Analysis of Boolean functions on *exotic* domains

Yuval Filmus
Technion – Israel Institute of Technology

PART I
What is analysis of Boolean functions?

Analysis of Boolean functions is

(mostly)

the study of Boolean-valued functions

from a spectral perspective.

Analysis of Boolean functions is

$\{0,1\}$ or $\{\pm 1\}$

(mostly)

the study of Boolean-valued functions

from a spectral perspective.

Analysis of Boolean functions is

(mostly)

the study of Boolean-valued functions

{0,1} or {±1}

Fourier analysis, representation theory, or equivalent

from a spectral perspective.

Analysis of Boolean functions is

(mostly)

{0,1} or {±1}

the study of Boolean-valued functions

Fourier analysis,
representation theory,
or equivalent

from a spectral perspective.

The functions are usually over a finite domain.

Where do Boolean functions come from?

Where do Boolean functions come from?

- Collection of subsets of a finite set (extremal combinatorics)

Where do Boolean functions come from?

- Collection of subsets of a finite set (extremal combinatorics)
- Voting scheme (social choice theory)

Where do Boolean functions come from?

- Collection of subsets of a finite set (extremal combinatorics)
- Voting scheme (social choice theory)
- Graph property (random graph theory, percolation)

Where do Boolean functions come from?

- Collection of subsets of a finite set (extremal combinatorics)
- Voting scheme (social choice theory)
- Graph property (random graph theory, percolation)
- Obstructions to decoding (coding theory)

Where do Boolean functions come from?

- Collection of subsets of a finite set (extremal combinatorics)
- Voting scheme (social choice theory)
- Graph property (random graph theory, percolation)
- Obstructions to decoding (coding theory)
- Subset of vertices in a graph (theoretical computer science)

Where do Boolean functions come from?

- Collection of subsets of a finite set (extremal combinatorics)
- Voting scheme (social choice theory)
- Graph property (random graph theory, percolation)
- Obstructions to decoding (coding theory)
- Subset of vertices in a graph (theoretical computer science)
- Classification function (statistical learning theory)

Functions on which domain?

Functions on which domain?

Boolean cube

- Most of the time, functions are over $\{0,1\}^n$

Functions on which domain?

Boolean cube

- Most of the time, functions are over $\{0,1\}^n$
- More rarely, over other product domains

Functions on which domain?

Boolean cube

- Most of the time, functions are over $\{0,1\}^n$
- More rarely, over other product domains
- Some applications: over finite groups or over $\binom{[n]}{k}$

Known as the "slice" or the Johnson association scheme

Erdős–Ko–Rado theory

Erdős–Ko–Rado theory

- Erdős–Ko–Rado theorem: if $k < n/2$ then an intersecting family $\mathcal{F} \subseteq \binom{[n]}{k}$ satisfies $|\mathcal{F}| \leq \binom{n-1}{k-1}$

Erdős–Ko–Rado theory

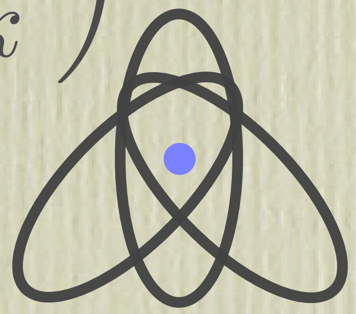
Every two sets intersect

- Erdős–Ko–Rado theorem: if $k < n/2$ then an intersecting family $\mathcal{F} \subseteq \binom{[n]}{k}$ satisfies $|\mathcal{F}| \leq \binom{n-1}{k-1}$

Erdős–Ko–Rado theory

Every two sets intersect

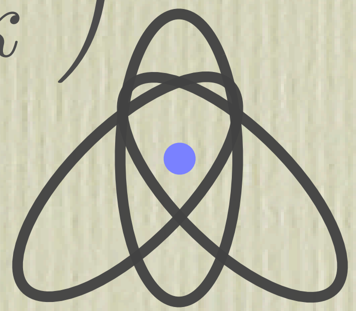
- Erdős–Ko–Rado theorem: if $k < n/2$ then an intersecting family $\mathcal{F} \subseteq \binom{[n]}{k}$ satisfies $|\mathcal{F}| \leq \binom{n-1}{k-1}$
  - Extremal families: "stars"



Erdős–Ko–Rado theory

Every two sets intersect

- Erdős–Ko–Rado theorem: if $k < n/2$ then an intersecting family $\mathcal{F} \subseteq \binom{[n]}{k}$ satisfies $|\mathcal{F}| \leq \binom{n-1}{k-1}$
  - Extremal families: “stars”

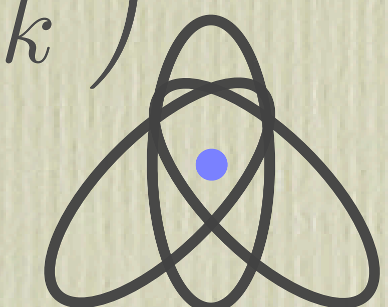


  - Analysis: almost extremal families close to stars

Erdős–Ko–Rado theory

Every two sets intersect

- Erdős–Ko–Rado theorem: if $k < n/2$ then an intersecting family $\mathcal{F} \subseteq \binom{[n]}{k}$ satisfies $|\mathcal{F}| \leq \binom{n-1}{k-1}$
  - Extremal families: "stars"



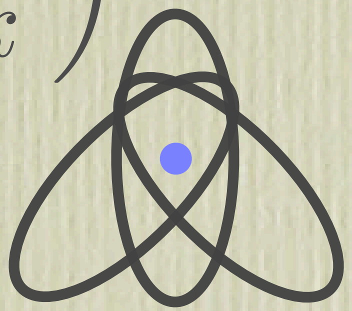
  - Analysis: almost extremal families close to stars

"Stability"

Erdős–Ko–Rado theory

Every two sets intersect

- Erdős–Ko–Rado theorem: if $k < n/2$ then an intersecting family $\mathcal{F} \subseteq \binom{[n]}{k}$ satisfies $|\mathcal{F}| \leq \binom{n-1}{k-1}$
  - Extremal families: "stars"



  - Analysis: almost extremal families close to stars

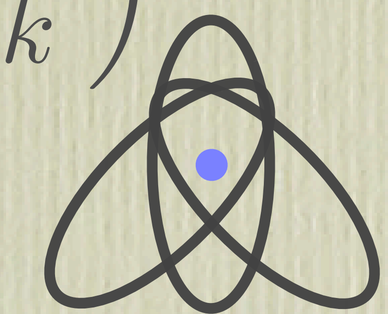
"Stability"

- Ellis–Friedgut–Pilpel: if any two permutations in $\mathcal{F} \subseteq S_n$ agree on at least t points then $|\mathcal{F}| \leq (n-t)!$

Erdős–Ko–Rado theory

Every two sets intersect

- Erdős–Ko–Rado theorem: if $k < n/2$ then an intersecting family $\mathcal{F} \subseteq \binom{[n]}{k}$ satisfies $|\mathcal{F}| \leq \binom{n-1}{k-1}$
  - Extremal families: "stars"



  - Analysis: almost extremal families close to stars

"Stability"

- Ellis–Friedgut–Pilpel: if any two permutations in $\mathcal{F} \subseteq S_n$ agree on at least t points then $|\mathcal{F}| \leq (n-t)!$
  - Only known proof through Analysis

PART II
Structure theorems

Friedgut–Kalai–Naor

Friedgut–Kalai–Naor

- If a Boolean function on $\{0,1\}^n$ satisfies
$$f(x_1,\ldots,x_n) = C + \sum_{i=1}^{n} a_i x_i$$
then it is a "dictatorship" (depends on one coordinate)

Friedgut–Kalai–Naor

- If a Boolean function on $\{0,1\}^n$ satisfies
$$f(x_1, \ldots, x_n) = C + \sum_{i=1}^{n} a_i x_i$$
then it is a "dictatorship" (depends on one coordinate)

- Friedgut–Kalai–Naor: a Boolean function satisfying
$$f(x_1, \ldots, x_n) \approx C + \sum_{i=1}^{n} a_i x_i$$
is close to a Boolean dictatorship

Friedgut–Kalai–Naor

- If a Boolean function on $\{0,1\}^n$ satisfies
$$f(x_1,\ldots,x_n) = C + \sum_{i=1}^n a_i x_i$$
then it is a "dictatorship" (depends on one coordinate)

- Friedgut–Kalai–Naor: a Boolean function satisfying
$$f(x_1,\ldots,x_n) \approx C + \sum_{i=1}^n a_i x_i$$
is close to a Boolean dictatorship

- F.: same holds over $\binom{[n]}{k}$

Friedgut–Kalai–Naor

- If a Boolean function on $\{0,1\}^n$ satisfies
$$f(x_1,\ldots,x_n) = C + \sum_{i=1}^n a_i x_i$$
then it is a "dictatorship" (depends on one coordinate)

- Friedgut–Kalai–Naor: a Boolean function satisfying
$$f(x_1,\ldots,x_n) \approx C + \sum_{i=1}^n a_i x_i$$
is close to a Boolean dictatorship

- F.: same holds over $\binom{[n]}{k}$

Implies stability for Erdős–Ko–Rado

Which functions on S_n are dictatorships?

Which functions on S_n are dictatorships?

- What is the analog of a linear function for S_n?

Which functions on S_n are dictatorships?

- What is the analog of a linear function for S_n?
- Think of S_n as group of $n \times n$ permutation matrices with entries x_{ij}

Which functions on S_n are dictatorships?

- What is the analog of a linear function for S_n?
- Think of S_n as group of $n \times n$ permutation matrices with entries x_{ij}
- Linear function: linear combination of x_{ij}

Which functions on S_n are dictatorships?

- What is the analog of a linear function for S_n?
- Think of S_n as group of $n \times n$ permutation matrices with entries x_{ij}
- Linear function: linear combination of x_{ij}
- Ellis–Friedgut–Pilpel: a Boolean linear function either depends on image of some point or on inverse image of some point

Which functions on S_n are dictatorships?

- What is the analog of a linear function for S_n?
- Think of S_n as group of $n \times n$ permutation matrices with entries x_{ij}
- Linear function: linear combination of x_{ij}
- Ellis–Friedgut–Pilpel: a Boolean linear function either depends on image of some point or on inverse image of some point

Dictatorship on S_n

Friedgut–Kalai–Naor on S_n

Friedgut–Kalai–Naor on S_n

- $\max(x_{11}, x_{22})$ close to $x_{11} + x_{22}$ but not to a dictatorship

Friedgut–Kalai–Naor on S_n

- $\max(x_{11}, x_{22})$ close to $x_{11} + x_{22}$ but not to a dictatorship
- Ellis–F.–Friedgut (1):
  Every Boolean function of magnitude c/n (for c small) which is close to a linear function is close to a maximum of c entries

Friedgut–Kalai–Naor on S_n

- $\max(x_{11}, x_{22})$ close to $x_{11} + x_{22}$ but not to a dictatorship
- Ellis–F.–Friedgut (1):
  Every Boolean function of magnitude c/n (for c small) which is close to a linear function is close to a maximum of c entries
- Ellis–F.–Friedgut (2):
  Every *balanced* Boolean function close to a linear function is close to a dictatorship

Higher-degree analogues

Higher-degree analogues

- Nisan–Szegedy: If a Boolean function equals a degree d polynomial then it is a $C(d)$-"junta" (depends on $C(d)$ coordinates)

Higher-degree analogues

- Nisan–Szegedy: If a Boolean function equals a degree d polynomial then it is a $C(d)$-“junta” (depends on $C(d)$ coordinates)
- Kindler–Safra: If a Boolean function is close to a degree d polynomial then it is close to a $C(d)$-junta

Higher-degree analogues

- Nisan–Szegedy: If a Boolean function equals a degree d polynomial then it is a $C(d)$-"junta" (depends on $C(d)$ coordinates)
- Kindler–Safra: If a Boolean function is close to a degree d polynomial then it is close to a $C(d)$-junta
- F.–Kindler–Mossel–Wimmer: Same true for slice

Higher-degree analogues

- Nisan–Szegedy: If a Boolean function equals a degree d polynomial then it is a $C(d)$-"junta" (depends on $C(d)$ coordinates)
- Kindler–Safra: If a Boolean function is close to a degree d polynomial then it is close to a $C(d)$-junta
- F.–Kindler–Mossel–Wimmer: Same true for slice
  - Stability for t-intersecting families of sets

Higher-degree analogues

- Nisan–Szegedy: If a Boolean function equals a degree d polynomial then it is a $C(d)$-“junta” (depends on $C(d)$ coordinates)
- Kindler–Safra: If a Boolean function is close to a degree d polynomial then it is close to a $C(d)$-junta
- F.–Kindler–Mossel–Wimmer: Same true for slice
  - Stability for t-intersecting families of sets
- Ellis–F.–Friedgut (3): Same true for S_n for sparse functions

PART III
Invariance principle

Central limit theorem

Central limit theorem

- Suppose x_i are random ±1 variables

Central limit theorem

- Suppose x_i are random ±1 variables
- Under what conditions does

$$\sum_i \alpha_i x_i$$

have a roughly normal distribution?

Central limit theorem

- Suppose x_i are random ±1 variables
- Under what conditions does

$$\sum_i \alpha_i x_i$$

have a roughly normal distribution?

- Berry–Esséen: as long as no α_i is too prominent

Lindeberg replacement trick

Lindeberg replacement trick

- How to prove Berry–Esséen?

Lindeberg replacement trick

- How to prove Berry–Esséen?
- Replace each x_i by standard Gaussian g_i:

Lindeberg replacement trick

- How to prove Berry–Esséen?
- Replace each x_i by standard Gaussian g_i:

$$\sum_i \alpha_i x_i \approx \sum_i \alpha_i g_i$$

Lindeberg replacement trick

- How to prove Berry–Esséen?
- Replace each x_i by standard Gaussian g_i:

$$\sum_i \alpha_i x_i \approx \sum_i \alpha_i g_i$$

- Properties of Gaussians imply

$$\sum_i \alpha_i g_i \sim N(0, \sum_i \alpha_i^2)$$

Invariance principle

Invariance principle

- Mossel–O'Donnel–Oleszkiewicz noticed that the same trick works for low-degree polynomials

Invariance principle

- Mossel–O'Donnel–Oleszkiewicz noticed that the same trick works for low-degree polynomials
- This time we need all the variable *influences* to be small

Invariance principle

- Mossel–O'Donnel–Oleszkiewicz noticed that the same trick works for low-degree polynomials
- This time we need all the variable *influences* to be small
- Implies that Majority vote is the voting rule most resistant to noise (asymptotically)

Invariance principle

- Mossel–O'Donnel–Oleszkiewicz noticed that the same trick works for low-degree polynomials
- This time we need all the variable *influences* to be small
- Implies that Majority vote is the voting rule most resistant to noise (asymptotically)
- Important corollaries in theoretical computer science

Caveat

Caveat

- Invariance principle only applies to (low-degree) *multilinear polynomials*

Caveat

- Invariance principle only applies to (low-degree) *multilinear polynomials*
- For example, $x_1^2+\ldots+x_n^2$ is constant while $g_1^2+\ldots+g_n^2$ is not

Caveat

- Invariance principle only applies to (low-degree) *multilinear polynomials*
- For example, $x_1^2+\ldots+x_n^2$ is constant while $g_1^2+\ldots+g_n^2$ is not
- Not a problem, since any function on Boolean cube has unique multilinear representation ("Fourier expansion")

Invariance principle on the slice

Invariance principle on the slice

- Relevant distributions:

Invariance principle on the slice

- Relevant distributions:
  - $(s_1,\ldots,s_n)$: uniform distribution on k–slice

Invariance principle on the slice

- Relevant distributions:
  - $(s_1,\ldots,s_n)$: uniform distribution on k–slice
  - $(x_1,\ldots,x_n)$: product distribution with same marginals (Ber(k/n))

Invariance principle on the slice

- Relevant distributions:
  - $(s_1,\ldots,s_n)$: uniform distribution on k–slice
  - $(x_1,\ldots,x_n)$: product distribution with same marginals (Ber(k/n))
  - $(g_1,\ldots,g_n)$: Gaussian product distribution with same mean and variance

Invariance principle on the slice

- Relevant distributions:
  - $(s_1,\ldots,s_n)$: uniform distribution on k–slice
  - $(x_1,\ldots,x_n)$: product distribution with same marginals (Ber(k/n))
  - $(g_1,\ldots,g_n)$: Gaussian product distribution with same mean and variance
- $s_1+\ldots+s_n$ constant but $x_1+\ldots+x_n$ isn't!

Invariance principle on the slice

Invariance principle on the slice

- Solution (Dunkl): Consider only multilinear polynomials satisfying:

$$\sum_{i=1}^{n} \frac{\partial f}{\partial x_i} = 0$$

Invariance principle on the slice

- Solution (Dunkl): Consider only multilinear polynomials satisfying:

$$\sum_{i=1}^{n} \frac{\partial f}{\partial x_i} = 0$$

- Every function on slice has a unique multilinear representation of this form

Invariance principle on the slice

- Solution (Dunkl): Consider only multilinear polynomials satisfying:

$$\sum_{i=1}^{n} \frac{\partial f}{\partial x_i} = 0$$

- Every function on slice has a unique multilinear representation of this form

- F.–Kindler–Mossel–Wimmer, F.–Mossel: invariance principle holds for such polynomials

Invariance principle on the slice

- Solution (Dunkl): Consider only multilinear polynomials satisfying:

$$\sum_{i=1}^{n} \frac{\partial f}{\partial x_i} = 0$$

- Every function on slice has a unique multilinear representation of this form
- F.–Kindler–Mossel–Wimmer, F.–Mossel: invariance principle holds for such polynomials
- Corollary: Majority is Stablest on the slice

Invariance principle on the slice

- Solut… …near polyn…
- Every… …ltilinear repre…
- F.–K… …: invariance principle holds for such polynomials
- Corollary: Majority is Stablest on the slice

Middle slice is a representative section of the Boolean cube from the point of view of low-degree "harmonic" multilinear polynomials

PART IV
Gelfand–Tsetlin basis for the slice

Fourier analysis on the slice

Fourier analysis on the slice

- On the Boolean cube we have Fourier analysis on $\mathbb{Z}_2^n$

Fourier analysis on the slice

- On the Boolean cube we have Fourier analysis on $\mathbb{Z}_2^n$
- On S_n we have representation theory

Fourier analysis on the slice

- On the Boolean cube we have Fourier analysis on $\mathbb{Z}_2^n$
- On S_n we have representation theory
- On the slice we also have representation theory: every multilinear “harmonic” polynomial decomposes as sum of its homogeneous parts (part of general theory of association schemes)

Gelfand–Tsetlin basis

Gelfand–Tsetlin basis

- Srinivasan constructs (implicitly) a canonical orthogonal basis for functions on the slice

Gelfand–Tsetlin basis

- Srinivasan constructs (implicitly) a canonical orthogonal basis for functions on the slice
- Basis is orthogonal with respect to *all* symmetric measures on $x_1,\ldots,x_n$!

Gelfand–Tsetlin basis

- Srinivasan constructs (implicitly) a canonical orthogonal basis for functions on the slice
- Basis is orthogonal with respect to *all* symmetric measures on $x_1,\ldots,x_n$!
- Basis depends on order of coordinates

Explicit basis

Explicit basis

- F. gives explicit construction of the basis

Explicit basis

- F. gives explicit construction of the basis
- Definition: $A = (a_1, \ldots, a_\ell) < B = (b_1, \ldots, b_\ell)$ if

$$a_1 < b_1, \ldots, a_\ell < b_\ell, b_1 < \cdots < b_\ell$$

Explicit basis

- F. gives explicit construction of the basis
- Definition: $A = (a_1, \ldots, a_\ell) < B = (b_1, \ldots, b_\ell)$ if

$$a_1 < b_1, \ldots, a_\ell < b_\ell, b_1 < \cdots < b_\ell$$

- Basis consists of all non-zero functions

$$\chi_B = \sum_{A<B} (x_{a_1} - x_{b_1}) \cdots (x_{a_\ell} - x_{b_\ell})$$

Explicit basis

- F. gives explicit construction of the basis
- Definition: $A = (a_1, \ldots, a_\ell) < B = (b_1, \ldots, b_\ell)$ if

$$a_1 < b_1, \ldots, a_\ell < b_\ell, b_1 < \cdots < b_\ell$$

- Basis consists of all non-zero functions

$$\chi_B = \sum_{A<B} (x_{a_1} - x_{b_1}) \cdots (x_{a_\ell} - x_{b_\ell})$$

- Norm of χ_B proportional to norm of

$$(x_1 - x_2) \cdots (x_{2|B|-1} - x_{2|B|})$$

Implications

Implications

- For small *d*, norm of $(x_1 - x_2) \cdots (x_{2d-1} - x_{2d})$ roughly identical for uniform distribution on *k*-slice and corresponding product distribution

Implications

- For small d, norm of $(x_1 - x_2) \cdots (x_{2d-1} - x_{2d})$ roughly identical for uniform distribution on k-slice and corresponding product distribution
- Basis implies that same is true for all low-degree harmonic polynomials! (F.–Mossel: basis-free argument)

Implications

- For small d, norm of $(x_1 - x_2) \cdots (x_{2d-1} - x_{2d})$ roughly identical for uniform distribution on k-slice and corresponding product distribution

- Basis implies that same is true for all low-degree harmonic polynomials! (F.–Mossel: basis-free argument)

- Basis is explicit orthogonal basis of eigenvectors for Johnson and Kneser graphs

Implications

- For small d, norm of $(x_1 - x_2) \cdots (x_{2d-1} - x_{2d})$ roughly identical for uniform distribution on k-slice and corresponding product distribution
- Basis implies that same is true for all low-degree harmonic polynomials! (F.–Mossel: basis-free argument)
- Basis is explicit orthogonal basis of eigenvectors for Johnson and Kneser graphs
- Simplifies Wimmer's proof of Friedgut's junta theorem on the slice

OPEN QUESTIONS

OPEN QUESTIONS

- More exotic domains:

OPEN QUESTIONS

- More exotic domains:
  - k-dimensional vector subspaces of n-dimensional vector space over finite field

OPEN QUESTIONS

- More exotic domains:
  - k-dimensional vector subspaces of n-dimensional vector space over finite field
  - Other groups

OPEN QUESTIONS

- More exotic domains:
  - *k*-dimensional vector subspaces of *n*-dimensional vector space over finite field
  - Other groups
  - "Multi-slice"

OPEN QUESTIONS

- More exotic domains:
  - k-dimensional vector subspaces of n-dimensional vector space over finite field
  - Other groups
  - "Multi-slice"
- More theorems on slice and symmetric group

THE END