Computer Science 294 Lecture 19 Notes

Daniel Raban

March 21, 2023

1 Dictator Testing and PCPPs

1.1 Dictator testing

Recall the setup of property testing: Given a “black box” computing a function f, if we can give it inputs x and see $f(x)$, can we test if f has some property? Or is it far from the class $\mathcal{C}$ of functions with this property? Today, we will look at testing if f is a dictator function.

Definition 1.1. An **r-query function** tester is a randomized algorithm with black-box axcess to some function f, that:

- chooses (up to) r queries (strings) $x^{(1)}, x^{(2)}, \dots, x^{(r)}$.
- chooses a predicate $\psi : \{\pm 1\}^r \to \{T, F\}$
- Queries $f(x^{(1)}), f(x^{(2)}), \dots, f(x^{(n)})$ and acespts iff $\psi(f(x^{(1)}), \dots, f(x^{(r)})) = T$.

Definition 1.2. Let $\mathcal{C}$ be a collection of functions from $\{\pm 1\}^n$ to $\{\pm 1\}$ (e.g. $\mathcal{C} = \{\chi_S\}_{S \subseteq [n]}\}$). An **$r$-local tester** for $\mathcal{C}$ **with rejection rate** $\lambda > 0$ is an r-query function tester such that:

- If $f \in \mathcal{C}$, the tester always accepts.
- For all $\varepsilon \in (0, 1]$, if f is ε-far from $\mathcal{C}$, then $\mathbb{P}(\text{tester rejects } f) \geq \lambda\varepsilon$.

Example 1.1 (Linearity testing)**.** Let $\mathcal{C} = \{\chi_S : S \subseteq [n]\}$. We have seen the BLR test, which is a 3-query local tester for $\mathcal{C}$. We want to

- Pick $x, y \sim \{\pm 1\}^n$ uniformly at random
- Prepare z such that $z_i = x_i y_i$ for $i \in [n]$.
- Accept iff $f(x)f(y)f(z) = 1$.

We saw that if $\mathbb{P}(\text{tester accepts } f) \geq 1 - \varepsilon$, then f is ε-close to a linear function.

Example 1.2 (Dictator testing)**.** Let $\mathcal{D} = \{x_i : i \in [n]\}$, and recall Arrow's theorem.

- Pick $x, y, z \in \{\pm 1\}^n$ uniformly at random, conditioned on $\mathrm{NAE}(x_i, y_i, z_i) = \mathrm{True}$ for all $i \in [n]$, where NAE is the "not all equal" function.
- Accept iff $\mathrm{NAE}(f(x), f(y), f(z))$.

Kalai's robust version of Arrow's theorem tells us that

$$\mathbb{P}(\text{tester accepts } f) = \frac{3}{4} - \frac{3}{4}\mathrm{Stab}_{-1/3}(f).$$

Here is a proof of the soundness of this test.

Proposition 1.1. *If $\mathbb{P}(\text{tester accepts } f) \geq 1 - \varepsilon$, then $W^1(f) \geq 1 - 4.5\varepsilon$.*

Proof. Suppose $\mathbb{P}(\text{tester accepts } f) \geq 1 - \varepsilon$. By Kalai's theorem, we get

$$\begin{aligned}
1 - \varepsilon &\leq \frac{3}{4} - \frac{3}{4}\mathrm{Stab}_{-1/3}(f) \\
&= \frac{3}{4} - \frac{3}{4}\left(W^0(f) + \left(-\frac{1}{3}\right)W^1(f) + \left(\frac{1}{9}\right)W^2(f) + \left(-\frac{1}{27}\right)W^3(f) + \cdots\right) \\
&\leq \frac{3}{4} + \frac{3}{4}\left(\frac{1}{3}W^1(f) + \frac{1}{27}W^3(f) + \cdots\right) \\
&\leq \frac{3}{4} + \frac{1}{4}W^1(f) + \frac{3}{4}\cdot\frac{1}{27}\underbrace{(W^3(f) + W^5(f) + W^7(f) + \cdots)}_{\leq 1 - W^1(f)} \\
&\leq \frac{3}{4} + \frac{1}{4}W^1(f) + \frac{3}{4}\cdot\frac{1}{27}(1 - W^1(f)).
\end{aligned}$$

Rearranging, we get that

$$1 - \frac{9}{2}\varepsilon \leq W^1(f).$$

□

Now FKN tells us that if $f : \{\pm 1\}^n \to \{\pm 1\}$ has $W^1(f) \geq 1 - \delta$, then f is $O(\delta)$-close to a dictator or an anti-dictator. This gives a 3-query local test to the class of dictators union anti-dictators with rejection rate $\lambda = \Omega(1)$).

Here is another tester, where the proof does not rely on the FKN result. The idea is to use BLR and Kalai's test.

Theorem 1.1. *There exists a 6-local tester for the class of dictators with rejection rate 0.1.*

Proof. Apply the BLR test, if it rejects, we reject. If it accepts, then apply Kalai's test and output the result. If

$$\mathbb{P}(\text{combined test accepts}) \geq 1 - 0.1\varepsilon,$$

then

(1) $\mathbb{P}(\text{BLR test accepts}) \geq 1 - 0.1\varepsilon$.

(2) $\mathbb{P}(\text{Kalai test accepts}) \geq 1 - 0.1\varepsilon$.

(1) tells us that there exists a set $S^* \subseteq [n]$ such that $\widehat{f}(S^*) \geq 10.2\varepsilon$ iff $\operatorname{dist}(f, \chi_{S^*}) \leq 0.1\varepsilon$. (2) tells us that $W^1(f) \geq 1 - 0.45\varepsilon$.

If $|S^*| = 1$, then we're done. Otherwise,

$$\begin{aligned}
1 &= \sum_S \widehat{f}(S)^2 \\
&= \sum_{S:|S|=1} \widehat{f}(S)^2 + \sum_{S:|S|\neq 1} \widehat{f}(S)^2 \\
&\geq 1 - 0.45\varepsilon + \widehat{f}(S^*)^2 \\
&\geq 1 - 0.45\varepsilon + (1 - 0.2\varepsilon)^2 \\
&\geq 0.5 + 0.8^2 \\
&> 1,
\end{aligned}$$

which is a contradiction. □

Can we do dictator testing in 3 queries? Yes! With probability 1/2, apply BLR's test, and with probability 1/2, apply Kalai's test. If $\mathbb{P}(\text{tester accepts } f) \geq 1 - 0.005\varepsilon$, then

$$\mathbb{P}(\text{BLR accepts } f) \geq 1 - 0.1\varepsilon, \qquad \mathbb{P}(\text{Kalai accepts } f) \geq 1 - 0.1\varepsilon.$$

Thus, the previous argument implies that f is ε-close to a dictator.

So we get the following theorem:

Theorem 1.2. *There exists a 3-local tester for the class of dictators with rejection rate* 0.05*.*

In general, this gives a trick to reduce the number of queries for a tester.

Theorem 1.3. *Let $S \subseteq [n]$, and let $\mathcal{D} = \{\chi_i : i \in S\}$. Then there exists a 3-local testor for $\mathcal{D}_S$ (with rejection rate* 0.01*).*

Proof. Combine BLR, Kalai's test, and a mysterious third test. Here, we will apply them in sequence, but we can always use the trick of picking a test at random to apply.

Suppose f passes BLR and Kalai's test with high probability. Then f is close to some dictator χ_i. We want an input y so that

$$\chi_i(y) = \begin{cases} 1 & i \in S \\ -1 & \text{otherwise.} \end{cases}$$

This equals y_i, so pick $y = 1_S$. Then

$$(1_S)_j = \begin{cases} 1 & j \in S \\ -1 & \text{otherwise} \end{cases}$$

The key idea is to apply LocalCorrect on $\mathbb{1}_S$, so that $\text{LocalCorrect}(f, 1_S) = \chi_i(x)$ with probability $1 - O(\varepsilon)$. □

1.2 Probabilisticly checkable proofs of proximity

Given a function $f : \{\pm 1\}^n \to \{\pm 1\}$, we can represent it as a very long string. If we let $N = 2^n$, then f can be represented by a string $w \in \{\pm 1\}^N$ (by its truth table). So we can think of property testing in terms of string testing, where we give an index i and receive w_i.

Definition 1.3. $\mathcal{C} \subseteq \{\pm 1\}^N$ has an r **query, length ℓ PCPP system (with rejection rate λ)** if there exists an r-local string tester T with black-box access to $(w, \pi) \in \{\pm 1\}^n \times \{\pm 1\}^\ell$ such that

- **completeness**: If $w \in \mathcal{C}$, there exists aπ such that T accepts (w, π) with probability 1.
- **soundness**:If w is ε-far from $\mathcal{C}$, then for all π^*,

$$\mathbb{P}(T \text{ rejects } (w, \pi^*)) \geq \lambda\varepsilon.$$

Theorem 1.4 (Long code construction)**.** *Every $\mathcal{C} \in \{\pm 1\}^N$ has a 3-query PCPP system with proof length 2^{2^N} (and rejection rate $\Omega(1)$).*

The idea is to embed every property into a property about dictators. Since we know how to test every property about dictators, we can test any property.

Proof idea. Fix an identification encoding $\text{enc} : \{\pm 1\}^N \to [2^N]$.

- A proof $w \in \mathcal{C}$ gives a truth-table π of the dictator function $\chi_{\text{enc}(w)} : \{\pm 1\}^{2^N} \to \{\pm 1\}$.

- The tester checks that π is a dictator function for some χ_i with $\mathrm{enc}^{-1}(i) \in \mathcal{C}$.

This tells us that π is $O(\varepsilon)$-close to a dictator function $\chi_{\mathrm{enc}(w')}$ for some $w' \in \mathcal{C}$. How do we check that $w' = w$?

- Pick a random $j \in [N]$. We want to check that $w_j = w'_j$, so we want to design an input $x^{(j)}$ such that $\chi_{\mathrm{enc}(w')}(x^{(j)}) = w'_j$. This is $x^{(j)}_{\mathrm{enc}(w')}$, so for every $y \in \{\pm 1\}^N$, write $x^{(j)}_{\mathrm{enc}(y)} = y_j$. $\square$

Theorem 1.5 (PCP(P) theorem, ALMSS, AS, BS, Dinur)**.** *Suppose mcC* $\subseteq \{\mp 1\}^N$ *is given explicitly by a small circuit C of size s: $C(w)$ is true iff $w \in \mathcal{C}$. Then $\mathcal{C}$ has a 3-query PCPP system with proof length* $\mathrm{poly}(s)$ *[shown by ALMSS, AS]. Moreover, there exists a system with proof length* $s(\log s)^{o(1)}$ *[shown by BS, Dinur].*

Remark 1.1. Is is still open to show that there exists a system with linear proof length.

Next time, we will show the connection between PCPP and hardness of approximation. We will see that MAX-3SAT is NP-Hard to approximate.