PRIVATE AND EFFICIENT ALGORITHM DESIGN FROM ROBUST ESTIMATORS

Mahbod Majid

CMU

PLAN

INTRO

STATISTICAL ESTIMATION

distribution: p_θ

samples: $X_1, \ldots, X_n \sim p_\theta$

STATISTICAL ESTIMATION

distribution: p_θ

samples: $X_1, \ldots, X_n \sim p_\theta$

estimator: $\hat{\theta}$

goal: $\|\theta - \hat{\theta}(X)\|$ **small**

STATISTICAL ESTIMATION

distribution: p_θ

samples: $X_1, \ldots, X_n \sim p_\theta$

estimator: $\hat{\theta}$

goal: $\|\theta - \hat{\theta}(X)\|$ **small**

1. robustness

works under η

fraction corruption

STATISTICAL ESTIMATION

distribution: p_θ

samples: $X_1, \ldots, X_n \sim p_\theta$

estimator: $\hat{\theta}$

goal: $\|\theta - \hat{\theta}(X)\|$ **small**

1. robustness
works under η
fraction corruption

2. privacy
changing a sample does not change the output distribution

EXPONENTIAL MECHANISM

EXPONENTIAL MECHANISM

score function

$$\text{score}(\theta; X)$$

EXPONENTIAL MECHANISM

score function

$$\text{score}(\theta; X)$$

low sensitivity

$$d_{\text{Ham}}(X, X') = 1 \implies |\,\text{score}(\theta, X) - \text{score}(\theta, X')\,| \leq 1$$

EXPONENTIAL MECHANISM

score function

$$\text{score}(\theta; X)$$

low sensitivity

$$d_{\text{Ham}}(X, X') = 1 \implies |\,\text{score}(\theta, X) - \text{score}(\theta, X')\,| \leq 1$$

sample

$$p(\theta) \propto \exp(-\varepsilon\ \text{score}(\theta; X))$$

ε-dp

EXPONENTIAL MECHANISM

INVERSE SENSITIVITY

good point detector

is (θ, X) a good pair?

EXPONENTIAL MECHANISM

INVERSE SENSITIVITY

good point detector

is (θ, X) a good pair?

low sensitivity score

$$\text{score}(\theta, X) = \min_{X'} \text{Ham}(X, X') \text{ such that } \theta \text{ is good for } X'$$

sensitivity 1

EXPONENTIAL MECHANISM

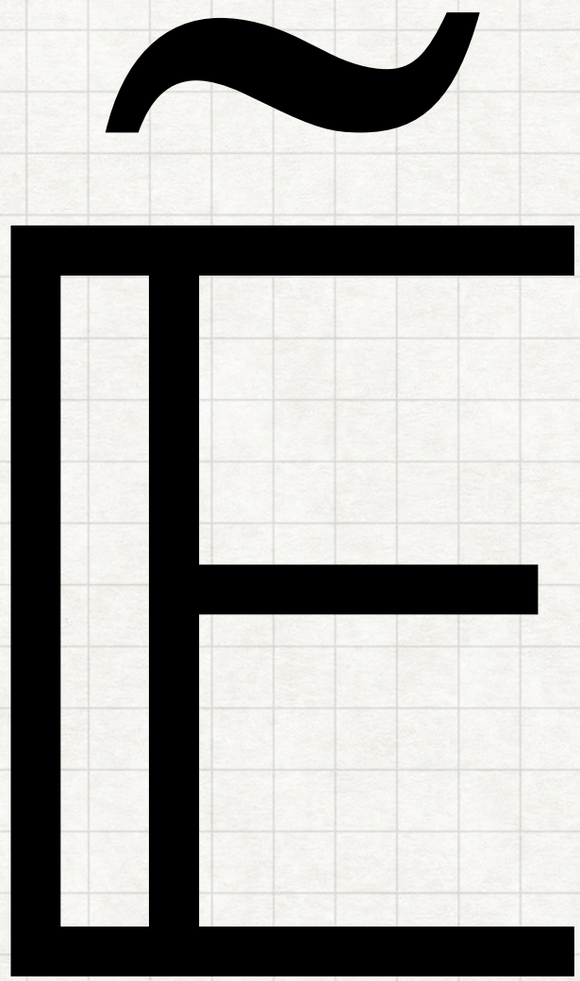
INVERSE SENSITIVITY

low sensitivity score

$$\text{score}(\theta, X) = \min_{X'} \text{Ham}(X, X') \text{ such that } \theta \text{ is good for } X'$$

key insight: inverse sensitivity exp mech outputs low scoring points when applied to robust estimators

EFFICIENCY



$\tilde{\mathbb{E}}$

a linear functional

$\tilde{\mathbb{E}}$: **polynomials** $\to \mathbb{R}$

$\tilde{\mathbb{E}}$

a linear functional

degree-d

$\tilde{\mathbb{E}}$: **polynomials** $\to \mathbb{R}$	$\tilde{\mathbb{E}}1 = 1$	$\tilde{\mathbb{E}}p^2(x) \geq 0$

$\tilde{\mathbb{E}}$

a linear functional

degree-d

$\tilde{\mathbb{E}} : \textbf{polynomials} \to \mathbb{R}$	$\tilde{\mathbb{E}}1 = 1$	$\tilde{\mathbb{E}}p^2(x) \geq 0$

$\vDash$

SATISFIES

$\tilde{\mathbb{E}}$

a linear functional

$\tilde{\mathbb{E}}$: **polynomials** $\to \mathbb{R}$

$\tilde{\mathbb{E}}1 = 1$

degree-d

$\tilde{\mathbb{E}}p^2(x) \geq 0$

$\models$

set of polynomial constraints

$A = \{p_i(x) \geq 0\}$

$$\tilde{\mathbb{E}}$$

a linear functional

$\tilde{\mathbb{E}}$: **polynomials** $\to \mathbb{R}$

$\tilde{\mathbb{E}}1 = 1$

degree-d

$\tilde{\mathbb{E}}p^2(x) \geq 0$

$$\vDash$$

set of polynomial constraints

$A = \{p_i(x) \geq 0\}$

degree-d

$$\tilde{\mathbb{E}} \vDash_d A \iff \tilde{\mathbb{E}} q^2(x) \prod_{i \in S} p_i(x) \geq 0$$

$\tilde{\mathbb{E}}$

a linear functional

$\tilde{\mathbb{E}}$: **polynomials** $\to \mathbb{R}$

$\tilde{\mathbb{E}}1 = 1$

degree-d

$\tilde{\mathbb{E}}p^2(x) \geq 0$

$\models$

set of polynomial constraints

$A = \{p_i(x) \geq 0\}$

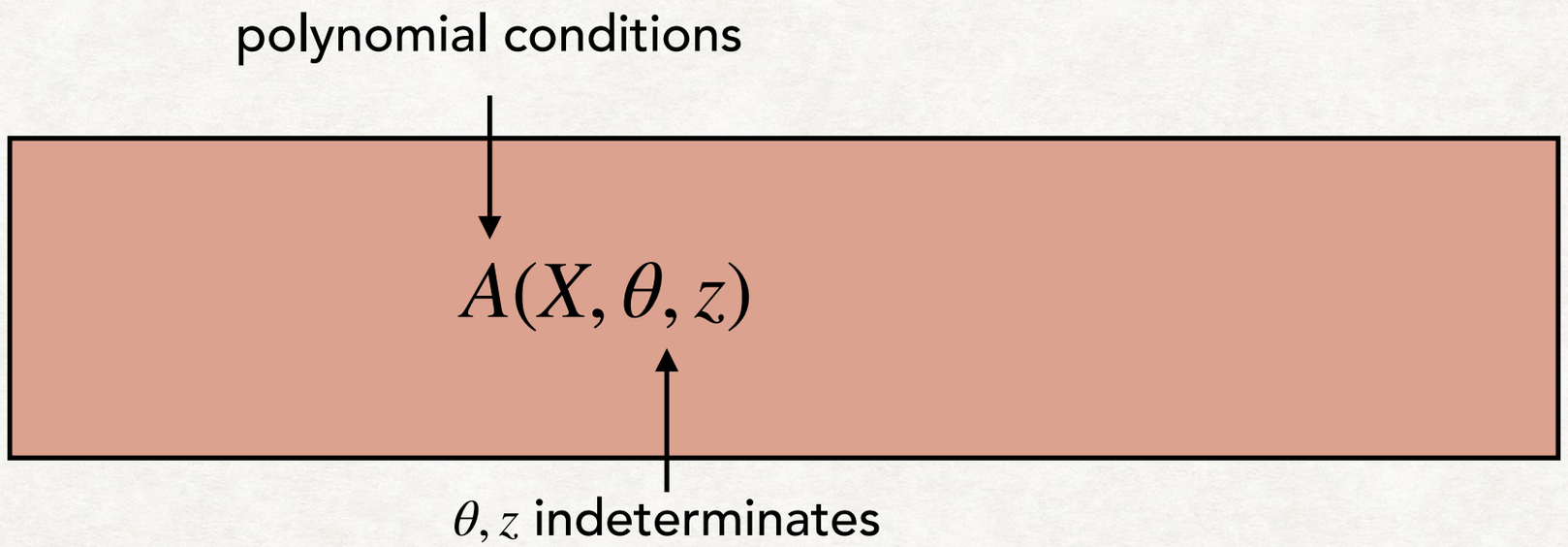
degree-d

$$\tilde{\mathbb{E}} \models_d A \iff \tilde{\mathbb{E}} q^2(x) \prod_{i \in S} p_i(x) \geq 0$$

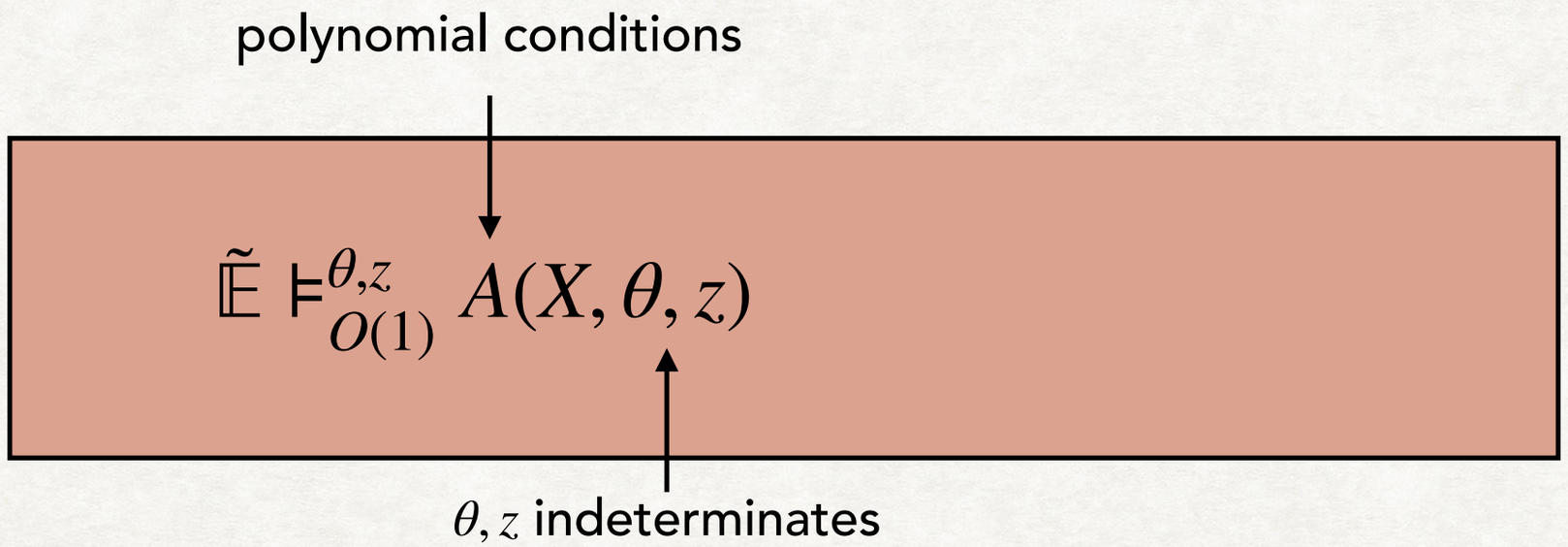
$n^{O(d)}$

SOS BASED ROBUST ESTIMATORS

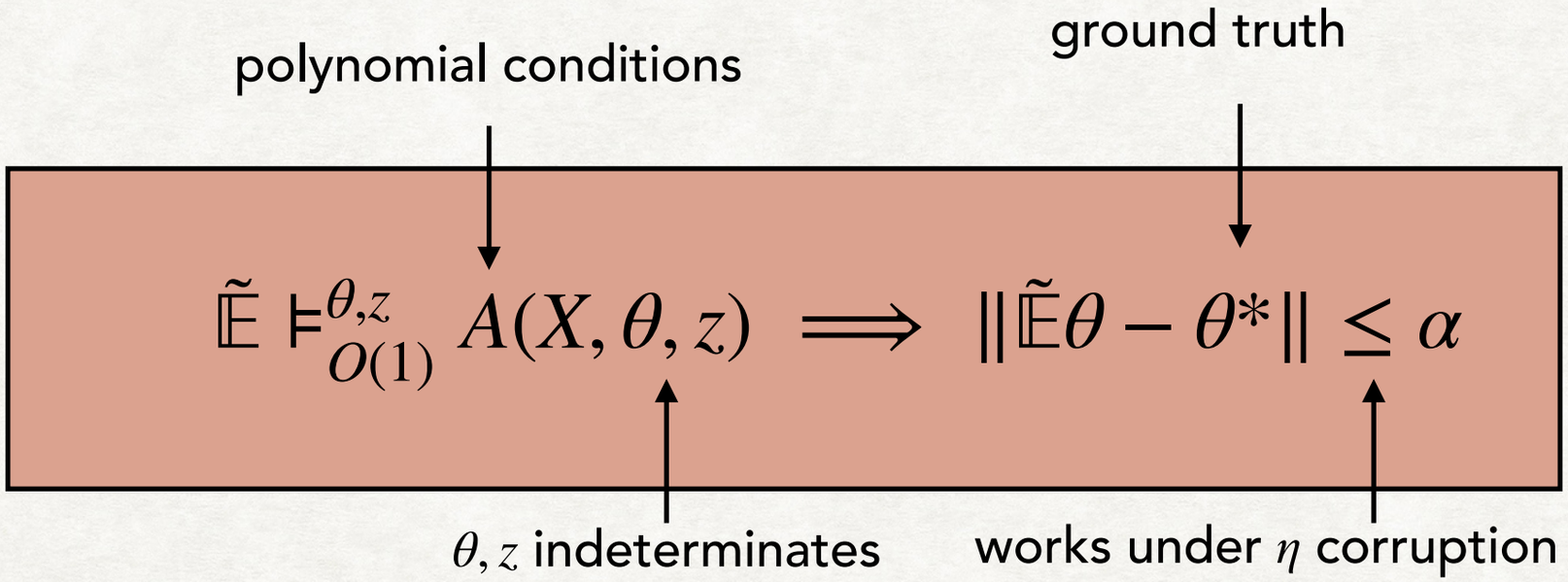
SOS BASED ROBUST ESTIMATORS



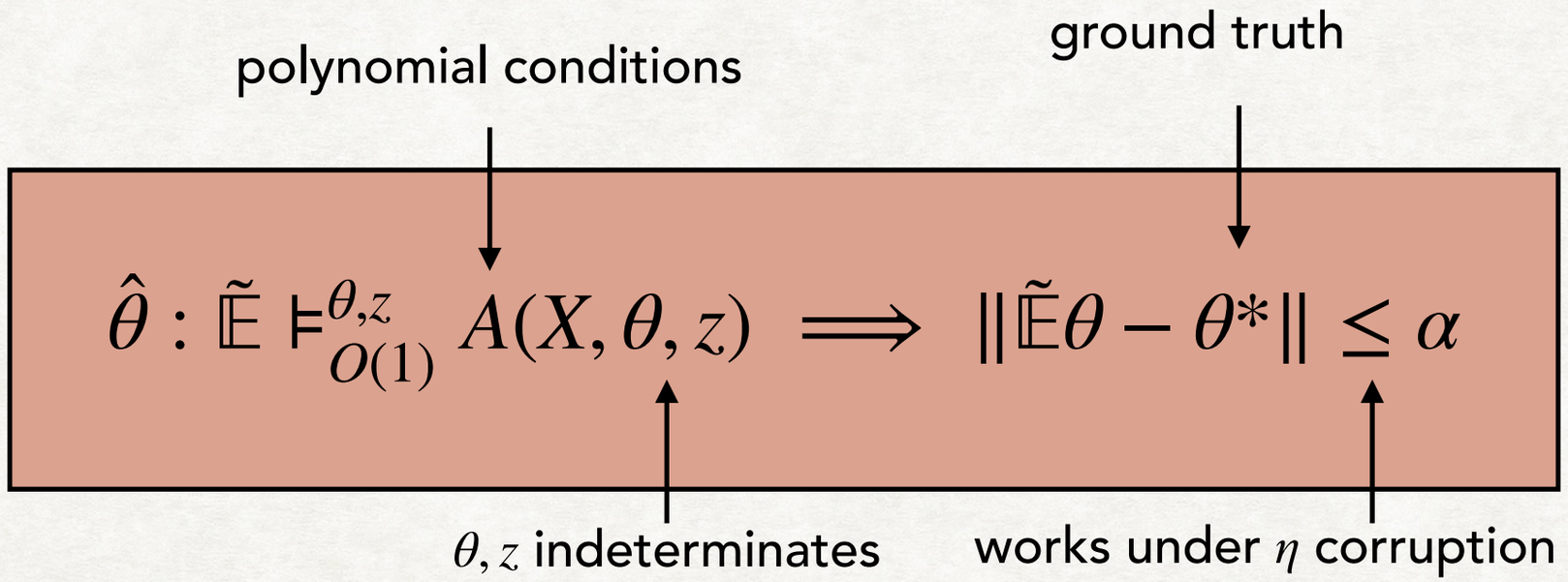
SOS BASED ROBUST ESTIMATORS



SOS BASED ROBUST ESTIMATORS



SOS BASED ROBUST ESTIMATORS



CHALLENGES

$$\hat{\theta} : \tilde{\mathbb{E}} \vdash^{\theta,z}_{O(1)} A(X,\theta,z) \implies \|\tilde{\mathbb{E}}\theta - \theta^*\| \leq \alpha$$

θ, z indeterminates

works under η corruption

sos based robust estimator

CHALLENGES

$$\hat{\theta} : \tilde{\mathbb{E}} \vdash^{\theta,z}_{O(1)} A(X,\theta,z) \implies \|\tilde{\mathbb{E}}\theta - \theta^*\| \leq \alpha$$

θ, z indeterminates

works under η corruption

sos based robust estimator

robust estimator

$$\text{score}(\theta, X) = \min_{X'} \text{Ham}(X, X') \text{ such that } \hat{\theta} \text{ thinks } (X, \theta) \text{ are good}$$

CHALLENGES

$$\hat{\theta} : \tilde{\mathbb{E}} \vdash^{\theta,z}_{O(1)} A(X,\theta,z) \implies \|\tilde{\mathbb{E}}\theta - \theta^*\| \leq \alpha$$

θ, z indeterminates

works under η corruption

sos based robust estimator

computing score

robust estimator

$$\text{score}(\theta, X) = \min_{X'} \text{Ham}(X, X') \text{ such that } \hat{\theta} \text{ thinks } (X, \theta) \text{ are good}$$

CHALLENGES

$$\hat{\theta} : \tilde{\mathbb{E}} \vdash^{\theta,z}_{O(1)} A(X,\theta,z) \implies \|\tilde{\mathbb{E}}\theta - \theta^*\| \leq \alpha$$

θ, z indeterminates

works under η corruption

sos based robust estimator

computing score

robust estimator

$$\text{score}(\theta, X) = \min_{X'} \text{Ham}(X, X') \text{ such that } \hat{\theta} \text{ thinks } (X, \theta) \text{ are good}$$

$$p(\theta) \propto \exp(-\varepsilon \ \text{score}(\theta; X))$$

CHALLENGES

$$\hat{\theta} : \tilde{\mathbb{E}} \vdash^{\theta,z}_{O(1)} A(X,\theta,z) \implies \|\tilde{\mathbb{E}}\theta - \theta^*\| \leq \alpha$$

θ, z indeterminates

works under η corruption

sos based robust estimator

computing score

robust estimator

$$\text{score}(\theta, X) = \min_{X'} \text{Ham}(X, X') \text{ such that } \hat{\theta} \text{ thinks } (X, \theta) \text{ are good}$$

efficient sampling

$$p(\theta) \propto \exp(-\varepsilon \ \text{score}(\theta; X))$$

EFFICIENT SCORE FUNCTIONS

EFFICIENT SCORE FUNCTIONS

$A(X, \theta, z)$

estimation program

$\text{score}(\theta, X) = \min_{X'} \text{Ham}(X, X')$ **such that** $\hat{\theta}$ **thinks** (X, θ) **are good**

inverse sensitivity

EFFICIENT SCORE FUNCTIONS

$$A(X, \theta, z)$$

estimation program

$$\text{score}(\theta, X) = \min_{X'} \text{Ham}(X, X') \text{ such that } \hat{\theta} \text{ thinks } (X, \theta) \text{ are good}$$

inverse sensitivity

move the counting inside the sos program

EFFICIENT SCORE FUNCTIONS

move the counting inside the sos program

number of points allowed to change

$$B_t := \{w_i^2 = w_i,$$

$$\sum_{i=1}^{n} w_i = n - t,$$

$$w_i X_i = w_i X_i'\}$$

$$C_t := B_t \cup A$$

new constraints

EFFICIENT SCORE FUNCTIONS

points allowed to change

$$B_t := \left\{ w_i^2 = w_i,\ \sum_{i=1}^{n} w_i = n - t,\ w_i X_i = w_i X_i' \right\}$$

$$C_t := B_t \cup A$$

new constraints

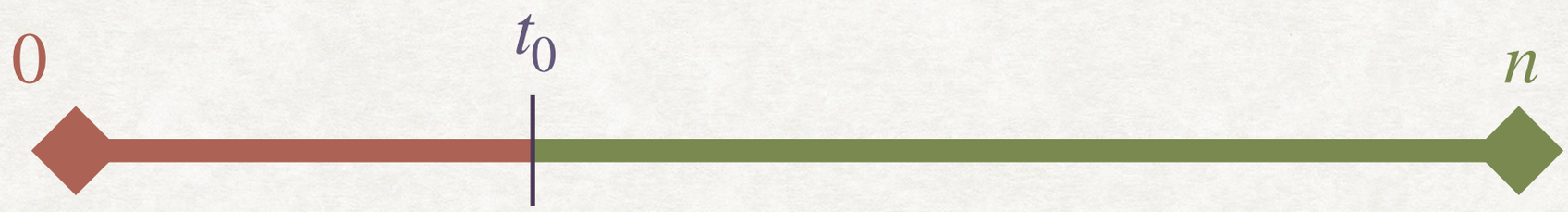
EFFICIENT SCORE FUNCTIONS

points allowed to change

$$B_t := \left\{ w_i^2 = w_i,\ \sum_{i=1}^{n} w_i = n - t,\ w_i X_i = w_i X_i' \right\}$$

$$C_t := B_t \cup A$$

new constraints



C_t's satisfiability

EFFICIENT SCORE FUNCTIONS

points allowed to change

$$B_t := \left\{ w_i^2 = w_i,\ \sum_{i=1}^{n} w_i = n - t,\ w_i X_i = w_i X_i' \right\}$$

$$C_t := B_t \cup A$$

new constraints

$$\text{score}(\theta; X) := \min_t \text{ such that}$$

$$\exists \text{ degree } O(1)\ \tilde{\mathbb{E}} \text{ in } X', w', \theta', z$$

$$\tilde{\mathbb{E}} \vDash C_t, \quad \|\tilde{\mathbb{E}}\theta' - \theta\| \leq \alpha$$

new score

EFFICIENT SCORE FUNCTIONS

$$\text{score}(\theta; X) := \min_{t} \text{ such that}$$

$$\exists \text{ degree } O(1)\ \tilde{\mathbb{E}} \text{ in } X', w', \theta', z$$

$$\tilde{\mathbb{E}} \vDash C_t, \quad \|\tilde{\mathbb{E}}\theta' - \theta\| \leq \alpha$$

new score

EFFICIENT SCORE FUNCTIONS

$$\text{score}(\theta; X) := \min_t \text{ such that}$$

$$\exists \text{ degree } O(1)\ \tilde{\mathbb{E}} \text{ in } X', w', \theta', z$$

$$\tilde{\mathbb{E}} \vdash C_t, \quad \|\tilde{\mathbb{E}}\theta' - \theta\| \leq \alpha$$

new score

accuracy

$$\tilde{\mathbb{E}} \vdash C_{\eta n} \implies \|\tilde{\mathbb{E}}\theta' - \theta^*\| \leq \tilde{O}(\eta)$$

sos proofs generalize

low scoring $\tilde{\mathbb{E}}$ gives high quality estimate

EFFICIENT SCORE FUNCTIONS

$$\text{score}(\theta; X) := \min_t \text{ such that}$$

$$\exists \text{ degree } O(1)\ \tilde{\mathbb{E}} \text{ in } X', w', \theta', z$$

$$\tilde{\mathbb{E}} \vdash C_t, \quad \|\tilde{\mathbb{E}}\theta' - \theta\| \leq \alpha$$

new score

accuracy

$$\tilde{\mathbb{E}} \vdash C_{\eta n} \implies \|\tilde{\mathbb{E}}\theta' - \theta^*\| \leq \tilde{O}(\eta)$$

sos proofs generalize

low scoring $\tilde{\mathbb{E}}$ gives high quality estimate

privacy

still low sensitivity

EFFICIENT SCORE FUNCTIONS

$$\text{score}(\theta; X) := \min_{t} \text{ such that}$$

$$\exists \text{ degree } O(1)\ \tilde{\mathbb{E}} \text{ in } X', w', \theta', z$$

$$\tilde{\mathbb{E}} \vDash C_t, \quad \|\tilde{\mathbb{E}}\theta' - \theta\| \leq \alpha$$

new score

computing score

EFFICIENT SCORE FUNCTIONS

$$\text{score}(\theta; X) := \min_t \text{ such that}$$

$$\exists \text{ degree } O(1)\ \tilde{\mathbb{E}} \text{ in } X', w', \theta', z$$

$$\tilde{\mathbb{E}} \vDash C_t, \quad \|\tilde{\mathbb{E}}\theta' - \theta\| \leq \alpha$$

new score

computing score

binary search?

EFFICIENT SCORE FUNCTIONS

$$\text{score}(\theta; X) := \min_{t} \text{ such that}$$

$$\exists \text{ degree } O(1)\ \tilde{\mathbb{E}} \text{ in } X', w', \theta', z$$

$$\tilde{\mathbb{E}} \vDash C_t, \quad \|\tilde{\mathbb{E}}\theta' - \theta\| \leq \alpha$$

new score

computing score

binary search?

issue: fix t, can't verify if $\tilde{\mathbb{E}}$ exists or not

bit complextiy

EFFICIENT SCORE FUNCTIONS

τt-approximate pseudo-expectation

$$\text{score}(\theta; X) := \min_t \text{ such that}$$

$$\exists \text{ degree } O(1)\ \mathscr{L} \text{ in } X', w', \theta', z$$

$$\mathscr{L} \vDash_{\tau t\text{-approx}} C_t, \quad \|\mathscr{L}\theta' - \theta\|_\infty \leq \alpha/\sqrt{d} + \tau t$$

new score

EFFICIENT SCORE FUNCTIONS

τt-approximate pseudo-expectation

$$\text{score}(\theta; X) := \min_t \text{ such that}$$

$$\exists \text{ degree } O(1)\ \mathscr{L} \text{ in } X', w', \theta', z$$

$$\mathscr{L} \vDash_{\tau t\text{-approx}} C_t, \quad \|\mathscr{L}\theta' - \theta\|_\infty \leq \alpha/\sqrt{d} + \tau t$$

new score

computing score

efficiently computable

ellipsoid + binary search

CHALLENGES

τt-approximate pseudo-expectation

$$\text{score}(\theta; X) := \min_t \text{ such that}$$

$$\exists \text{ degree } O(1) \ \mathscr{L} \text{ in } X', w', \theta', z$$

$$\mathscr{L} \vDash_{\tau t\text{-approx}} C_t, \quad \|\mathscr{L}\theta' - \theta\|_\infty \leq \alpha/\sqrt{d} + \tau t$$

new score

computing score	efficiently computable ellipsoid + binary search
efficient sampling	?

EFFICIENT SAMPLING

$$\text{score}(\theta; X) := \min_{t} \text{ such that}$$

$$\exists \text{ degree } O(1)\ \tilde{\mathbb{E}} \text{ in } X', w', \theta', z$$

$$\tilde{\mathbb{E}} \vDash C_t, \quad \|\tilde{\mathbb{E}}\theta' - \theta\| \leq \alpha$$

if $\text{score}(\theta; X)$ was convex

$\Longrightarrow$ we could sample efficiently

EFFICIENT SAMPLING

$$\text{score}(\theta; X) := \min_t \text{ such that}$$

$$\exists \text{ degree } O(1)\ \tilde{\mathbb{E}} \text{ in } X', w', \theta', z$$

$$\tilde{\mathbb{E}} \vDash C_t, \quad \|\tilde{\mathbb{E}}\theta' - \theta\| \leq \alpha$$

issue: score is not convex

$$\tilde{\mathbb{E}}_1 \vDash C_{t_1}, \tilde{\mathbb{E}}_2 \vDash C_{t_1} \nRightarrow \frac{1}{2}(\tilde{\mathbb{E}}_1 + \tilde{\mathbb{E}}_2) \vDash C_{\frac{1}{2}(t_1+t_2)}$$

EFFICIENT SAMPLING

$$\text{score}(\theta; X) := \min_t \text{ such that}$$

$$\exists \text{ degree } O(1)\ \tilde{\mathbb{E}} \text{ in } X', w', \theta', z$$

$$\tilde{\mathbb{E}} \vDash C_t, \quad \|\tilde{\mathbb{E}}\theta' - \theta\| \leq \alpha$$

issue: score is not convex

$$\tilde{\mathbb{E}}_1 \vDash C_{t_1}, \tilde{\mathbb{E}}_2 \vDash C_{t_1} \not\Rightarrow \frac{1}{2}(\tilde{\mathbb{E}}_1 + \tilde{\mathbb{E}}_2) \vDash C_{\frac{1}{2}(t_1+t_2)}$$

but, it's quasi-convex:

the sub-level sets $\{\theta : \text{score}(\theta; X) \leq t\}$ are convex

$\Longrightarrow$ we can design a sampler

CHALLENGES

$$\text{score}(\theta; X) := \min_{t} \text{ such that}$$

$$\exists \text{ degree } O(1)\ \tilde{\mathbb{E}} \text{ in } X', w', \theta', z$$

$$\tilde{\mathbb{E}} \vDash C_t, \quad \|\tilde{\mathbb{E}}\theta' - \theta\| \leq \alpha$$

computing score	efficiently computable approximate satisfiability, ellipsoid, binary search
efficient sampling	efficient and private sampler for quasi-convex score convex body sampling techniques

RECIPE

1. make a score function $S(\theta; X)$

   for sos based robust estimators, make the score as described in the previous slides

RECIPE

1. make a score function $\mathsf{S}(\theta; X)$
2. show it has bounded sensitivity

   $|\mathsf{S}(\theta; X) - \mathsf{S}(\theta, X')| \leq 1$

RECIPE

1. make a score function $S(\theta; X)$
2. show it has bounded sensitivity
3. show it is quasi-convex

   convex level sets

RECIPE

1. make a score function S($\theta; X$)
2. show it has bounded sensitivity
3. show it is quasi-convex
4. show it is efficiently computable

   can find the score up to error γ in time

   $\text{poly}\log(1/\gamma)$, we showed this for sos based scores

RECIPE

1. make a score function $\mathrm{S}(\theta; X)$
2. show it has bounded sensitivity
3. show it is quasi-convex
4. show it is efficiently computable
5. show it can be efficiently approximately minimized

   can find a point with score of $\min_{\theta} \mathrm{S} + 1$

RECIPE

1. make a score function S($\theta; X$) (exp mechanism)
2. show it has bounded sensitivity (privacy)
3. show it is quasi-convex (efficient sampling)
4. show it is efficiently computable (computing score)
5. show it can be efficiently approximately minimized (efficient sampling)

Theorem: Let V_η be the volume of points with score less than ηn, $\eta_0 > 0$. Then if there exists a point with score less than $\eta_0 n$, the exponential mechanism with score function S as above outputs a point with score less than $2\eta_0 n$ with high probability, as long as

$$n = \Omega\left(\max_{\eta_0 \le \eta \le 1} \frac{\log(V_\eta / V_{\eta_0})}{\varepsilon \cdot \eta} \right).$$

APPLICATIONS

GAUSSIAN MEAN ESTIMATION

assumption: $\|\mu\| \leq R$

Theorem: There exists a private and polynomial time algorithm that can estimate the mean of $\mathcal{N}(\mu, I)$ up to error α using n samples.

$$n = \tilde{O}\left(\frac{d}{\alpha^2} + \frac{d}{\alpha\varepsilon} + \frac{d \log R}{\varepsilon}\right), \quad \text{under } (\varepsilon,0)\text{-dp}$$

$$n = \tilde{O}\left(\frac{d}{\alpha^2} + \frac{d}{\alpha\varepsilon} + \frac{\log(1/\delta)}{\varepsilon}\right), \quad \text{under } (\varepsilon,\delta)\text{-dp}$$

LEARNING GAUSSIANS

assumption: $\|\mu\| \le R, \quad \frac{1}{K} \cdot I \preccurlyeq \Sigma \preccurlyeq K \cdot I$

Theorem: There exists a private and polynomial time algorithm that can estimate $\mathcal{N}(\mu, \Sigma)$ up to TV distance α using n samples.

$$n = \tilde{O}\left(\frac{d^2}{\alpha^2} + \frac{d^2}{\alpha\varepsilon} + \frac{d^2 \log K}{\varepsilon} + \frac{d \log R}{\varepsilon}\right), \quad \text{under } (\varepsilon,0)\text{-dp}$$

$$n = \tilde{O}\left(\frac{d^2}{\alpha^2} + \frac{d^2}{\alpha\varepsilon} + \frac{\log(1/\delta)}{\varepsilon}\right), \quad \text{under } (\varepsilon,\delta)\text{-dp}$$