Lecture 21

Today: ① hardness of approximate IQP sampling for classical computers

② Stockmeyer's approx. counting thm.

Refs:

[Bremner Montanaro Shepherd '15]
[Stockmeyer '83]
[Sipser '83]

Recall:

Approximate IQP sampling: Sample from a distribution $\tilde{p}$ that is ϵ-close to the output distribution of a given IQP circuit.

Goldberg Guo 2014

#P-hard

$PH \subseteq P^{\#P}$ (Toda's thm)

IQP output prob. estimation: Compute estimate of the output prob. $|\langle 0|U|0\rangle|^2$ to within 0.001 relative error.

Stockmeyer '83:

in $BPP^{NP} \subseteq \Sigma_3$

BPP output prob. estimation: Compute estimate of an output probability of a randomized classical poly-size circuit to within ϵ relative error.

Conjecture 1 [Average-case hardness of IQP output prob. estimation]

There is no algorithm in PH which succeeds at IQP output prob. estimation for a $1/30$ fraction of all instances.

Thm: [BMS 2015?] Suppose conjecture 1 holds. Then there is no efficient classical randomised alg. for approximate IQP sampling.

Pf: Suppose (to reach contradiction) that $\exists$ an efficient cl. randomised algorithm $\mathcal{A}$ for approximate IQP sampling.

Let $\vec{w}$ be chosen unif. at random.

Alg. $\mathcal{A}$ samples from $\tilde{p}$ s.t

$$\boxed{\sum_z |\tilde{p}(z) - \underbrace{p(z)}_{\text{true output distribution}}| \leq 10^{-8} \overset{\text{def}}{=} \delta}$$

Suppose we choose $y \in \{0,1\}^n$ unif. at random

$$\mathbb{E}_y \left[|\tilde{p}(y) - p(y)| \right] \leq \delta / 2^n$$

recall Markov's inequality: for r.v $Y \geq 0$ and $\Gamma > 0$ $\Pr[Y \geq \Gamma] \leq \frac{\mathbb{E}[Y]}{\Gamma}$

Markov $\Rightarrow$ with prob ≥ 0.95

$$(*) \quad \underbrace{|\tilde{p}(y) - p(y)| \leq \frac{\delta}{2^n} \frac{1}{(0.05)} = \frac{20\delta}{2^n}}$$

$$Y = |\tilde{p}(y) - p(y)|$$

$$\Gamma = \frac{\mathbb{E}[Y]}{0.05}$$

$$\Pr\left[|\tilde{p}(y) - p(y)| \geq \frac{20\delta}{2^n} \right] \leq 0.05$$

Now use Stockmeyer approx. counting to estimate $\tilde{p}(y)$:

$\Rightarrow$ classical alg in 3rd level of PH that computes $\tilde{r}(y)$

s.t

$$(**) \quad |\tilde{r}(y) - \tilde{p}(y)| \leq \delta \, \tilde{p}(y) \qquad (\text{recall } \delta = 10^{-8})$$

Show that $\tilde{r}(y)$ is a good approx to $p(y)$:

$$|\tilde{r}(y) - p(y)| \leq |\tilde{r}(y) - \tilde{p}(y)| + |\tilde{p}(y) - p(y)|$$

$$\overset{(**)}{\leq} \delta\, \tilde{p}(y) + |\tilde{p}(y) - p(y)| \qquad \tilde{p}(y) = p(y) + \tilde{p}(y) - p(y)$$

$$\leq \delta\, p(y) + \underbrace{(1+\delta)}_{\leq 2} \underbrace{|\tilde{p}(y) - p(y)|}_{\leq 20\delta/2^n} \quad \text{with prob} \geq 0.95$$

$$\leq \delta\, p(y) + \frac{40\delta}{2^n} \qquad \text{with prob} \geq 0.95$$

ANTICONCENTRATION:

Fact [BMS 2015]: $\Pr_y\left[\, p(y) \geq 0.5/2^n \,\right] \geq 1/12$

if this is true then $\frac{40\delta}{2^n} \leq 2\, p(y) \cdot 40\delta$

UNION BND WITH PROB $\geq \frac{1}{12} - \frac{1}{20} \geq \frac{1}{30}$

$$\Rightarrow |\tilde{r}(y) - p(y)| \leq (\delta + 80\delta)\, p(y) \leq 0.001\, p(y)$$

$$p(y) = |\langle y| H^{\otimes n} D_{\vec{\omega}} H^{\otimes n} |0\rangle|^2$$

$$= |\langle 0| X(y) H^{\otimes n} D_{\vec{\omega}} H^{\otimes n} |0\rangle|^2 \qquad X(y) = \prod_{j=1}^{n} X_j^{y_j}$$

$$= |\langle 0| H^{\otimes n} Z(y) D_{\vec{\omega}} H^{\otimes n} |0\rangle|^2$$

$$Z(y) = e^{\frac{i\pi}{2}\left(\sum_{j=1}^{n} z_j^{y_j}\right)} \qquad Z = e^{\frac{i\pi}{2} Z}$$

$$Z(y) D_{\vec{\omega}} = D_{\vec{\omega}'}$$

$\vec{\omega}'$ is uniform if $\vec{\omega}$ and y are.

$$= |\langle 0| H^{\otimes n} D_{\vec{\omega}'} H^{\otimes n} |0\rangle|^2$$

$\exists$ an alg in 3rd level of PH which solves IQP output prob. estimation for a fraction $\geq 1/30$ of all instances. Contradicts conjecture.

//

Stockmeyer Approximate Counting

[Stockmeyer 83, Sipser 83]

Let $S \subseteq \{0,1\}^n$

Let $H = (h_1, h_2, \ldots, h_n)$ where $h_i : \{0,1\}^n \to \{0,1\}^m$ $\quad m \le n$

h_i is a linear map over $\mathbb{F}_2$ (an $m \times n$ 0,1 matrix)

FOR EACH $z \in S$ $\exists$ a register where it doesn't collide.

Define

$$\mathrm{Hash}(S, m, H) = \begin{cases} 0, & \text{if } \forall z \in S \ \exists\ i \in [n] \text{ s.t. } h_i(z) \neq h_i(z') \quad z' \neq z \in S \\ 1, & \text{if } \exists\ z, y_1, y_2, \ldots, y_n \in S \text{ s.t. } h_j(z) = h_j(y_j) \quad j = 1, \ldots, n, \ z \neq y_j \end{cases}$$

$\exists$ z s.t. it collides in every register.

Easy lemma $\quad \mathrm{Hash}(S, m, H) = 0 \implies |S| \le n \cdot 2^m$

Pf: Consider $z \to (h_1(z), h_2(z), \ldots, h_n(z))$ $\quad \mathrm{Hash}(S, m, H) = 0 \Rightarrow$ each z has a unite image.

$\Rightarrow |S| \le$