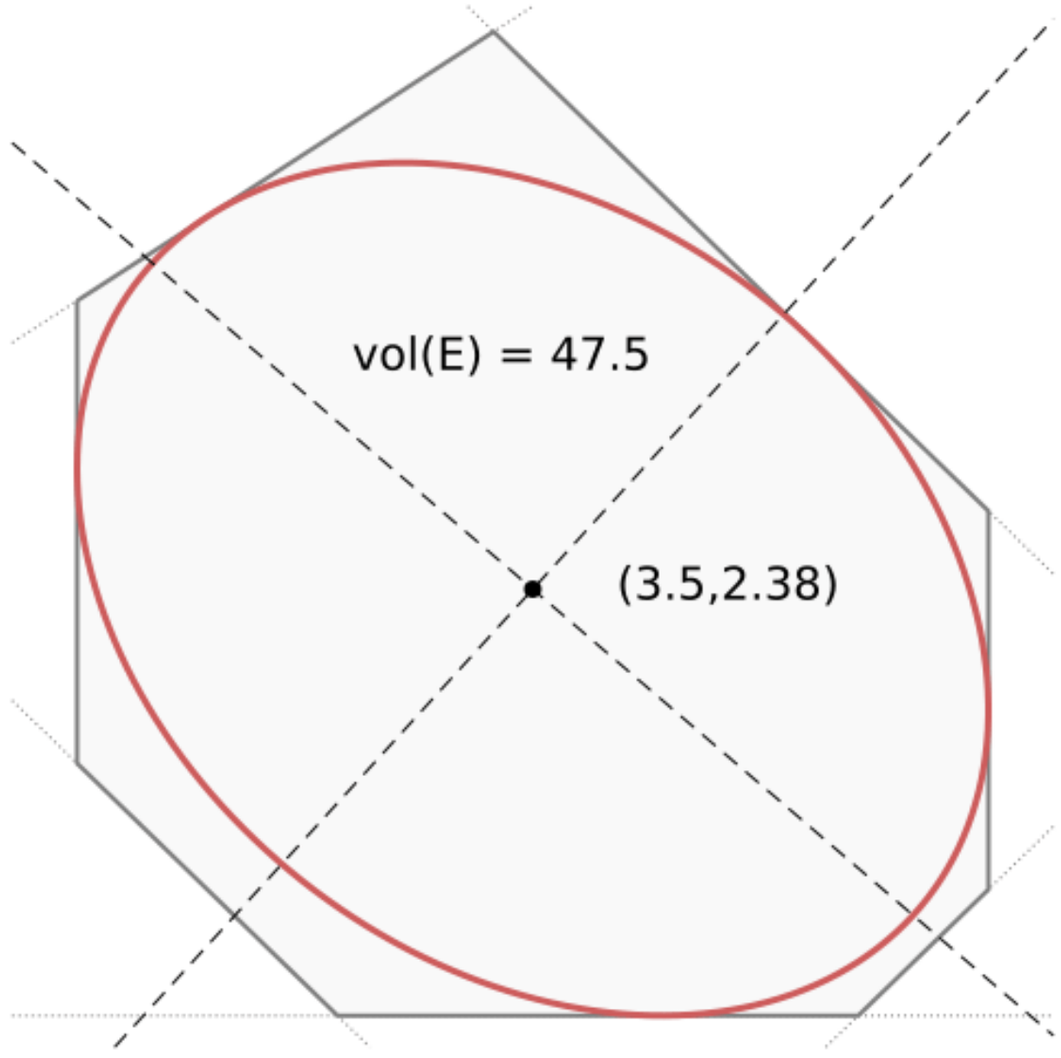
- Quadratic programming
- Regression analysis
- Classification tasks
- Geometric problems

Convex optimization solves real-world problems

$$\begin{aligned} \min_{x} \quad & c^\top x \\ \text{s.t.} \quad & b - Ax \in \mathcal{K} \end{aligned}$$

- Conic optimization program
- Optimization dataset $\mathcal{D} = \{c, b, A\}$
- Optimal solution $x^\star$ is dataset-specific
- Often, $x^\star(\mathcal{D}) \neq x^\star(\mathcal{D}')$ for different datasets $\mathcal{D}$ and $\mathcal{D}'$

- Quadratic programming
- Regression analysis
- Classification tasks
- Geometric problems



Formalization of privacy

- Optimization as a mapping $x^\star : \mathbb{D} \mapsto \mathbb{X}$
- Privacy adversary mapping $\mathcal{A} : \mathbb{X} \mapsto \mathbb{D}$
- **Privacy goal** is to mislead the adversary

- Let $\tilde{x}^\star$ be a random counterpart of $x^\star$
- For any two datasets $\mathcal{D}, \mathcal{D}' \in \mathbb{D}$:

  deterministic mapping: $x^\star(\mathcal{D}) \neq x^\star(\mathcal{D}')$

  randomized mapping: $\tilde{x}^\star(\mathcal{D}) \approx \tilde{x}^\star(\mathcal{D}')$

- ε−differential privacy (ε−DP):

$$\frac{\Pr[\tilde{x}^\star(\mathcal{D}\ ) = \hat{x}]}{\Pr[\tilde{x}^\star(\mathcal{D}') = \hat{x}]} \leqslant \exp(\varepsilon)$$

- Smaller ε implies stronger privacy

$$\exp(\varepsilon) \approx 1 + \varepsilon$$

Formalization of privacy

- Optimization as a mapping $x^\star : \mathbb{D} \mapsto \mathbb{X}$
- Privacy adversary mapping $\mathcal{A} : \mathbb{X} \mapsto \mathbb{D}$
- **Privacy goal** is to mislead the adversary

- Let $\tilde{x}^\star$ be a random counterpart of $x^\star$
- For any two datasets $\mathcal{D}, \mathcal{D}' \in \mathbb{D}$:

  deterministic mapping: $x^\star(\mathcal{D}) \neq x^\star(\mathcal{D}')$

  randomized mapping: $\tilde{x}^\star(\mathcal{D}) \approx \tilde{x}^\star(\mathcal{D}')$

- ε—differential privacy (ε—DP):

$$\frac{\Pr[\tilde{x}^\star(\mathcal{D}) = \hat{x}]}{\Pr[\tilde{x}^\star(\mathcal{D}') = \hat{x}]} \leqslant \exp(\varepsilon)$$

- Smaller ε implies stronger privacy

$$\exp(\varepsilon) \approx 1 + \varepsilon$$

Formalization of privacy

- Optimization as a mapping $x^\star : \mathbb{D} \mapsto \mathbb{X}$
- Privacy adversary mapping $\mathcal{A} : \mathbb{X} \mapsto \mathbb{D}$
- **Privacy goal** is to mislead the adversary

- Let $\tilde{x}^\star$ be a random counterpart of $x^\star$
- For any two datasets $\mathcal{D}, \mathcal{D}' \in \mathbb{D}$:

  deterministic mapping: $x^\star(\mathcal{D}) \neq x^\star(\mathcal{D}')$

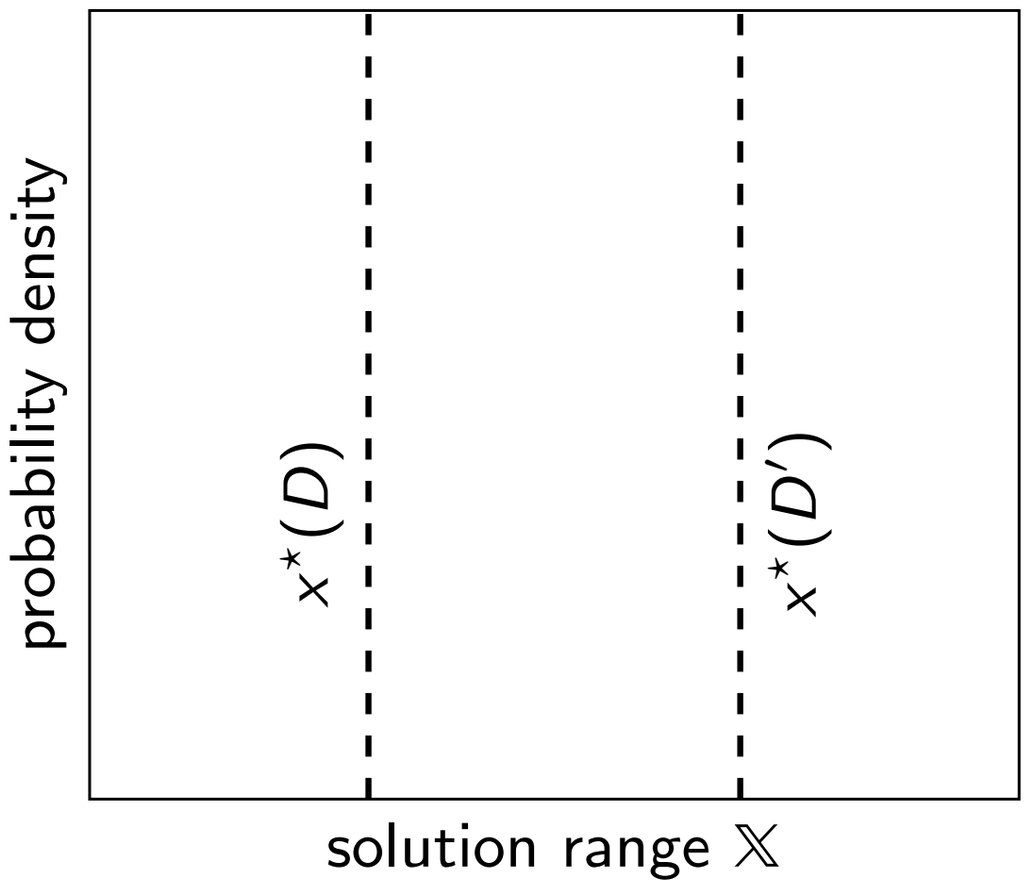
  randomized mapping: $\tilde{x}^\star(\mathcal{D}) \approx \tilde{x}^\star(\mathcal{D}')$

- ε—differential privacy (ε—DP):

$$\frac{\Pr[\tilde{x}^\star(\mathcal{D}) = \hat{x}]}{\Pr[\tilde{x}^\star(\mathcal{D}') = \hat{x}]} \leqslant \exp(\varepsilon)$$

- Smaller ε implies stronger privacy

$$\exp(\varepsilon) \approx 1 + \varepsilon$$



Formalization of privacy

- Optimization as a mapping $x^\star : \mathbb{D} \mapsto \mathbb{X}$
- Privacy adversary mapping $\mathcal{A} : \mathbb{X} \mapsto \mathbb{D}$
- **Privacy goal** is to mislead the adversary

- Let $\tilde{x}^\star$ be a random counterpart of $x^\star$
- For any two datasets $\mathcal{D}, \mathcal{D}' \in \mathbb{D}$:

deterministic mapping: $x^\star(\mathcal{D}) \neq x^\star(\mathcal{D}')$

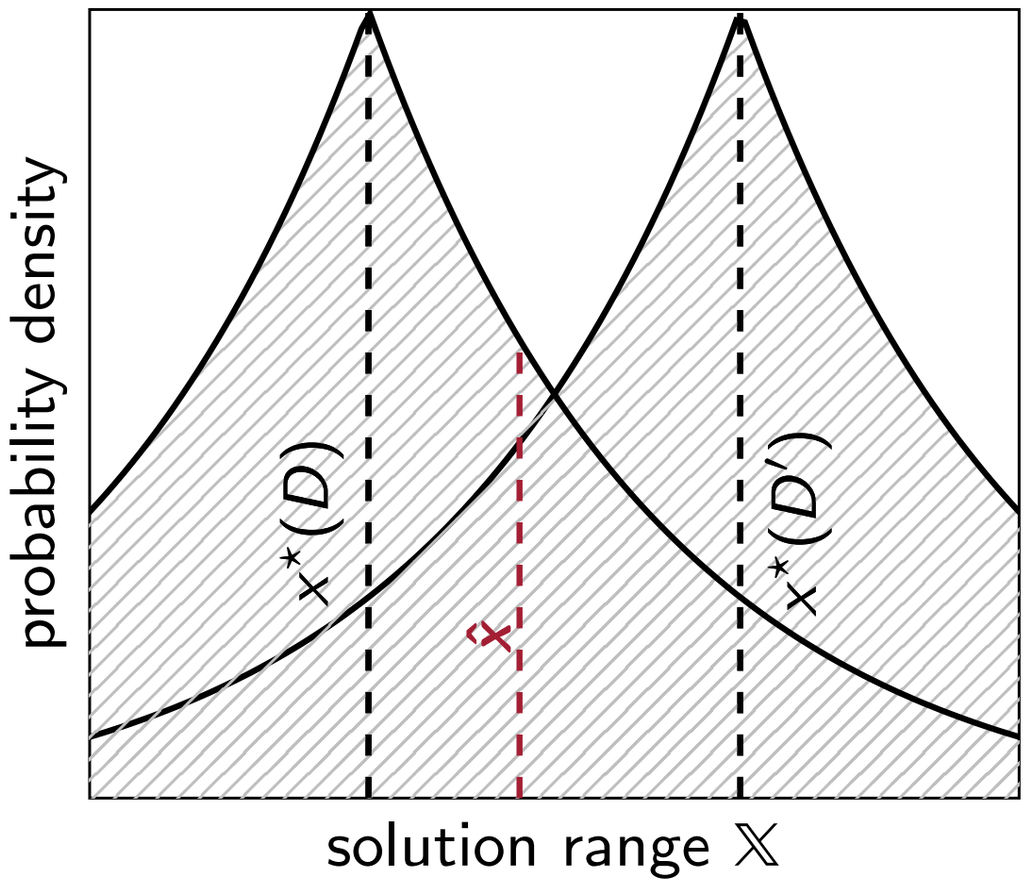
randomized mapping: $\tilde{x}^\star(\mathcal{D}) \approx \tilde{x}^\star(\mathcal{D}')$

- ε—differential privacy (ε—DP):

$$\frac{\Pr[\tilde{x}^\star(\mathcal{D}) = \hat{x}]}{\Pr[\tilde{x}^\star(\mathcal{D}') = \hat{x}]} \leqslant \exp(\varepsilon)$$

- Smaller ε implies stronger privacy

$$\exp(\varepsilon) \approx 1 + \varepsilon$$



Key principle of DP: obfuscate data but preserve its value

Key principle of DP: obfuscate data but preserve its value

The Starry Night by Vincent Van Gogh

1888 (Musée d'Orsay's, Paris)

Key principle of DP: obfuscate data but preserve its value

The Starry Night by Vincent Van Gogh

1888 (Musée d'Orsay's, Paris)

1889 (Museum of Modern Art, NYC)

Key principle of DP: obfuscate data but preserve its value

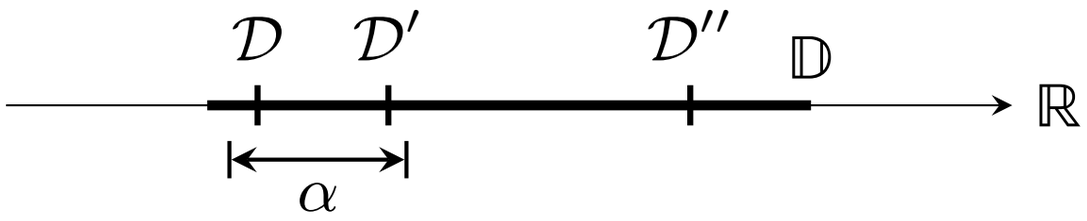
The Starry Night by Vincent Van Gogh

1888 (Musée d'Orsay's, Paris)

1889 (Museum of Modern Art, NYC)

The value of each painting is well over $100 million

Limits of DP applications to convex optimization



- $\|\mathcal{D} - \mathcal{D}'\| \leqslant \alpha$: $\mathcal{D}$ and $\mathcal{D}'$ are $\alpha-$adjacent
- $\mathcal{D}''$ is not $\alpha-$adjacent to $\mathcal{D}$ and $\mathcal{D}'$

The goal is to privatize $\alpha-$adjacent datasets
when releasing optimization results

Input perturbation

1. Optimization dataset perturbation

$$\tilde{\mathcal{D}} = \mathcal{D} + \zeta, \quad \zeta \sim \mathsf{Lap}(\alpha/\varepsilon)$$

2. Optimization on perturbed data $x^\star(\tilde{\mathcal{D}})$

Output perturbation

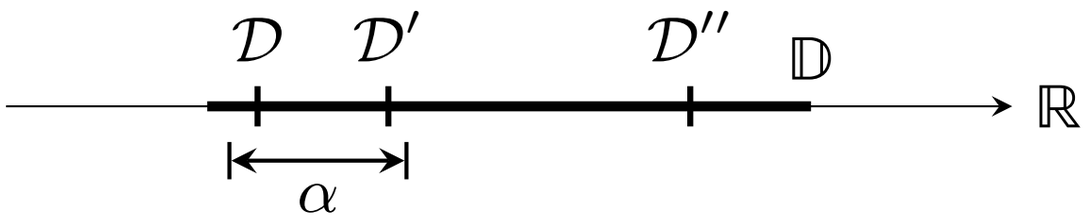
1. Worst-case sensitivity computation

$$\Delta_\alpha = \mathsf{max}_{\mathcal{D},\mathcal{D}' \in \mathbb{D}} \|\tilde{x}^\star(\mathcal{D}) - \tilde{x}^\star(\mathcal{D}')\|_1$$

2. Perturbation of optimization results

$$\tilde{x}^\star(\mathcal{D}) = x^\star(\mathcal{D}) + \zeta, \quad \zeta \sim \mathsf{Lap}(\Delta_\alpha/\varepsilon)$$

Limits of DP applications to convex optimization



- $\|\mathcal{D} - \mathcal{D}'\| \leqslant \alpha$: $\mathcal{D}$ and $\mathcal{D}'$ are $\alpha-$adjacent
- $\mathcal{D}''$ is not $\alpha-$adjacent to $\mathcal{D}$ and $\mathcal{D}'$

The goal is to privatize $\alpha-$adjacent datasets
when releasing optimization results

Input perturbation

1. Optimization dataset perturbation

$$\tilde{\mathcal{D}} = \mathcal{D} + \zeta, \quad \zeta \sim \mathsf{Lap}(\alpha/\varepsilon)$$

2. Optimization on perturbed data $x^\star(\tilde{\mathcal{D}})$

Output perturbation

1. Worst-case sensitivity computation

$$\Delta_\alpha = \mathsf{max}_{\mathcal{D},\mathcal{D}' \in \mathbb{D}} \, \|\tilde{x}^\star(\mathcal{D}) - \tilde{x}^\star(\mathcal{D}')\|_1$$

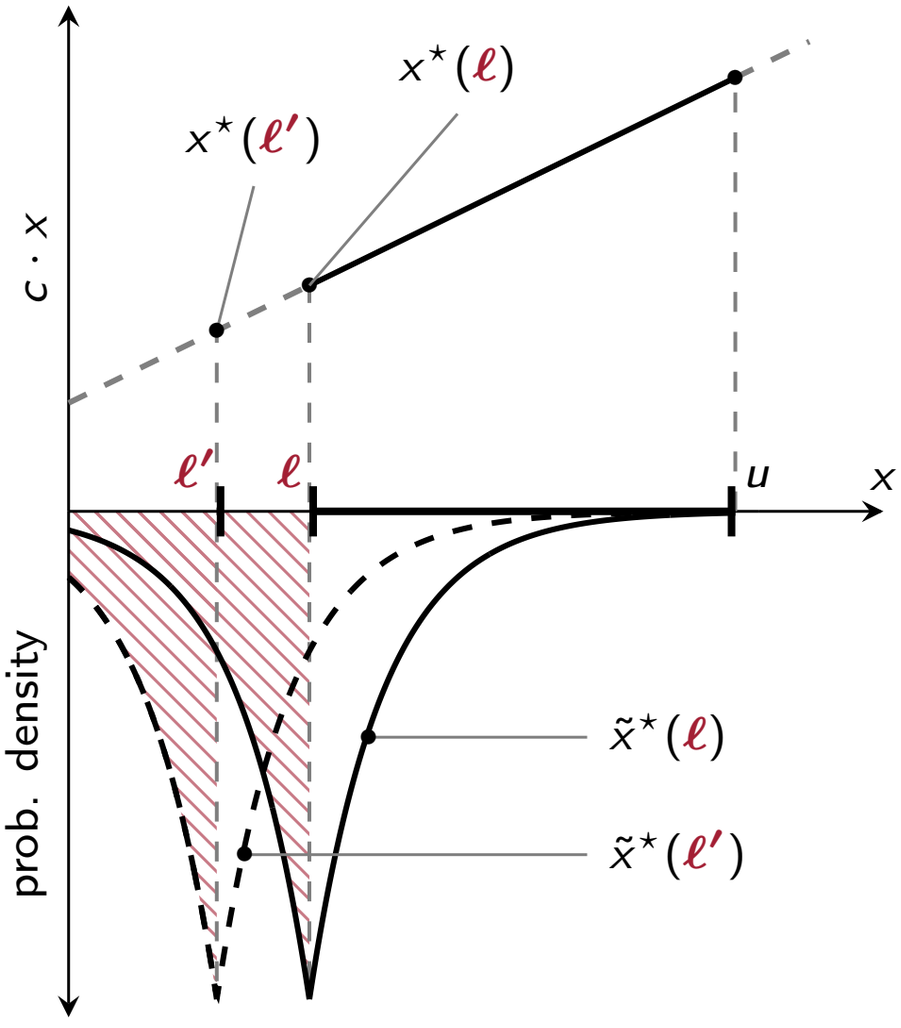
2. Perturbation of optimization results

$$\tilde{x}^\star(\mathcal{D}) = x^\star(\mathcal{D}) + \zeta, \quad \zeta \sim \mathsf{Lap}(\Delta_\alpha/\varepsilon)$$

Linear programming example

$$\begin{aligned} \min_{x} \quad & c \cdot x \\ \text{s.t.} \quad & \ell \leqslant x \leqslant u, \end{aligned}$$

- Datum ℓ must be indistinguishable from some adjacent value ℓ'
- Input perturbation of ℓ and output perturbation of $x^\star(\ell)$ are equivalent
- Two strategies yield **infeasible** results



Stochastic programming for private optimization queries

- Optimization vector as the linear decision rule of the form:

$$\tilde{x}(\mathcal{D}) = \overline{x}(\mathcal{D}) + X(\mathcal{D})\zeta$$

$\overline{x}$ – nominal solution vector (function of dataset)

X – solution recourse matrix (function of dataset)

- Vector $\overline{x}$ and matrix X are subject to stochastic optimization:

$$\min_{\overline{x}, X \in \mathcal{X}} \quad \mathbb{E}\left[c^\top(\overline{x} + X\zeta)\right]$$
$$\text{s.t.} \quad \Pr\left[b - A(\overline{x} + X\zeta) \in \mathcal{K}\right] \geqslant 1 - \eta$$

  - Minimize expected cost
  - Chance constraint to **guarantee feasibility**
  - $\mathcal{X}$ for data-independent query perturbation

- For example, an **identity query** perturbation is data-independent when

$$\mathcal{X} = \{X | X = \text{diag}[\mathbb{1}]\},$$

such that the identity query release takes the form

$$\tilde{x}(\mathcal{D}) = \overline{x}^\star(\mathcal{D}) + X^\star(\mathcal{D})\zeta = \overline{x}^\star(\mathcal{D}) + \zeta$$

Stochastic programming for private optimization queries

- Optimization vector as the linear decision rule of the form:

$$\tilde{x}(\mathcal{D}) = \overline{x}(\mathcal{D}) + X(\mathcal{D})\zeta$$

$\overline{x}$ – nominal solution vector (function of dataset)

X – solution recourse matrix (function of dataset)

- Vector $\overline{x}$ and matrix X are subject to stochastic optimization:

$$\min_{\overline{x}, X \in \mathcal{X}} \quad \mathbb{E}\left[c^\top(\overline{x} + X\zeta)\right]$$
$$\text{s.t.} \quad \Pr\left[b - A(\overline{x} + X\zeta) \in \mathcal{K}\right] \geqslant 1 - \eta$$

  - Minimize expected cost
  - Chance constraint to **guarantee feasibility**
  - $\mathcal{X}$ for data-independent query perturbation

- For example, an **identity query** perturbation is data-independent when

$$\mathcal{X} = \{X | X = \text{diag}[\mathbb{1}]\},$$

such that the identity query release takes the form

$$\tilde{x}(\mathcal{D}) = \overline{x}^\star(\mathcal{D}) + X^\star(\mathcal{D})\zeta = \overline{x}^\star(\mathcal{D}) + \zeta$$

Stochastic programming for private optimization queries

- Optimization vector as the linear decision rule of the form:

$$\tilde{x}(\mathcal{D}) = \overline{x}(\mathcal{D}) + X(\mathcal{D})\zeta$$

$\overline{x}$ – nominal solution vector (function of dataset)

X – solution recourse matrix (function of dataset)

- Vector $\overline{x}$ and matrix X are subject to stochastic optimization:

$$\min_{\overline{x}, X \in \mathcal{X}} \quad \mathbb{E}\left[c^\top(\overline{x} + X\zeta)\right]$$
$$\text{s.t.} \quad \Pr\left[b - A(\overline{x} + X\zeta) \in \mathcal{K}\right] \geqslant 1 - \eta$$

  - Minimize expected cost
  - Chance constraint to **guarantee feasibility**
  - $\mathcal{X}$ for data-independent query perturbation

- For example, an **identity query** perturbation is data-independent when

$$\mathcal{X} = \{X | X = \text{diag}[\mathbb{1}]\},$$

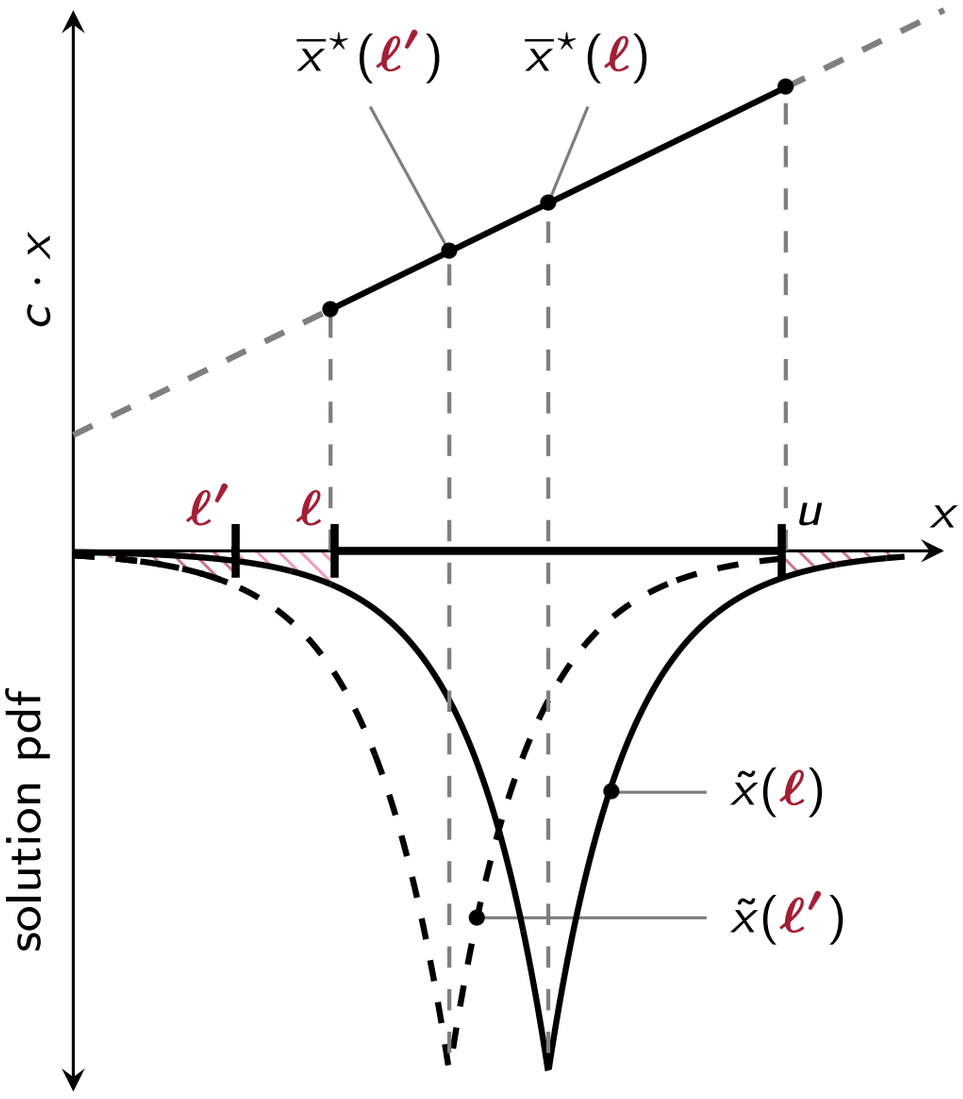
such that the identity query release takes the form

$$\tilde{x}(\mathcal{D}) = \overline{x}^\star(\mathcal{D}) + X^\star(\mathcal{D})\zeta = \overline{x}^\star(\mathcal{D}) + \zeta$$

Linear programming example (continued)

$$\begin{aligned} \min_{\overline{x}} \quad & \mathbb{E}\left[c \cdot (\overline{x} + \zeta)\right] \\ \text{s.t.} \quad & \Pr\left[\ell \leqslant \overline{x} + \zeta \leqslant u\right] \geqslant 1 - \eta, \end{aligned}$$

- Datum ℓ must be made indistinguishable from some adjacent value ℓ'
- Perturb. of $\overline{x}^\star$ is feasible with small prob.
- Sub-optimal due to feasibility requirement



We term this strategy **program perturbation**

Solution sensitivity Δ_α to $\alpha-$adjacent datasets

- How solution $x^\star(\mathcal{D})$ changes in $\mathcal{D}$?
- Non-convex, hierarchical problem
- Few special cases when Δ_α is known

$$\Delta_\alpha = \max_{\mathcal{D},\mathcal{D}' \in \mathbb{D}} \quad \|x^\star(\mathcal{D}) - x^\star(\mathcal{D}')\|_1$$
$$\text{s.t.} \quad \|\mathcal{D} - \mathcal{D}'\| \leqslant \alpha,$$

Sample-based solution from the robust optimization theory

$$\min_t \quad t$$
$$\text{s.t.} \quad \|x(\mathcal{D}_s) - x(\mathcal{D}'_s)\|_1 \leqslant t, \quad \forall s = 1, \ldots, S,$$

- Optimization in one variable t
- $(\mathcal{D}_s, \mathcal{D}'_s)$ is a pair of $\alpha-$adjacent datasets sampled from $\mathbb{D}$
- Minimum sample size requirement S to statistically lower bound Δ_α

Theorem (w.c. solution sensitivity Δ_α to $\alpha-$adjacent datasets)

With probability $(1-\gamma)$ and confidence level $(1-\beta)$, if the sample size

$$S \geqslant 1/(\gamma\beta) - 1,$$

the worst-case sensitivity of $x(\cdot)$ to $\alpha-$adjacent datasets will not exceed $t^\star$

Solution sensitivity Δ_α to $\alpha-$adjacent datasets

- How solution $x^\star(\mathcal{D})$ changes in $\mathcal{D}$?
- Non-convex, hierarchical problem
- Few special cases when Δ_α is known

$$\Delta_\alpha = \max_{\mathcal{D},\mathcal{D}' \in \mathbb{D}} \quad \|x^\star(\mathcal{D}) - x^\star(\mathcal{D}')\|_1$$
$$\text{s.t.} \quad \|\mathcal{D} - \mathcal{D}'\| \leqslant \alpha,$$

Sample-based solution from the robust optimization theory

$$\min_t \quad t$$
$$\text{s.t.} \quad \|x(\mathcal{D}_s) - x(\mathcal{D}'_s)\|_1 \leqslant t, \quad \forall s = 1, \ldots, S,$$

- Optimization in one variable t
- $(\mathcal{D}_s, \mathcal{D}'_s)$ is a pair of $\alpha-$adjacent datasets sampled from $\mathbb{D}$
- Minimum sample size requirement S to statistically lower bound Δ_α

Theorem (w.c. solution sensitivity Δ_α to $\alpha-$adjacent datasets)

With probability $(1-\gamma)$ and confidence level $(1-\beta)$, if the sample size

$$S \geqslant 1/(\gamma\beta) - 1,$$

the worst-case sensitivity of $x(\cdot)$ to $\alpha-$adjacent datasets will not exceed $t^\star$

Solution sensitivity Δ_α to $\alpha-$adjacent datasets

- How solution $x^\star(\mathcal{D})$ changes in $\mathcal{D}$?
- Non-convex, hierarchical problem
- Few special cases when Δ_α is known

$$\Delta_\alpha = \max_{\mathcal{D},\mathcal{D}' \in \mathbb{D}} \quad \|x^\star(\mathcal{D}) - x^\star(\mathcal{D}')\|_1$$
$$\text{s.t.} \quad \|\mathcal{D} - \mathcal{D}'\| \leqslant \alpha,$$

Sample-based solution from the robust optimization theory

$$\min_t \quad t$$
$$\text{s.t.} \quad \|x(\mathcal{D}_s) - x(\mathcal{D}'_s)\|_1 \leqslant t, \quad \forall s = 1, \ldots, S,$$

- Optimization in one variable t
- $(\mathcal{D}_s, \mathcal{D}'_s)$ is a pair of $\alpha-$adjacent datasets sampled from $\mathbb{D}$
- Minimum sample size requirement S to statistically lower bound Δ_α

Theorem (w.c. solution sensitivity Δ_α to $\alpha-$adjacent datasets)

With probability $(1-\gamma)$ and confidence level $(1-\beta)$, if the sample size

$$S \geqslant 1/(\gamma\beta) - 1,$$

the worst-case sensitivity of $x(\cdot)$ to $\alpha-$adjacent datasets will not exceed $t^\star$

Differential privacy guarantee for identity queries

Theorem ($\varepsilon-$DP identity query)

Calibrate $\zeta \sim \text{Lap}(\Delta_\alpha/\varepsilon)$ to the w.c. sensitivity Δ_α of the identity query to $\alpha-$adjacent optimization datasets. If the stochastic program returns the optimal solution on dataset $\mathcal{D}$, the identity query is $\varepsilon-$DP, i.e.,

$$\Pr[\overline{x}^\star(\mathcal{D}) + X(\mathcal{D})^\star \zeta = \hat{x}] \leqslant \Pr[\overline{x}^\star(\mathcal{D}') + X^\star(\mathcal{D}')\zeta = \hat{x}]\exp(\varepsilon).$$

for all $\hat{x}$ in the query's range.

$$\frac{\Pr[\overline{x}^\star(\mathcal{D}) + X^\star(\mathcal{D})\zeta = \hat{x}]}{\Pr[\overline{x}^\star(\mathcal{D}') + X^\star(\mathcal{D}')\zeta = \hat{x}]} \overset{(\dagger)}{=} \frac{\Pr[\zeta = \hat{x} - \overline{x}^\star(\mathcal{D})]}{\Pr[\zeta = \hat{x} - \overline{x}^\star(\mathcal{D}')]} \overset{(\star)}{=} \frac{\prod_{i=1}^n \exp\left(-\frac{\varepsilon\|\hat{x}_i - \overline{x}_i^\star(\mathcal{D})\|_1}{\Delta_\alpha}\right)}{\prod_{i=1}^n \exp\left(-\frac{\varepsilon\|\hat{x}_i - \overline{x}_i^\star(\mathcal{D}')\|_1}{\Delta_\alpha}\right)}$$

$$= \prod_{i=1}^n \exp\left(\frac{\varepsilon\|\hat{x}_i - \overline{x}_i^\star(\mathcal{D}')\|_1 - \varepsilon\|\hat{x}_i - \overline{x}_i^\star(\mathcal{D})\|_1}{\Delta_\alpha}\right) \overset{(\$)}{\leqslant} \prod_{i=1}^n \exp\left(\frac{\varepsilon\|\overline{x}_i^\star(\mathcal{D}) - \overline{x}_i^\star(\mathcal{D}')\|_1}{\Delta_\alpha}\right)$$

$$= \exp\left(\frac{\varepsilon\|\overline{x}^\star(\mathcal{D}) - \overline{x}^\star(\mathcal{D}')\|_1}{\Delta_\alpha}\right) \overset{(\S)}{\leqslant} \exp\left(\frac{\varepsilon\Delta_\alpha}{\Delta_\alpha}\right) = \exp(\varepsilon)$$

- $(\dagger)$ Per query-specific set $\mathcal{X}$
- $(\star)$ Per definition of Laplace's PDF
- $(\$)$ Per reverse inequality of norms
- $(\S)$ Per definition of sensitivity Δ_α

Differential privacy guarantee for identity queries

Theorem ($\varepsilon-$DP identity query)

Calibrate $\zeta \sim \text{Lap}(\Delta_\alpha/\varepsilon)$ to the w.c. sensitivity Δ_α of the identity query to $\alpha-$adjacent optimization datasets. If the stochastic program returns the optimal solution on dataset $\mathcal{D}$, the identity query is $\varepsilon-$DP, i.e.,

$$\Pr[\overline{x}^\star(\mathcal{D}) + X(\mathcal{D})^\star \zeta = \hat{x}] \leqslant \Pr[\overline{x}^\star(\mathcal{D}') + X^\star(\mathcal{D}')\zeta = \hat{x}]\exp(\varepsilon).$$

for all $\hat{x}$ in the query's range.

$$\frac{\Pr[\overline{x}^\star(\mathcal{D}) + X^\star(\mathcal{D})\zeta = \hat{x}]}{\Pr[\overline{x}^\star(\mathcal{D}') + X^\star(\mathcal{D}')\zeta = \hat{x}]} \overset{(\dagger)}{=} \frac{\Pr[\zeta = \hat{x} - \overline{x}^\star(\mathcal{D})]}{\Pr[\zeta = \hat{x} - \overline{x}^\star(\mathcal{D}')]} \overset{(\star)}{=} \frac{\prod_{i=1}^n \exp\left(-\frac{\varepsilon\|\hat{x}_i - \overline{x}_i^\star(\mathcal{D})\|_1}{\Delta_\alpha}\right)}{\prod_{i=1}^n \exp\left(-\frac{\varepsilon\|\hat{x}_i - \overline{x}_i^\star(\mathcal{D}')\|_1}{\Delta_\alpha}\right)}$$

$$= \prod_{i=1}^n \exp\left(\frac{\varepsilon\|\hat{x}_i - \overline{x}_i^\star(\mathcal{D}')\|_1 - \varepsilon\|\hat{x}_i - \overline{x}_i^\star(\mathcal{D})\|_1}{\Delta_\alpha}\right) \overset{(\$)}{\leqslant} \prod_{i=1}^n \exp\left(\frac{\varepsilon\|\overline{x}_i^\star(\mathcal{D}) - \overline{x}_i^\star(\mathcal{D}')\|_1}{\Delta_\alpha}\right)$$

$$= \exp\left(\frac{\varepsilon\|\overline{x}^\star(\mathcal{D}) - \overline{x}^\star(\mathcal{D}')\|_1}{\Delta_\alpha}\right) \overset{(\S)}{\leqslant} \exp\left(\frac{\varepsilon\Delta_\alpha}{\Delta_\alpha}\right) = \exp(\varepsilon)$$

- $(\dagger)$ Per query-specific set $\mathcal{X}$
- $(\star)$ Per definition of Laplace's PDF
- $(\$)$ Per reverse inequality of norms
- $(\S)$ Per definition of sensitivity Δ_α

Controlling sub-optimality w.r.t. non-private solution

- Privacy-preserving perturbation results in sub-optimality
- For a generic loss function $\ell(\cdot)$, the sub-optimality w.r.t. non-private solution is

$$\mathbb{E}\Big[\|\ell(\overline{x}^\star + X^\star\zeta) - \ell(x^\star)\|\Big] = \mathbb{E}\Big[\ell(\overline{x}^\star + X^\star\zeta)\Big] - \ell(x^\star)$$

since $\ell(x^\star)$ is the global optimum.

- We thus guarantee the minimum sub-optimality in expectation
- To guarantee the worst case performance, we adopt Conditional Value-at-Risk

$$\mathrm{CVaR}_{1-q}\left[\ell(\overline{x}^\star + X^\star\zeta)\right] = \frac{1}{1-q}\int_{1-q}^{1} \mathrm{VaR}_\beta\left[\ell(\overline{x}^\star + X^\star\zeta)\right] d\beta,$$

which is the expected value across the $q\%$ of the worst-case scenarios

Controlling sub-optimality w.r.t. non-private solution

- Privacy-preserving perturbation results in sub-optimality
- For a generic loss function $\ell(\cdot)$, the sub-optimality w.r.t. non-private solution is

$$\mathbb{E}\Big[\|\ell(\overline{x}^\star + X^\star\zeta) - \ell(x^\star)\|\Big] = \mathbb{E}\Big[\ell(\overline{x}^\star + X^\star\zeta)\Big] - \ell(x^\star)$$

since $\ell(x^\star)$ is the global optimum.

- We thus guarantee the minimum sub-optimality in expectation
- To guarantee the worst case performance, we adopt Conditional Value-at-Risk

$$\text{CVaR}_{1-q}\left[\ell(\overline{x}^\star + X^\star\zeta)\right] = \frac{1}{1-q}\int_{1-q}^{1} \text{VaR}_\beta\left[\ell(\overline{x}^\star + X^\star\zeta)\right] d\beta,$$

which is the expected value across the $q\%$ of the worst-case scenarios

Applications of private convex optimization

(LP) Private optimal power flow problem

(QP) Private monotone wind power curve fitting

(QP) Private power system security classification

(SDP) Private robust uncertainty set construction

Private optimal power flow (OPF) problem

$$
\begin{aligned}
\min_{\overline{x}, X \in \mathcal{X}} \quad & \mathbb{E}[c^\top(\overline{x} + X\zeta)] && \text{expected generation cost} \\
\text{s.t.} \quad & \mathbb{1}^\top(\overline{x} + X\zeta - \boldsymbol{d}) = 0 && \text{perturbed power balance} \\
& \Pr\begin{bmatrix} |F(\overline{x} + X\zeta - \boldsymbol{d})| \leqslant f^{\max} \\ x^{\min} \leqslant \overline{x} + X\zeta \leqslant x^{\max} \end{bmatrix} \geqslant 1 - \eta && \text{stochastic network limits}
\end{aligned}
$$

- Load vector $\boldsymbol{d}$ is private information
- Must be indistinguishable from any $\alpha-$adjacent load vector $\boldsymbol{d'}$ (in MWh)

- Queries in electricity markets
  - System costs (objective function)
  - Generation by a particular technology

Private optimal power flow (OPF) problem

$$\begin{aligned}
\min_{\overline{x}, X \in \mathcal{X}} \quad & \mathbb{E}[c^\top(\overline{x} + X\zeta)] && \text{expected generation cost} \\
\text{s.t.} \quad & \mathbb{1}^\top(\overline{x} + X\zeta - \boldsymbol{d}) = 0 && \text{perturbed power balance} \\
& \Pr\begin{bmatrix} |F(\overline{x} + X\zeta - \boldsymbol{d})| \leqslant f^{\max} \\ x^{\min} \leqslant \overline{x} + X\zeta \leqslant x^{\max} \end{bmatrix} \geqslant 1 - \eta && \text{stochastic network limits}
\end{aligned}$$

- Load vector $\boldsymbol{d}$ is private information
- Must be indistinguishable from any $\alpha-$adjacent load vector $\boldsymbol{d'}$ (in MWh)

- Queries in electricity markets
- System costs (objective function)
- Generation by a particular technology

1−DP system cost query on the IEEE 24-Bus RTS

perturbation strategy	OPF infeasibility (%)			OPF sub-optimality (%)		
	$\alpha = 1$	$\alpha = 3$	$\alpha = 10$	$\alpha = 1$	$\alpha = 3$	$\alpha = 10$
input	51.5	49.9	50.3	0.0	0.1	0.0
output	52.7	51.5	48.8	0.0	0.0	0.1
program	0.1	0.1	0.1	1.7	5.1	17.1

Private optimal power flow (OPF) problem

$$
\begin{aligned}
\min_{\overline{x}, X \in \mathcal{X}} \quad & \mathbb{E}[c^\top(\overline{x} + X\zeta)] && \text{expected generation cost} \\
\text{s.t.} \quad & \mathbb{1}^\top(\overline{x} + X\zeta - \boldsymbol{d}) = 0 && \text{perturbed power balance} \\
& \Pr\begin{bmatrix} |F(\overline{x} + X\zeta - \boldsymbol{d})| \leqslant f^{\max} \\ x^{\min} \leqslant \overline{x} + X\zeta \leqslant x^{\max} \end{bmatrix} \geqslant 1 - \eta && \text{stochastic network limits}
\end{aligned}
$$

- Load vector $\boldsymbol{d}$ is private information
- Must be indistinguishable from any $\alpha-$adjacent load vector $\boldsymbol{d'}$ (in MWh)

- Queries in electricity markets
  - System costs (objective function)
  - Generation by a particular technology

1−DP system cost query on the IEEE 24-Bus RTS

perturbation strategy	OPF infeasibility (%)			OPF sub-optimality (%)		
	$\alpha = 1$	$\alpha = 3$	$\alpha = 10$	$\alpha = 1$	$\alpha = 3$	$\alpha = 10$
input → / ←	51.5	49.9	50.3	0.0	0.1	0.0
output → / ←	52.7	51.5	48.8	0.0	0.0	0.1
program	0.1	0.1	0.1	1.7	5.1	17.1

Private optimal power flow (OPF) problem

$$
\begin{aligned}
\min_{\overline{x}, X \in \mathcal{X}} \quad & \mathbb{E}[c^\top(\overline{x} + X\zeta)] && \text{expected generation cost} \\
\text{s.t.} \quad & \mathbb{1}^\top(\overline{x} + X\zeta - \boldsymbol{d}) = 0 && \text{perturbed power balance} \\
& \Pr\begin{bmatrix} |F(\overline{x} + X\zeta - \boldsymbol{d})| \leqslant f^{\max} \\ x^{\min} \leqslant \overline{x} + X\zeta \leqslant x^{\max} \end{bmatrix} \geqslant 1 - \eta && \text{stochastic network limits}
\end{aligned}
$$

- Load vector $\boldsymbol{d}$ is private information
- Must be indistinguishable from any $\alpha-$adjacent load vector $\boldsymbol{d'}$ (in MWh)

- Queries in electricity markets
  - System costs (objective function)
  - Generation by a particular technology

1−DP system cost query on the IEEE 24-Bus RTS

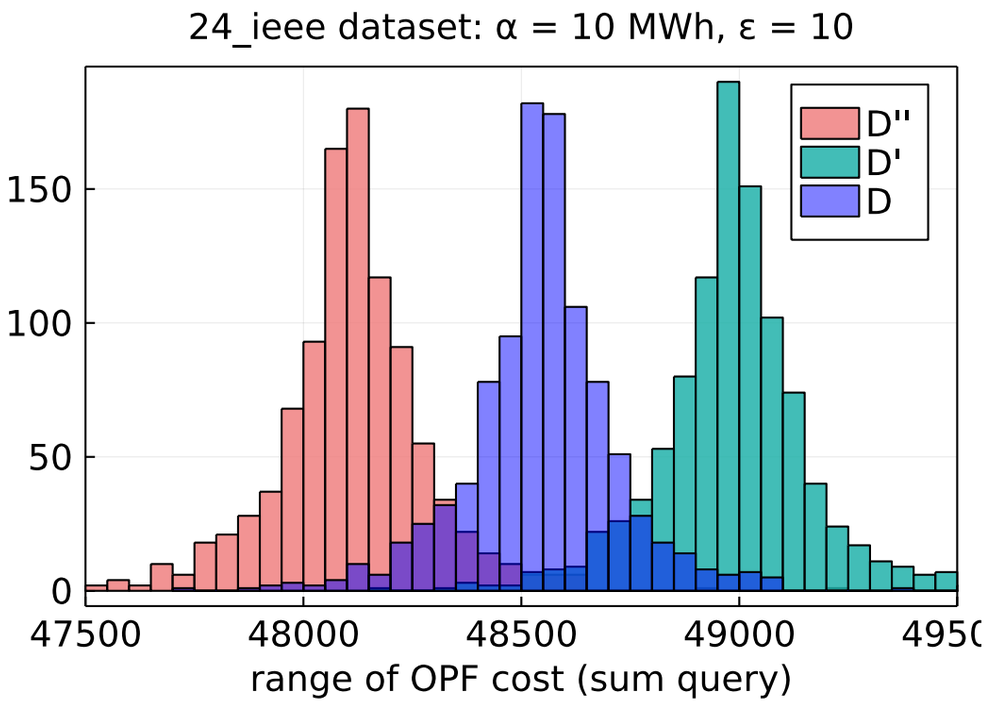
perturbation strategy	OPF infeasibility (%)			OPF sub-optimality (%)		
	$\alpha = 1$	$\alpha = 3$	$\alpha = 10$	$\alpha = 1$	$\alpha = 3$	$\alpha = 10$
input	51.5	49.9	50.3	0.0	0.1	0.0
output	52.7	51.5	48.8	0.0	0.0	0.1
program	0.1	0.1	0.1	1.7	5.1	17.1

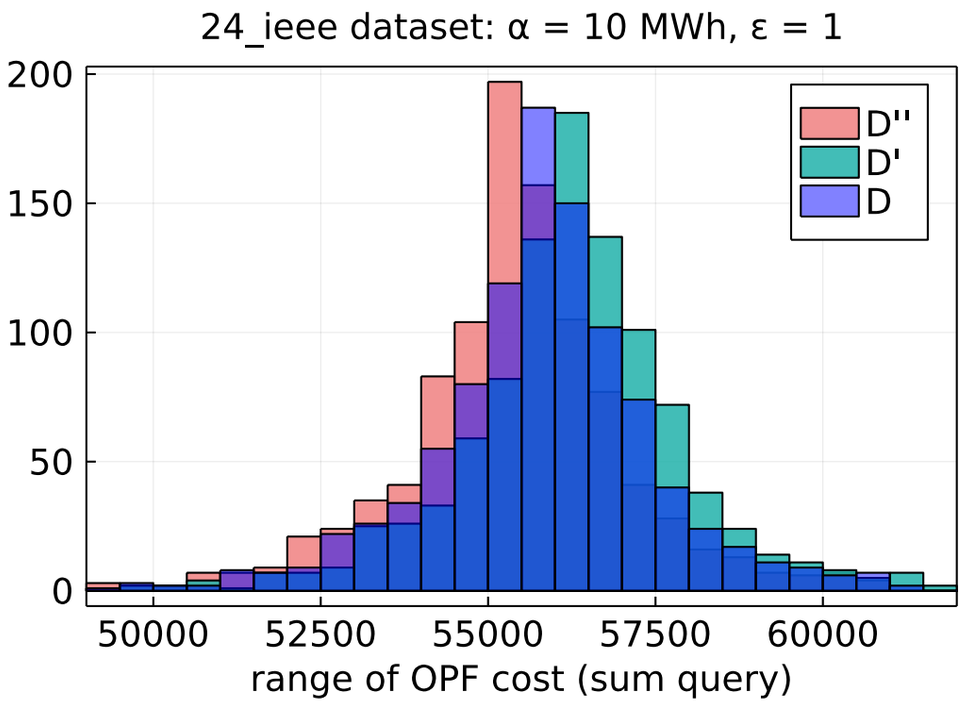
Private optimal power flow (OPF) problem

$$\begin{aligned}
\min_{\overline{x}, X \in \mathcal{X}} \quad & \mathbb{E}[c^\top(\overline{x} + X\zeta)] && \text{expected generation cost} \\
\text{s.t.} \quad & \mathbb{1}^\top(\overline{x} + X\zeta - \boldsymbol{d}) = 0 && \text{perturbed power balance} \\
& \Pr\begin{bmatrix} |F(\overline{x} + X\zeta - \boldsymbol{d})| \leqslant f^{\max} \\ x^{\min} \leqslant \overline{x} + X\zeta \leqslant x^{\max} \end{bmatrix} \geqslant 1 - \eta && \text{stochastic network limits}
\end{aligned}$$

- Load vector $\boldsymbol{d}$ is private information
- Must be indistinguishable from any $\alpha-$adjacent load vector $\boldsymbol{d'}$ (in MWh)

- Queries in electricity markets
  - System costs (objective function)
  - Generation by a particular technology





Private optimal power flow (OPF) problem

$$\begin{aligned}
\min_{\overline{x}, X \in \mathcal{X}} \quad & \mathbb{E}[c^\top(\overline{x} + X\zeta)] && \text{expected generation cost} \\
\text{s.t.} \quad & \mathbb{1}^\top(\overline{x} + X\zeta - \boldsymbol{d}) = 0 && \text{perturbed power balance} \\
& \Pr\begin{bmatrix} |F(\overline{x} + X\zeta - \boldsymbol{d})| \leqslant f^{\max} \\ x^{\min} \leqslant \overline{x} + X\zeta \leqslant x^{\max} \end{bmatrix} \geqslant 1 - \eta && \text{stochastic network limits}
\end{aligned}$$

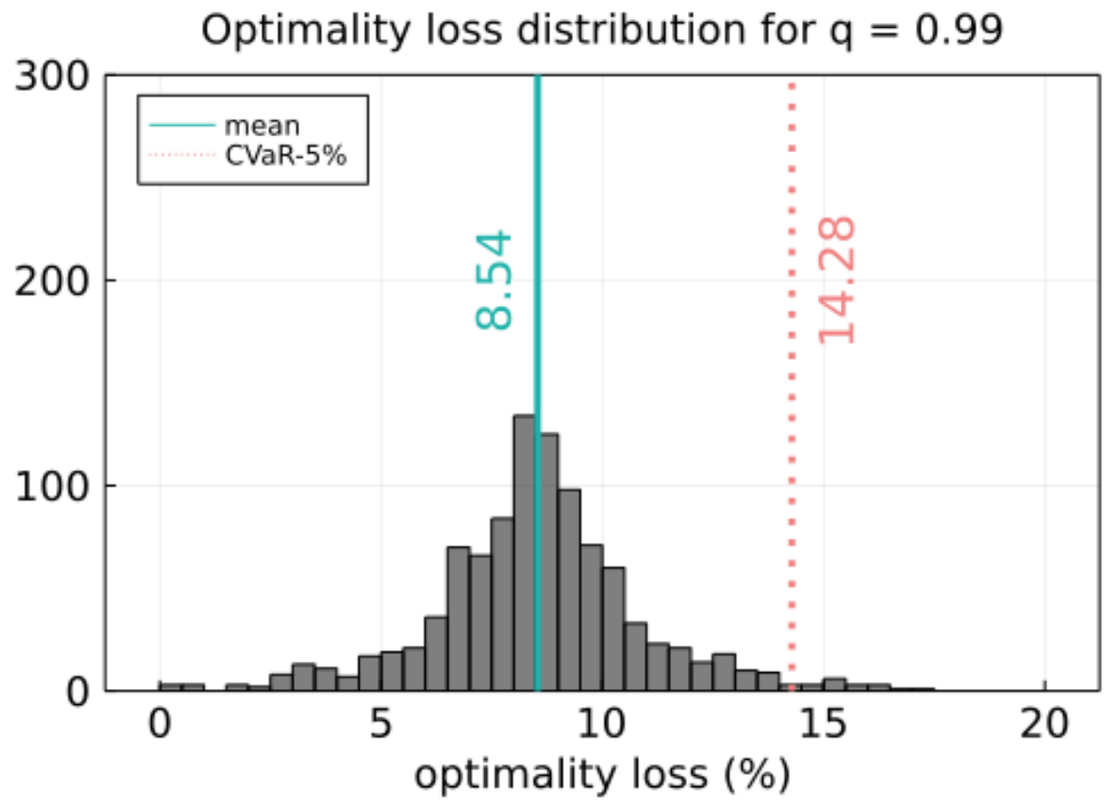
- Load vector $\boldsymbol{d}$ is private information
- Must be indistinguishable from any $\alpha-$adjacent load vector $\boldsymbol{d'}$ (in MWh)

- Query of an aggregated generation of 50% of units chosen at random
- Minimize the perturbed cost

$$\text{CVaR}_{1-q}\left[c^\top(\overline{x} + X\zeta)\right]$$

across q% of the worst case scenarios

- Queries in electricity markets
  - System costs (objective function)
  - Generation by a particular technology



Private monotone curve fitting

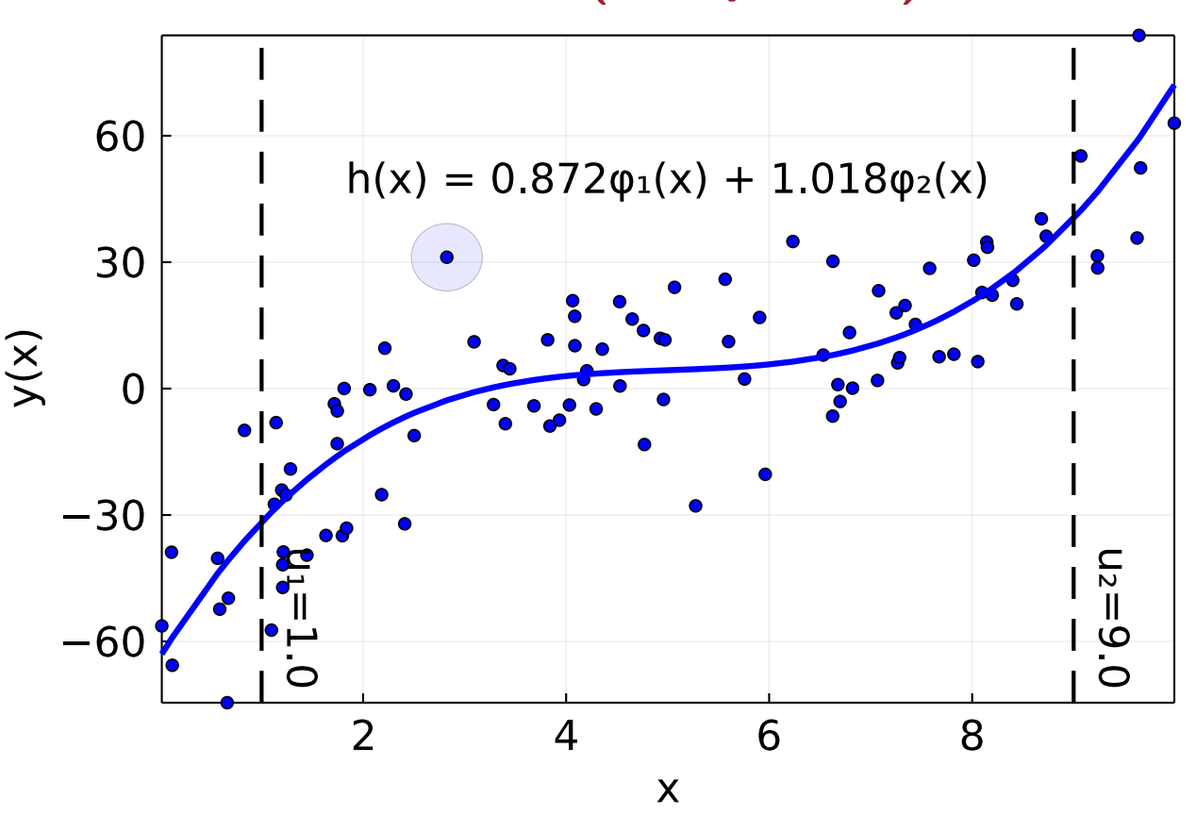
$$\min_{\beta} \quad \mathbb{E}\left[\sum_{i=1}^{n}\left(\underbrace{y_i - \varphi(x_i)^\top \beta}_{\text{business as usual}} \underbrace{-\varphi(x_i)^\top \zeta}_{\text{perturbation}}\right)^2\right]$$

$$\text{s.t.} \quad \mathbb{P}\left[C(\beta+\zeta) \geqslant \mathbb{0}\right] \geqslant 1-\eta,$$

- Dataset $\{(y_1, x_1), \ldots, (y_n, x_n)\}$
- Minimize regression loss function
- By finding optimal weights $\beta^\star$ ...
- ... of basis functions in vector $\varphi(x)$

- We want to make datasets indistinguishable in model weights $\beta^\star$ ...
- ... while preserving monotonic properties of the curve under perturbation

deterministic (non-private) solution



Private monotone curve fitting

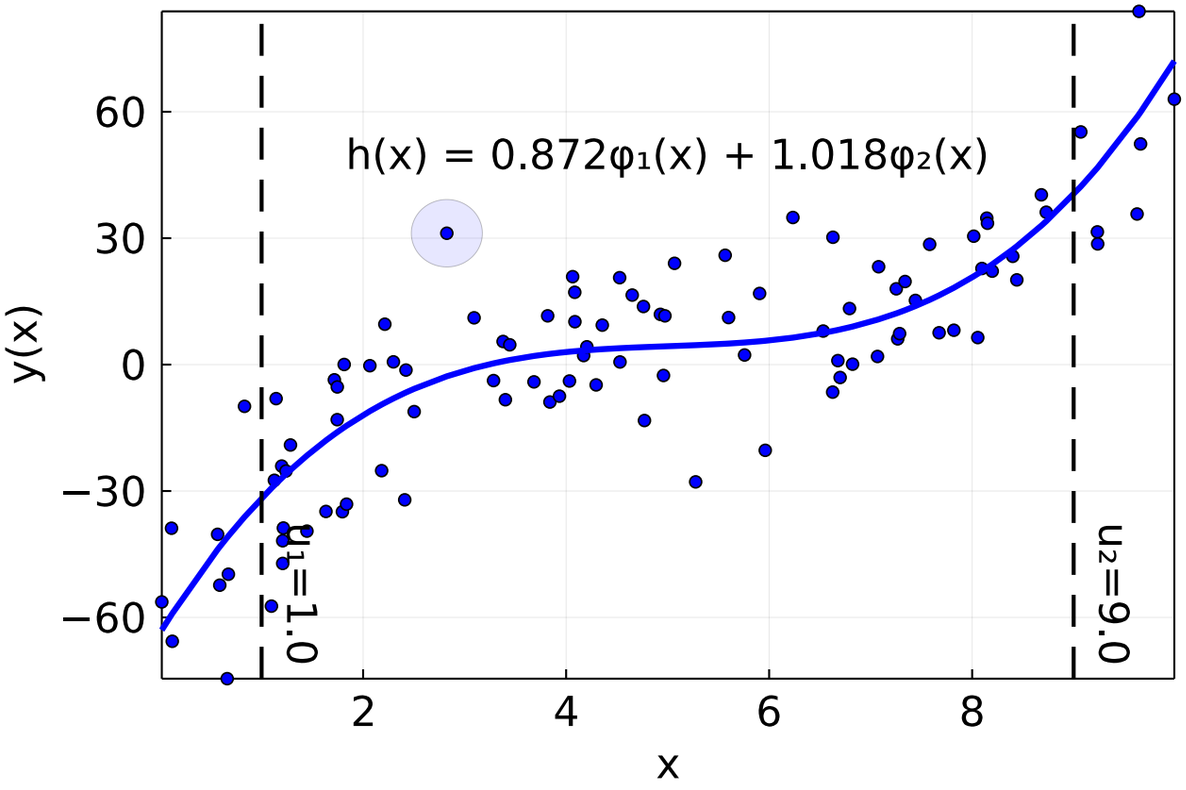
$$\min_{\beta} \quad \mathbb{E}\left[\sum_{i=1}^{n}\left(\underbrace{y_i - \varphi(x_i)^\top \beta}_{\text{business as usual}} \underbrace{-\varphi(x_i)^\top \zeta}_{\text{perturbation}}\right)^2\right]$$

$$\text{s.t.} \quad \mathbb{P}\left[C(\beta + \zeta) \geqslant \mathbb{0}\right] \geqslant 1 - \eta,$$

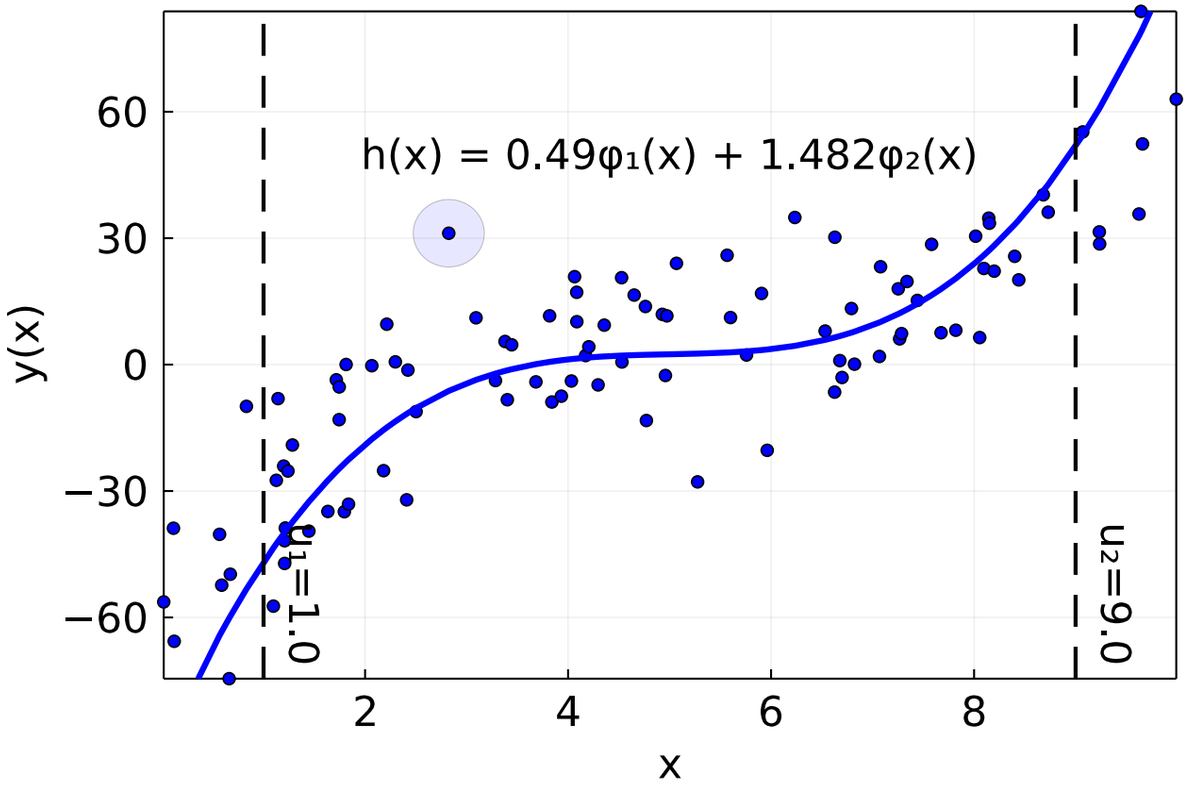
- Dataset $\{(y_1, x_1), \ldots, (y_n, x_n)\}$
- Minimize regression loss function
- By finding optimal weights $\beta^\star$ ...
- ... of basis functions in vector $\varphi(x)$

- We want to make datasets indistinguishable in model weights $\beta^\star$ ...
- ... while preserving monotonic properties of the curve under perturbation

deterministic (non-private) solution



stochastic (private) solution



Private monotone curve fitting

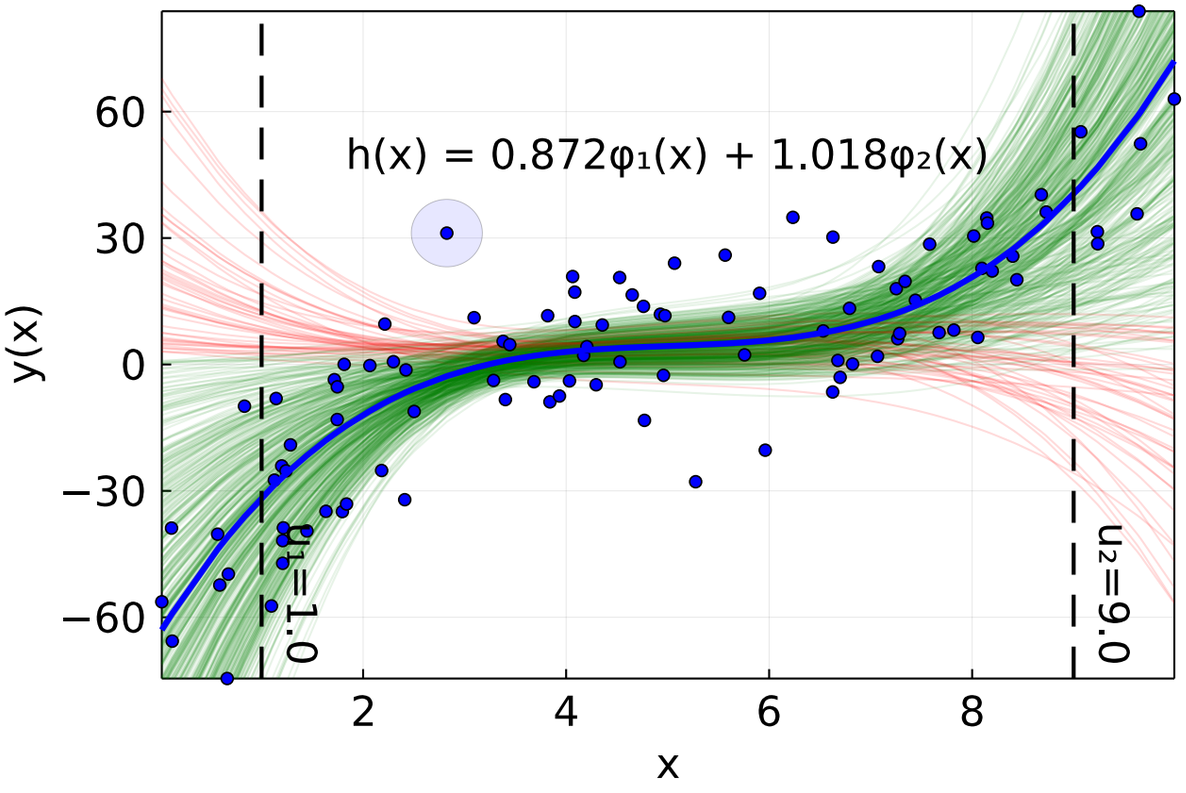
$$\min_{\beta} \quad \mathbb{E}\left[\sum_{i=1}^{n}\left(\underbrace{y_i - \varphi(x_i)^\top \beta}_{\text{business as usual}} \underbrace{-\varphi(x_i)^\top \zeta}_{\text{perturbation}}\right)^2\right]$$

$$\text{s.t.} \quad \mathbb{P}\left[C(\beta + \zeta) \geqslant \mathbb{0}\right] \geqslant 1 - \eta,$$

- Dataset $\{(y_1, x_1), \ldots, (y_n, x_n)\}$
- Minimize regression loss function
- By finding optimal weights $\beta^\star$ ...
- ... of basis functions in vector $\varphi(x)$

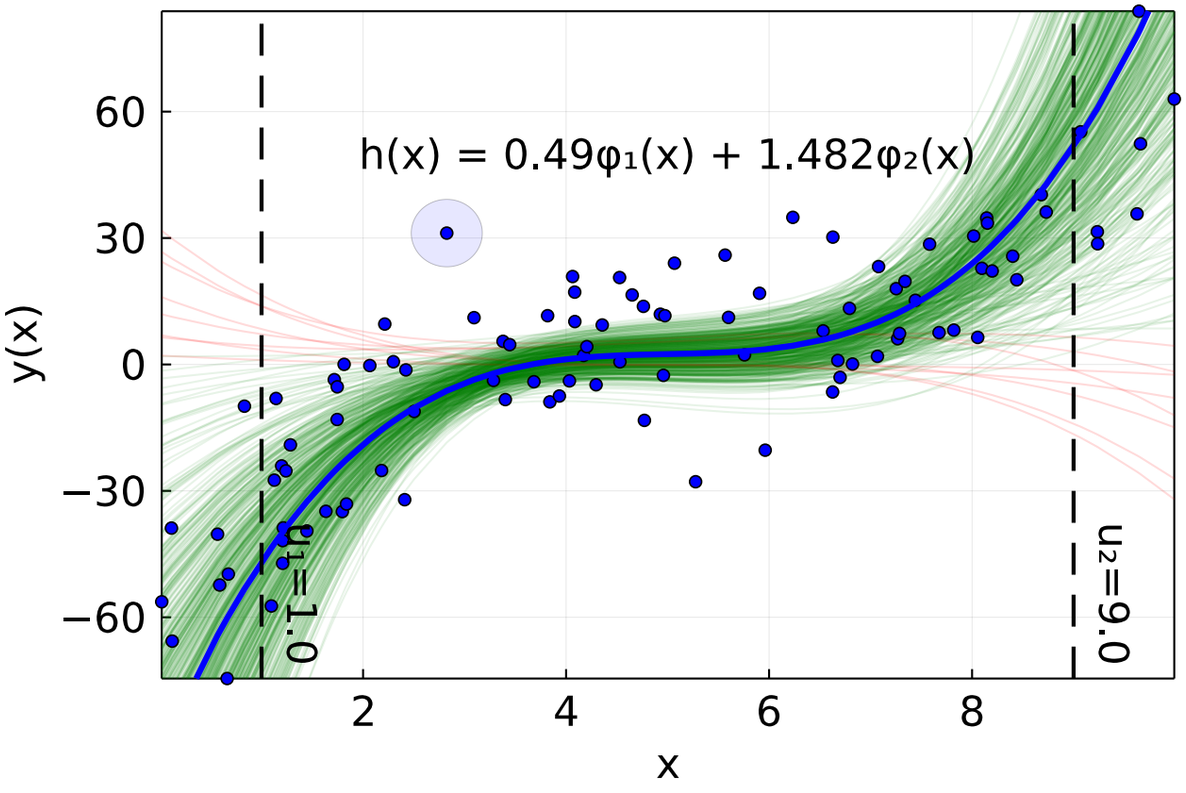
- We want to make datasets indistinguishable in model weights $\beta^\star$ ...
- ... while preserving monotonic properties of the curve under perturbation

output perturbation strategy



infeasible curve with probability 9.8%

program perturbation strategy



infeasible curve with probability 1.3%

Private monotone curve fitting

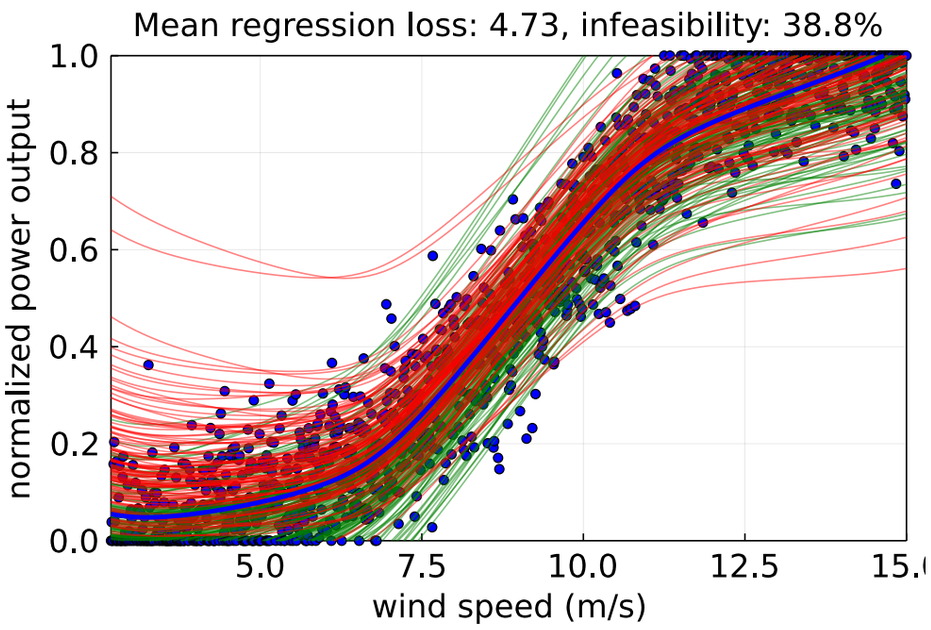
$$\min_{\beta} \quad \mathbb{E}\left[\sum_{i=1}^{n}\left(\underbrace{y_i - \varphi(x_i)^\top \beta}_{\text{business as usual}} \underbrace{-\varphi(x_i)^\top \zeta}_{\text{perturbation}}\right)^2\right]$$

$$\text{s.t.} \quad \mathbb{P}\left[C(\beta+\zeta) \geqslant \mathbb{0}\right] \geqslant 1-\eta,$$

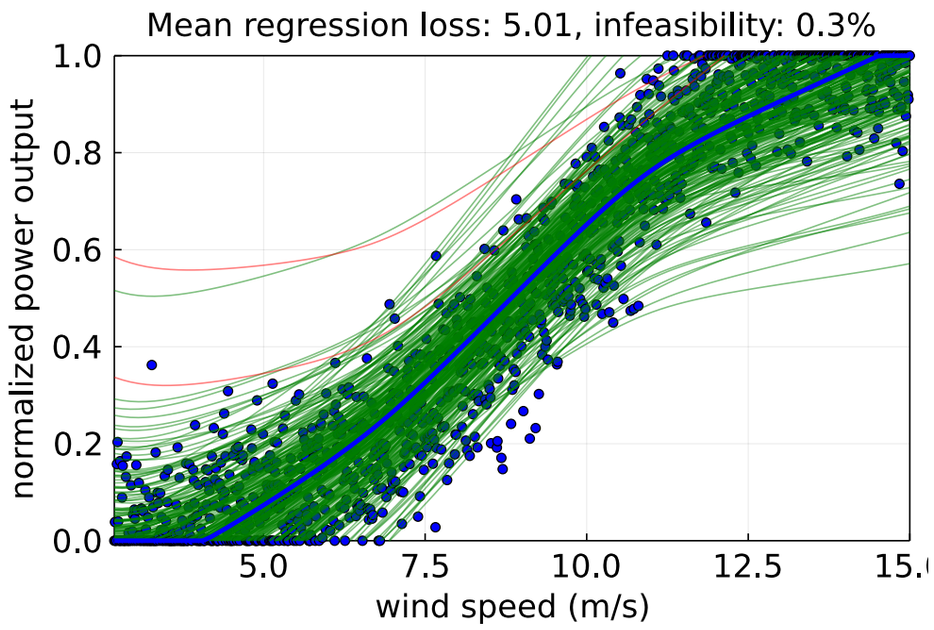
- Dataset $\{(y_1, x_1), \ldots, (y_n, x_n)\}$
- Minimize regression loss function
- By finding optimal weights $\beta^\star$ ...
- ... of basis functions in vector $\varphi(x)$

- We want to make datasets indistinguishable in model weights $\beta^\star$ ...
- ... while preserving monotonic properties of the curve under perturbation

Alstom.Eco.80



output perturbation



program perturbation

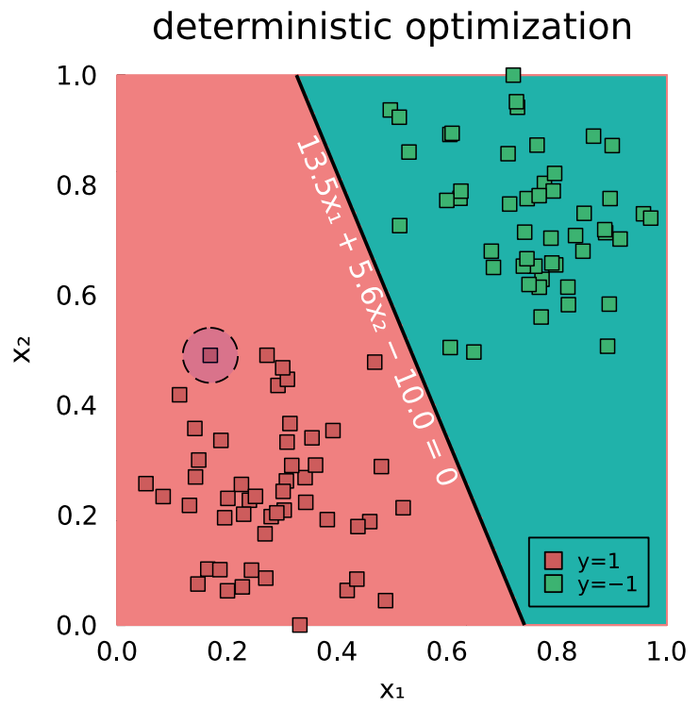
Private support vector machine (SVM) for classification

- Dataset $(x_1, y_1), \ldots, (x_m, y_m)$
- Feature $x_i \in \mathbb{R}^n$, label $y_i \in \{-1, 1\}$
- Computes a hyperplane $w^\top x_i - b$
- Classification rule $\text{sign}[w^{\star\top} \hat{x} - b^\star]$

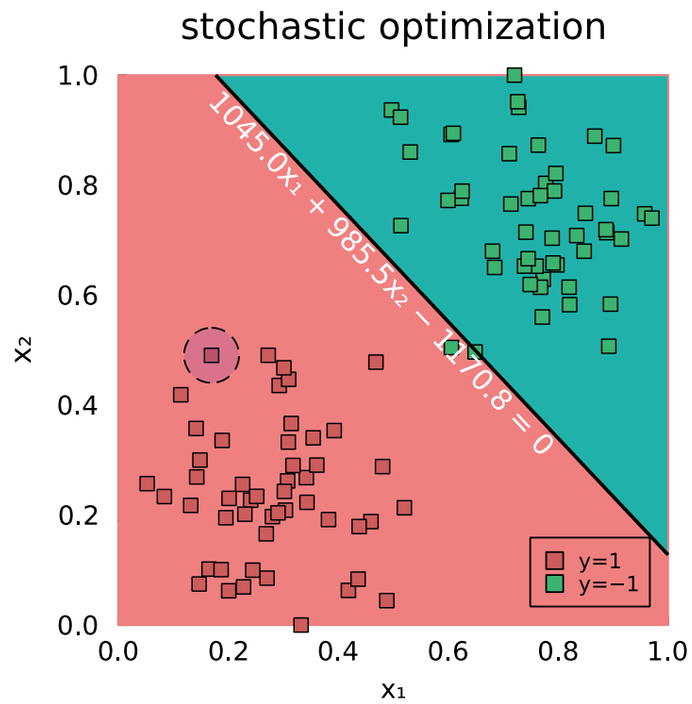
$$\min_{\tilde{b}(\zeta), \tilde{w}(\zeta), z} \quad \mathbb{E}\left[\lambda \|\overline{w}\|^2 + \tfrac{1}{m} \mathbb{1}^\top z + \lambda \|W\zeta\|^2\right]$$

$$\text{s.t. } \Pr\left[\begin{array}{l} y_i(\overline{w}^\top x_i - \overline{b}) \geqslant 1 - z_i - y_i((W\zeta)^\top x_i - B\zeta), \\ z_i \geqslant 0, \quad \forall i = 1, \ldots, m \end{array}\right] \geqslant 1 - \eta, \quad \begin{bmatrix} W \\ B \end{bmatrix} = \text{diag}[\mathbb{1}]$$

- Quering hyperplane parameters
- Deterministic hyperplane is very sensitive to perturbation
- Stochastic hyperplane, in contrast, is very robust to perturbation



accuracy 99.4%



accuracy 98.0%

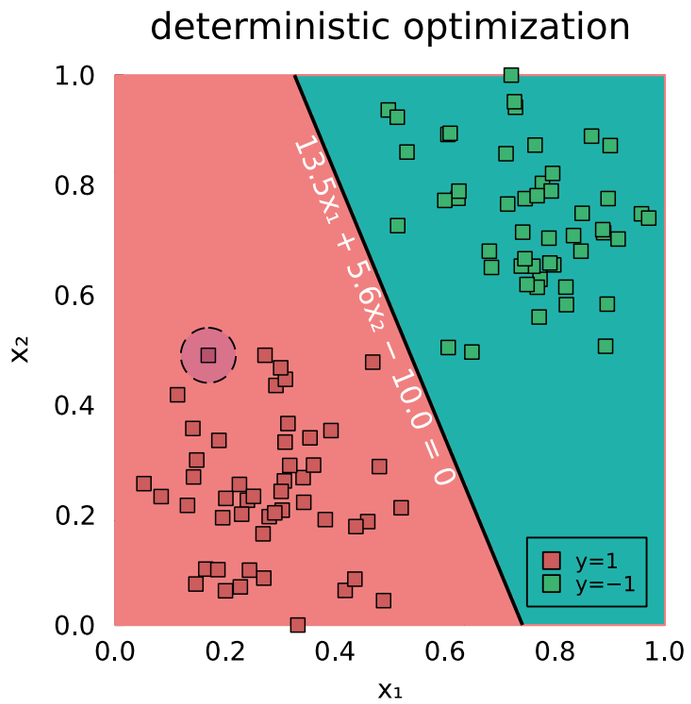
Private support vector machine (SVM) for classification

- Dataset $(x_1, y_1), \ldots, (x_m, y_m)$
- Feature $x_i \in \mathbb{R}^n$, label $y_i \in \{-1, 1\}$
- Computes a hyperplane $w^\top x_i - b$
- Classification rule $\text{sign}[w^{\star\top} \hat{x} - b^\star]$

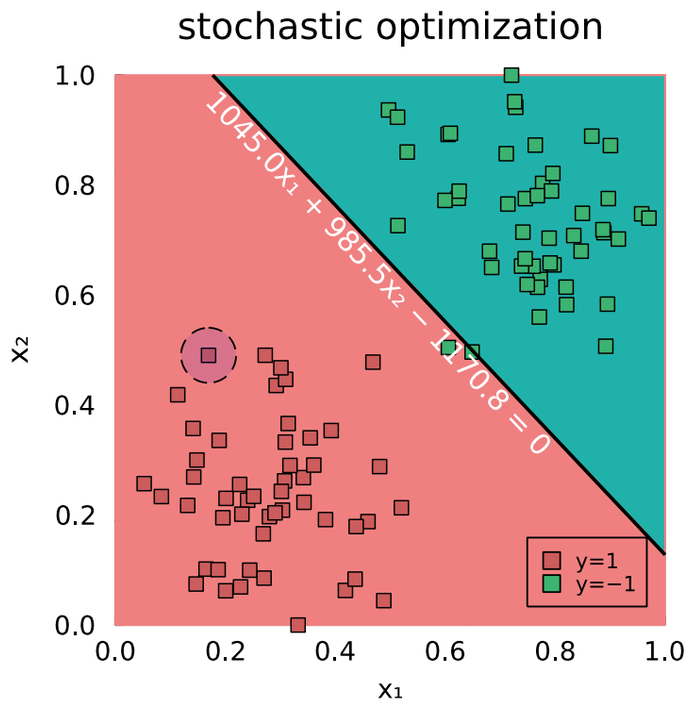
$$\min_{\tilde{b}(\zeta), \tilde{w}(\zeta), z} \quad \mathbb{E}\left[\lambda \|\overline{w}\|^2 + \tfrac{1}{m} \mathbb{1}^\top z + \lambda \|W\zeta\|^2\right]$$

$$\text{s.t. } \Pr\left[\begin{array}{l} y_i(\overline{w}^\top x_i - \overline{b}) \geqslant 1 - z_i - y_i((W\zeta)^\top x_i - B\zeta), \\ z_i \geqslant 0, \quad \forall i = 1, \ldots, m \end{array}\right] \geqslant 1 - \eta, \quad \begin{bmatrix} W \\ B \end{bmatrix} = \text{diag}[\mathbb{1}]$$

- Quering hyperplane parameters
- Deterministic hyperplane is very sensitive to perturbation
- Stochastic hyperplane, in contrast, is very robust to perturbation



accuracy 99.4%



accuracy 98.0%

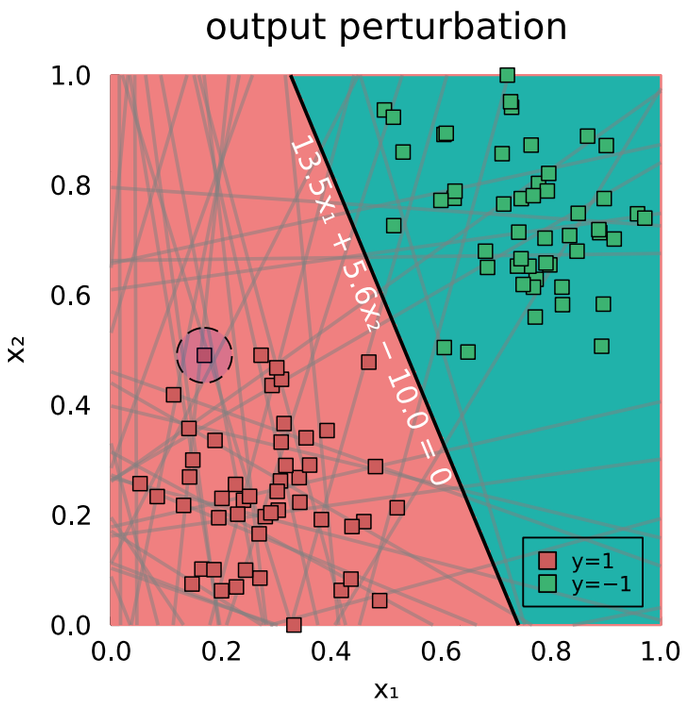
Private support vector machine (SVM) for classification

- Dataset $(x_1, y_1), \ldots, (x_m, y_m)$
- Feature $x_i \in \mathbb{R}^n$, label $y_i \in \{-1, 1\}$
- Computes a hyperplane $w^\top x_i - b$
- Classification rule $\text{sign}[w^{\star\top} \hat{x} - b^\star]$

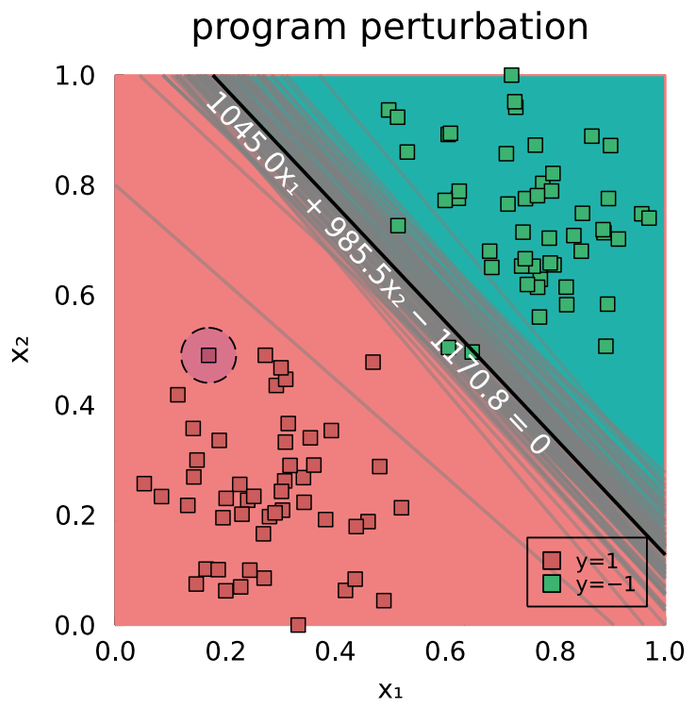
$$\min_{\tilde{b}(\zeta), \tilde{w}(\zeta), z} \quad \mathbb{E}\left[\lambda \|\overline{w}\|^2 + \tfrac{1}{m} \mathbb{1}^\top z + \lambda \|W\zeta\|^2\right]$$

$$\text{s.t. } \Pr\left[\begin{array}{l} y_i(\overline{w}^\top x_i - \overline{b}) \geqslant 1 - z_i - y_i((W\zeta)^\top x_i - B\zeta), \\ z_i \geqslant 0, \quad \forall i = 1, \ldots, m \end{array}\right] \geqslant 1 - \eta, \quad \begin{bmatrix} W \\ B \end{bmatrix} = \text{diag}[\mathbb{1}]$$

- Quering hyperplane parameters
- Deterministic hyperplane is very sensitive to perturbation
- Stochastic hyperplane, in contrast, is very robust to perturbation



mean accuracy 51.2%



mean accuracy 97.6%

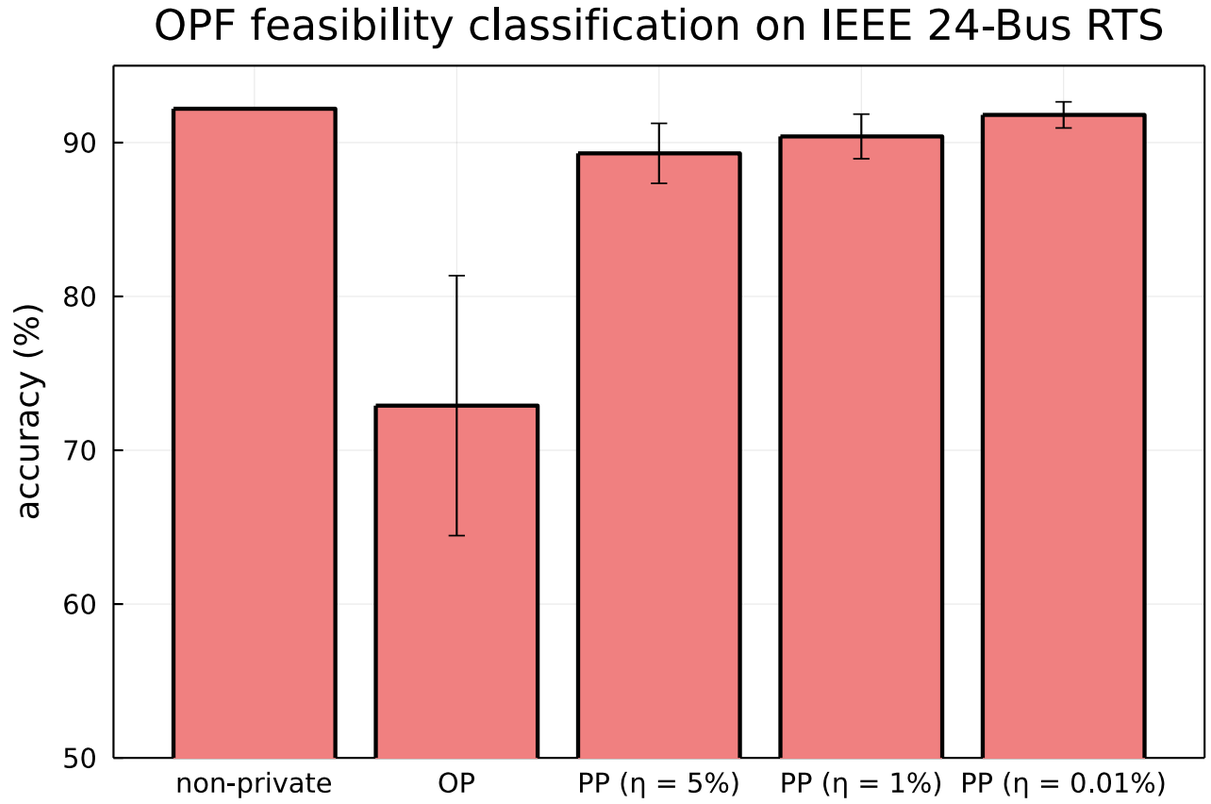
Private support vector machine (SVM) for classification

- Dataset $(x_1, y_1), \ldots, (x_m, y_m)$
- Feature $x_i \in \mathbb{R}^n$, label $y_i \in \{-1, 1\}$
- Computes a hyperplane $w^\top x_i - b$
- Classification rule $\text{sign}[w^{\star\top} \hat{x} - b^\star]$

$$\min_{\tilde{b}(\zeta), \tilde{w}(\zeta), z} \quad \mathbb{E}\left[\lambda \|\overline{w}\|^2 + \tfrac{1}{m} \mathbb{1}^\top z + \lambda \|W\zeta\|^2\right]$$

$$\text{s.t. } \Pr\left[\begin{array}{l} y_i(\overline{w}^\top x_i - \overline{b}) \geqslant 1 - z_i - y_i((W\zeta)^\top x_i - B\zeta), \\ z_i \geqslant 0, \quad \forall i = 1, \ldots, m \end{array}\right] \geqslant 1 - \eta, \quad \begin{bmatrix} W \\ B \end{bmatrix} = \text{diag}[\mathbb{1}]$$

- Load data to classify OPF feasibility
- Output perturbation (OP) accuracy:
  - Small mean value (72.9% vs. 92.2%)
  - Large standard deviation (16.9%)
- Program perturbation (PP) accuracy:
  - Close to non-private solution
  - Small standard deviation
  - Improves with tighter tolerance η to SVM constraint violations



Private inscribed ellipsoid fitting problem

Consider a bounded, non-empty polyhedral set:

$$\mathcal{U} = \left\{ x \in \mathbb{R}^n \;\middle|\; a_i^\top x \leqslant b_i,\ \forall i = 1, \ldots, m \right\}.$$

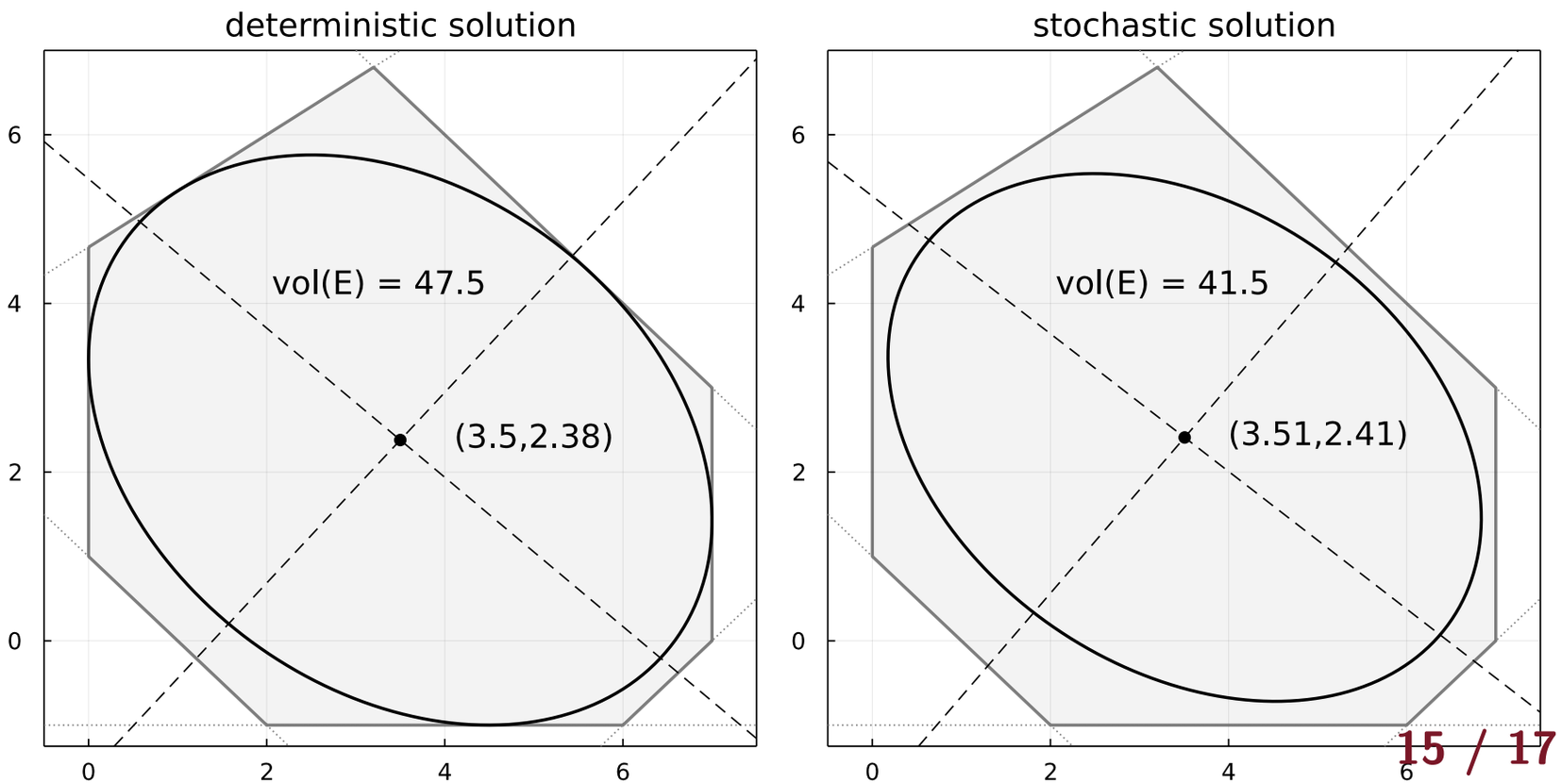
The maximum-volume inscribed ellipsoid

$$\mathcal{E} = \left\{ x = Yu + z \;\middle|\; \|u\| \leqslant 1 \right\}$$

where ellipsoid parameters Y and z are obtained by solving an SDP problem:

$$\begin{aligned} \max_{z, Y \succcurlyeq 0} \quad & \det[Y]^{\frac{1}{n}} \\ \text{s.t.} \quad & \|Ya_i\|_2 \leqslant b_i - a_i^\top z, \quad \forall i = 1, \ldots, m, \end{aligned}$$

- Program perturbation is sub-optimal w.r.t. $\mathrm{vol}(\mathcal{E})$
- Yet produces inscribed ellipsoids w.h.p.



Private inscribed ellipsoid fitting problem

Consider a bounded, non-empty polyhedral set:

$$\mathcal{U} = \left\{ x \in \mathbb{R}^n \;\middle|\; a_i^\top x \leqslant b_i,\ \forall i = 1, \ldots, m \right\}.$$

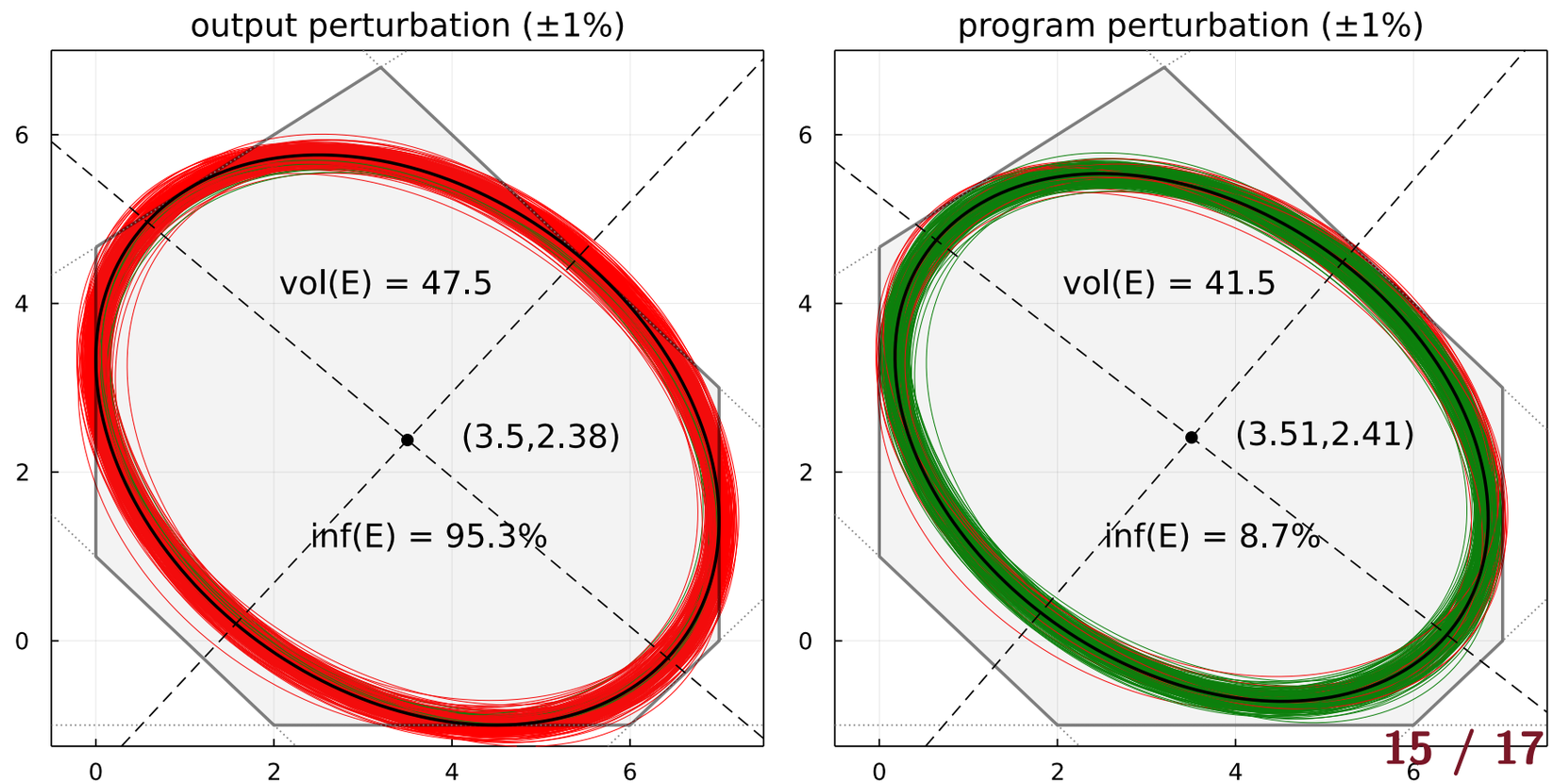
The maximum-volume inscribed ellipsoid

$$\mathcal{E} = \left\{ x = Yu + z \;\middle|\; \|u\| \leqslant 1 \right\}$$

where ellipsoid parameters Y and z are obtained by solving an SDP problem:

$$\begin{aligned} \max_{z, Y \succcurlyeq 0} \quad & \det[Y]^{\frac{1}{n}} \\ \text{s.t.} \quad & \|Ya_i\|_2 \leqslant b_i - a_i^\top z, \quad \forall i = 1, \ldots, m, \end{aligned}$$

- Program perturbation is sub-optimal w.r.t. $\mathrm{vol}(\mathcal{E})$
- Yet produces inscribed ellipsoids w.h.p.



Private inscribed ellipsoid fitting problem

Consider a bounded, non-empty polyhedral set:

$$\mathcal{U} = \left\{ x \in \mathbb{R}^n \;\middle|\; a_i^\top x \leqslant b_i,\ \forall i = 1, \ldots, m \right\}.$$

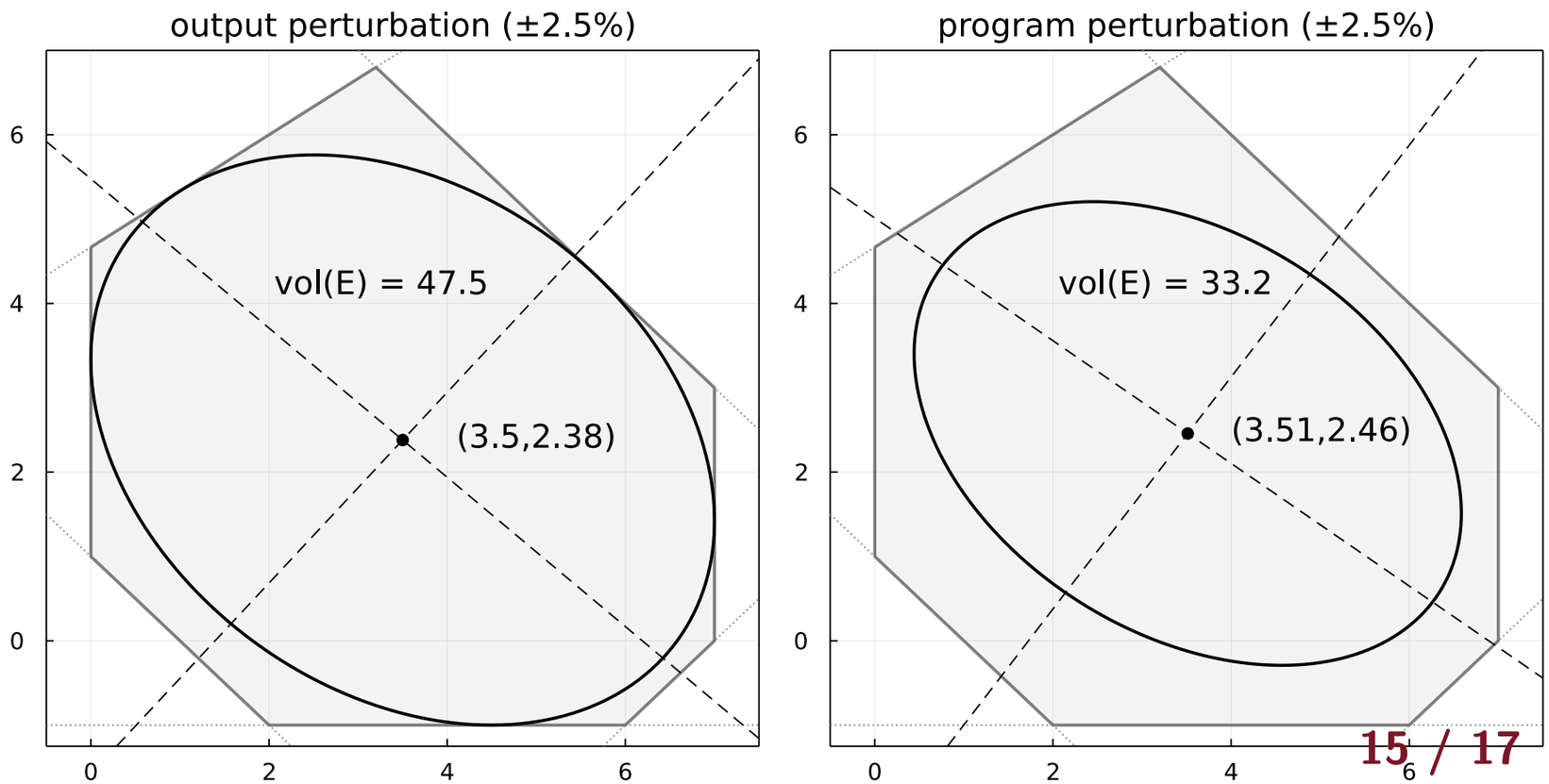
The maximum-volume inscribed ellipsoid

$$\mathcal{E} = \left\{ x = Yu + z \;\middle|\; \|u\| \leqslant 1 \right\}$$

where ellipsoid parameters Y and z are obtained by solving an SDP problem:

$$\begin{aligned} \max_{z, Y \succcurlyeq 0} \quad & \det[Y]^{\frac{1}{n}} \\ \text{s.t.} \quad & \|Ya_i\|_2 \leqslant b_i - a_i^\top z, \quad \forall i = 1, \ldots, m, \end{aligned}$$

- Program perturbation is sub-optimal w.r.t. vol($\mathcal{E}$)
- Yet produces inscribed ellipsoids w.h.p.



Private inscribed ellipsoid fitting problem

Consider a bounded, non-empty polyhedral set:

$$\mathcal{U} = \left\{ x \in \mathbb{R}^n \;\middle|\; a_i^\top x \leqslant b_i,\ \forall i = 1, \ldots, m \right\}.$$

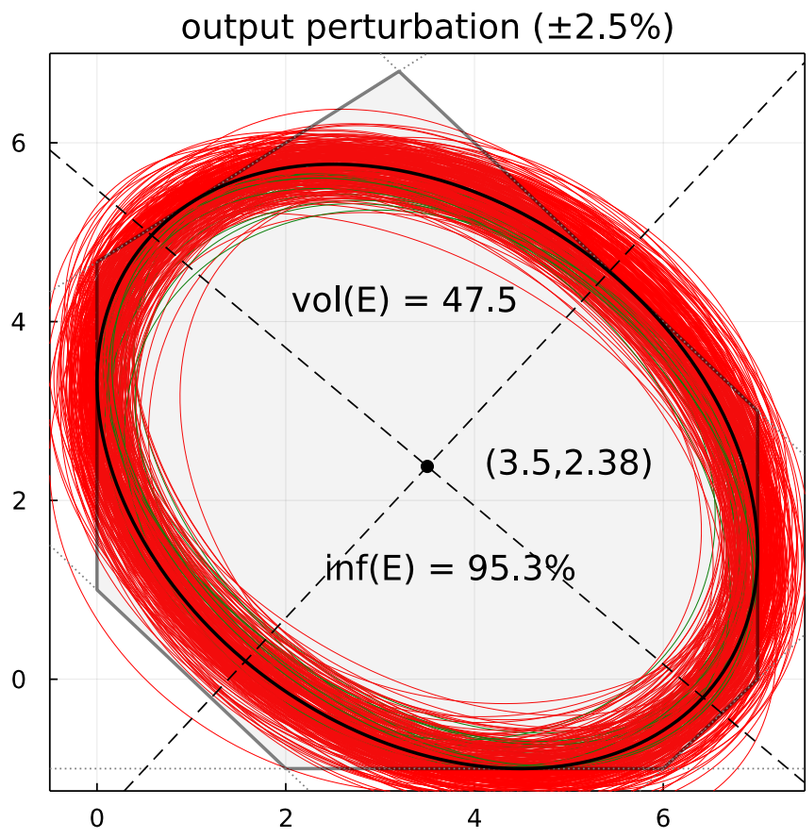
The maximum-volume inscribed ellipsoid

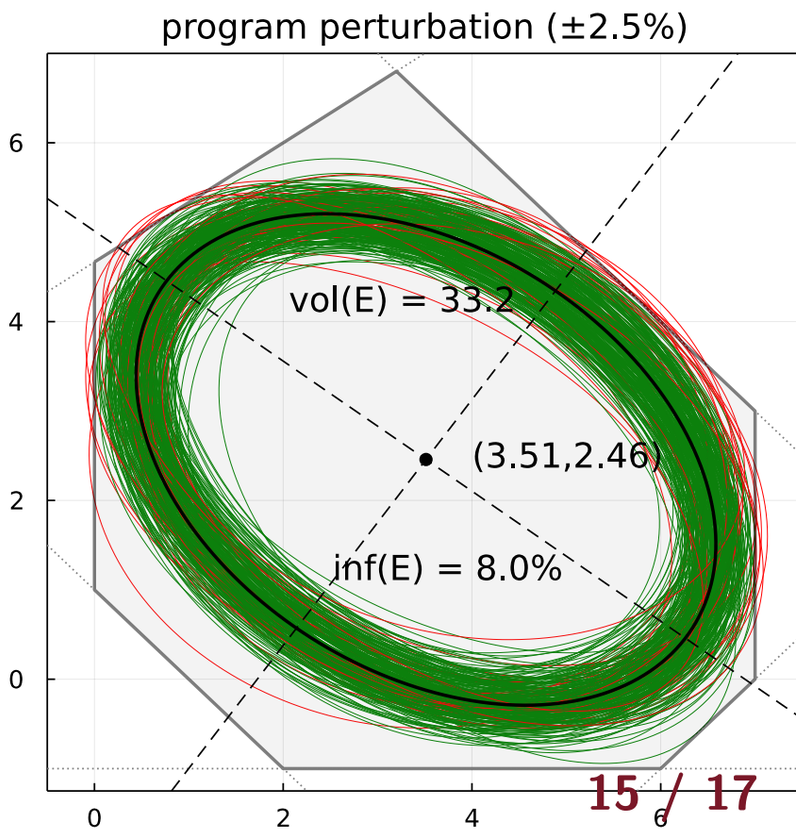
$$\mathcal{E} = \left\{ x = Yu + z \;\middle|\; \|u\| \leqslant 1 \right\}$$

where ellipsoid parameters Y and z are obtained by solving an SDP problem:

$$\begin{aligned} \max_{z, Y \succcurlyeq 0} \quad & \det[Y]^{\frac{1}{n}} \\ \text{s.t.} \quad & \|Ya_i\|_2 \leqslant b_i - a_i^\top z, \quad \forall i = 1, \ldots, m, \end{aligned}$$

- Program perturbation is sub-optimal w.r.t. vol($\mathcal{E}$)
- Yet produces inscribed ellipsoids w.h.p.





Conclusions

- New dimension of stochastic programming
  - Used to accommodate randomness of data
  - Now it provides data with algorithmic privacy
- Many results in stochastic programming directly apply
  - Feasibility guarantees (chance constraints)
  - Controllable cost of privacy (risk measures, e.g., CVaR)
- Formal privacy guarantees
  - Facilitating data sharing
  - Next-generation legal acts

Thank you for your attention!

Work in progress:

Dvorkin, V., Fioretto, F., Van Hentenryck, P., Kazempour, J. and Pinson, P.
Privacy-Preserving Perturbation of Convex Optimization Programs

References:

1. Dvorkin, V., Fioretto, F., Van Hentenryck, P., Kazempour, J. and Pinson, P.
   Differentially private convex optimization with feasibility guarantees
   Priprint, arXiv preprint arXiv:2006.12338.
2. Dvorkin, V., Fioretto, F., Van Hentenryck, P., Pinson, P. and Kazempour J.
   Differentially private optimal power flow for distribution grids
   IEEE Transactions on Power Systems, 2021
   Best 2019–2021 Paper Award
3. Dvorkin, V., Van Hentenryck, P., Kazempour, J. and Pinson P.
   Differentially private distributed optimal power flow
   2020 Conference on Decision and Control

Let's stay in touch:

DvorkinVladimir Vladimir-Dvorkin dvorkin@mit.edu