

ADDITIVE COMBINATORICS AND
QUANTUM TESTING / LEARNING:
AN OVERVIEW OF RECENT CONNECTIONS

Davi Castro-Silva

University of Cambridge

A SHARED PERSPECTIVE

Recovering **hidden algebraic structure** from *limited information*

- **Examples** (over qubits / $\mathbb{F}_2 = \{0, 1\}$):
 - Given (*query & sample access*) a set $A \subseteq \mathbb{F}_2^n$ of **bounded doubling**, recover a **subspace** $V \leq \mathbb{F}_2^n$ that efficiently covers A .
 - Given (*query access*) a function $f: \mathbb{F}_2^n \rightarrow [-1, 1]$ of high **Gowers U^3 norm**, recover its global **quadratic structure**.
 - Given (*sample access*) a quantum state $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$ of high **stabilizer fidelity**, recover a **stabilizer state** that correlates with $|\psi\rangle$.
 - Given (*query access*) a unitary $U \in \mathbb{C}^{2^n \times 2^n}$, decide if U is a **Clifford unitary** or *far from Clifford*.
 - Given (*query access*) a unitary $U \in \mathbb{C}^{2^n \times 2^n}$, decide if U is in the *third level* of the **Clifford hierarchy** or far from it.

A SHARED PERSPECTIVE

- **Common framework:**
 - We are given limited access to an object: (classical or quantum) queries, samples
 - We wish to:
 - Test membership in a structured class, or
 - Learn the “structured part” of the object.
- Relevant types of structure:
 - Efficient covering by translates of a **subspace** (*linear structure* in sets).
 - High correlation with a **quadratic phase** $(-1)^{q(x)}$ (*quadratic structure* in functions).
 - High fidelity with a **stabilizer state** (stabilizer formalism, QEC).
 - **Clifford** unitaries, and higher levels of the **Clifford hierarchy** (fault-tolerant QC).

Different manifestations, same underlying mathematical principles.

GOWERS UNIFORMITY NORMS

- The Gowers U^3 norm is a *local measure* of **quadratic behavior** of functions.

- **Multiplicative derivative:** For $f: \mathbb{F}_2^n \rightarrow \mathbb{C}$ and $a \in \mathbb{F}_2^n$,

$$\Delta_a f(x) = f(x+a)\overline{f(x)}$$

- If $f(x) = e^{2\pi i \phi(x)}$, then $\Delta_a f(x) = e^{2\pi i (\phi(x+a) - \phi(x))}$

- If $f(x) = (-1)^{q(x)}$ for a quadratic polynomial $q: \mathbb{F}_2^n \rightarrow \mathbb{F}_2$, then

$$\Delta_a \Delta_b \Delta_c f(x) = (-1)^{\partial_a \partial_b \partial_c q(x)} \equiv 1$$

- **Definition:** $\|f\|_{U^3} = \left(\mathbb{E}_{x,a,b,c \in \mathbb{F}_2^n} \Delta_a \Delta_b \Delta_c f(x) \right)^{1/8}$

- We similarly define the Gowers U^{k+1} norms for all $k \geq 1$.

- Each U^{k+1} norm is a local measure of **degree- k behavior**.

- These norms are useful for controlling the number of *additive patterns* inside a set.

QUADRATIC FOURIER ANALYSIS

- In additive combinatorics, we usually consider *bounded functions*: $\|f\|_\infty \leq 1$.
 - Trivial but very useful fact: $\|f\|_{U^3} \leq \|f\|_\infty$.
 - The extremizers of this inequality are **quadratic phase functions** $(-1)^{q(\cdot)}$.
- Direct inequality: $\|f\|_{U^3} \geq \mathbb{E}_{x \in \mathbb{F}_2^n} [f(x)(-1)^{q(x)}]$ for all quadratic $q: \mathbb{F}_2^n \rightarrow \mathbb{F}_2$.
- **Polynomial Gowers Inverse Theorem** (Gowers, Green, Manners and Tao'25):
If $f: \mathbb{F}_2^n \rightarrow [-1, 1]$ satisfies $\|f\|_{U^3} \geq \gamma$, then there is a quadratic $q: \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ such that
$$\mathbb{E}_{x \in \mathbb{F}_2^n} [f(x)(-1)^{q(x)}] \geq \text{poly}(\gamma).$$
- Direct ineq + Inverse thm: $\|f\|_{U^3} = \Omega(\|f\|_\infty)$ iff f correlates with an extremizer $(-1)^q$.
- Linear behavior of sets $A \subseteq \mathbb{F}_2^n$ is related to quadratic behavior of functions $f: \mathbb{F}_2^n \rightarrow [-1, 1]$.
 - PGI theorem is **equivalent to** efficient subspace cover of “smooth” sets (PFR).

A CHANGE IN PERSPECTIVE

- However, the natural analytic space of the U^3 norm is L^2 :

$$\sup\{\|f\|_{U^3} : \|f\|_p = 1\} = \begin{cases} 1, & \text{if } p \geq 2, \\ \infty, & \text{if } p < 2 \end{cases} \quad (\|f\|_p^p := \mathbb{E}_x |f(x)|^p)$$

- We can then define the U^3 norm of **quantum states**:

$$\text{For } |\psi_f\rangle = 2^{-n/2} \sum_{x \in \mathbb{F}_2^n} f(x) |x\rangle, \text{ define } \||\psi_f\rangle\|_{U^3} := \|f\|_{U^3}$$

- Eisner and Tao'12 characterized the extremizers of the inequality $\|f\|_{U^3} \leq \|f\|_2$:

$$\|f\|_{U^3} = \|f\|_2 \text{ iff } f(x) \propto \mathbf{1}_V(x) (-1)^{q(x)} i^{c \cdot x},$$

where V is an affine subspace, $q: \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ is quadratic, $c \in \{0, 1\}^n$.

(**Essentially:** iff f is a quadratic phase function supported on an affine subspace)

- This formula corresponds precisely to **stabilizer states** written in the computational basis!
- **Lemma:** $\||\psi\rangle\|_{U^3} \leq 1$ for all quantum states, and $\||\psi\rangle\|_{U^3} = 1$ iff $|\psi\rangle$ is a stabilizer state.

A CHANGE IN PERSPECTIVE

- Stabilizer states form a **fundamental class** of quantum states:
 - Prominent in the *phase-space formulation* of quantum mechanics.
 - Discrete analogues of **Gaussian states**.
 - Outputs of Clifford circuits (quantum error correction, classical simulation).
- **Examples:**
 - Graph states: $2^{-n/2} \sum_{x \in \mathbb{F}_2^n} (-1)^{q(x)} |x\rangle$ for a quadratic $q: \mathbb{F}_2^n \rightarrow \mathbb{F}_2$
 - Computational basis states: $|x\rangle$ for $x \in \mathbb{F}_2^n$
- Direct inequality: $\| |\psi\rangle \|_{U^3} \geq |\langle \phi | \psi \rangle|$ for all stabilizer states $|\phi\rangle \in (\mathbb{C}^2)^{\otimes n}$
- **Quantum Polynomial Gowers Inverse Theorem** (AD, BvDH, MT'25):
If a quantum state $|\psi\rangle$ satisfies $\| |\psi\rangle \|_{U^3} \geq \gamma$, then its **stabilizer fidelity** is at least $\text{poly}(\gamma)$.

TESTING / LEARNING STABILIZERS

- The Gowers norm provides a “test” for **high stabilizer fidelity**!
- We can write $\|\psi\|_{U^3}^8 = \frac{1}{2^n} \sum_{u \in \mathbb{F}_2^{2n}} |\langle \psi | W_u | \psi \rangle|^4$, which can be estimated using *Bell sampling*.
- **Tolerant testing of stabilizer states** (AD, BvDH, MT’25):
Given $\epsilon > 0$ and $O(1)$ copies of an n -qubit quantum state $|\psi\rangle$, there is an $O(n)$ -time quantum algorithm that distinguishes between:
 $(i) |\psi\rangle$ has stabilizer fidelity $\geq \epsilon$; $(ii) |\psi\rangle$ has stabilizer fidelity $\leq \epsilon^{1000}$.
- **Agnostic learning of stabilizer states** (Chen, Gong, Ye, Zhang’25):
Given $\epsilon > 0$ and $O(n)$ copies of an n -qubit quantum state $|\psi\rangle$, there is an $O(n^3)$ -time quantum algorithm that outputs a stabilizer state $|\phi^*\rangle$ s.t.
$$|\langle \phi^* | \psi \rangle|^2 \geq \max_{\phi \in \text{Stab}} |\langle \phi | \psi \rangle|^2 - \epsilon.$$
- This algorithm is completely different, has nothing to do with additive combinatorics :(
... or does it?

BACK TO ADDITIVE COMBINATORICS

- Recall **Example problem 2** (PGI problem):
 - Given (*query access*) a function $f: \mathbb{F}_2^n \rightarrow [-1, 1]$ of high Gowers U^3 norm, recover its global quadratic structure.
- **More precisely:** Given $\text{poly}(n)$ queries to $f: \mathbb{F}_2^n \rightarrow [-1, 1]$ such that $\|f\|_{U^3} \geq \gamma$, find in $\text{poly}(n)$ time a quadratic $q: \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ such that
$$\mathbb{E}_{x \in \mathbb{F}_2^n} [f(x)(-1)^{q(x)}] \geq \text{poly}(\gamma).$$
- **Agnostic stabilizer learning*:** Given $O(n)$ copies of a state $|\psi\rangle \in \mathbb{C}^{2^n}$ such that $\| |\psi\rangle \|_{U^3} \geq \gamma$, find in $O(n^3)$ time a stabilizer state $|\phi\rangle$ such that
$$|\langle \phi | \psi \rangle| \geq \text{poly}(\gamma).$$
- **Differences** to our PGI problem:
 - Assumes $\| |\psi\rangle \|_2 = 1$ instead of $\|f\|_\infty \leq 1$.
 - Access to **quantum samples** instead of *classical queries*.
 - Outputs a **stabilizer state** instead of a *quadratic phase function*.

BACK TO ADDITIVE COMBINATORICS

[Joint work with Jop Briët, Srinivasan Arunachalam, Arkopal Dutt, Tom Gur]

- We *dequantize* the q. learning algorithm, simulating its behavior classically in the L^∞ setting.
 - Assumes $\|f\|_\infty \leq 1$, access to classical queries, only classical computation.
 - “Rounds” the stabilizer state to a quadratic phase function (*graph state*).
 - We obtain an efficient classical algorithm for PGI.
- We *algorithmize* the implication $\text{PGI} \Rightarrow \text{efficient subspace cover}$ (*Example problem I*).
- **Algorithmic PFR:** Given query and sample access to a set $A \subseteq \mathbb{F}_2^n$ with $|A + A| \leq K|A|$, we can efficiently *learn* a small subspace V that covers A using $\text{poly}(K)$ translates.
- Through the stabilizer formalism, we establish a connection between *quadratic Fourier analysis* and *symplectic geometry*.
 - Such a connection was first conjectured by Green and Tao’08.

These methods are now additive combinatorics too :)

OPEN PROBLEMS AND ADS

- **Open problems:**
 - Can we efficiently estimate the **stabilizer fidelity** of a quantum state?
 - Develop the **Pauli uniformity** theory (non-commutative Gowers norms), and tests for higher levels of the Clifford hierarchy.
 - What about learning / testing outputs of the **third Clifford level**? In what sense are these states “cubic”?
- **Advertisements:**
 - QCOW3! (Quantum meets combinatorics, in Cambridge)
 - **Additive Combinatorics and Quantum** (ACQ) online seminar series
(co-organized with Jop Briët and Philippe van Dordrecht)