Today:

1. Hardness of approximate IQP sampling for classical computers
2. Stockmeyer's approx. counting thm.

Recall:

- Approximate IQP sampling:
  Sample from a distribution \( \tilde{\rho} \) that is \( \epsilon \)-close to the output distribution of a given IQP circuit.

- IQP output prob. estimation:
  Compute estimate of the output prob. \( \langle 0|1|0 \rangle^2 \) to within 0.001 relative error.

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

*P-hard

PH \subseteq P^#P

Stockmeyer '83:

- \( \text{BPP}^\text{NP} \leq \Sigma_3 \)

References:

- [Bremner, Montanaro, Shepherd 15]
- [Stockmeyer '83]
- [Sipser '83]
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 $\frac{1}{30}$ fraction of all instances.

\[ \text{Thm: Suppose conjecture 1 holds. Then there is no efficient classical randomised alg. for approximate IQP sampling.} \]

\[ \text{Pf: Suppose (to reach contradiction) that there is an efficient cl. randomised algorithm} \]
\[ \text{A for approximate IQP sampling.} \]

Let $\mathbf{z}$ be chosen uniformly at random.

Alg. $A$ samples from $\tilde{\rho}$ s.t.
\[ \sum_2 |\tilde{\rho}(z) - \rho(z)| \leq 10^{-8} \text{ def } S \]

Suppose we choose $y \in \{0,1\}^n$ uniformly at random
\[ \mathbb{E}_y \left[ |\tilde{\rho}(y) - \rho(y)| \right] \leq \frac{S}{2^n} \]
Recall Markov's inequality: for r.v. $Y > 0$ and $\Gamma > 0$ \( \Pr \{ Y > \Gamma \} \leq \frac{\mathbb{E}[Y]}{\Gamma} \).

Markov with prob $\geq 0.95$

\[
(\delta) \quad (\tilde{p}(y) - p(y)) \leq \frac{\delta}{2^n} \frac{1}{0.05} = \frac{20\delta}{2^n}
\]

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

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

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

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

\[ \Rightarrow \text{classical alg in 2nd level of PH that computes } \tilde{p}(y) \]

s.t.

\[ (\ast \star) \quad |\tilde{p}(y) - p(y)| \leq \delta \tilde{p}(y) \quad (\text{recall } \delta = 10^{-8}) \]
Show that \( \tilde{p}(y) \) is a good approx to \( p(y) \):

\[
|\tilde{p}(y) - p(y)| \leq |\tilde{p}(y) - \bar{p}(y)| + |\bar{p}(y) - p(y)|
\]

\[
\leq 8 \bar{p}(y) + 5 p(y) - p(y)
\]

\[
\leq 8 p(y) + (1+8) |\bar{p}(y) - p(y)|
\]

\[
\leq 2 \leq \frac{208}{2^n} \text{ with prob } \geq 0.95
\]

\[
\leq 8 p(y) + \frac{408}{2^n} \text{ with prob } \geq 0.95
\]

**Anticoncentration:**

\[ \Pr_y \left[ p(y) > \frac{0.5}{2^n} \right] \geq \frac{1}{12} \]

If \( m \) is the \( \frac{1}{12} - \frac{1}{20} \) with prob \( \geq \frac{1}{12} - \frac{1}{20} \) and \( \frac{1}{12} - \frac{1}{20} \) then \( \frac{408}{2^n} \leq 2 p(y) \cdot 408 \)

\[ \Rightarrow |\tilde{p}(y) - p(y)| \leq (8 + 808) p(y) \leq 0.001 p(y) \]
\[ \rho(y) = |\langle y | H^N | 0 \rangle|^2 \]
\[ = |\langle 0 | X(y) H^N | 0 \rangle|^2 \quad X(y) = \prod_{j=1}^{\mathcal{N}} X_j \]
\[ = |\langle 0 | H^N Z(y) D_z | 0 \rangle|^2 \]
\[ z(y) = e^{\frac{q}{\mathcal{N}} \sum_{j=1}^{\mathcal{N}} z_j} \]
\[ z = e^{\frac{q}{\mathcal{N}} z} \]
\[ z(y) D_z = D_z z \]
\[ \frac{1}{\mathcal{N}} \sum_{j=1}^{\mathcal{N}} \rho_j \]
\[ \rho(y) > \frac{1}{30} \]
\[ \sum_{j=1}^{\mathcal{N}} \rho_j \]

If an alg in 3rd level of PH which solves IQP output prob estimation for a fraction
\[ \frac{1}{30} \]

of all instances. Contradicts conjecture.
Let $S \subseteq \{0,1\}^n$

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

$h_i$ is a linear map over $F_2$
(an $m \times n$ 0,1 matrix)

For each $z \in S$ there is a register where it doesn't collide.

Define

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

Easy lemma

$$\text{Hash}(S, m, H) = 0 \Rightarrow |S| \leq n \cdot 2^m$$

PE: Consider $z \rightarrow (h_1(z), h_2(z), \ldots, h_n(z))$ $\text{Hash}(S, m, H) = 0 \Rightarrow$ each $z$ has a unique image.

$\Rightarrow |S| \leq$