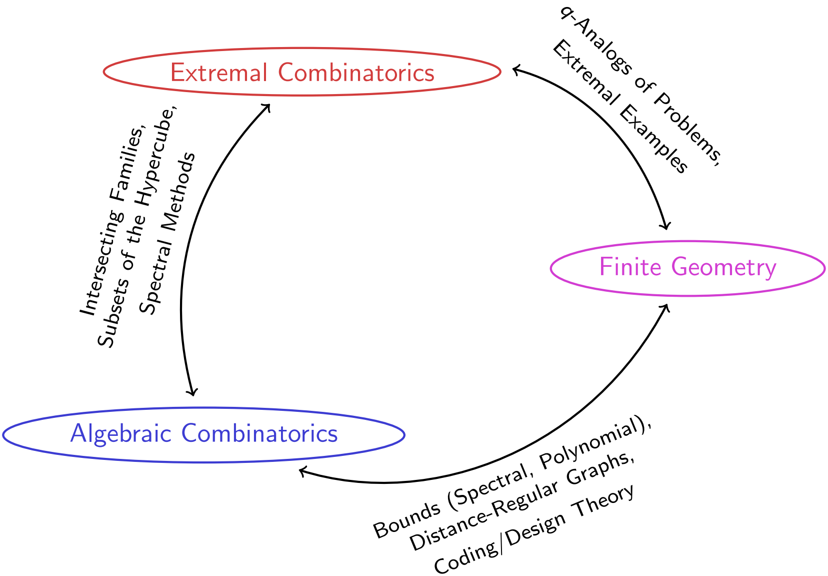
Low Degree Boolean Functions in Finite Geometry

Ferdinand Ihringer

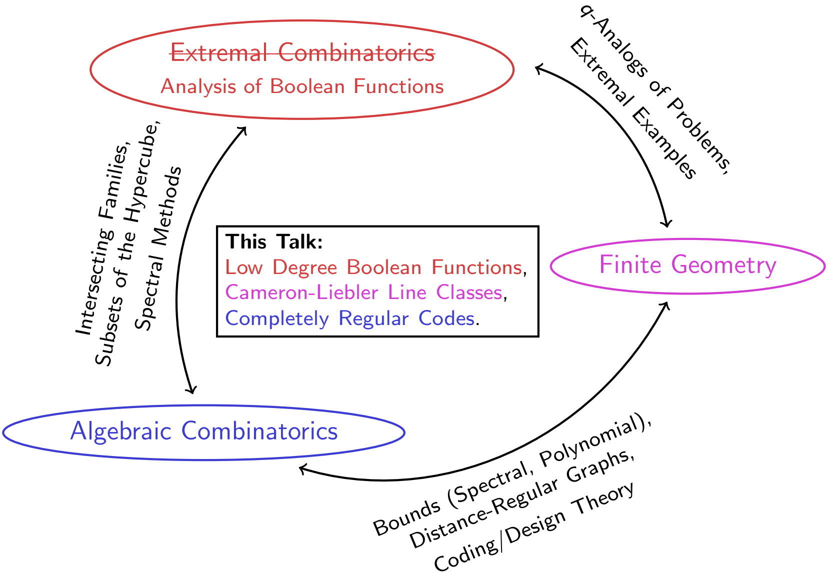
Ghent University, Belgium

21 August 2019, University of Delaware
Finite Geometry and Extremal Combinatorics

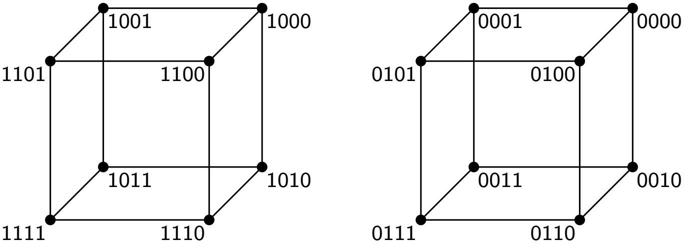
Connections



Connections



Families in the Hypercube

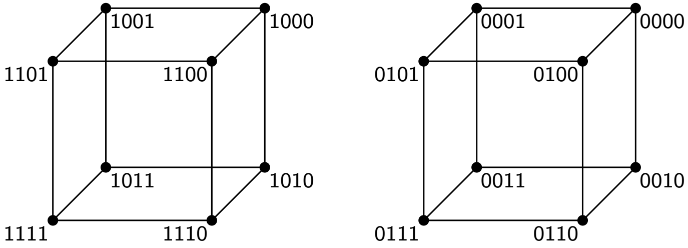


Goal: Investigate families in $\{0,1\}^n$.

Here $n = 4$.

Alternative model: $\{-1,1\}^n$.

Families in the Hypercube



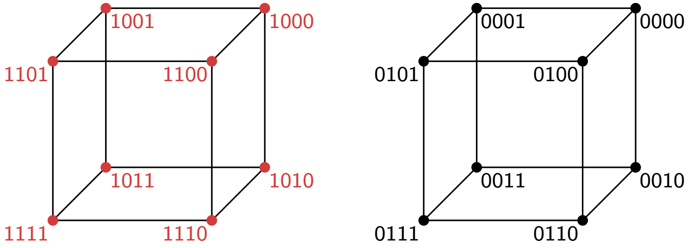
Goal: Investigate families in $\{0,1\}^n$. Here $n = 4$.

Alternative model: $\{-1,1\}^n$.

Methods:

- Write as **polynomial** $\{0,1\}^n \to \{0,1\}$ over $\mathbb{R}$, Variables: **coordinates**.
- Look at **spectrum**, Eigenspaces: **adjacency matrix** of graph.
- Approximate with **nice families**. Nice families: **dictators**/juntas.

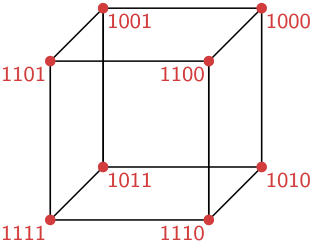
Dictator

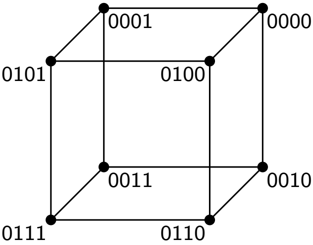


Polynomial f: x_1^+.

Here $x_i^+(v) = 1$ iff $v_i = 1$.

Dictator





Polynomial f: x_1^+.

Here $x_i^+(v) = 1$ iff $v_i = 1$.

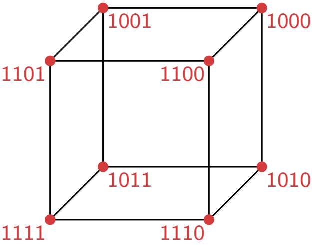
Spectrum: $(\frac{4}{5}, \frac{1}{5}, 0, 0, 0)$.

(Eigenspaces: V_0, V_1, V_2, V_3, V_4.)

Part in V_i divided by $\dim(V_i)$.

$V_0 = \langle 1 \rangle$, $V_0 + V_1 = \langle x_i^+ \rangle$, $V_0 + V_1 + V_2 = \langle x_i^+ x_j^+ \rangle$.

Dictator



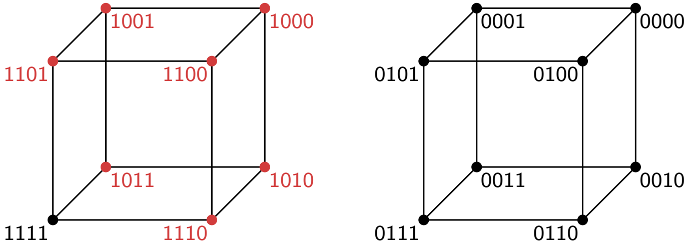
Polynomial f**:** x_1^+. Here $x_i^+(v) = 1$ iff $v_i = 1$.

Spectrum: $(\frac{4}{5}, \frac{1}{5}, 0, 0, 0)$. (Eigenspaces: V_0, V_1, V_2, V_3, V_4.)
Part in V_i divided by $\dim(V_i)$. $V_0 = \langle 1 \rangle, V_0 + V_1 = \langle x_i^+ \rangle, V_0 + V_1 + V_2 = \langle x_i^+ x_j^+ \rangle$.

Approximation g**:** x_1^+.

Closeness: $\Pr(f \neq g) = 0$.

Almost Dictator



Polynomial f**:** $x_1^+ - x_1^+ x_2^+ x_3^+ x_4^+$.

Here $x_i^+(v) = 1$ iff $v_i = 1$.

Spectrum: $(\frac{49}{65}, \frac{1}{5}, \frac{1}{65}, \frac{1}{65}, \frac{1}{65})$.

(Eigenspaces: V_0, V_1, V_2, V_3, V_4.)

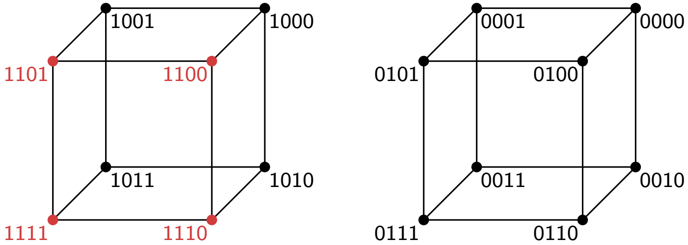
Part in V_i divided by $\dim(V_i)$.

$V_0 = \langle 1 \rangle$, $V_0 + V_1 = \langle x_i^+ \rangle$, $V_0 + V_1 + V_2 = \langle x_i^+ x_j^+ \rangle$.

Approximation g**:** x_1^+.

Closeness: $\Pr(f \neq g) = \frac{1}{16}$.

Junta



Polynomial f**:** $x_1^+ x_2^+$.

Here $x_i^+(v) = 1$ iff $v_i = 1$.

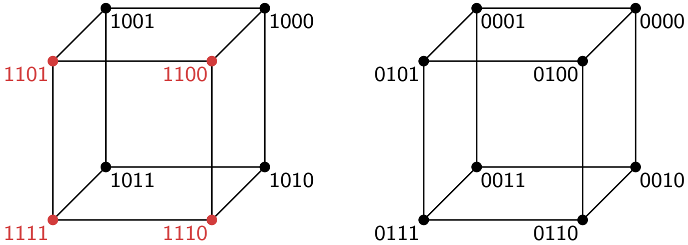
Spectrum: $(\frac{3}{5}, \frac{3}{10}, \frac{1}{10}, 0, 0)$.

(Eigenspaces: V_0, V_1, V_2, V_3, V_4.)

Degree 1 **Approximation** g**:** x_1^+.

Closeness: $\Pr(f \neq g) = \frac{1}{4}$.

Junta



Polynomial f**:** $x_1^+ x_2^+$.

Here $x_i^+(v) = 1$ iff $v_i = 1$.

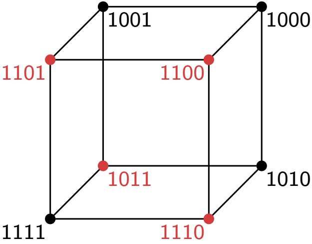
Spectrum: $(\frac{3}{5}, \frac{3}{10}, \frac{1}{10}, 0, 0)$.

(Eigenspaces: V_0, V_1, V_2, V_3, V_4.)

Degree 2 **Approximation** g**:** $x_1^+ x_2^+$.

Closeness: $\Pr(f \neq g) = 0$.

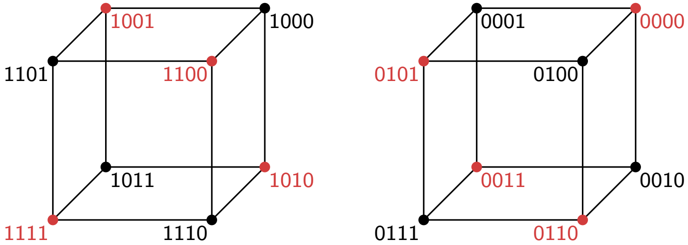
Bent Function



Polynomial f**:** $x_1^+x_2^+ + x_3^+x_4^+ - 2x_1^+x_2^+x_3^+x_4^+$. Over $\mathbb{F}_2$, $f = x_1x_2 + x_3x_4$.

Spectrum: $(\frac{9}{13}, \frac{1}{13}, \frac{1}{13}, \frac{1}{13}, \frac{1}{13})$.

Parity Code

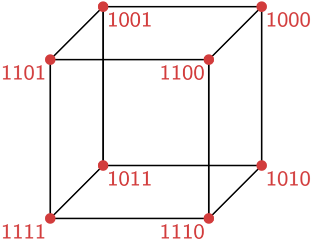


Polynomial f: too long.

Over $\mathbb{F}_2$, $f = 1 + x_1^+ + x_2^+ + x_3^+ + x_4^+$.

Spectrum: $(\frac{1}{2}, 0, 0, 0, \frac{1}{2})$.

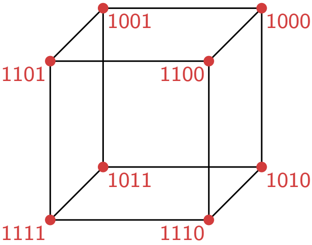
Classifying Degree 1

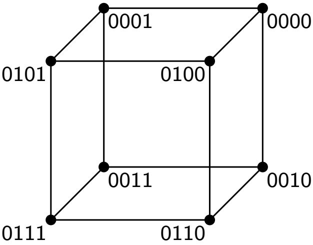


Theorem

A Boolean degree 1 function $f = c + \sum c_i x_i^+$ *is a* **dictator**.

Classifying Degree 1





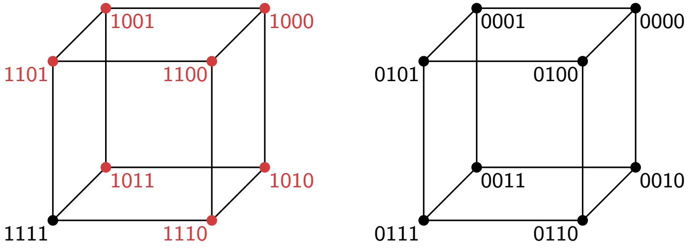
Theorem

A Boolean degree 1 function $f = c + \sum c_i x_i^+$ is a **dictator***.*

Proof.

- WLOG $f(00\ldots0) = 0$, so $c = 0$.
- WLOG $f(10\ldots0) = 1$, so $c_1 = 1$. $\square$

Classifying Almost Degree 1

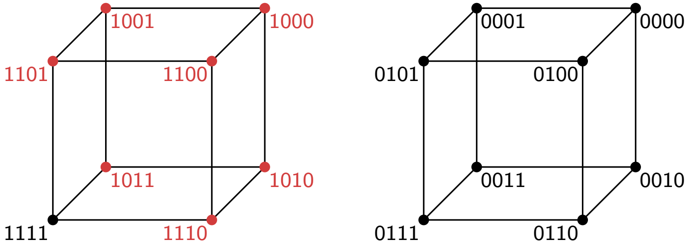


Definition

Two functions f and g are **ϵ-close** if $\mathbb{E}(|f-g|^2) = \|f-g\|^2 \leq \epsilon$.

If f and g Boolean, then $\|f-g\|^2 = \Pr(f \neq g)$.

Classifying Almost Degree 1



Definition

Two functions f and g are **ϵ-close** if $\mathbb{E}(|f-g|^2) = \|f-g\|^2 \leq \epsilon$.
If f and g Boolean, then $\|f-g\|^2 = \Pr(f \neq g)$.

Theorem (Friedgut-Kalai-Naor Theorem (2002))

If f is Boolean and ϵ-close to degree 1, then f is $O(\epsilon)$-close to a dictator.

Higher Degree

Trivial: Boolean degree 1 $\longrightarrow$ dictator.

FKN Theorem (2002): Boolean almost degree 1 $\longrightarrow$ almost dictator.

What about **higher degrees**?

Higher Degree

Trivial: Boolean degree 1 $\longrightarrow$ dictator.

FKN Theorem (2002): Boolean almost degree 1 $\longrightarrow$ almost dictator.

What about **higher degrees**?

Theorem (Nisan and Szegedy (1994))

Boolean degree $d \longrightarrow d2^{d-1}$-junta.[a][b]

[a] That is it depends on at most $d2^{d-1}$ coordinates.
[b] They also give an example which requires a $\Theta(2^d)$-junta.

Chiarelli, Hatami and Saks (2018): Tight bound of $O(2^d)$.
Current best by Wellens (2019): $\leq 4.416 \cdot 2^d$.

Higher Degree

Trivial: Boolean degree 1 $\longrightarrow$ dictator.

FKN Theorem (2002): Boolean almost degree 1 $\longrightarrow$ almost dictator.

What about **higher degrees**?

Theorem (Nisan and Szegedy (1994))

Boolean degree $d \longrightarrow d2^{d-1}$-junta.[a][b]

[a] That is it depends on at most $d2^{d-1}$ coordinates.
[b] They also give an example which requires a $\Theta(2^d)$-junta.

Chiarelli, Hatami and Saks (2018): Tight bound of $O(2^d)$.
Current best by Wellens (2019): $\leq 4.416 \cdot 2^d$.

Theorem (Kindler-Safra Theorem (2002))

Boolean almost degree $d \longrightarrow$ Almost $O(2^d)$-junta.

"What then should we do?" Luke 3:10

In the **hypercube**: Good understanding of low degree functions.

What about **other domains**?

For instance:

- A **slice** of the hypercube: all k-sets of $\{1, \ldots, n\}$.
- The **q-analog** of the slice: all k-spaces of $\mathbb{F}_q^n$.

"What then should we do?" Luke 3:10

In the **hypercube**: Good understanding of low degree functions.

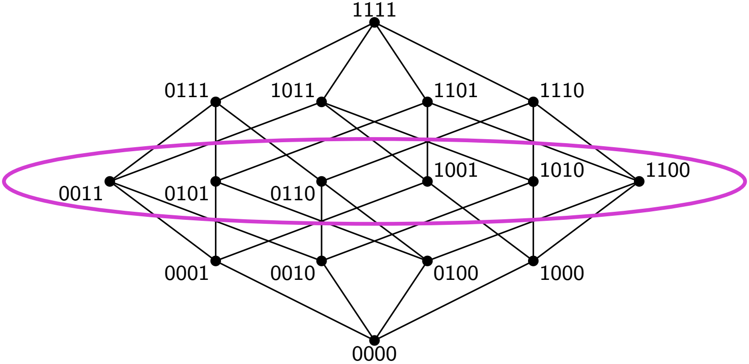
What about **other domains**?

For instance:

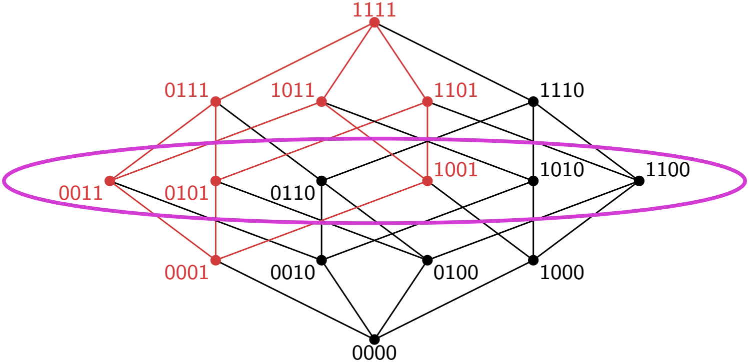
- A **slice** of the hypercube: all k-sets of $\{1, \ldots, n\}$.
- The **q-analog** of the slice: all k-spaces of $\mathbb{F}_q^n$.
- The **symmetric group** S_n.
- The rank n **bilinear forms**.

We will look at **k-sets** and **k-spaces**.

Subsets


1111
0111
1011
1101
1110
0011
0101
0110
1001
1010
1100
0001
0010
0100
1000
0000

Subsets



Theorem

Boolean degree 1 functions on k-sets of $\{1, \ldots, n\}$ *are* **trivial**.
I.e. they are **dictators** $(0, 1, x_i^+$ *or* $1 - x_i^+)$.

Various proofs: Meyerowitz (1992, see Martin (2004)), Filmus (2016), De Boeck, Storme, Svob (2017), Filmus and I. (2019).

FKN Theorem

Recall for hypercube: Boolean almost degree 1 $\longrightarrow$ almost dictator.

For k-sets of $\{1, \ldots, n\}$:

Theorem (Filmus (2016))

Boolean almost degree 1 $\longrightarrow$ almost sum of dictators (or complement).

FKN Theorem

Recall for hypercube: Boolean almost degree 1 $\longrightarrow$ almost dictator.

For k-sets of $\{1, \ldots, n\}$:

Theorem (Filmus (2016))

Boolean almost degree 1 $\longrightarrow$ almost sum of dictators (or complement).

Recall for hypercube:

- Boolean degree $d \longrightarrow O(2^d)$-junta.
- Boolean almost degree $d \longrightarrow$ Almost $O(2^d)$-junta.

1

FKN Theorem

Recall for hypercube: Boolean almost degree 1 $\longrightarrow$ almost dictator.

For k-sets of $\{1, \ldots, n\}$:

Theorem (Filmus (2016))

Boolean almost degree 1 $\longrightarrow$ almost sum of dictators (or complement).

Recall for hypercube:

- Boolean degree $d \longrightarrow O(2^d)$-junta.
- Boolean almost degree $d \longrightarrow$ Almost $O(2^d)$-junta.

For k-sets:

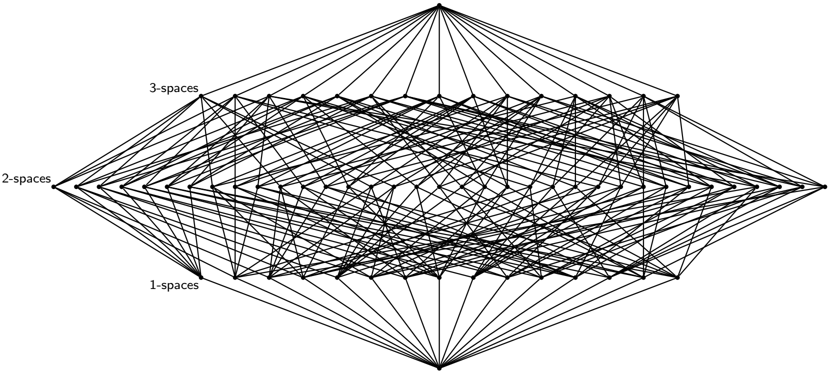
Filmus, I. (2019): Boolean degree $d \longrightarrow O(2^d)$-junta.[1]

Keller, Klein (2019): Boolean almost degree $d \longrightarrow$ Almost $O(2^d)$-junta.

---

[1] If $\max(k, n-k)$ large enough! Not tight!

Vector Spaces

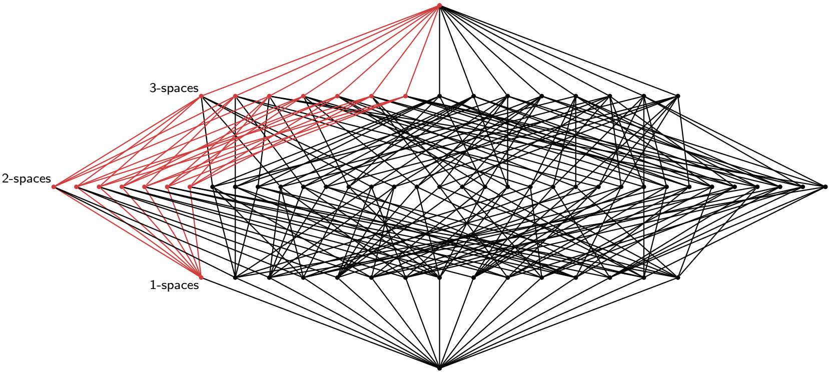


The subspace lattice of $\mathbb{F}_2^4$.

We consider ***k*-spaces** of a finite vector space!

Degree 1: $f = \sum_p c_p p^+$, p's are 1-spaces.
Here $p^+(S) = 1$ if $p \subseteq S$ and $p^+(S) = 0$ otherwise.

Trivial Degree 1 in Vector Spaces (I)



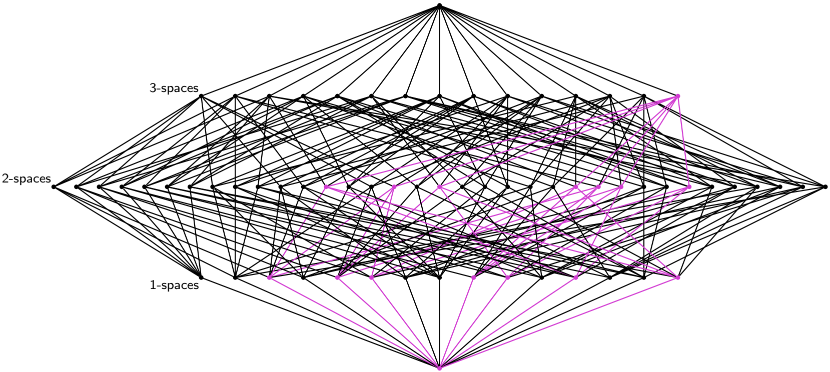
The subspace lattice of $\mathbb{F}_2^4$.

Example (Trivial Example 1)

Take all k-spaces through a fixed **1-space** p: p^+.

Or the complement: $1 - p^+$. (This is always possible.)

Trivial Degree 1 in Vector Spaces (II)



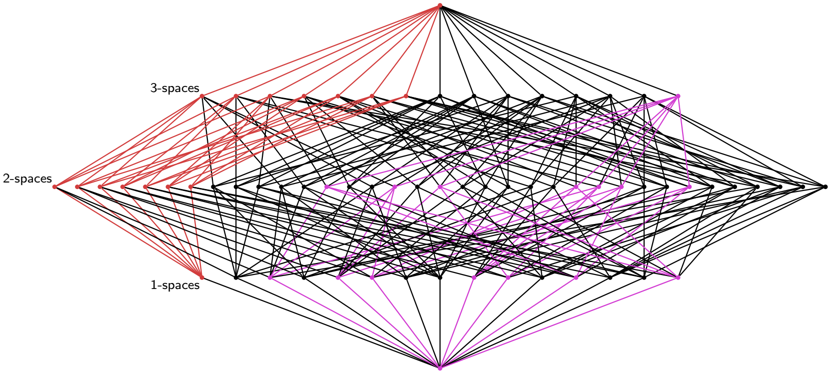
The subspace lattice of $\mathbb{F}_2^4$.

Example (Trivial Example 2)

Take all k-spaces in a fixed **hyperplane** π: π^+.

Proof: Write $\pi^+ = \alpha \sum_{p \in \pi} p^+ + \beta \sum_{p \notin \pi} p^+$.

Trivial Degree 1 in Vector Spaces (III)



The subspace lattice of $\mathbb{F}_2^4$.

Example (Trivial Example 3)

All through **1-space** p **or** in **hyperplane** π: $p^+ + \pi^+$.

Or the complement: $1 - (p^+ + \pi^+)$.

Degree 1 Functions on 2-spaces in $\mathbb{F}_q^n$

Cameron, Liebler (1982): Investigate action of subgroups of $P\Gamma L(4, q)$ on 1- and 2-spaces of $\mathbb{F}_q^4$.

Same number of orbits: Boolean degree 1 function.

Degree 1 Functions on 2-spaces in $\mathbb{F}_q^n$

Cameron, Liebler (1982): Investigate action of subgroups of $P\Gamma L(4, q)$ on 1- and 2-spaces of $\mathbb{F}_q^4$.

Same number of orbits: Boolean degree 1 function.

Conjecture (Cameron, Liebler (1982, very simplified))

If Boolean degree 1 function f on 2-spaces, then f or $1 - f$ is ...

- 1,
- p^+ *for a 1-space* p,
- π^+ *for a hyperplane* π, *or*
- $p^+ + \pi^+$ *for a 1-space* p *and a hyperplane* π, $p \notin \pi$.

Degree 1 Functions on 2-spaces in $\mathbb{F}_q^n$

Cameron, Liebler (1982): Investigate action of subgroups of $P\Gamma L(4, q)$ on 1- and 2-spaces of $\mathbb{F}_q^4$.

Same number of orbits: Boolean degree 1 function.

Conjecture (Cameron, Liebler (1982, very simplified))

If Boolean degree 1 *function* f *on 2-spaces, then* f *or* $1 - f$ *is ...*

- 1,
- p^+ *for a 1-space* p,
- π^+ *for a hyperplane* π, *or*
- $p^+ + \pi^+$ *for a 1-space* p *and a hyperplane* π, $p \notin \pi$.

- **Conjecture very natural**: true for subsets.
- **True** for 2-spaces of $\mathbb{F}_2^n$.
- **False** for 2-spaces of $\mathbb{F}_q^4$: First counterexample for $q = 3$ by **Drudge** (1998), later many more.

State of the Art

For 2-spaces in $\mathbb{F}_q^4$:

- Many **counterexamples**: Bruen, Cossidente, De Beule, Demeyer, Drudge, Feng, Gavrilyuk, Matkin, Metsch, Momihara, Pavese, Penttila, Rodgers, Xiang.
- **Existence conditions**: Metsch (2014), Gavrilyuk and Metsch (2014).

State of the Art

For 2-spaces in $\mathbb{F}_q^4$:

- Many **counterexamples**: Bruen, Cossidente, De Beule, Demeyer, Drudge, Feng, Gavrilyuk, Matkin, Metsch, Momihara, Pavese, Penttila, Rodgers, Xiang.
- **Existence conditions**: Metsch (2014), Gavrilyuk and Metsch (2014).

Boolean degree 1 functions f on k-spaces for $n > 4$:

Theorem (Drudge (1998), Gavrilyuk and Mogilnykh (2014), Gavrilyuk and Matkin (2018), Matkin (2018))

All trivial *for* $k = 2$ *and* $q \leq 5$*.*

Theorem (Filmus, I. (2019))

All trivial *for* $k \geq 2$ *and* $q \leq 5$*.*

Also several existence conditions on the size of f by Blokhuis, De Boeck, D'haeseleer, Metsch, Rodgers, Storme, Vansweevelt (all recent).

Almost Degree 1

Maybe we find **non-trivial almost degree 1**?

Definition

If $\|f - g\|^2 \leq \epsilon$ for a degree 1 function g, then f ϵ-close to degree 1.

Almost Degree 1

Maybe we find **non-trivial almost degree 1**?

Definition

If $\|f - g\|^2 \leq \epsilon$ for a degree 1 function g, then f ϵ-close to degree 1.

Recall FKN for k-sets:
Boolean almost degree 1 $\longrightarrow$ almost sum of dictators (or complement).

FKN theorem: **Structure** of almost degree 1 function.
Strong version: Almost degree 1 $\longrightarrow$ sum of trivial examples.

Almost Degree 1

Maybe we find **non-trivial almost degree 1**?

Definition

If $\|f-g\|^2 \leq \epsilon$ for a degree 1 function g, then f ϵ-close to degree 1.

Recall FKN for k-sets:
Boolean almost degree 1 $\longrightarrow$ almost sum of dictators (or complement).

FKN theorem: **Structure** of almost degree 1 function.
Strong version: Almost degree 1 $\longrightarrow$ sum of trivial examples.

Example (Bruen, Drudge for general n and k)

There exists non-trivial degree 1 function f of size $\sim \frac{1}{2}$.

Good News: This shows no **strong** FKN for $q \to \infty$, n fixed.

Almost Degree 1

Maybe we find **non-trivial almost degree 1**?

Definition

If $\|f-g\|^2 \leq \epsilon$ for a degree 1 function g, then f ϵ-close to degree 1.

Recall FKN for k-sets:
Boolean almost degree 1 $\longrightarrow$ almost sum of dictators (or complement).

FKN theorem: **Structure** of almost degree 1 function.
Strong version: Almost degree 1 $\longrightarrow$ sum of trivial examples.

Example (Bruen, Drudge for general n and k)

There exists non-trivial degree 1 function f of size $\sim \frac{1}{2}$.

Good News: This shows no **strong** FKN for $q \to \infty$, n fixed.

More natural: Fix q and k, and let $n \to \infty$. No idea!

Problems

Conjecture (Updated)

Show *that all Boolean degree* 1 *functions on* k*-spaces of* $\mathbb{F}_q^n$ *are trivial except for* $(n, k) = (4, 2)$.

Problems

Conjecture (Updated)

Show *that all Boolean degree* 1 *functions on* k*-spaces of* $\mathbb{F}_q^n$ *are trivial except for* $(n, k) = (4, 2)$*.*

Problem (FKN I)

Exists *a non-trivial Boolean almost degree* 1 *function for* $n \to \infty$*?*

Problem (FKN II)

What is the **general structure** *of (almost) Boolean degree* 1 *functions?*

Problems

Conjecture (Updated)

Show *that all Boolean degree* 1 *functions on* k*-spaces of* $\mathbb{F}_q^n$ *are trivial except for* $(n, k) = (4, 2)$.

Problem (FKN I)

Exists *a non-trivial Boolean almost degree* 1 *function for* $n \to \infty$*?*

Problem (FKN II)

What is the **general structure** *of (almost) Boolean degree* 1 *functions?*

Problem (Nisan-Szegedy)

Classification results *for Boolean degree* d *functions in geometric settings for* $d > 1$.

See De Winter-Metsch (2018) for a related problem on **intriguing sets**.

Recent Breakthrough in Complexity Theory

The **Unique Games Conjecture** claims that it is impossible to approximate many **NP-hard** problems in polynomial time.

Theorem (Khot, Minzer, Safra (2018))

Proof of the 2-to-2 Games Conjecture.[a]

[a] A slightly weakend Unique Games Conjecture.

Recent Breakthrough in Complexity Theory

The **Unique Games Conjecture** claims that it is impossible to approximate many **NP-hard** problems in polynomial time.

Theorem (Khot, Minzer, Safra (2018))

Proof of the 2-to-2 Games Conjecture.[a]

[a] A slightly weakend Unique Games Conjecture.

What they had to show:

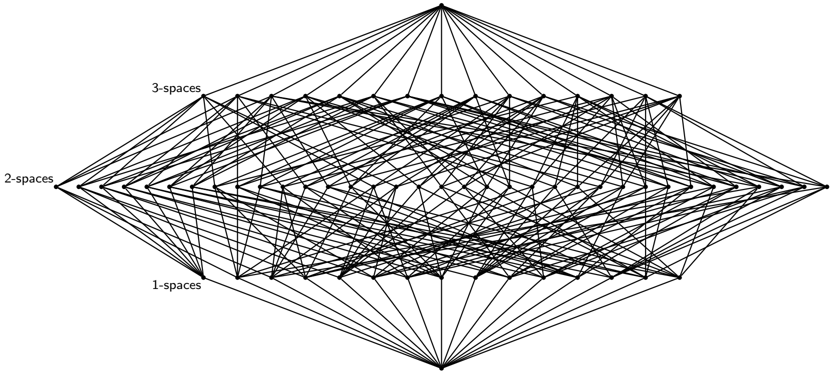
Theorem (Khot, Minzer, Safra (2018))

Let $\alpha \in (0,1)$. There ex. $\epsilon > 0$ s.t. for sufficiently large k and sufficiently large n: If f on k-spaces in $\mathbb{F}_2^n$ **significant mass on low degree** *(measured by α), then there ex. A of const. dim. and B of const. codim. with*

$$|\{x \in f : A \subseteq x \subseteq B\}| \geq \epsilon |\{x \text{ } k\text{-space} : A \subseteq x \subseteq B\}|.$$

Think of $\dim(A) = 1$ and $\dim(B) = n$. Then $f = A^+$ is example.

Vector Spaces

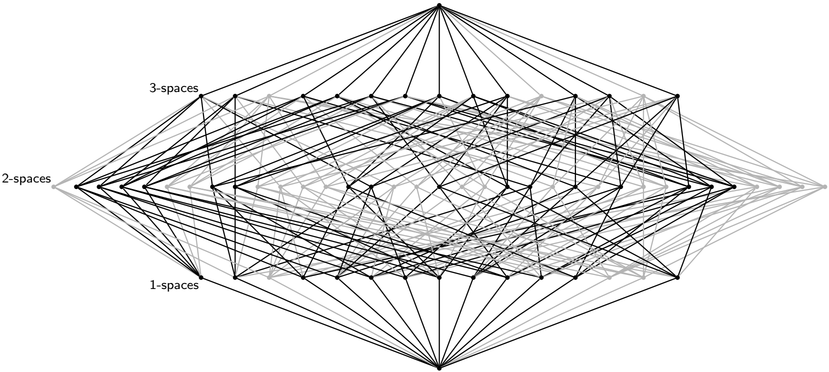


The subspace lattice of $\mathbb{F}_2^4$.

We consider ***k*-spaces** of a finite vector space!

Degree 1: $f = \sum_p c_p p^+$, p's are 1-spaces.
Here $p^+(S) = 1$ if $p \subseteq S$ and $p^+(S) = 0$ otherwise.

Bilinear Forms

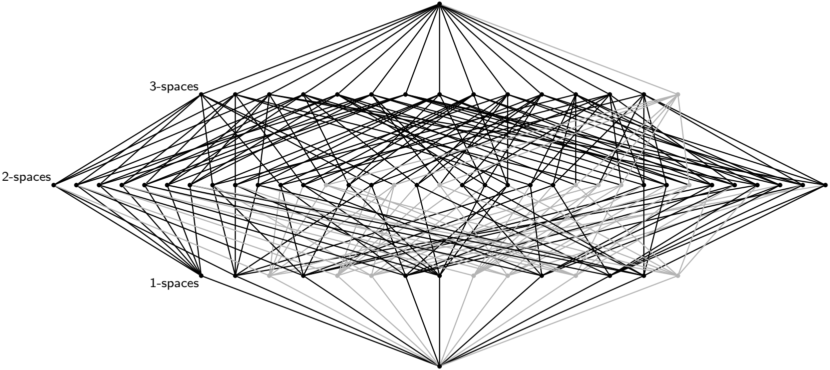


The bilinear forms lattice of $\mathbb{F}_2^2 \times \mathbb{F}_2^2$.

We consider only **subspaces** disjoint to fixed subspace!

Degree 1 on $\mathbb{F}_q^{a+b}$ **gives** degree 1 on bilinear forms on $\mathbb{F}_q^a \times \mathbb{F}_q^b$.
Obvious Conjecture in Filmus, I. (2019).

Affine Spaces

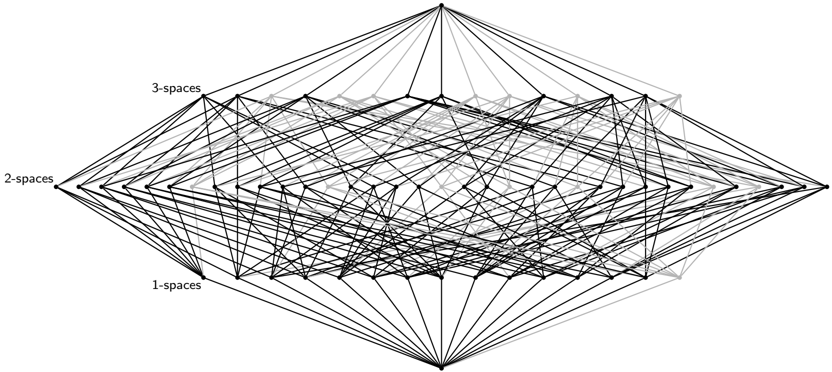


The affine subspace lattice of $\mathbb{F}_2^4$.

We consider only **subspaces** outside of fixed hyperplane!

Affine degree 1 on $\mathbb{F}_q^n$ **gives** degree 1 on $\mathbb{F}_q^n$.

Dual Affine Spaces

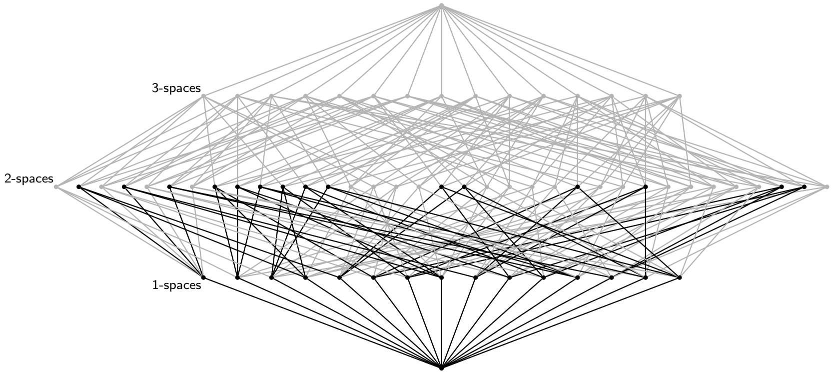


The dual affine subspace lattice of $\mathbb{F}_2^4$.

We consider only **subspaces** outside of fixed 1-space!

Degree 1 on $\mathbb{F}_q^n$ **gives** dual affine degree 1 on $\mathbb{F}_q^n$.

Polar Spaces



The subspace lattice of $Sp(\mathbb{F}_2^4)$.

Consider subspaces vanishing on a reflexive sesquilinear form!

For instance: $x_1 y_2 - x_2 y_1 + x_3 y_4 - x_4 y_3$.

Degree 1 on $\mathbb{F}_q^n$ **gives** degree 1 on polar space of $\mathbb{F}_q^n$.

For small dim called **tight set**.

Other Domains

Symmetric Group

- **Degree 1 classified** (Ellis, Friedgut, Pilpel (2011)).
- For degree > 1, **many non-trivial examples** (Filmus (2018)).

Other Domains

Symmetric Group

- **Degree 1 classified** (Ellis, Friedgut, Pilpel (2011)).
- For degree > 1, **many non-trivial examples** (Filmus (2018)).

More domains:

- Permutation **groups** (see int. fam., **Meagher**),
- Finite classical **buildings** (see int. fam., I., Metsch, Mühlherr (2018) and **Metsch** (2018, 2019)),
- Signed sets (see int. fam., Bollobás, **Leader** (1997)),
- **Polar spaces** (Filmus, I. (2019), D'haeseleer, De Boeck (2019)),

Thank you for your attention!