Testing Booleanity and the Uncertainty Principle

Tom Gur
Weizmann Institute of Science

Joint work with Omer Tamuz

Heisenberg's Uncertainty Principle

you are here

if you're neither here nor there, you aren't really anywhere
Let $f : \{0, 1\}^n \to \mathbb{R}$.
We say that $f$ Boolean if $\text{Im}(f) \subseteq \{-1, 1\}$.

Our goal is testing whether such $f$ is Boolean or not, using the minimum number of queries.

The naïve approach would be to make all of the $2^n$ possible queries.
Informal Statement of our Results

- We show that if a function has a sparse Fourier transform, then it can be tested for Booleanity very efficiently.
- This is obtained by showing a combinatorial lemma regarding functions on the hypercube:

**Lemma (Informal)**

A sparse function on the hypercube is either Boolean or far from being Boolean.

- The proof heavily relies on an uncertainty principle, which we show for the hypercube.
Functions on the hypercube can be generally written as a multilinear polynomial function.

The Walsh-Fourier Expansion is a change of basis with nice properties (e.g., diagonalization of the convolution operator).

**Definition (The Walsh-Fourier Expansion)**

Every function $f : \mathbb{Z}_2^n \rightarrow \mathbb{R}$ can be written as

$$\sum_{S \subseteq [n]} \hat{f}(S) \chi_S(x).$$

We say that $f$ is $k$-sparse if $|\text{supp}(\hat{f})| \leq k$. 
The Main Lemma

Lemma

Every $k$-sparse function $f : \mathbb{Z}_2^n \to \mathbb{R}$ is either Boolean, or satisfies

$$\Pr_x [f(x) \not\in \{-1, 1\}] \geq \Omega \left( \frac{1}{k^2} \right),$$

where $\Pr_x [\cdot]$ denotes the uniform distribution over the domain of $f$.

This is actually a special case of:

Theorem

Let $D \subset \mathbb{R}$ be a set with $d$ elements. Then, for any $k$-sparse function $f : \mathbb{Z}_2^n \to \mathbb{R}$, one of the following holds.

- Either $\Pr_x [f(x) \in D] = 1$,
- or $\Pr_x [f(x) \not\in D] \geq \frac{d!}{(k+d)^d}$. 
Generalizations

- The lemma above can be generalized for functions over several finite groups.
- The tester can be generalized for testing whether $\text{Im}(f) \in S$, for any finite set $S \subset \mathbb{R}$.
- We can make several relaxations of the precondition of the lemma in terms of entropy.
The Uncertainty Principle

- In Quantum Mechanics, $f : \mathbb{R}^3 \to \mathbb{C}$ represents the state of a particle in space, with $|f(x)|^2$ the density of its distribution at $x$.
- Its transform $|\hat{f}(x)|^2$ represents the distribution of its momentum.

Heisenberg uncertainty principle:

$$\text{Var}[f] \cdot \text{Var}[\hat{f}] \geq C.$$ 

- Stronger statement, conjectured by Hirschman 57, proved by Beckner 75: $H[f] + H[\hat{f}] \geq C$, for $f : \mathbb{R} \to \mathbb{C}$. 

Tom Gur
Testing Booleanity and the Uncertainty Principle
The Uncertainty Principle on the Hypercube

**Theorem**

Let $f : \mathbb{Z}_2^n \to \mathbb{C}$ have Fourier transform $\hat{f} : \mathbb{Z}_2^n \to \mathbb{C}$, and normalize $\|f\|_2 = \|\hat{f}\|_2 = 1$. Then

$$H[f] + H[\hat{f}] \geq n,$$

where $H[f] = -\sum_{x \in \mathbb{Z}_2^n} |f(x)|^2 \log_2 |f(x)|^2$.

- Note that a distribution on support $k$ can have entropy at most $\log k$. Hence,

$$|\text{supp } f| \cdot |\text{supp } \hat{f}| \geq 2^n.$$
Recall that given $f, g : \mathbb{Z}_2^n \to \mathbb{R}$, their convolution is defined as follows:

$$[f \ast g](x) = \sum_{y \in \mathbb{Z}_2^n} f(y)g(x + y),$$

and the convolution theorem states that $\hat{f} \cdot \hat{g} = \hat{f} \ast \hat{g}$. 

Tom Gur  
Testing Booleanity and the Uncertainty Principle
Observation

\(f\) is Boolean iff \(\hat{f} \ast \hat{f} = \delta\).

- To see this note that \(f(x) \in \{-1, 1\}\) iff \(f^2 = 1\).
- Apply the Fourier transform to both sides.
- By the convolution theorem \(\hat{f} \ast \hat{f} = \hat{1}\).
- \(\delta = \hat{1}\).
Proof (of the main lemma)

- Assume that $f$ is not Boolean, and let $|\text{supp } \hat{f}| = k$.
- We show that $\Pr[f(x) \neq \{-1, 1\}] \geq \Omega(1/k^2)$.
- Recall that $|\text{supp } f^2 - 1| \cdot |\text{supp } \hat{f} \ast \hat{f} - \delta| \geq 2^n$.

**Proposition**

For every $g : \mathbb{Z}_2^n \rightarrow \mathbb{R}$,

$$|\text{supp } g \ast g| \leq k^2.$$  \(1\)

- Hence $|\text{supp } \hat{f}^{(2)} + \delta| \leq k^2 + 1$.
- Thus

$$|\text{supp } f^2 - 1| \cdot (k^2 + 1) \geq 2^n.$$

- Rearranging yields the result.
Proof (of proposition)

- Let $A = \text{supp } g$.
- if $g \ast g(x) \neq 0$ then
  $$\sum_{y \in \mathbb{Z}_2^n} g(y)g(x + y) \neq 0.$$  
  Change of variable $z = x + y$.
  Hence $\exists y, z \in A$ such that $x = y + z$.
  Hence $x \in A + A$.
- $|A + A| \leq |A \times A| = k^2$. 

Tom Gur  Testing Booleanity and the Uncertainty Principle
Thank you!

Tom Gur

Testing Booleanity and the Uncertainty Principle