# MS&E 233
# Game Theory, Data Science and AI
# Lecture 13

Vasilis Syrgkanis
Assistant Professor
Management Science and Engineering
(by courtesy) Computer Science and Electrical Engineering
Institute for Computational and Mathematical Engineering

## Computational Game Theory for Complex Games

1

- Basics of game theory and zero-sum games (T)
- Basics of online learning theory (T)
- Solving zero-sum games via online learning (T)
- *HW1: implement simple algorithms to solve zero-sum games*
- Applications to ML and AI (T+A)
- *HW2: implement boosting as solving a zero-sum game*

2

- Basics of extensive-form games
- Solving extensive-form games via online learning (T)
- *HW3: implement agents to solve very simple variants of poker*

3

- General games, equilibria and online learning (T)
- Online learning in general games
- *HW4: implement no-regret algorithms that converge to correlated equilibria in general games*

## Data Science for Auctions and Mechanisms

4

- Basics and applications of auction theory (T+A)
- Basic Auctions and Learning to bid in auctions (T)
- *HW5: implement bandit algorithms to bid in ad auctions*

5

- Optimal auctions and mechanisms (T)
- Simple vs optimal mechanisms (T)
- *HW6: implement simple and optimal auctions, analyze revenue empirically*

6

- Basics of Statistical Learning Theory (T)
- Optimizing Mechanisms from Samples (T)
- *HW7: implement procedures to learn approximately optimal auctions from historical samples and in an online manner*

## Further Topics

7

- Econometrics in games and auctions (T+A)
- A/B testing in markets (T+A)
- *HW8: implement procedure to estimate values from bids in an auction, empirically analyze inaccuracy of A/B tests in markets*

## Guest Lectures

- Mechanism Design for LLMs, Renato Paes Leme, Google Research
- Auto-bidding in Sponsored Search Auctions, Kshipra Bhawalkar, Google Research

# Summarizing Last Lecture

**Myerson's Theorem.** When valuations are independently distributed, for any BIC, NNT and IR mechanism (and any BNE of a non-truthful mechanism), the payment contribution of each player is their expected virtual value

$$E[\hat{p}_i(v_i)] = E[\hat{x}_i(v_i) \cdot \phi_i(v_i)], \qquad \phi_i(v_i) = v_i - \frac{1 - F_i(v_i)}{f_i(v_i)}$$

**Corollary.** When valuations are independently distributed, for any Bayes-Nash equilibrium of any non-truthful mechanism, the payment contribution of each player is their expected virtual value

$$E[\hat{p}_i(v)] = E[\hat{x}_i(v_i) \cdot \phi_i(v_i)], \qquad \phi_i(v_i) = v_i - \frac{1 - F_i(v_i)}{f_i(v_i)}$$

**Myerson's Optimal Auction.** Assuming that virtual value functions are monotone non-decreasing, the mechanism that maximizes virtual welfare, achieves the largest possible revenue among all possible mechanisms and Bayes-Nash

$$x(v) = \mathrm{argmax}_{x \in X} \sum_i x \cdot \phi_i(v_i), \qquad p_i(v) = v_i x_i(v) - \int_0^{v_i} x_i(z, v_{-i})\, dz$$

$$\mathrm{Rev} = E\left[\max_{x \in X} \sum_i x \cdot \phi_i(v_i)\right]$$

Optimal auction is
1) cumbersome, 2) hard to understand, 3) hard to explain, 4) does not always allocate to the highest value player, 5) discriminates a lot, 6) is many times counter-intuitive, 7) can seem unfair!

# Second-Price with Player-Specific Reserves

- What if we simply run a second price auction but have different reserves for each bidder

- Each bidder $i$ has a reserve price $r_i$
- Reject all bidders with bid below the reserve
- Among all bidders with value $v_i \geq r_i$, allocate to highest bidder
- Charge winner max of their reserve and the next highest surviving bid

# Second-Price with Player-Specific Reserves

**Theorem.** There exist personalized reserve prices such that the above auction achieves at least ½ of the optimal auction revenue!

- Choose $\theta$ such that:

$$\Pr\left(\max_i \phi_i^+(v_i) \geq \theta\right) = 1/2$$

- Then set personalized reserve prices implied by:

$$\phi_i^+(v_i) \geq \theta \Leftrightarrow v_i \geq r_i$$

All these designs required knowledge of distributions of values $F_i$!

What can we do if we only have data from $F_i$?

# Learning Auctions from Samples

# Learning from Samples

- We are given a set $S$ of $m$ samples of value profiles

$$S = \left\{ v^j = \left( v_1^j, \dots, v_n^j \right) \right\}_{j=1}^{m}$$

- Each sample is drawn i.i.d. from the distribution of values

$$v_i^j \sim F_i, \qquad v^j \sim \boldsymbol{F} \overset{\text{def}}{=} F_1 \times \cdots \times F_n$$

- Samples can be collected from historical runs of truthful auction
- Bids of each bidder in each of the $m$ historical runs of the auction

# Desiderata

- Without knowledge of distributions $F_i$, we want to produce a mechanism $M_S$, that achieves good revenue on these distributions
- For some $\epsilon(m) \to 0$ as the number of samples grows:

$$\mathrm{Rev}(M_S) \stackrel{\text{def}}{=} E_{v\sim F}\left[\sum_i p_i^{M_S}(v)\right] \geq \mathrm{OPT}(\boldsymbol{F}) - \epsilon(m)$$

- Either in expectation over the draw of the samples, i.e.

$$E_S[\mathrm{Rev}(M_S)] \geq \mathrm{OPT}(\boldsymbol{F}) - \epsilon(m)$$

- Or with high-probability over the draw of the samples, i.e.

$$\text{w.p. } 1-\delta: \quad \mathrm{Rev}(M_S) \geq \mathrm{OPT}(\boldsymbol{F}) - \epsilon_\delta(m)$$

# Easy Start: Pricing from Samples

# Pricing from Samples

- Suppose we have only one bidder with $v \sim F$, for simplicity in $[0,1]$
- Optimal mechanism is to post the monopoly reserve price
- The optimal price $r$ is the one that maximizes
$$\mathrm{Rev}(r) = E_{v\sim F}[r \cdot 1\{v \geq r\}] = r \Pr(v \geq r) = r\left(1 - F(r)\right)$$
  which is the monopoly reserve price $\eta$ that solves:
$$\eta - \frac{1 - F(\eta)}{f(\eta)} = 0$$
- Choosing $\eta$ requires knowledge of the CDF $F$ and the pdf $f$
- Can we optimize $r$ if we have $m$ samples of $v$?

# The Obvious Algorithm

- We want to choose $r$ that maximizes

$$\max_{r\in[0,1]} \text{Rev}(r) \stackrel{\text{def}}{=} E_{v\sim F}[r\cdot 1\{v\geq r\}], \qquad \text{(population objective)}$$

- With $m$ samples $S$, we can optimize average revenue on samples!

$$\max_{r\in[0,1]} \text{Rev}_S(r) \stackrel{\text{def}}{=} \frac{1}{m}\sum_{j=1}^{m} r\cdot 1\{v^j\geq r\}, \qquad \text{(empirical objective)}$$

- This approach is called Empirical Reward Maximization (ERM)
- **Intuition.** Since each value is drawn from distribution $F$ the empirical average over i.i.d. draws from $F$, by law of large numbers, should be very close to expected value

Same as Empirical Risk Minimization (ERM) in Machine Learning (loss vs reward)

# A Potential Problem with ERM

- The Law of Large Numbers applies if we wanted to evaluate the revenue of a fixed reserve price, we had in mind using the samples
- If we optimize over a very large set of reserve prices, then by random chance, it could be that we find a reserve price that has a large revenue on the samples, but small on the distribution

- This behavior is called overfitting to the samples
- We need to argue that overfitting cannot arise when we optimize over the reserve price!

# Basic Elements of Statistical Learning Theory

# Uniform Convergence

- Uniform Convergence. Suppose that we show that, w.p. $1-\delta$

$$\forall r \in [0,1]:\ |\mathrm{Rev}_S(r) - \mathrm{Rev}(r)| \le \epsilon_\delta(m)$$

- Alert. Note that this is different than: $\forall r \in [0,1]$, w.p. $1-\delta$

$$|\mathrm{Rev}_S(r) - \mathrm{Rev}(r)| \le \epsilon_\delta(m)$$

- The first asks that with probability $1-\delta$, the empirical revenue of all reserve prices is close to their population revenue
- The second asks that for a given reserve price, with probability $1-\delta$ its empirical revenue is close to its population
- The second claims nothing about the probability of the *joint event* that this is satisfied for all prices simultaneously

# Uniform Converges Suffices for No-Overfitting

- Uniform Convergence. Suppose that we show that, w.p. $1-\delta$

$$\forall r \in [0,1]:\ |\mathrm{Rev}_S(r) - \mathrm{Rev}(r)| \le \epsilon_\delta(m)$$

- Empirical Risk Maximization reserve:

$$r_S = \underset{r\in[0,1]}{\mathrm{argmax}}\ \mathrm{Rev}_S(r)$$

**Theorem.** If uniform convergence holds then, w.p. $1-\delta$

$$\mathrm{Rev}(r_S) \ge \mathrm{Rev}(\eta) - 2\epsilon_\delta(m) = \mathrm{OPT}(F) - 2\epsilon_\delta(m)$$

# Uniform Converges Suffices for No-Overfitting

**Theorem.** If uniform convergence holds then, w.p. $1-\delta$

$$\mathrm{Rev}(r_S) \geq \mathrm{Rev}(\eta) - 2\epsilon_\delta(m) = \mathrm{OPT}(F) - 2\epsilon_\delta(m)$$

- By uniform convergence, with probability $1-\delta$:

$$\boxed{\mathrm{Rev}(\mathrm{r_S}) \geq \mathrm{Rev}_S(r_S) - \epsilon_\delta(m)}$$

- Since, $r_S$ optimizes the empirical objective

$$\boxed{\mathrm{Rev}_S(r_S) \geq \mathrm{Rev}_S(\eta)}$$

- By uniform convergence:

$$\mathrm{Rev}_S(\eta) \geq \mathrm{Rev}(\eta) - \epsilon_\delta(m)$$

- Putting it all together:

$$\mathrm{Rev}(r_s) \geq \mathrm{Rev}(\eta) - 2\epsilon_\delta(m)$$

This is the no-overfitting property: It **cannot be** that we found a reserve price that has *large empirical revenue* but very *small population revenue*

The *monopoly reserve* is a **feasible** reserve price but **was not chosen** by ERM. So, it must have had smaller empirical average revenue.

# LLN vs Uniform Convergence

Crucial Argument: with probability $1-\delta$: $\mathrm{Rev}(\mathrm{r}_S) \geq \mathrm{Rev}_S(r_S) - \epsilon_\delta(m)$

- Cannot be argued solely using Law of Large Numbers: if we have i.i.d. $X^j$ with mean $E[X]$

$$\left|\frac{1}{m}\sum_{j=1}^{m} X^j - E[X]\right| \to 0$$

- For reserve price $r$ that is chosen before looking at the samples, define $X^j(r) = r \cdot\ 1\{v^j \geq r\}$

$$|\mathrm{Rev}_S(r) - \mathrm{Rev}(r)| = \left|\frac{1}{m}\sum_{j} r \cdot 1\{v^j \geq r\} - E[r \cdot 1\{v \geq r\}]\right| \to 0$$

- Problem. The reserve price $r_S$ was chosen by looking at all the samples in $S$
  - If I tell you $r_S$ you learn something about the samples
  - Conditional on $r_S$ the samples are no-longer i.i.d.

- Uniform convergence, essentially means "*what I learn about S from $r_S$ is not that much…*"

# Concentration Inequalities and Uniform Convergence

- Concentration inequalities give us a stronger version of LLN

- Chernoff-Hoeffding Bound. If we have i.i.d. $X^j \in [0,1]$ with mean $E[X]$, w.p. $1-\delta$:

$$\left|\frac{1}{m}\sum_{j=1}^{m} X^j - E[X]\right| \le \epsilon_\delta(m) \stackrel{\text{def}}{=} \sqrt{\frac{\log(2/\delta)}{2m}}$$

- Crucial. The bound grows only logarithmically with $1/\delta$

# Union Bound

- Suppose we had only $K$ possible reserve prices $\left\{\frac{1}{K}, \frac{2}{K}, \frac{3}{K} \dots, 1\right\}$
- For each reserve price $r$ on the grid, for any probability $\delta'$, by Chernoff bound

$$\Pr\left((\text{Bad Event})_r\right) = \Pr\left(\left|\frac{1}{m}\sum_{j=1}^{m} X^j(r) - E[X(r)]\right| > \epsilon_{\delta'}(m)\right) \leq \delta'$$

- Union Bound. The probability of the union of events is at most the sum of the probabilities

$$\Pr\left(\cup_{r=1}^{K} (\text{Bad Event})_r\right) \leq \sum_{r=1}^{K} \Pr\left((\text{Bad Event})_r\right) \leq K \cdot \delta'$$

- Apply Chernoff bound with $\delta' = \delta/K$

$$\Pr\left(\cup_{r=1}^{K} (\text{Bad Event})_r\right) \leq \delta$$

- Probability(*exists reserve price whose empirical revenue is far from its population*) at most $\delta$

# Uniform Convergence via Union Bound

**Theorem.** Suppose we had $K$ possible reserve prices $\mathrm{Grid}_{\mathrm{K}} \stackrel{\text{def}}{=} \left\{\frac{1}{K}, \frac{2}{K}, \frac{3}{K} \dots, 1\right\}$

Then with probability at least $1 - \delta$

$$\forall r \in \mathrm{Grid}_{\mathrm{K}}: |\mathrm{Rev}_S(r) - \mathrm{Rev}(r)| \leq \epsilon_{\delta/K}(m) \stackrel{\text{def}}{=} \sqrt{\frac{\log(2K/\delta)}{2m}}$$

Problem. The optimal reserve $\eta$ can potentially not be among these $K$ reserves

Intuition. For a sufficiently large $K$, for any reserve price, we can find a reserve price on this discretized grid that achieves almost as good revenue

We don't lose much by optimizing over the grid!

# Discretization

- For a reserve price $r$, pick largest reserve price below $r$ on the grid
- Denote this discretization of $r$ as $r_K$

- By doing so, you allocate to any value you used to allocate before
- For any such value you receive revenue at least $r - 1/K$

- Overall, you lose revenue at most $1/K$

$$\mathrm{Rev}(r_K) \geq \mathrm{Rev}(r) - 1/K$$

# Discretized ERM

- Let's modify ERM to optimize only over the grid
$$r_S = \max_{r \in \mathrm{Grid}_K} \mathrm{Rev}_S(r)$$
- We can apply the uniform convergence over the grid
$$\boxed{\mathrm{Rev}(r_S) \geq \mathrm{Rev}_S(r_S) - \epsilon_{\delta/K}(m)}$$
We cannot overfit, when optimizing over the grid of reserves
- Since, $r_S$ optimizes the empirical objective over the grid
$$\boxed{\mathrm{Rev}_S(r_S) \geq \mathrm{Rev}_S(\eta_K)}$$
The *discretized monopoly reserve* is a **feasible** reserve in the grid but **was not chosen** by ERM.
- By uniform convergence over the grid:
$$\mathrm{Rev}_S(\eta_K) \geq \mathrm{Rev}(\eta_K) - \epsilon_{\delta/K}(m)$$
- By the discretization error argument:
$$\mathrm{Rev}(\eta_K) \geq \mathrm{Rev}(\eta) - 1/K$$

**Theorem.** The revenue of the reserve price output by discretized ERM over the K-grid satisfies, with probability $1 - \delta$

$$\mathrm{Rev}(r_S) \geq \mathrm{OPT}(F) - 2\sqrt{\frac{\log(2K/\delta)}{2m}} - \frac{1}{K}$$

Choosing $K = 1/m$

$$\mathrm{Rev}(r_S) \geq \mathrm{OPT}(F) - 3\sqrt{\frac{\log(2m/\delta)}{2m}}$$

Desideratum satisfied!
$\epsilon_\delta(m) \to 0$ as $m$ grows

# The Limits of Discretization

- Do we really need to optimize over the discrete grid?
- What if we insist on optimizing over $[0,1]$. Can we still overfit?

- Now that we have infinite possible reserves, we cannot apply the union bound argument ($K = \infty$)!
- How do we argue about optima over continuous, infinite cardinality spaces?

# Sneak Peek

- Would have been ideal if we only have to argue about behavior of our optimization space, *on the given set of samples*
- As opposed to the unknown distribution of values

- What if we can find  a small set of reserves and argue that for all reserves there is an approximately equivalent one in the small set, in terms of revenue on the samples

- Maybe then it suffices to invoke the union bound over the smaller space, even though we optimize over the bigger space

# Statistical Learning Theory

# General Framework

- Given samples $S = \{v_1, \dots, v_m\}$ that are i.i.d. from distribution $F$
- Given a hypothesis/function space $H$
- Given a reward function $r(v; h)$

- Goal is to maximize the expected reward over distribution $F$
$$R(h) = E_{v \sim F}[r(v; h)]$$

# Desiderata

- Without knowledge of distribution $F$, we want to produce a hypothesis $h_S$, that achieves good reward on this distribution
- For some $\epsilon(m) \to 0$ as the number of samples grows:

$$R(h_S) \stackrel{\text{def}}{=} E_{v\sim F}[r(v;h)] \geq \max_{h\in H} R(h) - \epsilon(m)$$

- Either in expectation over the draw of the samples, i.e.

$$E_S[R(h_S)] \geq \max_{h\in H} R(h) - \epsilon(m)$$

- Or with high-probability over the draw of the samples, i.e.

$$\text{w.p. } 1-\delta: \quad R(h_S) \geq \max_{h\in H} R(h) - \epsilon_\delta(m)$$

# Desiderata (Mechanism Design from Samples)

- Without knowledge of $\boxed{\text{Distribution of value profiles } F}$, we want to produce a hypothesis $h_S$, that achieves good $\boxed{\text{Revenue}}$ on this distribution
- For some $\epsilon(m) \to 0$ as the number of samples grows:

$$R(h_S) \stackrel{\text{def}}{=} E_{v\sim F}\boxed{\left[\sum_i p_i(v)\right]} \geq \max_{h\in H} R(h) - \epsilon(m)$$

- Either in expectation over the draw of the samples, i.e.

$$E_S[R(h_S)] \geq \max_{h\in H} R(h) - \epsilon(m)$$

- Or with high-probability over the draw of the samples, i.e.

$$\text{w.p. } 1-\delta: \quad R(h_S) \geq \max_{h\in H} R(h) - \epsilon_\delta(m)$$

# The Obvious Algorithm

- We want to choose $r$ that maximizes

$$\max_{h \in H} R(h) \stackrel{\text{def}}{=} E_{v \sim F}[r(v; h)], \qquad \text{(population objective)}$$

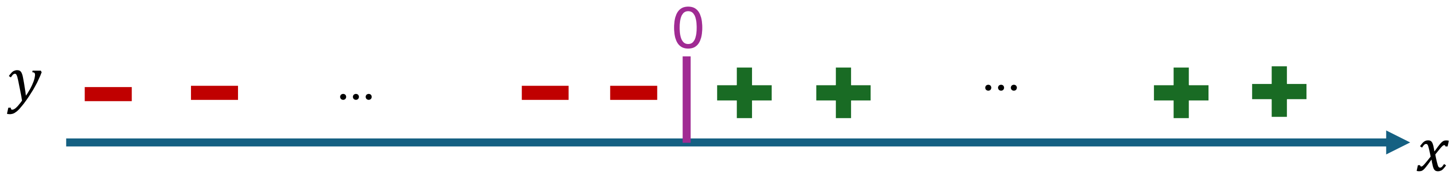
- With $m$ samples, we can optimize average reward on samples!

$$\max_{h \in H} R_S(h) \stackrel{\text{def}}{=} \frac{1}{m} \sum_{j=1}^{m} r(v_j; h), \qquad \text{(empirical objective)}$$

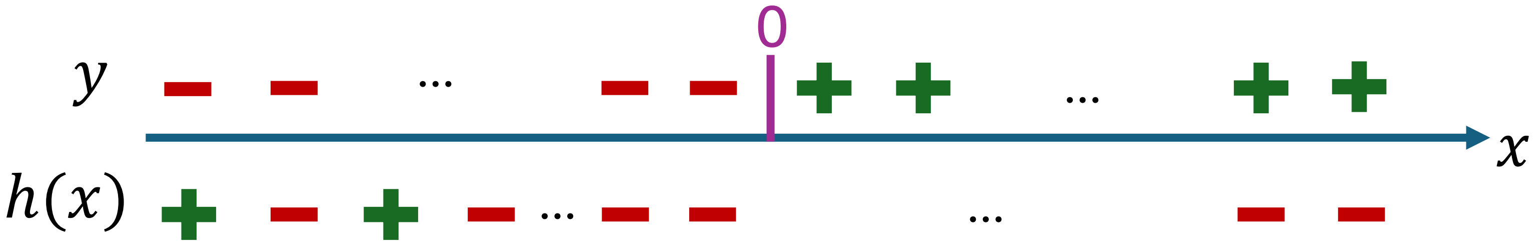
- This approach is called Empirical Reward Maximization (ERM)
- **Intuition.** Since each value is drawn from distribution $F$ the empirical average over i.i.d. draws from $F$, by law of large numbers, should be very close to expected value

# Standard Classification Example

- Suppose samples $v = (x, y)$ where $x \sim U[-1,1]$ and $y \in \{-1, 1\}$




- We want to choose a "labeling" function $h(x) \in \{-1,1\}$

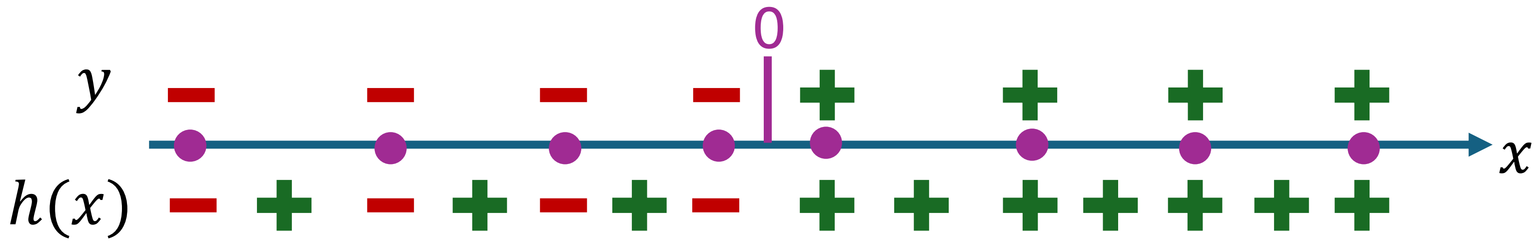



- That achieves good accuracy

$$r(v; h) = 1\{h(x) = y\}$$

# ERM Gone Bad

- Suppose we choose the following $h_S$: label all samples correctly and predict $+1$ for any value that is not on the samples

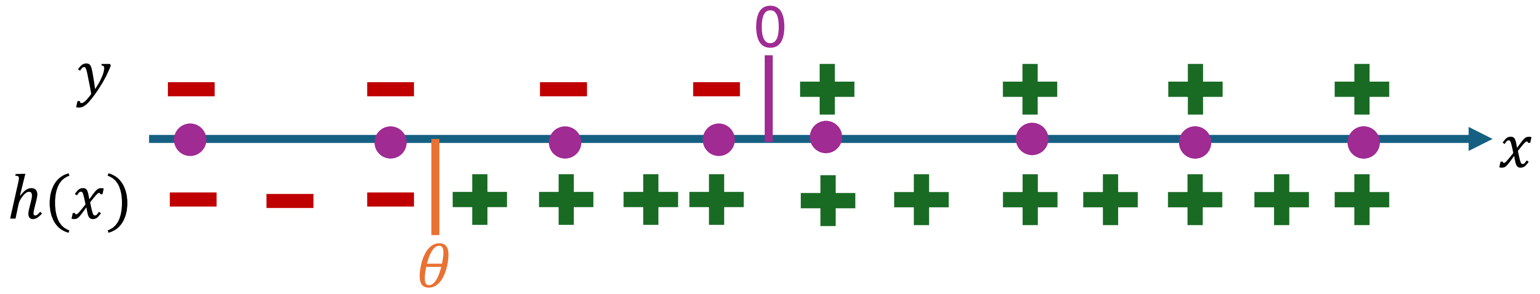



- The empirical average reward of this $h_S$ is $1$. The largest possible!
- The expected reward of this $h_S$ is ½
- The discrepancy between the empirical reward of the ERM solution and its population reward never vanishes! Overifitting!

# ERM Over Threshold Functions

- Suppose we restrict to optimizing over threshold functions
- Label every $x \geq \theta$ with $+1$ and every $x < \theta$ with $-1$

$$H = \{x \to 1(x \geq \theta) - 1(x < \theta) : \theta \in \Theta\}$$

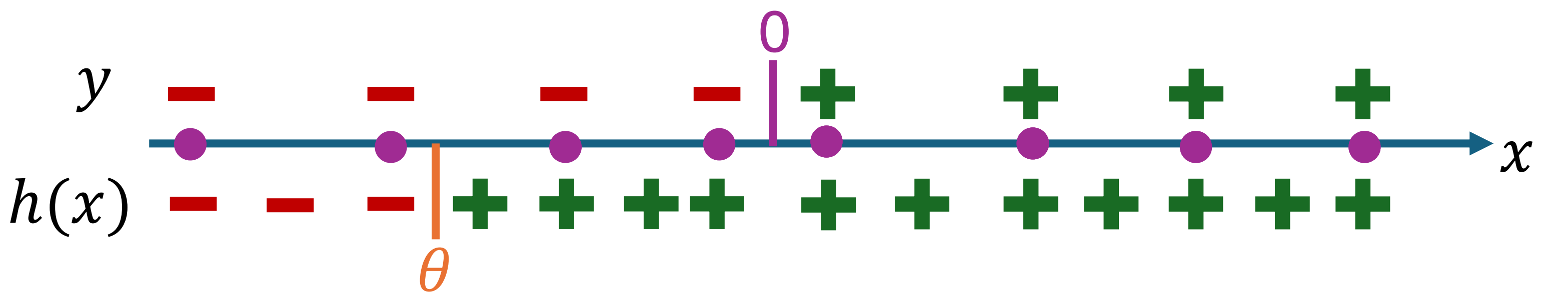



- Optimizing over such $\theta$ we will never be able to overfit
- How do we argue this?
- Discretization argument fails!
- No matter how we discretize, there exists a distribution of $x$ that will have a very large discretization error

# Sufficient Hypothesis Subspace on Samples

- Suppose we restrict to optimizing over threshold functions
- Label every $x \geq \theta$ with $+1$ and every $x < \theta$ with $-1$

$$H = \{x \to 1(x \geq \theta) - 1(x < \theta) : \theta \in \Theta\}$$




- Given the $m$ samples, then on the samples there are at most $m + 1$ equivalent hypothesis: choose the threshold on the sample (or $\theta = 1$)
- Every other hypothesis produces the exact same labeling of the samples and achieves the same empirical reward
- Is there an argument that only takes union bound over this set?

# Back to the General Framework

- We will try to argue the expected performance

$$E_S[R(h_S)] \geq \max_{h \in H} R(h) - \epsilon(m)$$

- Expected Sample Average *Representativeness*: suppose that

$$\text{Rep} = \boxed{E_S\left[\sup_{h \in H} R_S(h) - R(h)\right]} \leq \epsilon(m)$$

How good is the sample average in terms of **representing** the population expectation, in the worst case over $H$

- Then we can prove expected error of $\epsilon(m)$

$$E_S[R(h_S)] = E[R_S(h_S)] - E[R_S(h_S) - R(h_S)] \geq E[R_S(h_S)] - \epsilon(m)$$

- Since $h_S$ optimizes $R_S(h)$ and $h_* = \text{argmax}_{h \in H} R(h)$ is feasible

$$E[R_S(h_S)] \geq \boxed{E[R_S(h_*)] = R(h_*)}$$

$h_*$ does not depend on the samples

$$E[R_S(h_*)] \overset{\text{def}}{=} \frac{1}{m} \sum_j E\left[h\left(v^j; h_*\right)\right] = E[h(v; h_*)] = R(h_*)$$

If we can bound representativeness

$$\mathrm{Rep} = E_S\left[\sup_h R_S(h) - R(h)\right] \leq \epsilon(m)$$

Then we can bound expected performance

$$E[R(h_S)] \geq E[R(h_*)] - \epsilon(m)$$