CS229r : IT & CS

4/2/2019

LECTURE 17

TODAY

INFORMATION = AMORTIZED COMMUNICATION

* Interactive Correlated Sampling

(~~Aside~~ Warning: Will refer to notes from Lecture 16 for some parts)

Definitions from last time

1. $f^{\otimes n} : \mathcal{X}^n \times \mathcal{Y}^n \to R^n$

$$f(x_1 .. x_n; y_1 .. y_n) = (f(x_1; y_1) \dots f(x_n, y_n)).$$

2. Π ~~computes~~ solves $f^{\otimes n}$ with ϵ-error if

$$\forall i \quad \Pi(x_1 .. x_n, y_1 .. y_n)_i = f(x_i; y_i) \quad \text{w.p.} \geq 1-\epsilon.$$

3. $$CC^n_\epsilon(f) = \min_{\substack{\Pi : \Pi \text{ solves } f^{\otimes n} \\ \text{with error } \epsilon}} \{CC(\Pi)\}$$ ← w/w.o. prior.

$$IC^n_\epsilon(f) = \min_{\substack{\Pi : \text{ same} \\ \text{as above}}} \{IC(\Pi)\}$$ ← defined with some prior μ.

Theorem [Braverman-Rao]

$$\forall \mu \quad CC^n_{\epsilon,\mu}(f) = IC^n_{\epsilon,\mu}(f)\cdot(1+o_n(1))$$

---

1. $IC^n_{\epsilon,\mu}(f) = n\cdot IC^1_{\epsilon,\mu}(f).$

$\Uparrow$

(a) $IC^n_{\epsilon,\mu}(f) \le n\cdot IC^1_{\epsilon,\mu}(f)$

Proof: Suppose π solve f with error ϵ. then $\pi^{\otimes n}$ solves $f^{\otimes n}$ with error ϵ.

$$IC(\pi^{\otimes n}) = n\cdot IC(\pi)$$

(b) $IC^n_{\epsilon,\mu}(f) \ge n\cdot IC^1_{\epsilon,\mu}(f)$

see page 6 of 2.16 notes + 7

More ~~Crucial Step~~:

Corollary: $CC^n_{\epsilon,\mu}(f) \ge IC^n_{\epsilon,\mu}(f) \ge n\cdot IC^1_{\epsilon,\mu}(f)$

Need to show

$$\cancel{IC^1_{\epsilon,\mu}(f)}\ CC^n_{\epsilon,\mu}(f) \le n\cdot IC^1_{\epsilon,\mu}(f)\cdot(1+o(1))$$

[New "compression protocol"].

Interactive Correlated Sampling

$$\text{Alice} \leftarrow P \qquad \overset{\epsilon}{\longleftrightarrow} \qquad Q \rightarrow \text{Bob}$$

$$\begin{array}{ccc} \text{Alice} & & \text{Bob} \\ \downarrow & & \downarrow \\ x \sim P & & y \end{array}$$

s.t. $\forall x \quad \Pr[y = x] \geq 1 - \epsilon$.

Comm. $\leq \quad D(P\|Q) + O\left(\sqrt{D(P\|Q)} + \log \frac{1}{\epsilon}\right)$.

Key Idea

- Suppose $C = \frac{Q(x)}{P(x)}$ known [very unreasonable!]
- Alice outputs first x_i s.t. (x_i, a_i) satisfies $a_i < P(x$
- Bob: Scale Q by factor C
  - Now needs to output one of the set

$$S = \{ (x_j, a_j) \mid a_j < C \cdot Q(x_j) \}$$

  - Which one?
  - Alice send $\log C + O(1)$ bits of hash of x_i to Bob
  - hopefully ~~isolates~~ identifies x_i uniquely in S.

  Alice outputs the unique ~~ele~~ element

- **Challenge:** ~~P(x)~~ $Q(x)/P(x)$ is unknown!

- Can we try to guess then check?

- Answer: YES!.

  faster than linear is good to get $o(1)$ behavior.

- Will try $\frac{Q(x)}{P(x)} \le 2^{1^2}, 2^{2^2}, 2^{3^2}, \ldots$

  $= C_1, C_2 \ldots C_t$ needs to be sub-exp.

  - say T = correct C_t.
  - ~~suffices~~ to argue that at ~~correct~~ when ~~we first~~ reach $C_t > \frac{Q(x)}{P(x)}$, ~~succeed w.p.~~ ~~(X_i, a_i) is the unique point under $C_t \cdot Q(x)$~~

    with hash values matching

- for every $t = 1 \ldots T$ for every (x_j, a_j) $j < i$

  either $a_j > C_{t(j)} \cdot Q(x_j)$

  or $h(x_j) \neq h(x_i)$ for first $\log C_{t(j)}$ bits

- Analysis - for every t w.h.p. have $O(C_t)$ elements in set. $[\text{error} \le \epsilon \cdot 2^{-t}]$

  - $\Pr[\text{hash matches for any element}] \le \frac{\epsilon \cdot 2^{-t}}{C_t}$

  $\Rightarrow \Pr[t \text{ round failure}] \le \epsilon 2^{-t}$

Final Compression Protocol

- Compress each round to $D(P_v^A \| P_v^B) \mid v$ on i^{th} level.
- Total comm. $= D(P\|Q) + O\left(\sqrt{D(P\|Q)} + \log\frac{1}{\epsilon}\right)$

$$= IC + O(\sqrt{IC} + \log 1/\epsilon).$$

$\boxtimes$