Robustness of Empirical Revenue Maximization in Auction Learning

Tao Lin (PKU->Harvard),

Joint with

Xiaotie Deng (PKU), *Ron Lavi* (Technion), *Qi Qi* (HKUST),

Wenwei Wang (HKUST->Alibaba), *Xiang Yan* (SJTU)

"A Game-Theoretic Analysis of Empirical Revenue Maximization with Endogenous Sampling"

NeurIPS 2020

Key Points

- Auction + incentive-aware learning

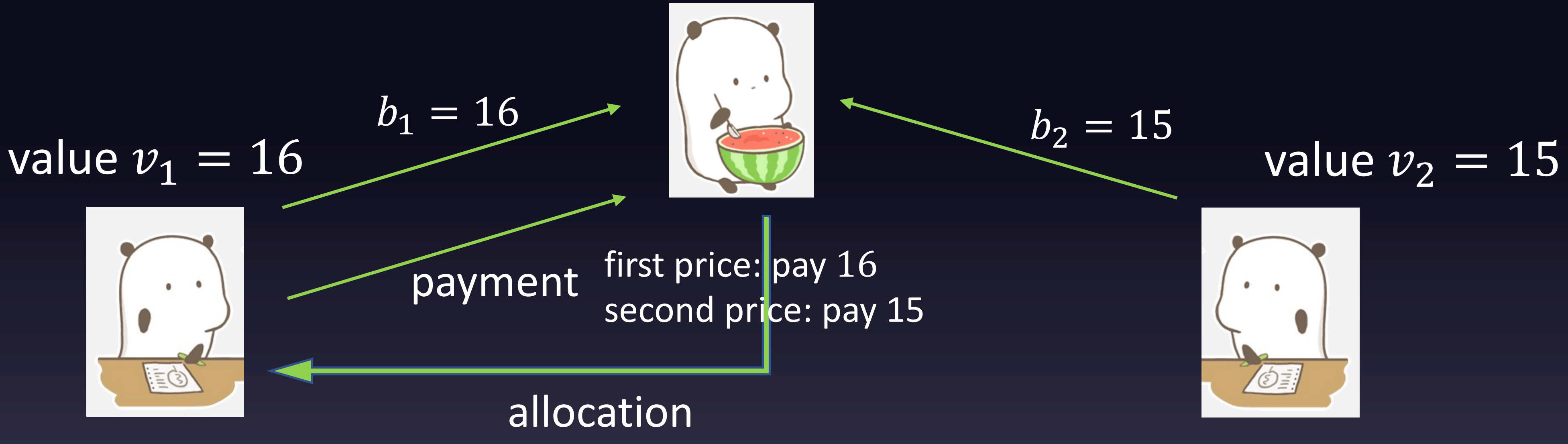
Main Result

Empirical Revenue Maximization (ERM) is a *robust* learning algorithm against sample manipulation, as long as

1) the number of manipulated samples is ***small***;
2) robustness is measured ***in expectation*** (rather than worst-case)

- Corollaries: a) in repeated auctions, ERM is an approximately truthful learning algorithm; b) uniform price auction is "*group*-strategyproof in the large".

Auctions



Examples

1) Second price auction: highest bidder wins, pays the 2^{nd} highest bid.
2) Second price auction with *reservation price* p: highest bidder wins (if bid > p), pays
$$\max\{2^{\text{nd}}\ \text{bid}, p\}$$
3) Posted-price auction: single-bidder version of 2); the bidder pays p if $v \geq p$

The optimal auction (Myerson's)

- One item for sell
- K bidders with i.i.d. values $v_i \sim F$ for the item

Theorem (*Myerson*, 1981)

The revenue-optimal auction is the second price auction with reservation price

$$p^* = \underset{p \in \mathbf{R}}{\operatorname{argmax}}\{Rev_F(p)\}, \qquad \underbrace{Rev_F(p) := p\big(1 - F(p)\big) = p \Pr_{v \sim F}[v \geq p]}_{\text{expected revenue of the auction with posted price } p}$$

Assuming distributional knowledge is problematic!

Game theory has a great advantage in explicitly analyzing the consequences of trading rules that presumably really are common knowledge; it is deficient to the extent it assumes other features to be common knowledge, such as one agent's probability assessment about another's preferences or information.

-- Robert B. Wilson (1985)

Learning optimal auction from samples

- Suppose we have N samples $\boldsymbol{s} = (s_1, s_2, \dots, s_N) \sim F$
- We want to learn a good auction (reservation price) from $\boldsymbol{s}$
  - Cole & Roughgarden (2014), Dhangwatnotai et al (2015), Huang et al (2015), Morgenstern & Roughgarden (2015), Gonczarowski & Nisan (2017), Guo et al (2019), …

Definition: Empirical Revenue Maximization (*Dhangwatnotai et al*, 2015)

- N samples $\boldsymbol{s} = (s_1, s_2, \dots, s_N) \sim F$
- Output the optimal reservation price for the empirical distribution $E = \text{Uniform}\{s_1, s_2, \dots, s_N\}$

$$\text{ERM}(\boldsymbol{s}) = \underset{p \in \mathbf{R}}{\text{argmax}}\{\, Rev_E(p)\} = \underset{p \in \mathbf{R}}{\text{argmax}}\{\, p\,(1 - E(p))\}$$

ERM is important!

- ERM is the **Empirical Risk Minimization** in the auction learning problem:

Learning a classifier:

$$c^* = \underset{c \in \boldsymbol{C}}{\operatorname{argmin}}\{\, loss_F(c) \,\}$$

Empirical Risk Minimization:

$$c_{\boldsymbol{s}}^* = \underset{c \in \boldsymbol{C}}{\operatorname{argmin}}\{\, loss_E(c) \,\}$$

Empirical Revenue Maximization:

$$p_{\boldsymbol{s}}^* = \underset{p \in \mathbf{R}}{\operatorname{argmax}}\{\, Rev_E(p) \,\}$$

- ERM has good performance: $\left(1 - O\left(\sqrt{\frac{\log N}{N}}\right)\right)$-optimal expected revenue [*Huang et al* '15]

Definition: Empirical Revenue Maximization (*Dhangwatnotai et al*, 2015)

- N samples $\boldsymbol{s} = (s_1, s_2, \dots, s_N) \sim F$
- Output the optimal reservation price for the empirical distribution $E = \mathrm{Uniform}\{s_1, s_2, \dots, s_N\}$

$$\mathrm{ERM}(\boldsymbol{s}) = \underset{p \in \mathbf{R}}{\operatorname{argmax}}\{\, Rev_E(p)\} = \underset{p \in \mathbf{R}}{\operatorname{argmax}}\{\, p\,(1 - E(p))\}$$

But, assuming sample access is still problematic!

Where do we get samples?

- Exogenous – by market research, by magic?

Definition: Empirical Revenue Maximization (*Dhangwatnotai et al*, 2015)

- N samples $\boldsymbol{s} = (s_1, s_2, \dots, s_N) \sim F$
- Output the optimal reservation price for the empirical distribution $E = \text{Uniform}\{s_1, s_2, \dots, s_N\}$

$$\text{ERM}(\boldsymbol{s}) = \underset{p \in \mathbf{R}}{\text{argmax}}\{ Rev_E(p)\} = \underset{p \in \mathbf{R}}{\text{argmax}}\{ p\,(1 - E(p))\}$$

But, assuming sample access is still problematic!

Where do we get samples?

- ~~Exogenous – by market research, by magic?~~

- *Endogenous* – from bidders
  e.g., repeated auctions

Incentive issue: bidders may provide false samples to lower $\mathrm{ERM}(\boldsymbol{s})$!

Definition: Empirical Revenue Maximization (*Dhangwatnotai et al*, 2015)

- N samples $\boldsymbol{s} = (s_1, s_2, \ldots, s_N) \sim F$
- Output the optimal reservation price for the empirical distribution $E = \mathrm{Uniform}\{s_1, s_2, \ldots, s_N\}$

$$\mathrm{ERM}(\boldsymbol{s}) = \operatorname*{argmax}_{p \in \mathbf{R}}\{ Rev_E(p)\} = \operatorname*{argmax}_{p \in \mathbf{R}}\{ p\,(1 - E(p))\}$$

Example 1

bidder i provides	ERM		utility = value - payment
$\boldsymbol{s} = (0, 0, 100)$	100	$0 \cdot \Pr_E[v \geq 0] = 0 \cdot 1 = 0$ $100 \cdot \Pr_E[v \geq 100] = 100 \cdot \frac{1}{3} = \frac{100}{3}$	0
$\boldsymbol{s}' = (0, 0, 0)$	0	$0 \cdot \Pr_E[v \geq 0] = 0 \cdot 1 = 0$ $p \cdot \Pr_E[v \geq p] = 0 \cdot 0 = 0 \quad \forall p > 0$	100

Definition: Empirical Revenue Maximization (*Dhangwatnotai et al*, 2015)

- N samples $\boldsymbol{s} = (s_1, s_2, \ldots, s_N) \sim F$
- Output the optimal reservation price for the empirical distribution $E = \mathrm{Uniform}\{s_1, s_2, \ldots, s_N\}$

$$\mathrm{ERM}(\boldsymbol{s}) = \operatorname*{argmax}_{p \in \mathbf{R}} \{ Rev_E(p) \} = \operatorname*{argmax}_{p \in \mathbf{R}} \{ p \Pr_E[v \geq p] \}$$

Example 2

bidder i provides

ERM

$\boldsymbol{s} = (100, 100, 100)$

100

$100 \cdot \Pr_E[v \geq 100] = 100 \cdot 1 = 100$
$p \cdot \Pr_E[v \geq p] = 0 \quad \forall p > 100$

$\boldsymbol{s}' = \left(100, 100, \frac{200}{3}\right)$

$\frac{200}{3} = 66.7$

$100 \cdot \Pr_E[v \geq 100] = 100 \cdot \frac{2}{3} = \frac{200}{3}$
$\frac{200}{3} \cdot \Pr_E\left[v \geq \frac{200}{3}\right] = \frac{200}{3}$

Definition: Empirical Revenue Maximization (*Dhangwatnotai et al*, 2015)

- N samples $\boldsymbol{s} = (s_1, s_2, \dots, s_N) \sim F$
- Output the optimal reservation price for the empirical distribution $E = \text{Uniform}\{s_1, s_2, \dots, s_N\}$

$$\text{ERM}(\boldsymbol{s}) = \operatorname*{argmax}_{p \in \mathbf{R}}\{ Rev_E(p)\} = \operatorname*{argmax}_{p \in \mathbf{R}}\{ p\Pr_E[v \geq p]\}$$

Main result: ERM is robust in expectation!

Informal Theorem 1 (this work)

For any bounded F, if *at most* $m = o(\sqrt{N})$ samples are manipulated, then the *expected* change of $\mathrm{ERM}(\boldsymbol{s})$ is at most $\Delta = O\left(m^{2/3}\frac{\log^2 N}{N^{1/3}}\right) \to 0$ (as $N \to \infty$)

Main result: ERM is robust in expectation!

Formally:

- Suppose we have N values $v_1 , \ldots , v_N$
- where $N - m$ values $v_{-I} = \{v_{m+1}, \ldots , v_N\}$ are i.i.d. samples from F.
- other m values $x_I = \{v_1, \ldots , v_m\}$ can be changed to any m values $b_I \in \mathbf{R}_+^m$

- $\mathrm{ERM}(x_I , v_{-I})$ --> $\mathrm{ERM}(b_I , v_{-I})$.

Definition: expected incentive-awareness measure

$$\Delta_{N,m}^F = \mathrm{E}_{v_{-I} \sim F^{N-m}} \left[\sup_{x_I,\, b_I \in \mathbf{R}_+^m} \frac{\mathrm{ERM}(x_I, v_{-I}) - \mathrm{ERM}(b_I, v_{-I})}{\mathrm{ERM}(x_I, v_{-I})} \right]$$

Related works & our work

- *Lavi et al.* (WWW'19) proposed $\Delta^F_{N,1}$ and showed $\Delta^F_{N,1} \to 0$ for discrete F
- *Yao* (arXiv'18) showed $\Delta^F_{N,1} \to 0$ for any $[1, D]$-bounded F *No convergence rate is given!*

Theorem 1 (our): Upper bound on $\Delta^F_{N,m}$

Assuming $m = o(\sqrt{N})$

- Universally for any $[1, D]$-bounded F, $\Delta^F_{N,m} = O\left(m^{2/3} \frac{\log^2 N}{N^{1/3}}\right) \to 0$
- Universally for any MHR F, $\Delta^F_{N,m} = O\left(m \frac{\log^3 N}{\sqrt{N}}\right) \to 0$ MHR: $\frac{f(x)}{1-F(x)}$ increases

Definition: expected incentive-awareness measure

$$\Delta^F_{N,m} = \mathrm{E}_{v_{-I} \sim F^{N-m}}\left[\sup_{x_I, b_I \in \mathbf{R}^m_+} \frac{\mathrm{ERM}(x_I, v_{-I}) - \mathrm{ERM}(b_I, v_{-I})}{\mathrm{ERM}(x_I, v_{-I})}\right]$$

Theorem 2 (ongoing work): Lower bound on $\Delta^F_{N,m}$

- For bounded F, $\Delta^F_{N,m} = \Omega\left(m \frac{1}{\sqrt{N}}\right)$,

Theorem 1 (our): Upper bound on $\Delta^F_{N,m}$

Assuming $m = o(\sqrt{N})$

- Universally for any $[1, D]$-bounded F, $\Delta^F_{N,m} = O\left(m^{2/3} \frac{\log^2 N}{N^{1/3}}\right) \to 0$
- Universally for any MHR F, $\Delta^F_{N,m} = O\left(m \frac{\log^3 N}{\sqrt{N}}\right) \to 0$

MHR: $\frac{f(x)}{1-F(x)}$ increases

Definition: expected incentive-awareness measure

$$\Delta^F_{N,m} = \mathrm{E}_{v_{-I} \sim F^{N-m}}\left[\sup_{x_I,\, b_I \in \mathbf{R}^m_+} \frac{\mathrm{ERM}(x_I, v_{-I}) - \mathrm{ERM}(b_I, v_{-I})}{\mathrm{ERM}(x_I, v_{-I})}\right]$$

Theorem 2 (ongoing work): Lower bound on $\Delta^F_{N,m}$

- For bounded F, $\Delta^F_{N,m} = \Omega\left(m\frac{1}{\sqrt{N}}\right)$, in particular, if $m \gg \sqrt{N}$, $\Delta^F_{N,m} = \Omega(1)$

Theorem 1 (our): Upper bound on $\Delta^F_{N,m}$

Assuming $m = o(\sqrt{N})$

- Universally for any $[1, D]$-bounded F, $\Delta^F_{N,m} = O\left(m^{2/3}\frac{\log^2 N}{N^{1/3}}\right) \to 0$
- Universally for any MHR F, $\Delta^F_{N,m} = O\left(m\frac{\log^3 N}{\sqrt{N}}\right) \to 0$

MHR: $\frac{f(x)}{1-F(x)}$ increases

Definition: expected incentive-awareness measure

$$\Delta^F_{N,m} = \mathrm{E}_{v_{-I}\sim F^{N-m}}\left[\sup_{x_I,\, b_I \in \mathbf{R}^m_+} \frac{\mathrm{ERM}(x_I, v_{-I}) - \mathrm{ERM}(b_I, v_{-I})}{\mathrm{ERM}(x_I, v_{-I})}\right]$$

Theorem 2 (ongoing work): Lower bound on $\Delta_{N,m}^F$

- For bounded F, $\Delta_{N,m}^F = \Omega\left(m\frac{1}{\sqrt{N}}\right)$, in particular, if $m \gg \sqrt{N}$, $\Delta_{N,m}^F = \Omega(1)$
- For MHR F, $\Delta_{N,m}^F = \Omega(\ ?\ )$

Theorem 1 (our): Upper bound on $\Delta_{N,m}^F$

Assuming $m = o(\sqrt{N})$

- Universally for any $[1, D]$-bounded F, $\Delta_{N,m}^F = O\left(m^{2/3}\frac{\log^2 N}{N^{1/3}}\right) \to 0$
- Universally for any MHR F, $\Delta_{N,m}^F = O\left(m\frac{\log^3 N}{\sqrt{N}}\right) \to 0$

MHR: $\frac{f(x)}{1-F(x)}$ increases

Definition: expected incentive-awareness measure

$$\Delta_{N,m}^F = \mathrm{E}_{v_{-I}\sim F^{N-m}}\left[\sup_{x_I,\, b_I \in \mathbf{R}_+^m} \frac{\mathrm{ERM}(x_I, v_{-I}) - \mathrm{ERM}(b_I, v_{-I})}{\mathrm{ERM}(x_I, v_{-I})}\right]$$

Corollary: Repeated auctions

(cf. *differential privacy techniques* in [LHW'18], [ACKTM'19])

- T rounds of second price auctions
  - Each bidder participates in $\leq m$ rounds,
  - $m \ll T$
  - Each round has one item, K bidders (e.g., $K = 1\ or\ 2$), with iid values

Corollary 1. If $m = o\left(\sqrt{T_1 K}\right)$, the *two-phase ERM algorithm* is ϵ_1-BIC and $(1 - \epsilon_2)$ -revenue optimal, with

- $\epsilon_1 = O\left(m^{5/3} \frac{\log^2 T_1 K}{(T_1 K)^{1/3}}\right) \to 0$, and $\epsilon_2 = O\left(\frac{T_1}{T} + \sqrt{\frac{\log T_1 K}{T_1 K}}\right)$

Two-phase ERM: Divide the T rounds into two phases:

- T_1 rounds of exploration: set reservation price to 0.
- T_2 rounds of exploitation: set reservation price to $\mathrm{ERM}(\boldsymbol{s})$, where
  - $\boldsymbol{s} = (b_1, \ldots, b_{T_1 K})$ are the first round bids.

Corollary 2: Uniform-price auctions

("strategyproofness in the large" [Azevedo & Budish '18]])

- one-shot uniform-price auction:
- N copies of a good
- N unit-demand bidders with i.i.d. values $\boldsymbol{v}$ from F submit bids $\boldsymbol{b}$.
- Auctioneer sets a price $p = P(\boldsymbol{b})$
- Each bidder i with bid $b_i \geq p$ receives a copy of the good and pays p, obtaining utility $v_i - p$; otherwise the utility is 0.

- **Assumption (joint deviation):** we allow any $m \geq 1$ bidders to coordinate and submit non-truthful bids *jointly*!

Corollary: (m, ϵ)-**group BIC**: No bidder gains ϵ more utility from joint deviation, where, for $P = \mathrm{ERM}$ and any bounded F, $\epsilon = D\Delta_{N,m}^{F,P} \to 0$

Summary

See details at

- (Single-dimensional) Auction + (incentive-aware) Learning
- Bidders have incentives to misreport samples to fool the **Empirical Revenue Maximization**/**Empirical Risk Minimization** **algorithm.**

Takeaway

Empirical Risk Minimization is a ***robust*** learning algorithm in the auction learning problem, as long as

1) robustness is measured ***in expectation*** (rather than worst-case)
2) misreported samples are ***few***

- Future works: a) more complex auction environment?

  b) tighten the bounds on $\Delta^{F}_{N,m}$