Self-testing

Thomas Van Himbeeck

April 8, 2021

Lemma 1 (de Finetti). *Let $\boldsymbol{p} = p(x_1, \cdots x_n)$ be permutation invariant. Then for any $k \leq n$, the distribution obtained by tracing out k variables is close to a convex combination of iid distributions:*

$$|p(x_1, \cdots x_{n-k}) - \int \mu(q) \bigotimes_{i=1}^{n-k} q(x_i)| \leq \epsilon_{dF}(k, n) \tag{1}$$

where $\epsilon(n, k) \to 0$, when $n \to \infty$ and $n/k \to c$ remain proportional for some constant c.

Lemma 2 (Azuma-Hoeffding). *Let $0 \leq X_i \leq 1$ be iid. bounded random variables, with $E[X_i] = \mu$ then*

$$\Pr\left[\left|\frac{1}{n}\sum_{i=1}^{n} X_i - \mu\right| \geq \delta\right] \leq \epsilon_{AH}(\delta, n) \tag{2}$$

with $\epsilon_2(\delta, n) \to 0$ when $n \to \infty$ and δ is constant

Our protocol

1. Start with n boxes.
2. Pick a box $J \in [n]$ uniformly at random
3. ~~Of the remaining boxes, pick a subset $\mathcal{S} \subset [n] \backslash \{J\}$, of size $|\mathcal{S}| = k = \lfloor 0.1n \rceil$, uniformly at~~ random.
4. Play the GHZ game in each of the remaining boxes, with result $X_i \in \{0, 1\}$ for $i \in [n] \backslash (\{J\} \cup \mathcal{S})$.
5. Verify if the average GHZ game score is higher than some threshold μ

$$\Omega: \quad \sum_{i \in [n] \backslash (\{J\} \cup S)} X_i \geq \mu \tag{3}$$

If the test Ω passes, then we conclude with high probability that the expected value of the GHZ test of the randomly chosen box J satisfies

$$T: \quad E[X_J] \geq \mu - \delta\,, \tag{4}$$

Proposition 1 (Security statement)**.** *For any implementation of the boxes, the joint probability that that the test* Ω *passes and that the conclusion* T *is false, is smaller than* ϵ*:* $\Pr[\Omega \cap \bar{T}] \leq \epsilon$*, where* ϵ *is a function of* n *and* δ*.*

Proof. Denote by $\boldsymbol{p} = p(x_1, \cdots x_n)$ the joint distribution of the results of the GHZ games, for a given strategy (states and measurements) implemented by the adversary. We want to upper-bound the quantity $\Pr[\Omega \cap \bar{T}]_{\boldsymbol{p}} = \sum_{j,\mathcal{S}} p(j, \cancel{\mathcal{S}}) \Pr[\Omega \cap \bar{T} | j, \mathcal{S}]_{\boldsymbol{p}}$, which we note is invariant under permutations acting on $\boldsymbol{p}$. We thus have $\Pr[\Omega \cap \bar{T}]_{\boldsymbol{p}} = \Pr[\Omega \cap \bar{T}]_{\bar{\boldsymbol{p}}}$, where $\bar{\boldsymbol{p}}$ is the symmetrized version of $\boldsymbol{p}$, and this implies that

$$\Pr[\Omega \cap \bar{T}]_{\bar{\boldsymbol{p}}} = \Pr[\Omega \cap \bar{T} | j', \mathcal{S}']_{\bar{\boldsymbol{p}}} \tag{5}$$

where we have chosen a particular value for the random element $J = j' = 1$ and the set $\mathcal{S}' = \{n-k+1, \cdots n\}$, which we implicitly assume fixed from now. The events Ω and T now only involve the $n-k$ first systems and so we can trace out the last k systems.

By the de Finetti theorem we know that the resulting distribution $\bar{\boldsymbol{p}}' = \bar{p}(x_1, \cdots x_{n-k})$ is ϵ_2 close to a convex combination of iid. distributions and so

$$\Pr[\Omega \cap \bar{T}]_{\bar{\boldsymbol{p}}'} \leq \max_{\{\boldsymbol{q} \ iid.\}} \Pr[\Omega \cap \bar{T}]_{\boldsymbol{q}} + \epsilon_{dF}(k, n) \tag{6}$$

Now for each iid distribution $\boldsymbol{q} = \prod_{i=1}^{n-k} q(x_i)$, the proposition $E[X_1] \leq \mu - \delta$ is either false or true. Assuming, it is true, then, by the Azuma-Hoeffding inequality, we find

$$\Pr[\Omega \cap \bar{T}]_{\boldsymbol{q}} = \Pr\left[\sum_{i=2}^{n-k} I_i \geq \mu\right]_{\boldsymbol{q}} \leq \epsilon_{AH}(\delta, n-k-1) \tag{7}$$

and so we conclude the proposition with $\epsilon = \epsilon_{dF}(k, n) + \epsilon_{AH}(\delta, n-k-1)$ $\square$