Higher-order Fourier Analysis over Finite Fields, and Applications

Pooya Hatami
Coding Theory:
Task: Reliably transmit a message through an unreliable channel.

\[ m \in F_2^k \]

\[ F_2^N \]

\[ c_m \]
Coding Theory:
Task: Reliably transmit a message through an unreliable channel.

$m \in F^k_2$

$c_m$

$\tilde{c}_m$

$\delta$

$F^N_2$
Coding Theory:
Task: Reliably transmit a message through an unreliable channel.

Good code:
(i) Large minimum distance $\delta$ while having large rate $\frac{k}{N}$. 
Coding Theory:
Task: Reliably transmit a message through an unreliable channel.

\[ m \in \mathbb{F}_2^k \]

Good code:
(i) Large minimum distance \( \delta \) while having large rate \( \frac{k}{N} \).
(ii) Efficiently testable and decodable.
Hadamard Codes:

\[ m \in \mathbb{F}_2^k \longrightarrow c_m \in \mathbb{F}_2^{2^k} \]

\( c_m \): evaluation vector of \( m_1 x_1 + m_2 x_2 + \cdots + m_k x_k \in \mathbb{F}_2[x_1, \ldots, x_k] \)
Reed Muller codes:

Degree $\leq d$ polynomials in $\mathbb{F}_2[x_1, \ldots, x_k]$
Reed Muller codes:

Problem 1.
How many degree $\leq d$ polynomials in $\mathbb{F}_2[x_1, \ldots, x_n]$ are there in $B_\delta(f)$?
Polynomial Decompositions:

Degree 4 polynomial $P \in \mathbb{F}_2[x_1, \ldots, x_n]$. 
Polynomial Decompositions:

Degree 4 polynomial $P \in \mathbb{F}_2[x_1, \ldots, x_n]$. Is

$$P(x) = Q_1(x)Q_2(x) + Q_3(x)Q_4(x),$$

for some degree $\leq 3$ polynomials $Q_1, \ldots, Q_4$?
Polynomial Decompositions:

Degree 4 polynomial $P \in \mathbb{F}_2[x_1, ..., x_n]$. Is

$$P(x) = Q_1(x)Q_2(x) + Q_3(x)Q_4(x),$$

for some degree $\leq 3$ polynomials $Q_1, ..., Q_4$?

Problem 2.
Given a degree $d$ polynomial $P$ and a prescribed decomposition. Find such a decomposition of $P$ or say it is not possible.
Polynomial Decompositions:

Degree 4 polynomial $P \in \mathbb{F}_2[x_1, \ldots, x_n]$. Is

$$P(x) = Q_1(x)Q_2(x) + Q_3(x)Q_4(x),$$

for some degree $\leq 3$ polynomials $Q_1, \ldots, Q_4$?

Problem 2.
Given a degree $d$ polynomial $P$ and a prescribed decomposition, **Efficiently** find such a decomposition of $P$ or say it is not possible.
Algebraic Property Testing:

Is \( f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2 \) a degree \( d \) polynomial?

Problem 3. Which "algebraic" properties are testable?
Algebraic Property Testing:

Is \( f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2 \) a degree \( d \) polynomial?

[AKKLR’05] Query \( f \) only on constant number of inputs.

1. Always accept if \( \text{deg}(f) \leq d \).
2. Reject w.h.p. if \( \delta_d(f) > \epsilon \).
Algebraic Property Testing:

Is $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ a degree $d$ polynomial?

[AKKLR’05] Query $f$ only on constant number of inputs.

1. Always accept if $\text{deg}(f) \leq d$.
2. Reject w.h.p. if $\delta_d(f) > \epsilon$.

Problem 3.
Which “algebraic” properties are testable?
Higher-order Fourier analysis over finite fields, which is an extension of Fourier analysis.

[Bergelson, Green, Kaufman, Gowers, Lovett, Meshulam, Samorodnitsky, Tao, Viola, Wolf ...]
Fourier Analysis over $\mathbb{F}_p^n$

Study $f : \mathbb{F}_p^n \rightarrow \mathbb{R}$ by looking at how it correlates with linear phases.

\[
f(x) = \sum_{\sigma \in \mathbb{F}_p^n} \hat{f}(\sigma) \cdot \omega \sum \sigma_i x_i
\]
Fourier Analysis over $\mathbb{F}_p^n$

Study $f : \mathbb{F}_p^n \rightarrow \mathbb{R}$ by looking at how it correlates with linear phases.

$$f(x) = \sum_{\sigma : |\hat{f}(\sigma)| \geq \epsilon} \hat{f}(\sigma) \cdot \omega \sum \sigma_i x_i + f_{psd}$$
Higher-order Fourier Analysis over $\mathbb{F}_p^n$

Study $f : \mathbb{F}_p^n \rightarrow \mathbb{R}$ by looking at how it correlates with higher degree polynomial phases, $\omega^P(x_1,\ldots,x_n)$.

⋄ Not orthogonal, no unique expansion.

⋄ $f = \sum_{i=1}^C \lambda_i \omega^P_i(x) + f_{psd}$?
Higher-order Fourier Analysis over $\mathbb{F}_p^n$

Study $f : \mathbb{F}_p^n \to \mathbb{R}$ by looking at how it correlates with higher degree polynomial phases, $\omega^P(x_1,\ldots,x_n)$.

- Not orthogonal, no unique expansion.

- $f = \sum_{i=1}^C \lambda_i \omega^{P_i(x)} + f_{psd}$?

[Bergelson, Green, Tao, Ziegler] establish such decomposition theorems via inverse theorems for certain norms called Gowers norms.
Higher-order Fourier Analysis over $\mathbb{F}_p^n$

Study $f : \mathbb{F}_p^n \to \mathbb{R}$ by looking at how it correlates with higher degree polynomial phases, $\omega^P(x_1, \ldots, x_n)$.

⋄ Not orthogonal, no unique expansion.

⋄ $f = \sum_{i=1}^{C} \lambda_i \omega^{P_i(x)} + f_{psd}$?

Theorem [Trevisan-Tulsiani-Vadhan, Gowers]
For any collection $G$ of functions $g : X \to \mathbb{D}$ the following holds.

Every function $f$ can be written as

$$f = F(g_1, \ldots, g_C) + f_{psd}$$
Higher-order Fourier Analysis over $\mathbb{F}_p^n$

Study $f : \mathbb{F}_p^n \to \mathbb{R}$ by looking at how it correlates with higher degree polynomial phases, $\omega^P(x_1,\ldots,x_n)$.

◊ Not orthogonal, no unique expansion.

◊ $f = \sum_{i=1}^{C} \lambda_i \omega^P_i(x) + f_{psd}$?

Theorem [Trevisan-Tulsiani-Vadhan, Gowers]

For any collection $G$ of functions $g : \mathbb{F}_p^n \to \mathbb{D}$ the following holds.

Every function $f$ can be written as

$$f = \sum_{\sigma \in \mathbb{F}_p^n} \hat{F}(\sigma) \omega^{\sum_i \sigma_i g_i} + f_{psd}$$
Higher-order Fourier Analysis over $\mathbb{F}_p^n$

Study $f : \mathbb{F}_p^n \rightarrow \mathbb{R}$ by looking at how it correlates with higher degree polynomial phases, $\omega^P(x_1,\ldots,x_n)$.

\[ f = \sum_{i=1}^C \lambda_i \omega^{P_i(x)} + f_{psd} \]
Higher-order Fourier Analysis over $\mathbb{F}_p^n$

Study $f : \mathbb{F}_p^n \to \mathbb{R}$ by looking at how it correlates with higher degree polynomial phases, $\omega^P(x_1, \ldots, x_n)$.

\[ f = \sum_{i=1}^{C} \lambda_i \omega^P_i(x) + f_{psd} \]

Need to understand the joint distribution of a collection of degree $d$ polynomials.
Higher-order Fourier Analysis over $\mathbb{F}_p^n$

Study $f : \mathbb{F}_p^n \to \mathbb{R}$ by looking at how it correlates with higher degree polynomial phases, $\omega^{P(x_1, \ldots, x_n)}$.

$f = \sum_{i=1}^C \lambda_i \omega^{P_i(x)} + f_{psd}$

Problem: $P_1, \ldots, P_C \in \mathcal{P}_{\leq d}(\mathbb{F}_p^n)$. $X, Y \in \mathbb{F}_p^n$ uniform. Characterize the distribution of

$$
\begin{pmatrix}
P_1(X) & \ldots & P_{10}(X) \\
P_1(X + Y) & \ldots & P_{10}(X + Y) \\
\vdots & & \vdots \\
P_1(X + 4Y) & \ldots & P_{10}(X + 4Y)
\end{pmatrix}
$$
Higher-order Fourier Analysis over $\mathbb{F}_p^n$

Study $f : \mathbb{F}_p^n \rightarrow \mathbb{R}$ by looking at how it correlates with higher degree polynomial phases, $\omega^P(x_1,\ldots,x_n)$.

⋄ $f = \sum_{i=1}^C \lambda_i \omega^{P_i(x)} + f_{psd}$

Problem: $P_1,\ldots,P_C \in \mathcal{P}_{\leq d}(\mathbb{F}_p^n)$. $X, Y \in \mathbb{F}_p^n$ uniform. Characterize the distribution of

$$
\begin{pmatrix}
P_1(X) & \cdots & P_{10}(X) \\
P_1(X + Y) & \cdots & P_{10}(X + Y) \\
\vdots & & \vdots \\
P_1(X + 4Y) & \cdots & P_{10}(X + 4Y)
\end{pmatrix}
$$

[HHL ‘15 (general case), BFHHL’13 (affine linear forms)]

[KL’08 and GT’09]: Distribution of $(P_1(X),\ldots,P_C(X))$. 
Problem 1. [KLP ’10, BL ’15]
Number of degree $d$ polynomials in $\mathbb{F}_p[x_1, \ldots, x_n]$ in hamming ball of radius $\delta_e - \epsilon$ is $2^{O(n^{d-e})}$.
Problem 1. [KLP ’10, BL ’15]
Number of degree $d$ polynomials in $\mathbb{F}_p[x_1, \ldots, x_n]$ in hamming ball of radius $\delta e - \epsilon$ is $2^{O(n^{d-e})}$.

Problem 2. [BHL ’15]
Polynomial time algorithm for finding prescribed polynomial decompositions.
Problem 1. [KLP ’10, BL ’15]
Number of degree $d$ polynomials in $\mathbb{F}_p[x_1, \ldots, x_n]$ in hamming ball of radius $\delta_e - \epsilon$ is $2^{O(nd-e)}$.

Problem 2. [BHL ’15]
Polynomial time algorithm for finding prescribed polynomial decompositions.

Problem 3. [BFL ’12, BFHHL ’13]
Characterization of testable algebraic (i.e. affine invariant) properties.
Problem 1. [KLP ’10, BL ’15]
Number of degree $d$ polynomials in $\mathbb{F}_p[x_1, \ldots, x_n]$ in hamming ball of radius $\delta_e - \epsilon$ is $2^{O(n^d-e)}$.

Problem 2. [BHL ’15]
Polynomial time algorithm for finding prescribed polynomial decompositions.

Problem 3. [BFL ’12, BFHHL ’13]
Characterization of testable algebraic (i.e. affine invariant) properties.

Problem 4. Is there a constant query tester that given $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ distinguishes between the following?

$\triangleright$ $f$ is $\geq \epsilon$-correlated to some cubic, or

$\triangleright$ $f$ is $\leq \delta(\epsilon)$-correlated to all cubics,

where $0 < \delta(\epsilon) \leq \epsilon$. 
Problem 1. [KLP ’10, BL ’15]
Number of degree $d$ polynomials in $\mathbb{F}_p[x_1, \ldots, x_n]$ in hamming ball of radius $\delta e - \epsilon$ is $2^{O(n^{d-e})}$.

Problem 2. [BHL ’15]
Polynomial time algorithm for finding prescribed polynomial decompositions.

Problem 3. [BFL ’12, BFHHL ’13]
Characterization of testable algebraic (i.e. affine invariant) properties.

Open Problem. Is there a constant query tester that given $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ distinguishes between the following?

- $f$ is $\geq \epsilon$-correlated to some cubic, or
- $f$ is $\leq \delta(\epsilon)$-correlated to all cubics,
where $0 < \delta(\epsilon) \leq \epsilon$. 
Theorem. [BHT]

There is a poly\(\left( n \right)\)-time deterministic algorithm that given a polynomial \(P\), and \(\Gamma : \mathbb{F}_p^\ell \rightarrow \mathbb{F}_p\), and \(d_1, \ldots, d_\ell \geq 1\), either
- outputs \(P_1, \ldots, P_r\) of degrees \(d_1, \ldots, d_\ell\), s.t. \(P = \Gamma(P_1, \ldots, P_d)\), or
- correctly outputs NOT POSSIBLE.
Proof illustration: Find $P_1, P_2$ of degree $\leq d - 1$ such that

$$P = P_1 \cdot P_2$$
Proof illustration: Find $P_1, P_2$ of degree $\leq d - 1$ such that

$$P = P_1 \cdot P_2$$

Algorithmic Regularity Lemma for Polynomials [BHT]:

$$P = \Lambda(Q_1, \ldots, Q_r)$$
Proof illustration: Find $P_1, P_2$ of degree $\leq d - 1$ such that

$$P = P_1 \cdot P_2$$

เราจะการณ์ความถี่ [BHT]:

$$P = \Lambda(Q_1, \ldots, Q_r)$$

มี $x_j$ ที่ทำให้ $\forall i, \deg(Q_i) = \deg(Q_i | x_j=0)$.

$$P |_{x_j=0} = \Lambda(Q_1 | x_j=0, \ldots, Q_r | x_j=0)$$
Proof illustration: Find $P_1, P_2$ of degree $\leq d - 1$ such that

$$P = P_1 \cdot P_2$$

▷ Algorithmic Regularity Lemma for Polynomials [BHT]:

$$P = \Lambda(Q_1, \ldots, Q_r)$$

▷ $\exists x_j$ s.t. for all $i$, $\deg(Q_i) = \deg(Q_i|_{x_j=0})$.

$$P|_{x_j=0} = \Lambda(Q_1|_{x_j=0}, \ldots, Q_r|_{x_j=0})$$

▷ Recurse on $P|_{x_j=0}$.

- If NOT POSSIBLE, then output NOT POSSIBLE.
- Otherwise we find $P'_1, P'_2$ such that $P|_{x_j=0} = P'_1 P'_2$. 
Proof illustration: Find $P_1, P_2$ of degree $\leq d - 1$ such that

$$P = P_1 \cdot P_2$$

▷ Algorithmic Regularity Lemma for Polynomials [BHT]:

$$P = \Lambda(Q_1, \ldots, Q_r)$$

▷ $\exists x_j$ s.t. for all $i$, $\deg(Q_i) = \deg(Q_i|_{x_j=0})$.

$$P|_{x_j=0} = \Lambda(Q_1|_{x_j=0}, \ldots, Q_r|_{x_j=0})$$

▷ Recurse on $P|_{x_j=0}$.

- If NOT POSSIBLE, then output NOT POSSIBLE.
- Otherwise we find $P'_1, P'_2$ such that $P|_{x_j=0} = P'_1 P'_2$.

$$\Lambda(Q'_1, \ldots, Q'_r) = P'_1 P'_2$$
Proof illustration: Find $P_1, P_2$ of degree $\leq d - 1$ such that

$$P = P_1 \cdot P_2$$

▶ Algorithmic Regularity Lemma for Polynomials [BHT]:

$$P = \Lambda(Q_1, \ldots, Q_r)$$

▶ There exists $x_j$ s.t. for all $i$, $\deg(Q_i) = \deg(Q_i|_{x_j=0})$.

$$P|_{x_j=0} = \Lambda(Q_1|_{x_j=0}, \ldots, Q_r|_{x_j=0})$$

▶ Recurse on $P|_{x_j=0}$.

bir. If NOT POSSIBLE, then output NOT POSSIBLE.

bir. Otherwise we find $P'_1, P'_2$ such that $P|_{x_j=0} = P'_1 P'_2$.

$$\Lambda(Q'_1, ..., Q'_r) = G_1(Q'_1, ..., Q'_r, R_1, ..., R_C) \cdot G_2(Q'_1, ..., Q'_r, R_1, ..., R_C)$$
**Proof illustration:** Find $P_1, P_2$ of degree $\leq d - 1$ such that

$$ P = P_1 \cdot P_2 $$

▷ Algorithmic Regularity Lemma for Polynomials [BHT]:

$$ P = \Lambda(Q_1, \ldots, Q_r) $$

▷ $\exists x_j$ s.t. for all $i$, $\deg(Q_i) = \deg(Q_i|_{x_j=0})$.

$$ P|_{x_j=0} = \Lambda(Q_1|_{x_j=0}, \ldots, Q_r|_{x_j=0}) $$

▷ Recurse on $P|_{x_j=0}$.

- If NOT POSSIBLE, then output NOT POSSIBLE.
- Otherwise we find $P'_1, P'_2$ such that $P|_{x_j=0} = P'_1 P'_2$.

$$ \Lambda(a_1, \ldots, a_r) = G_1(a_1, \ldots, a_r, 0, \ldots, 0) \cdot G_2(a_1, \ldots, a_r, 0, \ldots, 0) $$
**Proof illustration:** Find $P_1, P_2$ of degree $\leq d - 1$ such that

$$P = P_1 \cdot P_2$$

▶ Algorithmic Regularity Lemma for Polynomials [BHT]:

$$P = \Lambda(Q_1, \ldots, Q_r)$$

▶ $\exists x_j$ s.t. for all $i$, $\deg(Q_i) = \deg(Q_i|_{x_j=0})$.

$$P|_{x_j=0} = \Lambda(Q_1|_{x_j=0}, \ldots, Q_r|_{x_j=0})$$

▶ Recurse on $P|_{x_j=0}$.

- If NOT POSSIBLE, then output NOT POSSIBLE.
- Otherwise we find $P'_1, P'_2$ such that $P|_{x_j=0} = P'_1 P'_2$.

$$P = \Lambda(Q_1, \ldots, Q_r) = G_1(Q_1, \ldots, Q_r, 0, \ldots, 0) \cdot G_2(Q_1, \ldots, Q_r, 0, \ldots, 0)$$