Distinguishing Distributions When Samples Are Strategically Transformed

Hanrui Zhang
Duke

Yu Cheng
UIC

Vincent Conitzer
Duke

Example: Academic Job Market

- ML-theory
- ML-flexible
- ML-applied
- ML-theory

θ: “types”

<table>
<thead>
<tr>
<th>0.8</th>
<th>0.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.8</td>
<td>0.2</td>
</tr>
</tbody>
</table>

S: “samples”

<table>
<thead>
<tr>
<th>0.8</th>
<th>0.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.8</td>
<td>0.2</td>
</tr>
</tbody>
</table>

(EP) Θ

- “How do I distinguish myself from other types?”
- “How many ideas (years) do I need for that?”

Principal’s problem:
- “How do I tell ML-flexible agents from others?”
- “After how many papers should I feel confident?”

The Problem

agent θ generates iid samples

agent receives samples D

agent wants to convince principal to accept, no matter what type he is

agent generates a report R from D

r = [r₁, ..., rₘ]: iid samples

principal sets a policy f

policy f(R) ∈ [0, 1] maps report R to probability of accepting R

principal observes policy f

policy f = [f₁, ..., fₘ] of signals from samples, where (r₁, ..., rₘ) ∈ E

Theorem.

For any x and y, d_{TV}(x, y) = MaxSep(x, y)

Theorem.

To distinguish x from any y where d_{TV}(x, y) ≥ ε:

- Collect T = Ω(ρ / ε²) signals, where ρ is the width of Σ
- Accept if d_{TV}(x, z) < ε / 2, where z is empirical distribution of signals
- Policy is independent of y

Take-home message:

- Efficient learner & identity tester exist; width measures complexity of the space

See Also

When Samples Are Strategically Selected. Z-C-C. In ICML’19

Optimal Policy: the General Case

(Good) agent’s perspective:
- “How do I distinguish myself from bad types?”
- Answer: report as far from bad types as possible

\[ d_{TV}(x, y) = \max_{\alpha \in \Delta(S)} \min_{\beta \in \Delta(T)} d_{TV}(\alpha, \beta) \]

where x, y ∈ Δ(Σ), α, β ∈ Δ(Σ)

Principal’s perspective:
- “How do I tell good agents from others?”
- Answer: ask for a set of signals that maximize both good types

\[ \text{MaxSep}(x, y) = \max_{\alpha \in \Delta(S)} (\max_{\beta \in \Delta(T)} \alpha(A) \cdot \max_{\beta \in \Delta(T)} \beta(A)) \]

Theorem.

When signals are partially ordered:

- The revelation principle holds

\[ d_{TV}(x, y) = \min_{\alpha \in \Delta(S)} d_{TV}(x, \alpha) \]

Take-home message:

- With strategic transformation, d_{TV} = MaxSep plays the role of d_{TV} in classical tasks

When Signals Are Partially Ordered

Observation: no one ever wants to publish an ICML paper (which is by no means true in reality)

- But, why?
- Answer: because the signal space is partially ordered!

\[ S = \Xi \]

Theorem.

When Signals Are Partially Ordered

- The revelation principle holds

\[ d_{TV}(x, y) = \min_{\alpha \in \Delta(S)} d_{TV}(x, \alpha) \]

Take-home message:

- Efficient learner & identity tester exist; width measures complexity of the space

See Also

When Samples Are Strategically Selected. Z-C-C. In ICML’19

Future Work:

- Develop a general model for any Σ
- Explore more complex settings
- Improve the efficiency of the learner

Take-home message:

- With strategic transformation, d_{TV} = MaxSep plays the role of d_{TV} in classical tasks

See Also

When Samples Are Strategically Selected. Z-C-C. In ICML’19

Future Work:

- Develop a general model for any Σ
- Explore more complex settings
- Improve the efficiency of the learner

Take-home message:

- With strategic transformation, d_{TV} = MaxSep plays the role of d_{TV} in classical tasks

See Also

When Samples Are Strategically Selected. Z-C-C. In ICML’19