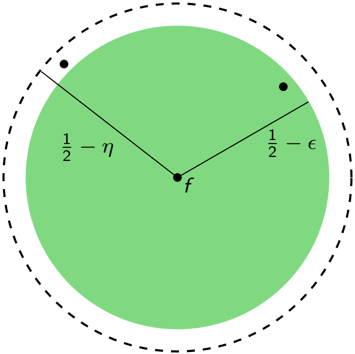
# Algorithmic Questions in Higher-Order Fourier Analysis





Madhur Tulsiani

TTI Chicago


Based on joint works with Arnab Bhattacharyya, Eli Ben-Sasson, Pooya Hatami, Noga Ron-Zewi, Luca Trevisan, Salil Vadhan and Julia Wolf

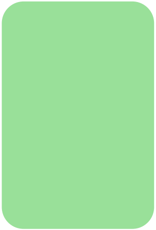
# Decomposition Theorems

# Decomposition Theorems

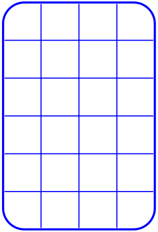
Object of study

Family of algorithms or functions

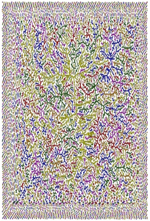
# Decomposition Theorems



$=$



$+$



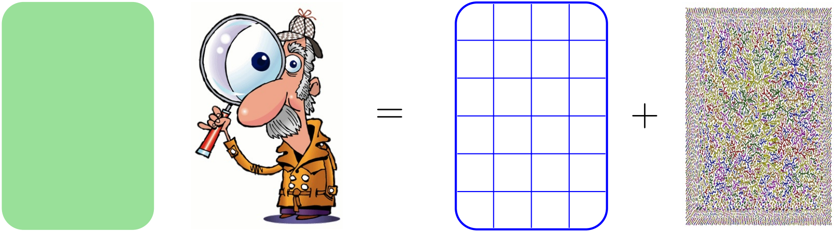
Object of study

Family of algorithms or functions

Structured

No apparent structure (Pseudorandom)

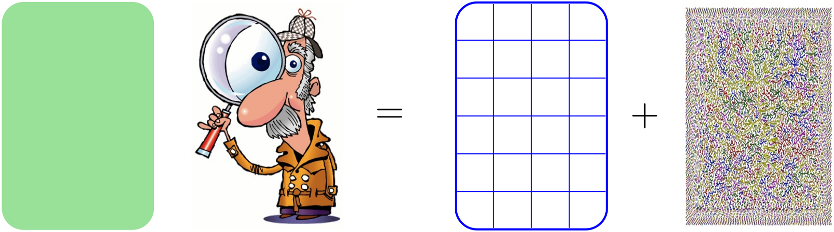
# Decomposition Theorems



Object of study | Family of algorithms or functions = Structured + No apparent structure (Pseudorandom)

- Decompose an object in to structured and pseudorandom parts.

# Decomposition Theorems



Object of study | Family of algorithms or functions = Structured + No apparent structure (Pseudorandom)

- Decompose an object in to structured and pseudorandom parts.
- Can often ignore the pseudorandom part for many applications. Structured part easier to study.

# Fourier analysis

- Space of functions $g : \mathbb{F}_2^n \to \mathbb{R}$.

# Fourier analysis

- Space of functions $g : \mathbb{F}_2^n \to \mathbb{R}$.

- Functions

$$\chi_\alpha(x) \;=\; (-1)^{\alpha \cdot x} \;=\; (-1)^{\sum_j \alpha_j x_j}$$

  form an orthonormal basis under the inner product $\langle f, g \rangle = \mathbb{E}_x \left[ f(x) g(x) \right]$.

# Fourier analysis

- Space of functions $g : \mathbb{F}_2^n \to \mathbb{R}$.

- Functions
$$\chi_\alpha(x) \;=\; (-1)^{\alpha \cdot x} \;=\; (-1)^{\sum_j \alpha_j x_j}$$
form an orthonormal basis under the inner product $\langle f, g \rangle = \mathbb{E}_x \left[ f(x) g(x) \right]$.

- Any function $g$ can be written as
$$g \;=\; \sum_{\alpha \in \mathbb{F}_2^n} \hat{g}(\alpha) \chi_\alpha \;.$$

# Fourier analysis

- Space of functions $g : \mathbb{F}_2^n \to \mathbb{R}$.

- Functions
$$\chi_\alpha(x) \;=\; (-1)^{\alpha \cdot x} \;=\; (-1)^{\sum_j \alpha_j x_j}$$
form an orthonormal basis under the inner product $\langle f, g \rangle = \mathbb{E}_x \left[ f(x) g(x) \right]$.

- Any function $g$ can be written as
$$g \;=\; \sum_{\alpha \in \mathbb{F}_2^n} \hat{g}(\alpha) \chi_\alpha \;.$$

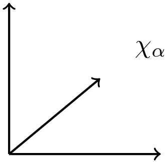
- [Parseval]: $\|g\|^2 \;=\; \langle g, g \rangle \;=\; \mathbb{E}_x \left[ (g(x))^2 \right] \;=\; \sum_\alpha \left( \hat{g}(\alpha) \right)^2$.

# A basic decomposition in Fourier analysis

$$g : \mathbb{F}_2^n \to [-1, 1]$$

# A basic decomposition in Fourier analysis

$$g : \mathbb{F}_2^n \to [-1, 1]$$



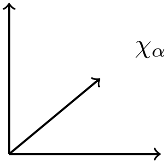
$$\chi_\alpha(x) = (-1)^{\alpha \cdot x} = (-1)^{\sum_i \alpha_j x_j}$$

$$\alpha \in \mathbb{F}_2^n$$

$$g = \sum_S \widehat{g}(\alpha)\chi_\alpha$$

# A basic decomposition in Fourier analysis

$$g : \mathbb{F}_2^n \to [-1, 1]$$



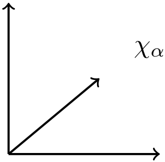
$$\chi_\alpha(x) = (-1)^{\alpha \cdot x} = (-1)^{\sum_i \alpha_j x_j}$$

$$\alpha \in \mathbb{F}_2^n$$

$$g = \sum_S \widehat{g}(\alpha)\chi_\alpha = \sum_{|\widehat{g}(\alpha)| > \epsilon} \widehat{g}(\alpha)\chi_\alpha + \sum_{|\widehat{g}(\alpha)| \le \epsilon} \widehat{g}(\alpha)\chi_\alpha = \sum_{i=1}^{k} c_i \chi_{\alpha_i} + f$$

# A basic decomposition in Fourier analysis

$g : \mathbb{F}_2^n \to [-1, 1]$



$$\chi_\alpha(x) = (-1)^{\alpha \cdot x} = (-1)^{\sum_i \alpha_j x_j}$$

$$\alpha \in \mathbb{F}_2^n$$

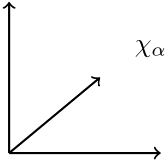
$$g = \sum_S \widehat{g}(\alpha)\chi_\alpha = \sum_{|\widehat{g}(\alpha)| > \epsilon} \widehat{g}(\alpha)\chi_\alpha + \sum_{|\widehat{g}(\alpha)| \le \epsilon} \widehat{g}(\alpha)\chi_\alpha = \sum_{i=1}^{k} c_i \chi_{\alpha_i} + f$$

- $k \le 1/\epsilon^2$.

simple structure

# A basic decomposition in Fourier analysis

$$g : \mathbb{F}_2^n \to [-1, 1]$$



$$\chi_\alpha(x) = (-1)^{\alpha \cdot x} = (-1)^{\sum_i \alpha_j x_j}$$
$$\alpha \in \mathbb{F}_2^n$$

$$g = \sum_S \widehat{g}(\alpha)\chi_\alpha = \sum_{|\widehat{g}(\alpha)| > \epsilon} \widehat{g}(\alpha)\chi_\alpha + \sum_{|\widehat{g}(\alpha)| \leq \epsilon} \widehat{g}(\alpha)\chi_\alpha = \sum_{i=1}^{k} c_i \chi_{\alpha_i} + f$$

- $k \leq 1/\epsilon^2$. simple structure
- $f$ has small correlation with linear functions. pseudorandom

$$\forall \alpha, |\langle f, \chi_\alpha \rangle| = |\mathbb{E}_x [f(x)\chi_\alpha(x)]| \leq \epsilon$$

# Getting high: Quadratic Fourier Analysis [Gowers 98, Green 07]

- "Fourier pseudorandomness" often insufficient for many applications (e.g. counting 4-term APs in a set).

# Getting high: Quadratic Fourier Analysis [Gowers 98, Green 07]

- "Fourier pseudorandomness" often insufficient for many applications (e.g. counting 4-term APs in a set).
- [Gowers 98]: Defined uniformity norms (Gowers norms). "Right" notion of pseudorandomness for many applications.

$$\|f\|_{U^2}^4 = \mathbb{E}_{x,y,z}\left[f(x) \cdot f(x+y) \cdot f(x+z) \cdot f(x+y+z)\right].$$

Think $f =$ indicator of a set. $\|f\|_{U^2}$ counts 2-dimensional "boxes" in set.

# Getting high: Quadratic Fourier Analysis [Gowers 98, Green 07]

- "Fourier pseudorandomness" often insufficient for many applications (e.g. counting 4-term APs in a set).
- [Gowers 98]: Defined uniformity norms (Gowers norms). "Right" notion of pseudorandomness for many applications.

$$\|f\|_{U^2}^4 = \mathbb{E}_{x,y,z}\left[f(x)\cdot f(x+y)\cdot f(x+z)\cdot f(x+y+z)\right].$$

Think $f =$ indicator of a set. $\|f\|_{U^2}$ counts 2-dimensional "boxes" in set.

- Can define higher norms similarly

$$\|f\|_{U^3}^8 = \mathbb{E}_{x,y,z,w}\left[\begin{array}{l} \mathrm{f(x)\ f(x{+}y)\ f(x{+}z)\ f(x{+}y{+}z)} \\ \mathrm{f(x{+}w)\ f(x{+}y{+}w)\ f(x{+}z{+}w)\ f(x{+}y{+}z{+}w)} \end{array}\right]$$

# Norms, Shnorms... so what?

- $\|f\|_{U^2}$ measures correlation with Fourier characters (linear phase functions).

$$\left(\max_{\alpha}\left|\hat{f}(\alpha)\right|\right)^4 \le \|f\|_{U_2}^4 \le \left(\max_{\alpha}\left|\hat{f}(\alpha)\right|\right)^2$$

# Norms, Shnorms... so what?

- $\|f\|_{U^2}$ measures correlation with Fourier characters (linear phase functions).

$$\left(\max_{\alpha}\left|\hat{f}(\alpha)\right|\right)^4 \le \|f\|_{U_2}^4 \le \left(\max_{\alpha}\left|\hat{f}(\alpha)\right|\right)^2$$

- [Green-Tao 05, Samorodnitsky 07]: Gowers $U^3$ norm approximately measures correlation with the set of quadratic phase functions. ($(-1)^{Q(x)}$ for $Q(x) = x^T Ax + b^T x + c$).

# Norms, Shnorms... so what?

- $\|f\|_{U^2}$ measures correlation with Fourier characters (linear phase functions).

$$\left(\max_{\alpha}\left|\hat{f}(\alpha)\right|\right)^4 \leq \|f\|_{U_2}^4 \leq \left(\max_{\alpha}\left|\hat{f}(\alpha)\right|\right)^2$$

- [Green-Tao 05, Samorodnitsky 07]: Gowers $U^3$ norm approximately measures correlation with the set of quadratic phase functions. ($(-1)^{Q(x)}$ for $Q(x) = x^T Ax + b^T x + c$). For $f : \mathbb{F}_2^n \to [-1, 1]$,
  - $\|f\|_{U^3} \leq \epsilon \implies$ for all $Q, \left|\left\langle f, (-1)^Q \right\rangle\right| \leq \epsilon$.

# Norms, Shnorms... so what?

- $\|f\|_{U^2}$ measures correlation with Fourier characters (linear phase functions).

$$\left(\max_{\alpha}\left|\hat{f}(\alpha)\right|\right)^4 \le \|f\|_{U_2}^4 \le \left(\max_{\alpha}\left|\hat{f}(\alpha)\right|\right)^2$$

- [Green-Tao 05, Samorodnitsky 07]: Gowers $U^3$ norm approximately measures correlation with the set of quadratic phase functions. ($(-1)^{Q(x)}$ for $Q(x) = x^T Ax + b^T x + c$). For $f : \mathbb{F}_2^n \to [-1, 1]$,
  - $\|f\|_{U^3} \le \epsilon \implies$ for all $Q, \left|\langle f, (-1)^Q \rangle\right| \le \epsilon$.
  - $\|f\|_{U^3} \ge \epsilon \implies$ for some $Q, \left|\langle f, (-1)^Q \rangle\right| \ge \eta(\epsilon)$.

# Decompositions in Quadratic Fourier Analysis

**Theorem (Gowers-Wolf 09)**

*Given* $\epsilon > 0$*, any* $g : \mathbb{F}_2^n \to [-1,1]$ *can be decomposed as*

$$g \;=\; \sum_{i=1}^{k} c_i(-1)^{Q_i} + f + e$$

*for quadratic functions* $Q_1, \ldots, Q_k$ *such that*

# Decompositions in Quadratic Fourier Analysis

**Theorem (Gowers-Wolf 09)**

*Given* $\epsilon > 0$, *any* $g : \mathbb{F}_2^n \to [-1, 1]$ *can be decomposed as*

$$g \ = \ \sum_{i=1}^{k} c_i (-1)^{Q_i} + f + e$$

*for quadratic functions* $Q_1, \ldots, Q_k$ *such that*

- $\|f\|_{U^3} \leq \epsilon$, $\|e\|_1 \leq \epsilon$ *pseudorandom*

# Decompositions in Quadratic Fourier Analysis

**Theorem (Gowers-Wolf 09)**

*Given* $\epsilon > 0$*, any* $g : \mathbb{F}_2^n \to [-1, 1]$ *can be decomposed as*

$$g \;=\; \sum_{i=1}^{k} c_i(-1)^{Q_i} + f + e$$

*for quadratic functions* $Q_1, \ldots, Q_k$ *such that*

- $\|f\|_{U^3} \leq \epsilon$, $\|e\|_1 \leq \epsilon$ — *pseudorandom*
- $\sum_i |c_i| \leq M(\epsilon)$ *for* $M(\epsilon) = \exp(1/\epsilon^C)$. — *structure*

# Decompositions in Quadratic Fourier Analysis

**Theorem (Gowers-Wolf 09)**

*Given $\epsilon > 0$, any $g : \mathbb{F}_2^n \to [-1, 1]$ can be decomposed as*

$$g \;=\; \sum_{i=1}^{k} c_i (-1)^{Q_i} + f + e$$

*for quadratic functions $Q_1, \ldots, Q_k$ such that*

- $\|f\|_{U^3} \leq \epsilon$, $\|e\|_1 \leq \epsilon$ — *pseudorandom*
- $\sum_i |c_i| \leq M(\epsilon)$ *for* $M(\epsilon) = \exp(1/\epsilon^C)$. — *structure*

Similar to basic Fourier decomposition, where we get

$$g = \sum_{i=1}^{k} c_i \chi_{\alpha_i}(x) + f,$$

with $|\langle f, \chi_\alpha \rangle| \leq \epsilon$ for all $\alpha$ and $k \leq 1/\epsilon^2$ (also implies $\sum_i |c_i| \leq 1/\epsilon$).

# Decompositions in Higher-Order Fourier Analysis

**Theorem (Gowers-Wolf 10)**

*Given $\epsilon > 0$ and $p > d$, there exists $M(\epsilon, p)$ such that any $g : \mathbb{F}_p^n \to [-1, 1]$ can be decomposed as*

$$g \ = \ \sum_{i=1}^{k} c_i \cdot \omega^{P_i} + f + e$$

*for $P_1, \ldots, P_k \in \mathcal{P}_d$ (polynomials of degree at most $d$) such that*

- $\|f\|_{U^{d+1}} \leq \epsilon$, $\|e\|_1 \leq \epsilon$
- $\sum_i |c_i| \leq M(\epsilon, p)$.

# Decompositions in Higher-Order Fourier Analysis

**Theorem (Gowers-Wolf 10)**

*Given $\epsilon > 0$ and $p > d$, there exists $M(\epsilon, p)$ such that any $g : \mathbb{F}_p^n \to [-1, 1]$ can be decomposed as*

$$g = \sum_{i=1}^{k} c_i \cdot \omega^{P_i} + f + e$$

*for $P_1, \ldots, P_k \in \mathcal{P}_d$ (polynomials of degree at most $d$) such that*

- $\|f\|_{U^{d+1}} \leq \epsilon$, $\|e\|_1 \leq \epsilon$
- $\sum_i |c_i| \leq M(\epsilon, p)$.

- Stronger decomposition theorems proved by [HL 11] and [BFL 12].
- Decomposition theorems for the case when $p \leq d$ require non-classical polynomials.

Q1: Can we compute these decompositions efficiently?

# Algorithmic version of the basic Fourier decomposition

**Theorem (Goldreich-Levin 89)**

*There is a randomized algorithm, which given* $\epsilon, \delta > 0$ *and oracle access to* $g : \mathbb{F}_2^n \to [-1, 1]$, *runs in time* $O\left(n^2 \log n \cdot (1/\epsilon^2) \cdot \log(1/\delta)\right)$ *and outputs a decomposition*

$$g = \sum_{i=1}^{k} c_i \cdot \chi_{\alpha_i} + f$$

*such that*

# Algorithmic version of the basic Fourier decomposition

**Theorem (Goldreich-Levin 89)**

*There is a randomized algorithm, which given $\epsilon, \delta > 0$ and oracle access to $g : \mathbb{F}_2^n \to [-1, 1]$, runs in time $O\left(n^2 \log n \cdot (1/\epsilon^2) \cdot \log(1/\delta)\right)$ and outputs a decomposition*

$$g = \sum_{i=1}^{k} c_i \cdot \chi_{\alpha_i} + f$$

*such that*

- $k = O(1/\epsilon^2)$

# Algorithmic version of the basic Fourier decomposition

**Theorem (Goldreich-Levin 89)**

*There is a randomized algorithm, which given* $\epsilon, \delta > 0$ *and oracle access to* $g : \mathbb{F}_2^n \to [-1, 1]$*, runs in time* $O\left(n^2 \log n \cdot (1/\epsilon^2) \cdot \log(1/\delta)\right)$ *and outputs a decomposition*

$$g \;=\; \sum_{i=1}^{k} c_i \cdot \chi_{\alpha_i} + f$$

*such that*

- $k = O(1/\epsilon^2)$
- $\mathbb{P}[\exists i \text{ such that } |c_i - \widehat{g}(\alpha_i)| \geq \epsilon] \leq \delta$

# Algorithmic version of the basic Fourier decomposition

**Theorem (Goldreich-Levin 89)**

*There is a randomized algorithm, which given $\epsilon, \delta > 0$ and oracle access to $g : \mathbb{F}_2^n \to [-1, 1]$, runs in time $O\left(n^2 \log n \cdot (1/\epsilon^2) \cdot \log(1/\delta)\right)$ and outputs a decomposition*

$$g \;=\; \sum_{i=1}^{k} c_i \cdot \chi_{\alpha_i} + f$$

*such that*

- $k = O(1/\epsilon^2)$
- $\mathbb{P}[\exists i$ *such that* $|c_i - \widehat{g}(\alpha_i)| \geq \epsilon] \leq \delta$
- $\mathbb{P}[\exists \alpha$ *such that* $\left|\widehat{f}(\alpha)\right| \geq \epsilon] \leq \delta$

- Finding large Fourier coefficients has many applications.

# What's so different about quadratics?

- Set of quadratic phase functions ($(-1)^Q$) is not an orthonormal basis. No Parseval's identity.

# What's so different about quadratics?

- Set of quadratic phase functions ($(-1)^Q$) is not an orthonormal basis. No Parseval's identity.
- Proof of decomposition by Gowers and Wolf is non-constructive (using the Hahn-Banach theorem).

# What's so different about quadratics?

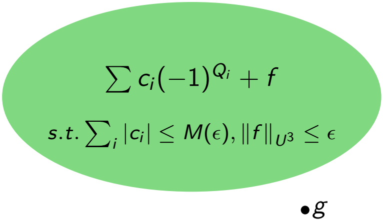
- Set of quadratic phase functions ($(-1)^Q$) is not an orthonormal basis. No Parseval's identity.
- Proof of decomposition by Gowers and Wolf is non-constructive (using the Hahn-Banach theorem).

$$\sum c_i(-1)^{Q_i} + f$$

$$s.t. \sum_i |c_i| \leq M(\epsilon), \|f\|_{U^3} \leq \epsilon$$

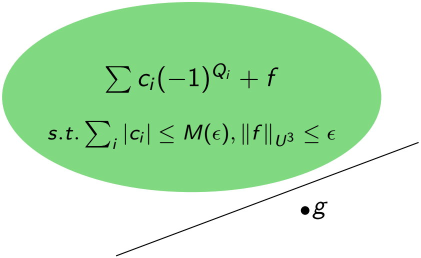
# What's so different about quadratics?

- Set of quadratic phase functions ($(-1)^Q$) is not an orthonormal basis. No Parseval's identity.
- Proof of decomposition by Gowers and Wolf is non-constructive (using the Hahn-Banach theorem).



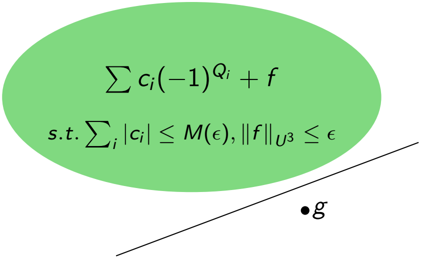
# What's so different about quadratics?

- Set of quadratic phase functions ($(-1)^Q$) is not an orthonormal basis. No Parseval's identity.
- Proof of decomposition by Gowers and Wolf is non-constructive (using the Hahn-Banach theorem).



# What's so different about quadratics?

- Set of quadratic phase functions ($(-1)^Q$) is not an orthonormal basis. No Parseval's identity.
- Proof of decomposition by Gowers and Wolf is non-constructive (using the Hahn-Banach theorem).




- Use inverse theorem for Gowers norm to get a contradiction.

# A quadratic Goldreich-Levin Theorem

**Theorem (T, Wolf 11)**

*For* $M(\epsilon) = \exp(1/\epsilon^C)$, *can compute in time poly*$(n, M(\epsilon), \log(1/\delta))$, *a decomposition*

$$g = \sum_{i=1}^{k} c_i (-1)^{Q_i} + f + e$$

*such that*

- *with probability* $1 - \delta$, $\|f\|_{U^3} \leq \epsilon$ *and* $\|e\|_1 \leq \epsilon$.
- $\sum_i |c_i| \leq M(\epsilon)$ *and* $k \leq (M(\epsilon))^2$.

# Improved quadratic Goldreich-Levin Theorem

**Theorem (BRTW 12)**

*For* $M(\epsilon) = O(\exp(\log^4(1/\epsilon)))$, *can compute in time* $poly(n, M(\epsilon), \log(1/\delta))$, *a decomposition*

$$g = \sum_{i=1}^{k} c_i (-1)^{Q_i} + f + e$$

*such that*

- *with probability* $1 - \delta$, $\|f\|_{U^3} \leq \epsilon$ *and* $\|e\|_1 \leq \epsilon$.
- $\sum_i |c_i| \leq M(\epsilon)$ *and* $k \leq (M(\epsilon))^2$.

# A constructive proof of decomposition [TTV 09]

Goal: Given $g : \mathbb{F}_2^n \to [-1, 1]$, find a decomposition $g = \sum_i c_i(-1)^{Q_i} + f$ such that $\|f\|_{U^3} \leq \epsilon$.

# A constructive proof of decomposition [TTV 09]

Goal: Given $g : \mathbb{F}_2^n \to [-1,1]$, find a decomposition $g = \sum_i c_i(-1)^{Q_i} + f$ such that $\|f\|_{U^3} \leq \epsilon$.

Algorithm:

- $h_0 = 0,\ f_0 = g - h_0, t = 1.$

# A constructive proof of decomposition [TTV 09]

Goal: Given $g : \mathbb{F}_2^n \to [-1, 1]$, find a decomposition $g = \sum_i c_i (-1)^{Q_i} + f$ such that $\|f\|_{U^3} \leq \epsilon$.

Algorithm:

- $h_0 = 0$, $f_0 = g - h_0, t = 1$.
- while there is a quadratic function $Q_t$ such that $\langle f_{t-1}, (-1)^{Q_t} \rangle > \eta$

# A constructive proof of decomposition [TTV 09]

Goal: Given $g : \mathbb{F}_2^n \to [-1,1]$, find a decomposition $g = \sum_i c_i (-1)^{Q_i} + f$ such that $\|f\|_{U^3} \le \epsilon$.

Algorithm:

- $h_0 = 0$, $f_0 = g - h_0, t = 1$.
- while there is a quadratic function $Q_t$ such that $\left\langle f_{t-1}, (-1)^{Q_t} \right\rangle > \eta$
  - $h_t = h_{t-1} + \eta \cdot (-1)^{Q_t} = \sum_{r=1}^{t} \eta \cdot (-1)^{Q_r}$
  - $f_t = g - h_t$
  - $t = t + 1$

# A constructive proof of decomposition [TTV 09]

Goal: Given $g : \mathbb{F}_2^n \to [-1, 1]$, find a decomposition $g = \sum_i c_i (-1)^{Q_i} + f$ such that $\|f\|_{U^3} \leq \epsilon$.

Algorithm:

- $h_0 = 0$, $f_0 = g - h_0, t = 1$.
- while there is a quadratic function $Q_t$ such that $\langle f_{t-1}, (-1)^{Q_t} \rangle > \eta$
  - $h_t = h_{t-1} + \eta \cdot (-1)^{Q_t} = \sum_{r=1}^{t} \eta \cdot (-1)^{Q_r}$
  - $f_t = g - h_t$
  - $t = t + 1$
- return $h_t$

# A constructive proof of decomposition [TTV 09]

Goal: Given $g : \mathbb{F}_2^n \to [-1, 1]$, find a decomposition $g = \sum_i c_i (-1)^{Q_i} + f$ such that $\|f\|_{U^3} \leq \epsilon$.

Algorithm:

- $h_0 = 0$, $f_0 = g - h_0, t = 1$.
- while there is a quadratic function $Q_t$ such that $\langle f_{t-1}, (-1)^{Q_t} \rangle > \eta$
  - $h_t = h_{t-1} + \eta \cdot (-1)^{Q_t} = \sum_{r=1}^{t} \eta \cdot (-1)^{Q_r}$
  - $f_t = g - h_t$
  - $t = t + 1$
- return $h_t$

Convergence: $\|f_{t-1}\|^2 - \|f_t\|^2 = 2\eta \langle f_{t-1}, (-1)^{Q_t} \rangle - \eta^2 \geq \eta^2$.

# A constructive proof of decomposition [TTV 09]

Goal: Given $g : \mathbb{F}_2^n \to [-1,1]$, find a decomposition $g = \sum_i c_i(-1)^{Q_i} + f$ such that $\|f\|_{U^3} \le \epsilon$.

Algorithm:

- $h_0 = 0,\ f_0 = g - h_0, t = 1.$
- while there is a quadratic function $Q_t$ such that $\langle f_{t-1}, (-1)^{Q_t} \rangle > \eta$
  - $h_t = h_{t-1} + \eta \cdot (-1)^{Q_t} = \sum_{r=1}^{t} \eta \cdot (-1)^{Q_r}$
  - $f_t = g - h_t$
  - $t = t + 1$
- return $h_t$

Convergence: $\|f_{t-1}\|^2 - \|f_t\|^2 = 2\eta \langle f_{t-1}, (-1)^{Q_t} \rangle - \eta^2 \ge \eta^2$.

[Samorodnitsky 07]: $\forall Q \left|\langle (-1)^Q, f \rangle\right| \le \eta(\epsilon) \implies \|f\|_{U^3} \le \epsilon$.

# A constructive proof of decomposition [TTV 09]

Goal: Given $g : \mathbb{F}_2^n \to [-1,1]$, find a decomposition $g = \sum_i c_i(-1)^{Q_i} + f$ such that $\|f\|_{U^3} \le \epsilon$.

Algorithm:

- $h_0 = 0$, $f_0 = g - h_0$, $t = 1$.
- while there is a quadratic function $Q_t$ such that $\langle f_{t-1}, (-1)^{Q_t} \rangle > \eta$
  - $h_t \;=\; h_{t-1} + \eta \cdot (-1)^{Q_t} \;=\; \sum_{r=1}^{t} \eta \cdot (-1)^{Q_r}$
  - $f_t \;=\; g - h_t$
  - $t \;=\; t + 1$
- return $h_t$

Convergence: $\|f_{t-1}\|^2 - \|f_t\|^2 \;=\; 2\eta \langle f_{t-1}, (-1)^{Q_t} \rangle - \eta^2 \;\ge\; \eta^2$.

[Samorodnitsky 07]: $\forall Q \left|\langle (-1)^Q, f \rangle\right| \le \eta(\epsilon) \implies \|f\|_{U^3} \le \epsilon$.

# The algorithmic problem

Question: Given $f : \mathbb{F}_2^n \to \{-1, 1\}$, does there exist $Q$ such that $\langle f, (-1)^Q \rangle \geq \epsilon$? If yes, find one.

# The algorithmic problem

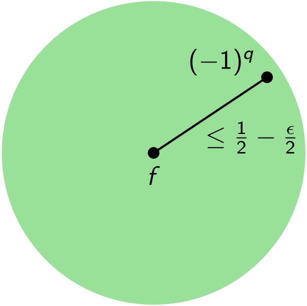
Question: Given $f : \mathbb{F}_2^n \to \{-1, 1\}$, does there exist $Q$ such that $\langle f, (-1)^Q \rangle \geq \epsilon$? If yes, find one.

Truth-tables of functions $(-1)^Q$ form the Reed-Muller code of order 2.

# The algorithmic problem

Question: Given $f : \mathbb{F}_2^n \to \{-1, 1\}$, does there exist $Q$ such that $\langle f, (-1)^Q \rangle \geq \epsilon$? If yes, find one.

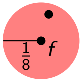
Truth-tables of functions $(-1)^Q$ form the Reed-Muller code of order 2. Want a codeword inside a ball of distance $1/2 - \epsilon/2$ around $f$ (if one exists).



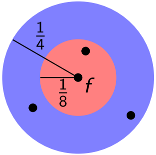
Q2: Decoding beyond the list-decoding radius

# Finding codewords at large distances

# Finding codewords at large distances

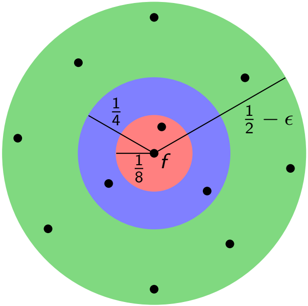


# Finding codewords at large distances




- List decoding radius is $\frac{1}{4}$.
  [GKZ 08, Gopalan 10, BL 14]

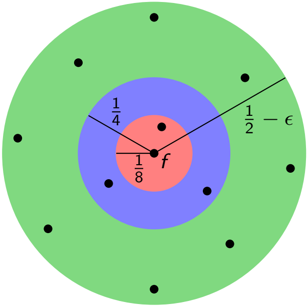
# Finding codewords at large distances




- List decoding radius is $\frac{1}{4}$.
  [GKZ 08, Gopalan 10, BL 14]

- Number of codewords within distance $\frac{1}{2} - \epsilon$ may be exponential.

# Finding codewords at large distances




- List decoding radius is $\frac{1}{4}$.
  [GKZ 08, Gopalan 10, BL 14]
- Number of codewords within distance $\frac{1}{2} - \epsilon$ may be exponential.
- But we only need to find one codeword! In time $poly(n)$ (polylogarithmic in code length).

# Finding codewords at large distances

- Given (the coefficients of) a degree-$d$ polynomial $P : \mathbb{F}_p^n \to \mathbb{F}_p$, the Reed-Muller encoding of $P$ is of length $p^n$ and is given by the table of values $\{P(x)\}_{x \in \mathbb{F}_p^n}$.

# Finding codewords at large distances

- Given (the coefficients of) a degree-$d$ polynomial $P : \mathbb{F}_p^n \to \mathbb{F}_p$, the Reed-Muller encoding of $P$ is of length $p^n$ and is given by the table of values $\{P(x)\}_{x \in \mathbb{F}_p^n}$.

- Problem: Given $F : \mathbb{F}_p^n \to \mathbb{F}_p$, if there exists $P \in \mathcal{P}_d$ such that

$$\Delta(F, P) \ \leq \ 1 - \frac{1}{p} - \epsilon$$

  find a $P' \in \mathcal{P}_d$ such that

$$\Delta(F, P') \ \leq \ 1 - \frac{1}{p} - \eta$$

# Finding codewords at large distances

- Given (the coefficients of) a degree-$d$ polynomial $P : \mathbb{F}_p^n \to \mathbb{F}_p$, the Reed-Muller encoding of $P$ is of length $p^n$ and is given by the table of values $\{P(x)\}_{x \in \mathbb{F}_p^n}$.

- Problem: Given $F : \mathbb{F}_p^n \to \mathbb{F}_p$, if there exists $P \in \mathcal{P}_d$ such that

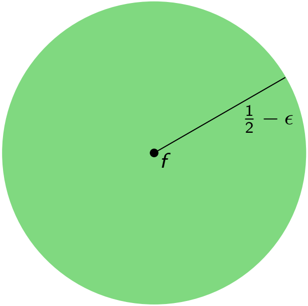
$$\Delta(F, P) \ \leq \ 1 - \frac{1}{p} - \epsilon$$

  find a $P' \in \mathcal{P}_d$ such that

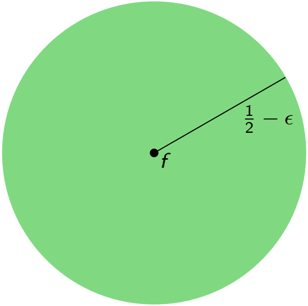
$$\Delta(F, P') \ \leq \ 1 - \frac{1}{p} - \eta$$

- If there exists a Reed-Muller codeword within a ball of radius $1 - \frac{1}{p} - \epsilon$, find one within a ball of radius $1 - \frac{1}{p} - \eta$.

# Finding a single codeword: the quadratic case

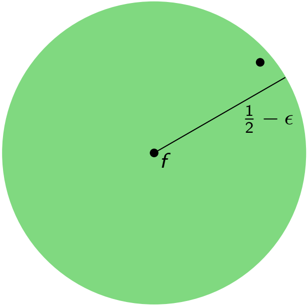


# Finding a single codeword: the quadratic case



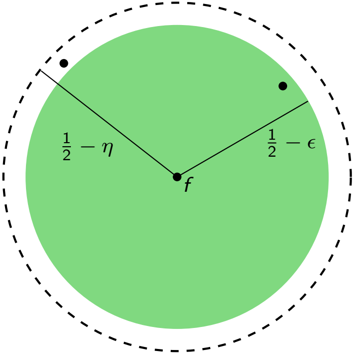

- [Samorodnitsky 07]: Approximate solution to testing problem using Gowers norm.

# Finding a single codeword: the quadratic case



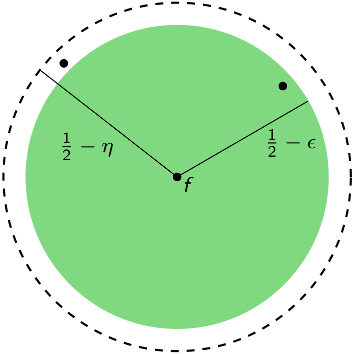

- [Samorodnitsky 07]: Approximate solution to testing problem using Gowers norm.
  - $\exists q \ \langle f, (-1)^Q \rangle \geq \epsilon \implies \|f\|_{U^3} \geq \epsilon$

# Finding a single codeword: the quadratic case




- [Samorodnitsky 07]: Approximate solution to testing problem using Gowers norm.
  - $\exists q \; \langle f, (-1)^Q \rangle \geq \epsilon \implies \|f\|_{U^3} \geq \epsilon$
  - $\|f\|_{U^3} \geq \epsilon \implies \exists Q \; \langle f, (-1)^Q \rangle \geq \eta(\epsilon)$

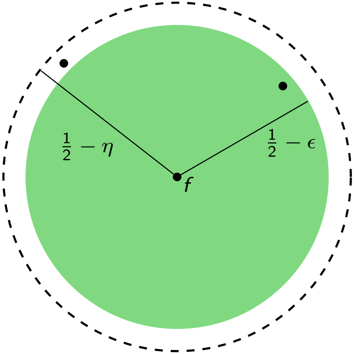
# Finding a single codeword: the quadratic case




- [Samorodnitsky 07]: Approximate solution to testing problem using Gowers norm.
  - $\exists q \ \langle f, (-1)^Q \rangle \geq \epsilon \implies \|f\|_{U^3} \geq \epsilon$
  - $\|f\|_{U^3} \geq \epsilon \implies \exists Q \ \langle f, (-1)^Q \rangle \geq \eta(\epsilon)$

- [TW 11] convert Samorodnitsky's proof into an algorithm. Find codeword within distance $\frac{1}{2} - \eta$ if there is one within $\frac{1}{2} - \epsilon$.

# Finding a single codeword: the quadratic case

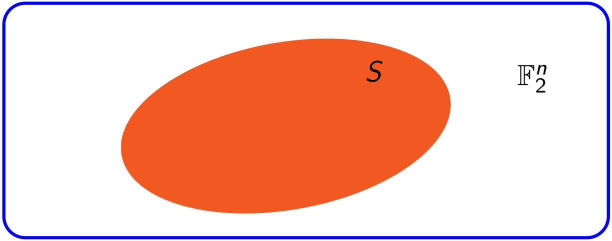



- [Samorodnitsky 07]: Approximate solution to testing problem using Gowers norm.
  - $\exists q \; \langle f, (-1)^Q \rangle \geq \epsilon \implies \|f\|_{U^3} \geq \epsilon$
  - $\|f\|_{U^3} \geq \epsilon \implies \exists Q \; \langle f, (-1)^Q \rangle \geq \eta(\epsilon)$

- [TW 11] convert Samorodnitsky's proof into an algorithm. Find codeword within distance $\frac{1}{2} - \eta$ if there is one within $\frac{1}{2} - \epsilon$.

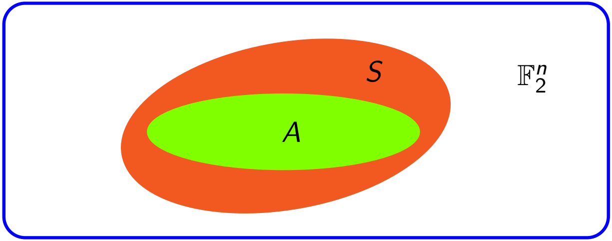
- First example of any kind of decoding beyond the list decoding radius.

# Algorithmic versions of combinatorial theorems



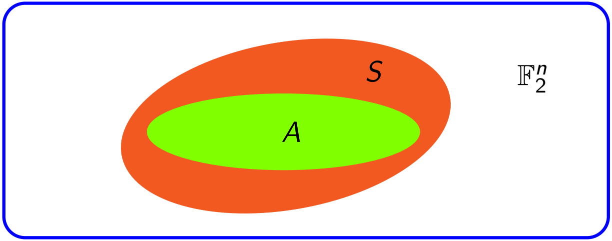

- Samorodnitsky's proof applies various combinatorial theorems (e.g. Balog-Szemerédi-Gowers) to "nice" subsets of $\mathbb{F}_2^n$.

# Algorithmic versions of combinatorial theorems



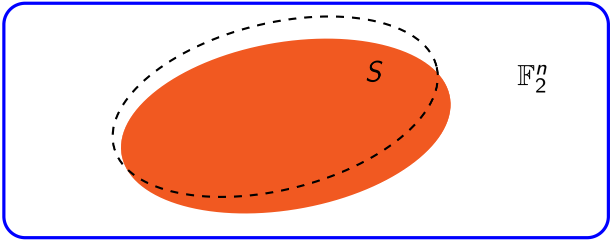

- Samorodnitsky's proof applies various combinatorial theorems (e.g. Balog-Szemerédi-Gowers) to "nice" subsets of $\mathbb{F}_2^n$.
- [BSG]: If $S \subseteq \mathbb{F}_2^n$ satisfies $\mathbb{P}_{x,y \in S}[x + y \in S] \geq \epsilon$, then there exists $A \subseteq S$ with certain additive properties.

# Algorithmic versions of combinatorial theorems



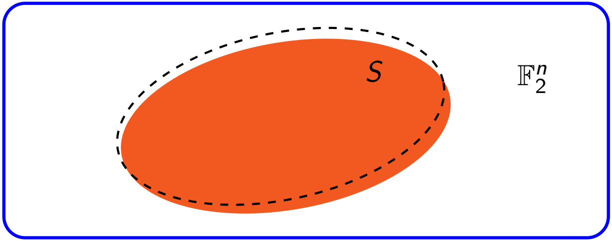

- Samorodnitsky's proof applies various combinatorial theorems (e.g. Balog-Szemerédi-Gowers) to "nice" subsets of $\mathbb{F}_2^n$.
- [BSG]: If $S \subseteq \mathbb{F}_2^n$ satisfies $\mathbb{P}_{x,y \in S}[x + y \in S] \geq \epsilon$, then there exists $A \subseteq S$ with certain additive properties.
- $S$ and $A$ are exponential in size. Need to work with randomized membership oracles. Gives a noisy version of the set $S$.

# Algorithmic versions of combinatorial theorems



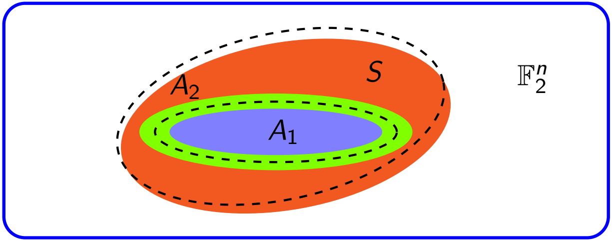

- Samorodnitsky's proof applies various combinatorial theorems (e.g. Balog-Szemerédi-Gowers) to "nice" subsets of $\mathbb{F}_2^n$.
- [BSG]: If $S \subseteq \mathbb{F}_2^n$ satisfies $\mathbb{P}_{x,y \in S}[x + y \in S] \geq \epsilon$, then there exists $A \subseteq S$ with certain additive properties.
- $S$ and $A$ are exponential in size. Need to work with randomized membership oracles. Gives a noisy version of the set $S$.

# Algorithmic versions of combinatorial theorems



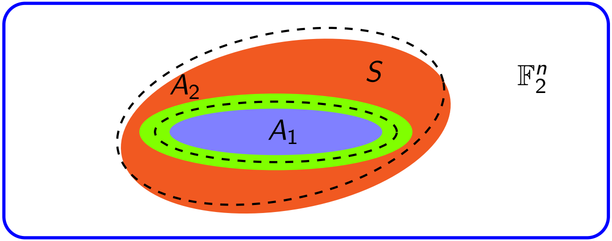

- Modify proofs of combinatorial theorems to go from algorithms in the hypothesis to algorithms in conclusion.

# Algorithmic versions of combinatorial theorems




- Modify proofs of combinatorial theorems to go from algorithms in the hypothesis to algorithms in conclusion.
- Statements of the form: "Given (approximate) membership oracle for $S$, it can be converted to an oracle $A$ whose output is sandwiched between $A_1$ and $A_2$ with certain additive properties."

# Algorithmic versions of combinatorial theorems




- Modify proofs of combinatorial theorems to go from algorithms in the hypothesis to algorithms in conclusion.
- Statements of the form: "Given (approximate) membership oracle for $S$, it can be converted to an oracle $A$ whose output is sandwiched between $A_1$ and $A_2$ with certain additive properties."
- Prove "robust" versions of theorems from additive combinatorics.

# Finding subspace structure

Most combinatorial results used here find and refine subspace structure in $S \subseteq \mathbb{F}_2^n$.

- [BSG]: If $\mathbb{P}_{x,y\in S}[x+y\in S] \geq \epsilon$ then $\exists A \subseteq S$ s.t.

$$|A| \geq \epsilon^{O(1)}|S| \text{ and } |A+A| \leq \epsilon^{-O(1)}|A|.$$

# Finding subspace structure

Most combinatorial results used here find and refine subspace structure in $S \subseteq \mathbb{F}_2^n$.

- [BSG]: If $\mathbb{P}_{x,y \in S}[x + y \in S] \geq \epsilon$ then $\exists A \subseteq S$ s.t.

$$|A| \geq \epsilon^{O(1)}|S| \text{ and } |A + A| \leq \epsilon^{-O(1)}|A|.$$

- [Freiman-Ruzsa]: $|A + A| \leq K \cdot |A| \implies \text{Span}(A) \leq 2^{O(K)} \cdot |A|$.

# Finding subspace structure

Most combinatorial results used here find and refine subspace structure in $S \subseteq \mathbb{F}_2^n$.

- [BSG]: If $\mathbb{P}_{x,y \in S}[x + y \in S] \geq \epsilon$ then $\exists A \subseteq S$ s.t.

$$|A| \geq \epsilon^{O(1)}|S| \text{ and } |A + A| \leq \epsilon^{-O(1)}|A|.$$

- [Freiman-Ruzsa]: $|A + A| \leq K \cdot |A| \implies \text{Span}(A) \leq 2^{O(K)} \cdot |A|$.

- [CS 09]: If $|A + A| \leq K \cdot |A|$, then $\mathbf{1}_A * \mathbf{1}_A$ has a large set of "almost periods" i.e., there is a large set $X \subseteq \mathbb{F}_2^n$ s.t

$$\mathbf{1}_A * \mathbf{1}_A(\cdot) \approx \mathbf{1}_A * \mathbf{1}_A(\cdot + x) \quad \forall x \in X$$

$\mathbf{1}_A * \mathbf{1}_A(\cdot) \approx$ distribution of sum of two random elements from $A$.

# Finding subspace structure

- [Sanders 10]: Stronger inverse theorem for $U^3$-norm using almost periodicity from [CS 09].

# Finding subspace structure

- [Sanders 10]: Stronger inverse theorem for $U^3$-norm using almost periodicity from [CS 09].
- [BRTW 14]: Sampling-based proof of [CS 09]. Improved quadratic Goldreich-Levin.

# Finding subspace structure

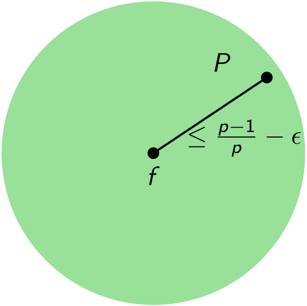
- [Sanders 10]: Stronger inverse theorem for $U^3$-norm using almost periodicity from [CS 09].
- [BRTW 14]: Sampling-based proof of [CS 09]. Improved quadratic Goldreich-Levin.
- Question: Can sampling based proofs be used to find better subspace structure?

# Decompositions for higher-degrees

- Question: Given $F : \mathbb{F}_p^n \to \mathbb{F}_p$, does there exist a polynomial $P \in \mathcal{P}_d$ such that $\left|\left\langle \omega^F, \omega^P \right\rangle\right| \geq \epsilon$? If yes, find one.

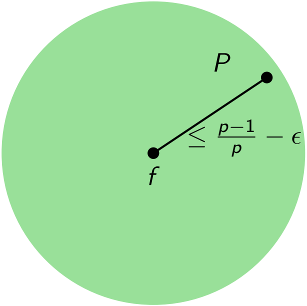
# Decompositions for higher-degrees

- Question: Given $F : \mathbb{F}_p^n \to \mathbb{F}_p$, does there exist a polynomial $P \in \mathcal{P}_d$ such that $\left|\left\langle \omega^F, \omega^P \right\rangle\right| \geq \epsilon$? If yes, find one.



# Decompositions for higher-degrees

- Question: Given $F : \mathbb{F}_p^n \to \mathbb{F}_p$, does there exist a polynomial $P \in \mathcal{P}_d$ such that $\left|\left\langle \omega^F, \omega^P \right\rangle\right| \geq \epsilon$? If yes, find one.




- Can be solved for the special case when $F \in \mathcal{P}_k$ and $p > k$, inverse theorem by [GT 09].

# Decomposition Theorems and Regularity

- [GT 09]: Actually prove a decomposition theorem when $F \in \mathcal{P}_k$:

$$\omega^F = \Gamma(P_1, \ldots, P_m) + f_2$$

where $P_1, \ldots, P_m \in \mathcal{P}_d$ and $\|f_2\|_{U^{d+1}} \leq \epsilon$.

# Decomposition Theorems and Regularity

- [GT 09]: Actually prove a decomposition theorem when $F \in \mathcal{P}_k$:

$$\omega^F = \Gamma(P_1, \ldots, P_m) + f_2$$

  where $P_1, \ldots, P_m \in \mathcal{P}_d$ and $\|f_2\|_{U^{d+1}} \le \epsilon$.

- Here, $\Gamma : \mathbb{F}_p^m \to \mathbb{R}$. By (linear) Fourier analysis

$$\Gamma(P_1, \ldots, P_m) \;=\; \sum_{c_1, \ldots, c_m} \widehat{\Gamma}(c_1, \ldots, c_m) \cdot \omega^{\sum_i c_i P_i}$$

  which gives decomposition in the required form.

# Decomposition Theorems and Regularity

- [GT 09]: Actually prove a decomposition theorem when $F \in \mathcal{P}_k$:

$$\omega^F = \Gamma(P_1, \ldots, P_m) + f_2$$

  where $P_1, \ldots, P_m \in \mathcal{P}_d$ and $\|f_2\|_{U^{d+1}} \leq \epsilon$.

- Here, $\Gamma : \mathbb{F}_p^m \to \mathbb{R}$. By (linear) Fourier analysis

$$\Gamma(P_1, \ldots, P_m) \; = \; \sum_{c_1, \ldots, c_m} \widehat{\Gamma}(c_1, \ldots, c_m) \cdot \omega^{\sum_i c_i P_i}$$

  which gives decomposition in the required form.

- Proof by [GT 09] and many other applications require the factor $\mathcal{B} = \{P_1, \ldots, P_m\}$ to satisfy certain “regularity” properties. Obtaining regularity is the main challenge in converting their proof to an algorithm.

# Polynomial Regularity Lemmas

- Regulariy lemmas for polynomials are useful for several applications of higher-order Fourier analysis.
- Analogues of Szemerédi regularity lemma. Regular partition a graph is highly structured. So is a regular collection of polynomials.

# Polynomial Regularity Lemmas

- Regulariy lemmas for polynomials are useful for several applications of higher-order Fourier analysis.
- Analogues of Szemerédi regularity lemma. Regular partition a graph is highly structured. So is a regular collection of polynomials.
- Different notions of regulariy for a factor $\mathcal{B} = \{P_1, \ldots, P_m\}$:

# Polynomial Regularity Lemmas

- Regulariy lemmas for polynomials are useful for several applications of higher-order Fourier analysis.
- Analogues of Szemerédi regularity lemma. Regular partition a graph is highly structured. So is a regular collection of polynomials.
- Different notions of regulariy for a factor $\mathcal{B} = \{P_1, \dots, P_m\}$:
  - [GT 09]: For all $(c_1, \dots, c_m) \in \mathbb{F}_p^m \setminus \{0^m\}$, $\mathrm{rank}_{d-1}(c_1 P_1 + \cdots + c_m P_m) \geq \Lambda(m)$.

# Polynomial Regularity Lemmas

- Regulariy lemmas for polynomials are useful for several applications of higher-order Fourier analysis.
- Analogues of Szemerédi regularity lemma. Regular partition a graph is highly structured. So is a regular collection of polynomials.
- Different notions of regulariy for a factor $\mathcal{B} = \{P_1, \ldots, P_m\}$:
  - [GT 09]: For all $(c_1, \ldots, c_m) \in \mathbb{F}_p^m \setminus \{0^m\}$, $\text{rank}_{d-1}(c_1 P_1 + \cdots + c_m P_m) \geq \Lambda(m)$.
  - [KL 08]: For all $(c_1, \ldots, c_m) \in \mathbb{F}_p^m \setminus \{0^m\}$, $\sum c_i P_i$ and it's derivatiives have high-rank.
- Polynomial Regularity Lemmas: Given $\mathcal{B} = \{P_1, \ldots, P_m\}$, it can be refined to $\mathcal{B}' = \{P'_1, \ldots, P'_{m'}\}$ which is regular.

# Polynomial Regularity Lemmas

- Regulariy lemmas for polynomials are useful for several applications of higher-order Fourier analysis.
- Analogues of Szemerédi regularity lemma. Regular partition a graph is highly structured. So is a regular collection of polynomials.
- Different notions of regulariy for a factor $\mathcal{B} = \{P_1, \ldots, P_m\}$:
  - [GT 09]: For all $(c_1, \ldots, c_m) \in \mathbb{F}_p^m \setminus \{0^m\}$, $\text{rank}_{d-1}(c_1 P_1 + \cdots + c_m P_m) \geq \Lambda(m)$.
  - [KL 08]: For all $(c_1, \ldots, c_m) \in \mathbb{F}_p^m \setminus \{0^m\}$, $\sum c_i P_i$ and it's derivatiives have high-rank.
- Polynomial Regularity Lemmas: Given $\mathcal{B} = \{P_1, \ldots, P_m\}$, it can be refined to $\mathcal{B}' = \{P_1', \ldots, P_{m'}'\}$ which is regular.
- Like Szemerédi's regularity lemma, proofs find a certificate of non-regularity and make progress by local modification.

# Q3: Algorithmic Regularity Lemmas

# Algorithmic notions of regularity

- Algorithmic step in the regularity lemma is finding a certificate of non-regularity.

# Algorithmic notions of regularity

- Algorithmic step in the regularity lemma is finding a certificate of non-regularity.

- [BHT 15]: Slightly modified notions of regularity (equivalent up to some loss of parameters) and corresponding algorithmic lemmas.

# Algorithmic notions of regularity

- Algorithmic step in the regularity lemma is finding a certificate of non-regularity.
- [BHT 15]: Slightly modified notions of regularity (equivalent up to some loss of parameters) and corresponding algorithmic lemmas.
  - [GT 09]: For all $(c_1, \ldots, c_m) \in \mathbb{F}_p^m \setminus \{0^m\}$, $\|c_1 P_1 + \cdots + c_m P_m\|_{U^d} \leq \delta(m)$.

# Algorithmic notions of regularity

- Algorithmic step in the regularity lemma is finding a certificate of non-regularity.
- [BHT 15]: Slightly modified notions of regularity (equivalent up to some loss of parameters) and corresponding algorithmic lemmas.
  - [GT 09]: For all $(c_1, \ldots, c_m) \in \mathbb{F}_p^m \setminus \{0^m\}$, $\|c_1 P_1 + \cdots + c_m P_m\|_{U^d} \leq \delta(m)$.
  - [KL 08]: For all $(c_1, \ldots, c_m) \in \mathbb{F}_p^m \setminus \{0^m\}$, $\sum c_i P_i$ and it's derivatiives have small-bias.

# Algorithmic notions of regularity

- Algorithmic step in the regularity lemma is finding a certificate of non-regularity.
- [BHT 15]: Slightly modified notions of regularity (equivalent up to some loss of parameters) and corresponding algorithmic lemmas.
  - [GT 09]: For all $(c_1, \ldots, c_m) \in \mathbb{F}_p^m \setminus \{0^m\}$, $\|c_1 P_1 + \cdots + c_m P_m\|_{U^d} \leq \delta(m)$.
  - [KL 08]: For all $(c_1, \ldots, c_m) \in \mathbb{F}_p^m \setminus \{0^m\}$, $\sum c_i P_i$ and it's derivatiives have small-bias.
- Show these notions provide required equidistribution for various known applications.

# Further questions

- Higher-degree decomposition theorems.

# Further questions

- Higher-degree decomposition theorems.
- (Approximate) Decoding beyond the list decoding radius for other codes. Even for distances slightly beyond the list-decoding radius.

# Further questions

- Higher-degree decomposition theorems.
- (Approximate) Decoding beyond the list decoding radius for other codes. Even for distances slightly beyond the list-decoding radius.
- Do algorithms really need to be derived from proofs of existence? Can there be a simpler algorithm for which a solution is guaranteed by the proof?

# Further questions

- Higher-degree decomposition theorems.
- (Approximate) Decoding beyond the list decoding radius for other codes. Even for distances slightly beyond the list-decoding radius.
- Do algorithms really need to be derived from proofs of existence? Can there be a simpler algorithm for which a solution is guaranteed by the proof?
- Regularity lemmas give terrible quantitative bounds. Is there a way to use weaker regularity properties and obtain better bounds?

Thank You

---

Questions?