An Algorithmic Polynomial Freiman-Ruzsa Theorem

Via Dequantisation

Tom Gur

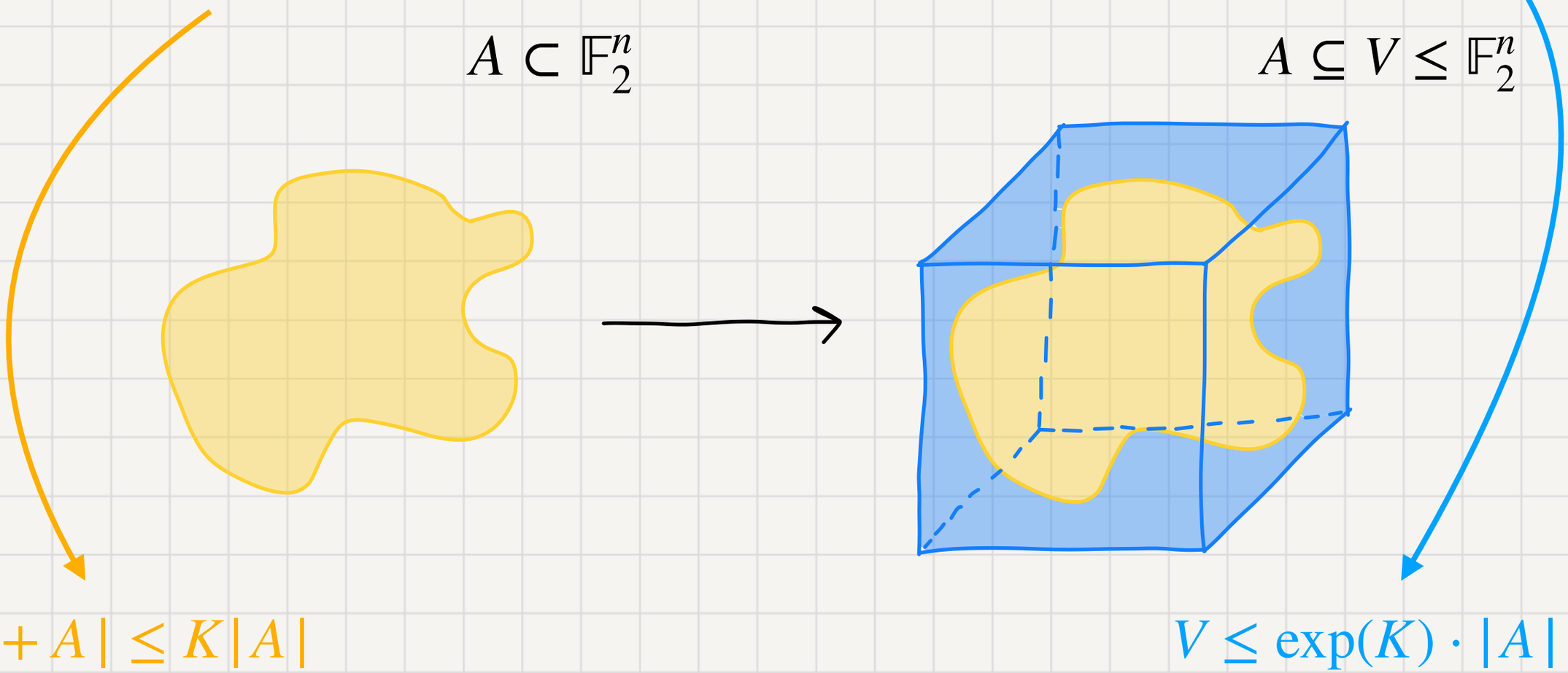
UNIVERSITY OF CAMBRIDGE

Joint work with Davi Castro-Silva, Jop Briët, Srinivasan Arunachalam, and Arkopal Dutt

The Freiman-Ruzsa Theorem

"Approximately-symmetric" sets are contained in "small" subspaces

$A \subset \mathbb{F}_2^n$



$|A+A| \leq K|A|$

$A \subseteq V \leq \mathbb{F}_2^n$

$V \leq \exp(K) \cdot |A|$

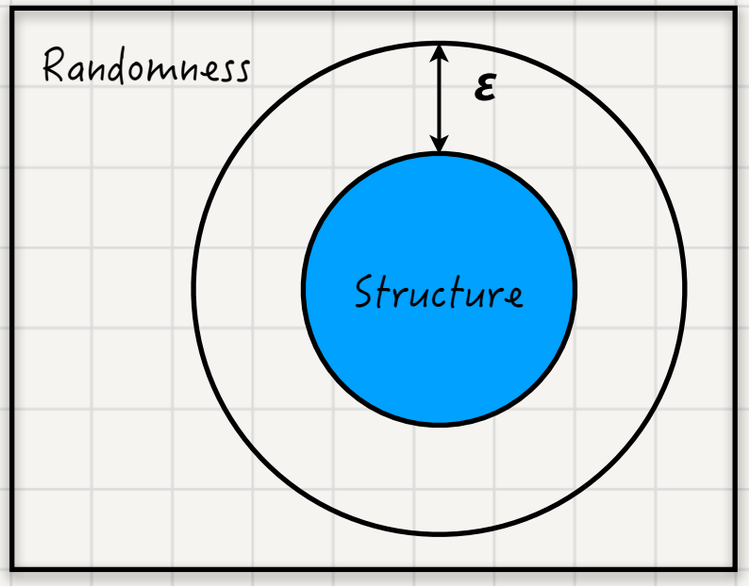
Sumset $A + A = \{a + a' \,;\, a, a' \in A\}$

Doubling-constant K measures approximate subgroup structure

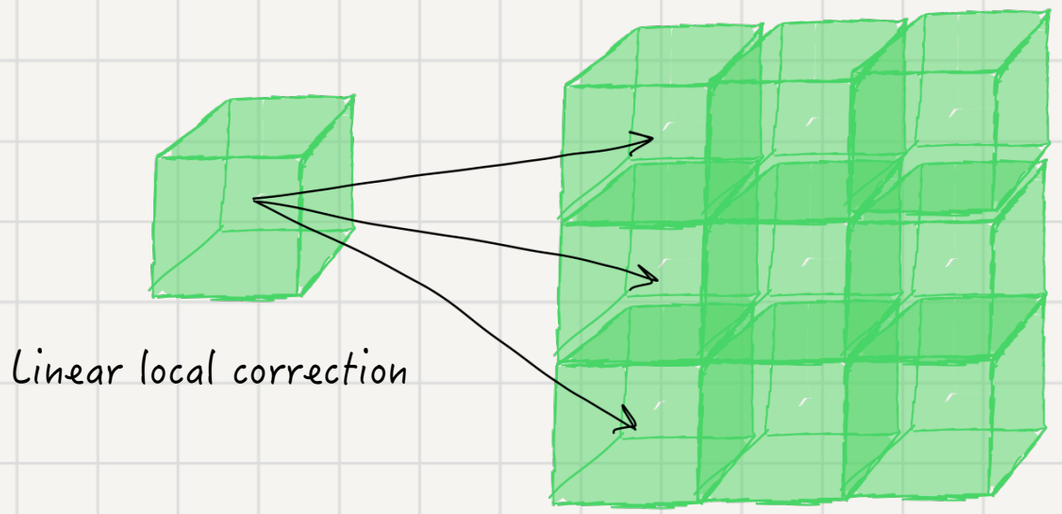
Observation: Sets that are $\frac{1}{K}$-dense in a subspace have doubling K

Why is it useful in TCS?

Property testing



Quantum complexity



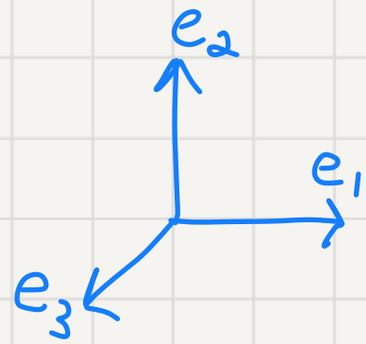
Worst-case to average-case reductions

Constraint satisfaction problems, sparsification, derandomisation , communication complexity, coding theory, structure-vs-randomness decompositions, pseudo-randomness, PAC learning, and much more.

Two caveats: 1) Large subspace 2) Non-algorithmic

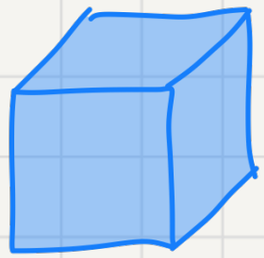
Freiman-Ruzsa Theorem. Let $A \subseteq \mathbb{F}_2^n$ s.t. $|A+A| \le K|A|$. Then $A \subseteq V$ for a subset $V \le \mathbb{F}_2^n$ of size $V \le \exp(K) \cdot |A|$

Can we get $\mathrm{poly}(K)$?



Structure

$A = \mathbb{F}_2^m$



$|A+A| = |A|$

A is a subspace

Randomness

$A = \{e_1, e_2, \ldots, e_k\}$

$|A+A| = O(|A|^2)$

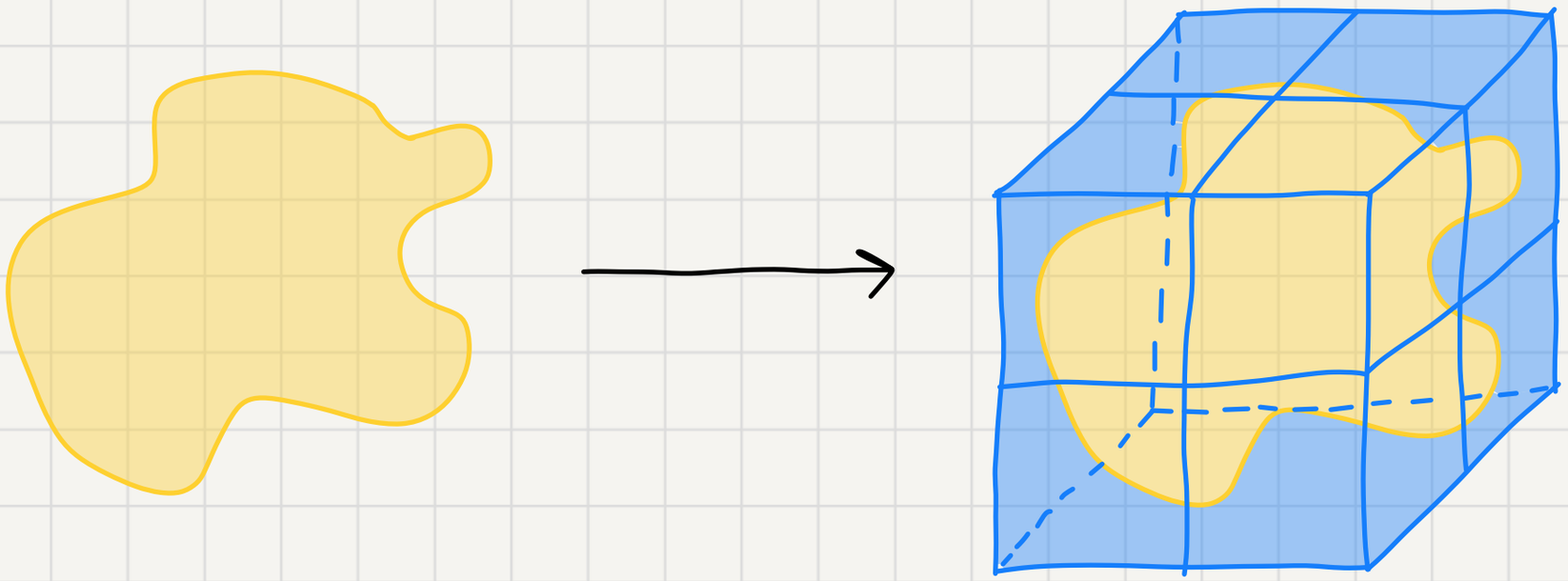
$|\mathrm{Span}(A)| = 2^k$

Consider $A = \{e_1, e_2, \ldots, e_k\} \cup \mathbb{F}_2^{n-k}$

$|A+A| = O(k^2 \cdot 2^{n-k}) = O(k|A|)$ but $\mathrm{Span}(A) = 2^n \ge \frac{2^k}{k}|A|$

However, A can be **covered** by $k+1$ translates of a subspace V, $|V| < |A|$

Polynomial Freiman-Ruzsa (PFR) Conjecture [Marton '99]: we can always cover the set by polynomially many translates of a small subspace.



PFR Theorem (Gowers, Green, Manners, Tao'25)

Let $A \subseteq \mathbb{F}_2^n$ s.t. $|A+A| \leq K|A|$ for doubling-constant $K \geq 1$. Then A can be covered by $\mathrm{poly}(K)$ translates of a subspace $V \leq \mathbb{F}_2^n$ of size $|V| \leq |A|$

Caveat: non-algorithmic

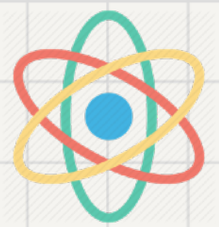
Main result

Algorithmic Polynomial Freiman-Ruzsa Theorem

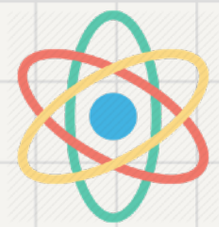
Let $A \subseteq \mathbb{F}_2^n$ s.t. $|A+A| \leq K|A|$ for doubling-constant $K \geq 1$. There is an efficient algorithm that learns a PFR subspace: a subspace $V \leq \mathbb{F}_2^n$ of size $|V| \leq |A|$ s.t. A can be covered by $\mathrm{poly}(K)$ translates of $|V|$.

Efficient: $\tilde{O}(n^4)$ time, $\tilde{O}(n^2)$ queries, and $O(n)$ random samples from A

Learns a PFR subspace: outputs an explicit basis for V w.h.p.



Quantum proof for a classical theorem

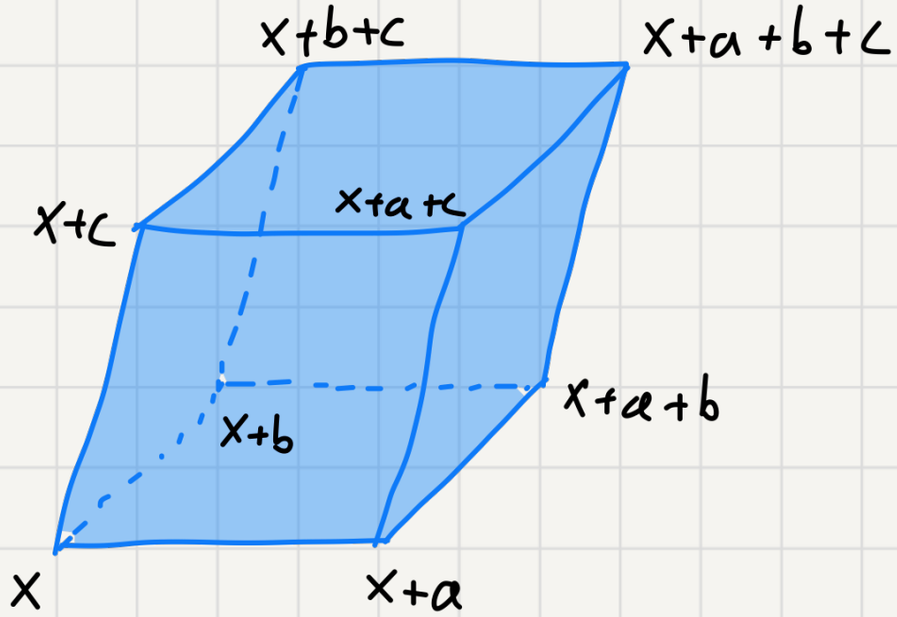


Proof strategy

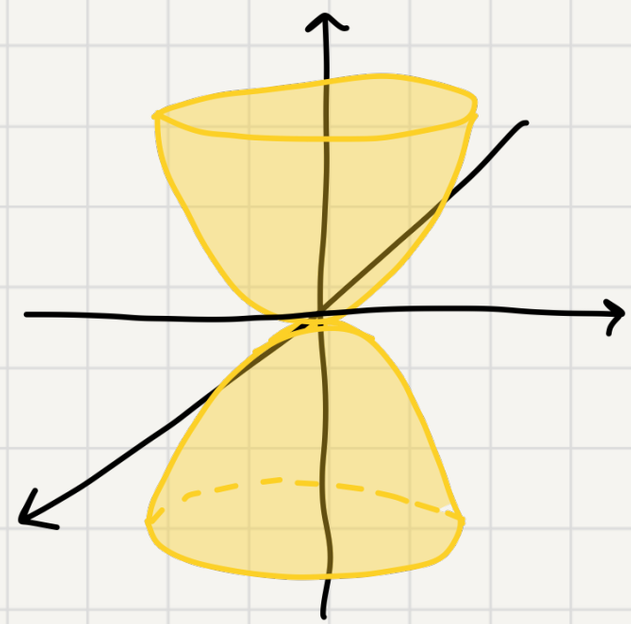
Natural approach: Make GGMT's proof algorithmic

Problem: Proof via the entropy method; **exponential sums**

Instead, we take a detour to the **Polynomial Gowers Inverse Theorem**



Gowers U^3 norm
(local)



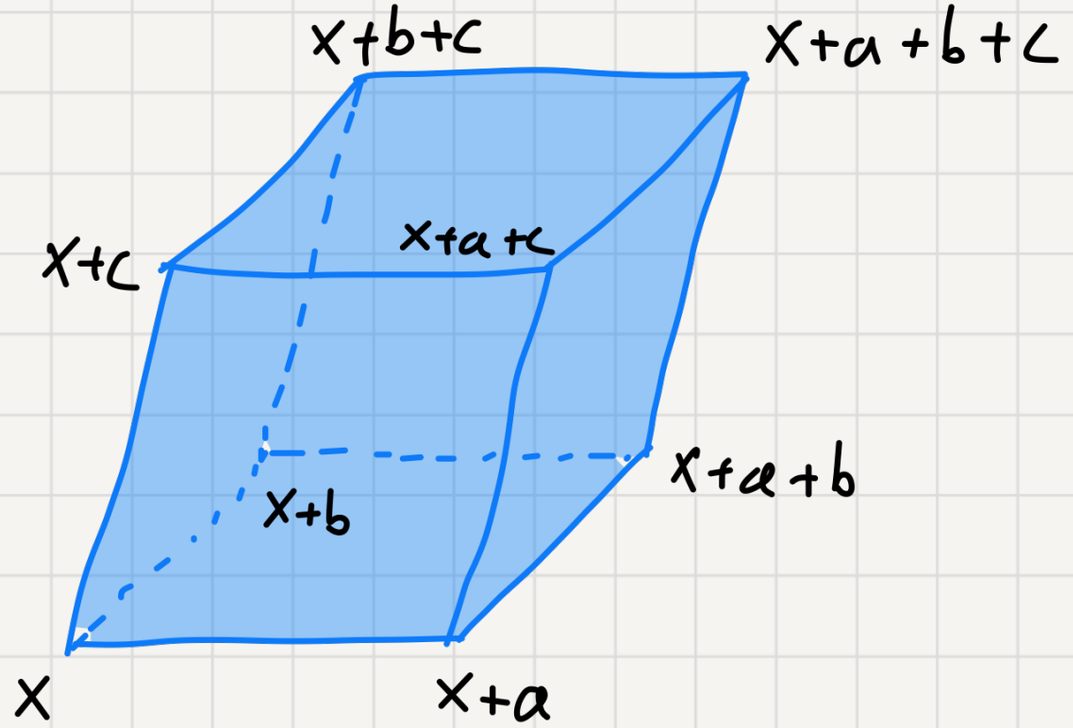
Quadratic structure
(global)

Gowers Uniformity Norms

The Gowers U^3 norm is a local measure of quadratic structure of a function $f : \mathbb{F}_2^n \to \mathbb{C}$

$$\|f\|_{U^3} = \left(\mathbb{E}_{x,a,b,c \in \mathbb{F}_2^n} \prod_{\omega \in \{0,1\}^3} \mathscr{C}^{|\omega|} f(x + \omega_1 a + \omega_2 b + \omega_3 c) \right)^{1/8}$$

Geometrically:



$$f(x)\overline{f(x+a)f(x+b)f(x+c)}f(x+a+b)f(x+a+c)f(x+b+c)\overline{f(x+a+b+c)}$$

Gowers Uniformity Norms

The Gowers U^3 norm is a local measure of quadratic structure

of a function $f : \mathbb{F}_2^n \to \mathbb{C}$

$$\|f\|_{U^3} = \left(\mathbb{E}_{x,a,b,c \in \mathbb{F}_2^n} \prod_{\omega \in \{0,1\}^3} \mathscr{C}^{|\omega|} f\left(x + \omega_1 a + \omega_2 b + \omega_3 c\right) \right)^{1/8}$$

Analytically: Multiplicative derivative $\Delta_h f(x) := f(x+h)\overline{f(x)}$

Then, $\|f\|_{U^3}^8 = \mathbb{E}_{x,a,b,c \in \mathbb{F}_2^n} \Delta_a \Delta_b \Delta_c f(x)$

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

then $\Delta_a \Delta_b \Delta_c f(x) = 1$

If f correlates with a quadratic phase, it must have large U^3 norm

$$\|f\|_{U^3} \geq \left| \mathbb{E}_{x \in \mathbb{F}_2^n} \left[f(x)(-1)^{q(x)} \right] \right|$$

for all quadratic $q : \mathbb{F}_2^n \to \mathbb{F}_2$

Gowers $\mathbf{U^3}$ Inverse Theorem [Samorodnitsky'07, Green-Tao'08]

If $f : \mathbb{F}_2^n \to [-1,1]$ satisfies $\|f\|_{U^3} \geq \gamma$, then there exists quadratic q s.t.

$$\mathbb{E}_{x \in \mathbb{F}_2^n} \left[f(x)(-1)^{q(x)} \right] \geq c(\gamma) > 0.$$

Polynomial Gowers Inverse (PGI) Theorem [GGMT25]: $c(\gamma) = \mathrm{poly}(\gamma)$

Theorem [Lovett '10, Green-Tao '10]: PGI is equivalent to PFR

Proof strategy (revised)

Polynomial Freiman-Ruzsa (PFR) -> Polynomial Gowers Inverse (PGI)

PGI is **combinatorially** equivalent to PFR, so the plan is:

1) Show an **algorithmic** PGI Theorem

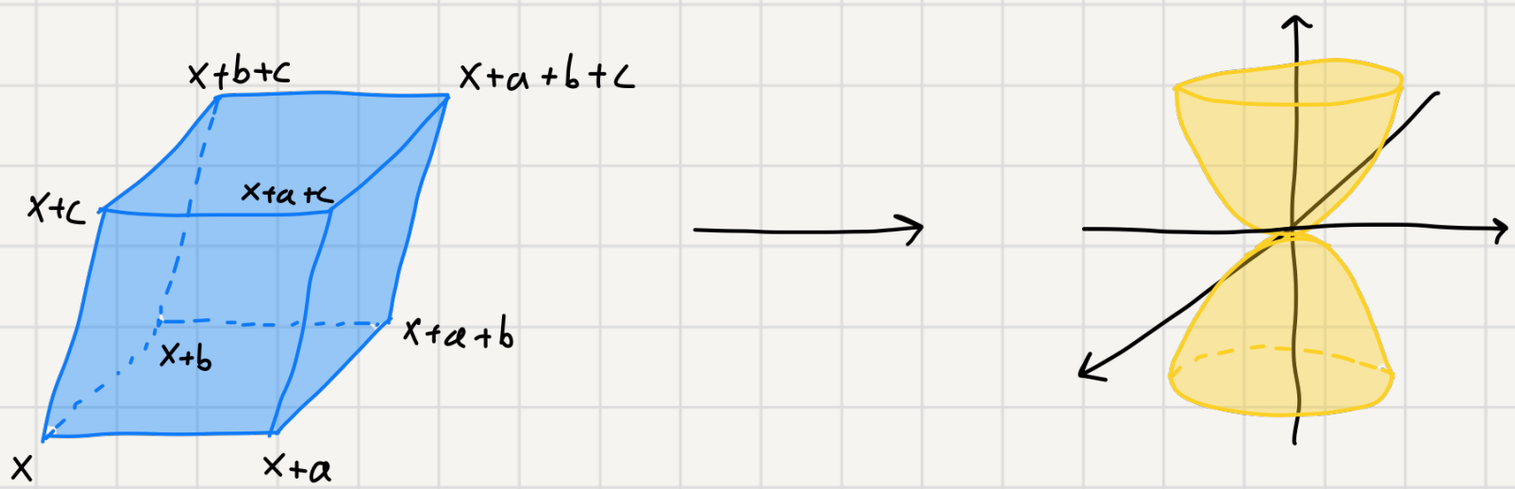
2) Make the PGI-PFR equivalence **algorithmic**.

New goal

Algorithmic Polynomial Gowers Inverse Theorem

Let $f : \mathbb{F}_2^n \to [-1,1]$ s.t. $\|f\|_{U^3} \geq \gamma$. There exists an efficient algorithm that finds a quadratic polynomial $q : \mathbb{F}_2^n \to \mathbb{F}_2$ s.t.

$$\mathbb{E}_{x \in \mathbb{F}_2^n} \left[f(x)(-1)^{q(x)} \right] \geq \mathrm{poly}(\gamma)$$



Gowers U^3 norm
(local)

Quadratic structure
(global)

Key insight: We can use the combinatorial result as a black-box

Proof outline

1) Given access to $f : \mathbb{F}_2^n \to [-1,1]$, efficiently learn an ϵ-maximal quadratic correlator q^* s.t.

$$\left| \mathbb{E}_{x \in \mathbb{F}_2^n} \left[f(x)(-1)^{q^*(x)} \right] \right| \geq \max_{q:\deg(q)=2} \left| \mathbb{E}_{x \in \mathbb{F}_2^n} \left[f(x)(-1)^{q(x)} \right] \right| - \epsilon$$

2) Use the combinatorial PGI theorem:

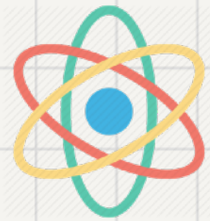
If $\|f\|_{U^3} \geq \gamma$, then then there exists quadratic q and $C > 0$ s.t.

$$\mathbb{E}_{x \in \mathbb{F}_2^n} \left[f(x)(-1)^{q(x)} \right] \geq \gamma^C$$

The algorithm in (1) with $\epsilon = \gamma^{C+1}$ solves the algorithmic PGI problem

3) Algorithmic PFR follows by the algorithmic PGI-PFR equivalence

Learning ϵ-maximal quadratic correlators



Proof by de-quantising quantum stabiliser learning

Definition An n-qubit state $|\psi\rangle$ is a stabiliser state if there exist independent, mutually commuting Pauli operators $P_1, \ldots, P_n \in \{I, X, Y, Z\}^{\otimes n}$ such that $P_i|\psi\rangle = |\psi\rangle$ for every $i \in [n]$.

Observation [Eisner-Tao '12] A stabiliser state is equivalent to a function $f : \mathbb{F}_2^n \to \mathbb{C}$ satisfying $\|f\|_{U^3} = \|f\|_2 = 1$

Equivalently: $f(x) \propto \mathbf{1}_V(x)(-1)^{q(x)} i^{c \cdot x}$

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

Theorem [AD25, BvDH, MT'25]. If $f : \mathbb{F}_2^n \to \mathbb{C}$ satisfying $\|f\|_{U^3} \geq \gamma \|f\|_2$, then there is a stabiliser state ϕ such that

$$\left| \mathbb{E}_{x \in \mathbb{F}_2^n} \left[f(x) \overline{\phi(x)} \right] \right| \geq \mathrm{poly}(\gamma) \|f\|_2$$

Stabiliser learning is a quantum version of the algorithmic PGI problem

Theorem [Chen, Gong, Ye and 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 stabiliser state $|\phi^*\rangle$ s.t.

$$|\langle \phi^* | \psi \rangle|^2 \geq \max_{\phi \in \mathrm{Stab}} |\langle \phi | \psi \rangle|^2 - \epsilon \,.$$

Side-by-side comparison

Algorithmic PGI. Query $f : \mathbb{F}_2^n \to [-1,1]$ to learn $q^* : \mathbb{F}_2^n \to \mathbb{F}_2$ s.t.

$$\left|\mathbb{E}_{x\in\mathbb{F}_2^n}\left[f(x)(-1)^{q^*(x)}\right]\right| \geq \max_{q:\deg(q)=2}\left|\mathbb{E}_{x\in\mathbb{F}_2^n}\left[f(x)(-1)^{q(x)}\right]\right| - \epsilon$$

Theorem [Chen, Gong, Ye and Zhang'25]. Given copies of $|\psi\rangle$, learn a stabiliser state $|\phi^*\rangle$ s.t. $|\langle\phi^*|\psi\rangle|^2 \geq \max_{\phi\in\mathrm{Stab}} |\langle\phi|\psi\rangle|^2 - \epsilon$.

1) L^2 vs L^∞ normalisation

2) Quantum samples vs classical queries

3) Stabilisers vs quadratic phases

4) Quantum vs classical algorithm

Quantum algorithms

Quantum Polynomial Gowers Inverse Theorem

Let $f : \mathbb{F}_2^n \to [-1,1]$ s.t. $\|f\|_{U^3} \geq \gamma$. There exists an efficient algorithm that finds a quadratic q s.t. $\mathbb{E}_{x \in \mathbb{F}_2^n}\left[f(x)(-1)^{q(x)}\right] \geq \mathrm{poly}(\gamma)$

Efficient: $\tilde{O}(n^3)$ time, $\tilde{O}(n)$ quantum queries to f

Quantum Polynomial Freiman-Ruzsa Theorem

Let $A \subseteq \mathbb{F}_2^n$ s.t. $|A + A| \leq K|A|$ for doubling-constant $K \geq 1$. There is an efficient algorithm that learns a PFR subspace $V \leq \mathbb{F}_2^n$ of size $|V| \leq |A|$.

Dequantising via Symplectic Geometry

We then dequantise the quantum stabiliser learning algorithm

Connection between quadratic Fourier analysis and symplectic geometry

> [6]There appear to be some intriguing parallels with symplectic geometry here. Roughly speaking, the vanishing (3.16) is an assertion that the graph $\{(h, Mh) : h \in G\}$ is a "Lagrangian manifold" on the "phase space" $G \times \widehat{G}$. This graph can also be interpreted (essentially) as the "wave front set" $\{(x, \nabla\phi(x)) : x \in G\}$ of the original function $e(\phi)$. A similar interpretation persists in the proofs of Theorem 2.3 and 2.7 below. Thus we see hints of some kind of "combinatorial symplectic geometry" emerging, though we do not see how to develop these possible connections further.
>
> Green and Tao, An inverse theorem for the Gowers U^3 norm (2008)

Symplectic inner product of $(a,b),(c,d) \in \mathbb{F}_2^{2n}$ is $[(a,b),(c,d)] := ad - bc$

Lagrangian $L \leq \mathbb{F}_2^{2n}$ is a maximal isotropic subspace $[u,v] = 0 \quad \forall u, v \in L$

A stabiliser state ϕ is associated with a unique Lagrangian subspace $L(\phi)$

Study $\left|\mathbb{E}_{x \in \mathbb{F}_2^n} f(x)\overline{\phi(x)}\right|$ via the characteristic weight $P_f(L(\phi))$

controlled by the quadratic structure of f

Looking ahead

Quantum computation and additive combinatorics

A few examples: 1) Stabiliser states & Gowers norms

2) Clifford hierarchy & Higher-order Fourier analysis

3) Algorithmic structure vs randomness theorems

4) Quantum local correction & Bogolyubov theorems

Upcoming survey with Jop Briët, Davi Castro-Silva, and Arkopal Dutt

There is a deep connection. Let's find it!