On Boolean Degree 1 Functions (Cameron-Liebler Sets) in Finite Vector Spaces

Ferdinand Ihringer

SUSTech, Shenzhen, China

20 August 2024

Graphs and Groups, Complexity and Convexity (G2C2)

Hebei Normal University, Shijiazhuang, China

A Simple Question

Let $f : \mathbb{R}^n \to \mathbb{R}$ be an **affine function**, that is

$$f(x) = c + \sum c_i x_i.$$

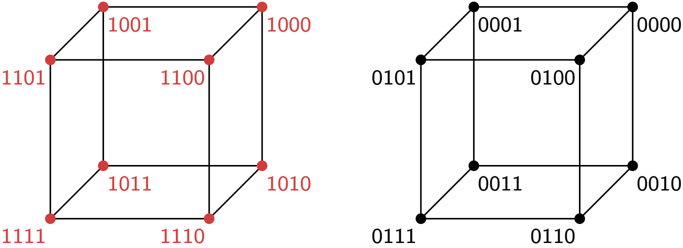
Definition

We call f **Boolean** over D if $f(x) \in \{0, 1\}$ for all $x \in D$.

Question

What are the Boolean affine functions for the ***hypercube*** $D = \{0, 1\}^n$*?*

Dictator



Polynomial f: x_1.

We only need x_1 to determine $f(x)$.

The Degree 1 Functions on the Hypercube

Example

The constant functions $f(x) = 0$ and $f(x) = 1$.

Example

The functions $f(x) = x_i$ and $f(x) = 1 - x_i$.

Proposition

Let f be an ***affine Boolean function*** *on the* ***hypercube****.*
Then $f(x) = c + \sum c_i x_i$ is one of 0, 1, x_i, or $1 - x_i$.

The Degree 1 Functions on the Hypercube

Example

The constant functions $f(x) = 0$ and $f(x) = 1$.

Example

The functions $f(x) = x_i$ and $f(x) = 1 - x_i$.

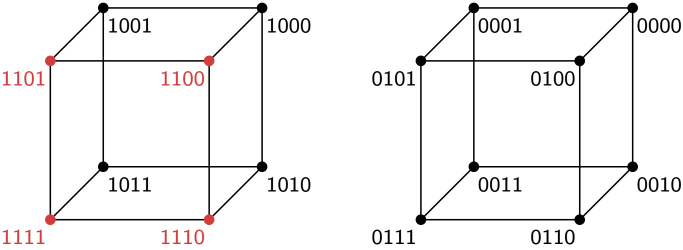
Proposition

*Let f be an **affine Boolean function** on the **hypercube**. Then $f(x) = c + \sum c_i x_i$ is one of 0, 1, x_i, or $1 - x_i$.*

Proof.

WLOG $f(00\ldots0) = 0$. Hence, $c = 0$.
WLOG $f(10\ldots0) = 1$. Hence, $c_1 = 1$.
Now all the other c_i's must be 0. $\square$

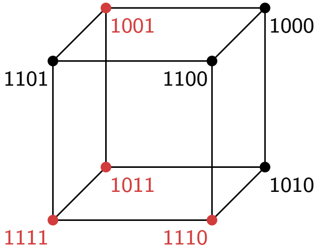
Degree 2, Example 1



Polynomial f: x_1x_2.

We only need x_1, x_2 to determine $f(x)$.

Degree 2, Example 2



Polynomial f: $1 - x_1 + (x_1 + x_2 - 1)x_3 + (x_1 - x_2)x_4$.

We need x_1, x_2, x_3, x_4 to determine $f(x)$!

Some Generalizations (I)

Question

What about Boolean degree 2 functions f on the hypercube?

Answer: Then f or $1 - f$ is one of these:[1]

- 0,
- x_i,
- $x_i + x_j - x_i x_j$,
- $x_i x_j + (1 - x_i) x_k$,
- $x_i x_j + x_i x_k + x_j x_k - x_i - x_j - x_k$,
- $f(x) = 1$ iff $x_i \leq x_j \leq x_k \leq x_\ell$ or $x_i \geq x_j \geq x_k \geq x_\ell$.

Degree 2: Camion, Carlet, Charpin & Sendrier (1991).
Degree 3: Kirienko (2004), Zverev (2008).

[1] I stole this list from Yuval Filmus.

Some Generalizations (II)

Question

What about Boolean degree d functions f on the hypercube?

Only m relevant variables: m-junta.

Theorem (Nisan, Szegedy (1991))

A Boolean degree d function on the hypercube is a $d \cdot 2^{d-1}$-junta.

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

Carlet and Tarannikov (2002): Lower bound of $3 \cdot 2^{d-1} - 2$.

Two applications: cryptography, complexity theory. One C in G2C2!

Some Generalizations (III)

Question

*What about **almost** affine Boolean functions f on the hypercube?*

That is, $\|f - g\|_2 < \varepsilon$ *for some affine function* g*.*

Friedgut, Kalai, and Naor (2002): If f is Boolean and almost affine, then f is almost a Boolean affine function.

Kindler, Safra (2002): Similar result for degree d.

Some Other Words

We already **know**: Boolean degree 1 function.

Other used words which might mean the same (depending on **context**):

- Equitable bipartition.
- Regular set.
- Perfect 2-coloring.
- Cameron-Liebler set.
- Completely regular code.
- Tight set.
- Anti-1-design.
- Dual degree 1.
- Graphical design.
- Intriguing set.

“What should we do then?” Luke 3:10, NIV[3]

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

What about **other domains**?

For instance:

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

We will look at **k-sets** and **k-spaces**.[2]

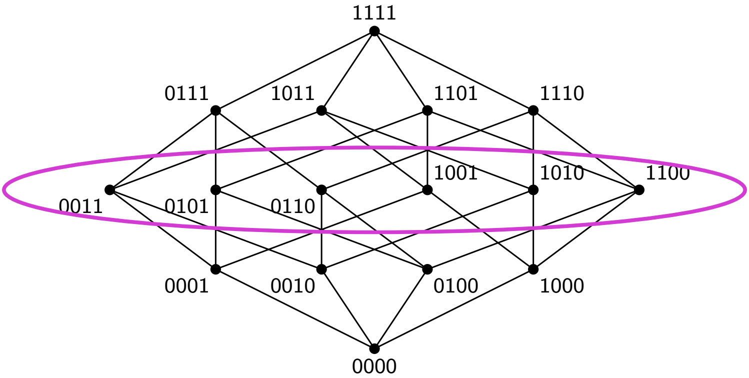
See Dafni, Filmus, Lifshitz, Lindzey, and Vinyals (2020) for results on **Sym**(n).

They use a **convex polytope**! One C in G2C2!

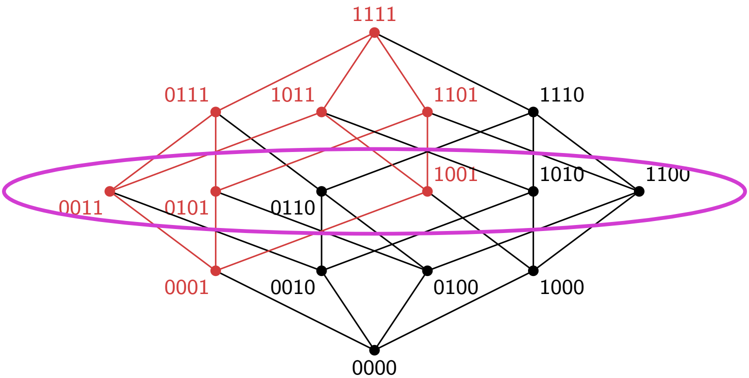
[2] Cf. Kiermaier, Mannaert, Wassermann (2024).

[3] Alternative quotes: “What is to be done?”. Tolstoy, 1866; Lenin, 1902.

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 $1 - x_i)$.* *(For $n-k, k \geq 2$.)*

Various proofs: Meyerowitz (1992, see Martin (2004)), Filmus (2016), Filmus and Ih. (2019). Also De Boeck, Strome, Svob (2016), but only for $k \mid n$.

Bounded Degree

Recall FKN 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).

Bounded Degree

Recall FKN 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 $d \longrightarrow \gamma(d)$-junta.

Theorem (Filmus, Ih. (2019))

If $\min(k, n-k) \geq C^d$: Boolean degree $d \longrightarrow \gamma(d)$-junta.

Keller, Klein (2019): stability version.

Bounded Degree

Recall FKN 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 $d \longrightarrow \gamma(d)$-junta.

Theorem (Filmus, Ih. (2019))

If $\min(k, n-k) \geq C^d$: Boolean degree $d \longrightarrow \gamma(d)$-junta.

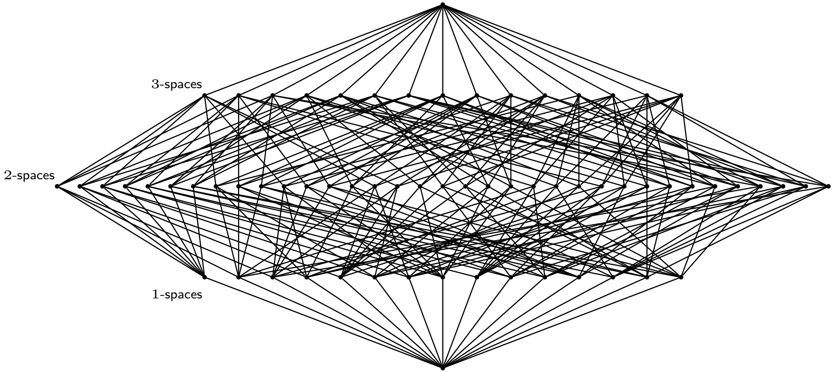
Keller, Klein (2019): stability version.

Theorem (Filmus (2023))

If $\min(k, n-k) \geq 2d$: Boolean degree $d \longrightarrow \gamma'(d)$-junta.

Note: We have $\gamma(2) = 4$, but there is an example in $J(8, 4)$ with 5 relevant variables, so $\gamma'(2) \neq \gamma(2)$.

Vector Spaces



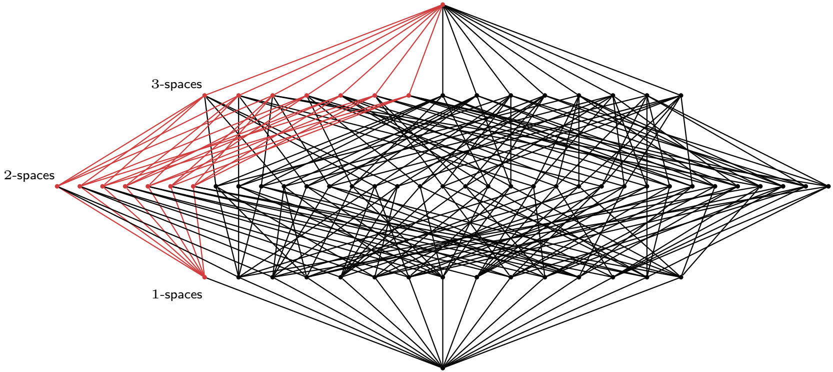
The subspace lattice of $\mathbb{F}_2^4$.

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

Degree 1: $f = \sum_P c_P x_P$, P's are 1-spaces.
Here $x_P(S) = 1$ if $P \subseteq S$ and $x_P(S) = 0$ otherwise.

Degree 1, alternative: $f = \sum_H c_H x_H$, H's are $(n-1)$-spaces.
Here $x_H(S) = 1$ if $S \subseteq H$ and $x_H(S) = 0$ otherwise.

Trivial Degree 1 in Vector Spaces (I)



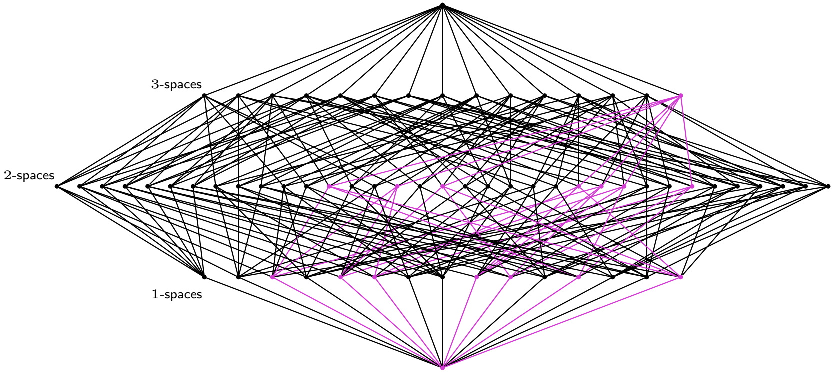
The subspace lattice of $\mathbb{F}_2^4$.

Example (Trivial Example 1)

Take all k-spaces through a fixed **1-space** P: x_P.

Or the complement: $1 - x_P$. (This is always possible.)

Trivial Degree 1 in Vector Spaces (II)



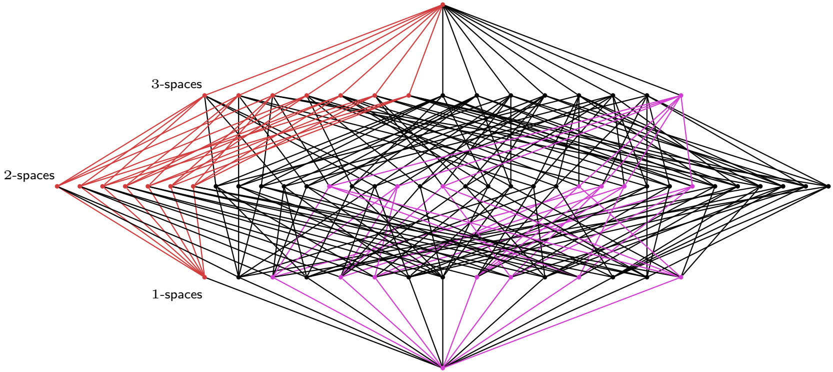
The subspace lattice of $\mathbb{F}_2^4$.

Example (Trivial Example 2)

Take all k-spaces in a fixed **hyperplane** H: x_H.

Degree 1 in x_P's? Write $H = \alpha \sum_{P \subseteq H} x_P + \beta \sum_{P \not\subseteq H} x_P$.

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 H**: $x_P + x_H$.

Or the complement: $1 - x_P - x_H$.

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 ...

- 0,
- x_P *for a 1-space P,*
- x_H *for a hyperplane H, or*
- $x_P + x_H$ *for a 1-space P and a hyperplane H, $P \not\subseteq H$.*

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

State of the Art

For 2-spaces in $\mathbb{F}_q^4$ many **counterexamples**, e.g.:

Bruen, Cossidente, De Beule, Demeyer, Drudge, Feng, Gavrilyuk, Matkin, Metsch, Momihara, Pavese, Penttila, Rodgers, Xiang, Zou.

Restrictions on sizes of non-trivial examples for 2-spaces in $\mathbb{F}_q^4$, e.g.:

- Metsch (2010),
- Metsch (2014),
- Gavrilyuk, Metsch (2014).

Restrictions in a **more general setting**:

- Metsch (2017),
- Rodgers, Storme, Vansweevelt (2018),
- Blokhuis, De Boeck, D'haeseleer (2019),
- De Beule, Mannaert, Storme (2022),
- Ihringer (2024?),
- De Beule, Mannaert, Storme (2024?).

Classification Results

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* $q \in \{2, 3, 4, 5\}$.

Proof: Clever computations and induction on n.

Theorem (Filmus, Ih. (2019))

All trivial *for* $k \geq 2$ *and* $q \in \{2, 3, 4, 5\}$.

Proof: Induction on k.

Classification Results

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* $q \in \{2, 3, 4, 5\}$.

Proof: Clever computations and induction on n.

Theorem (Filmus, Ih. (2019))

All trivial *for* $k \geq 2$ *and* $q \in \{2, 3, 4, 5\}$.

Proof: Induction on k.

Theorem (Ih. (2024, AMS Proceedings, accepted))

All trivial *for* $k \geq 2$ *and* $\max(n - k, k) \geq c_0(k, q)$.

This insight came a day after much **Moutai**, **Tsingtao beer**, and **KTV**.

The Structure of the Proof

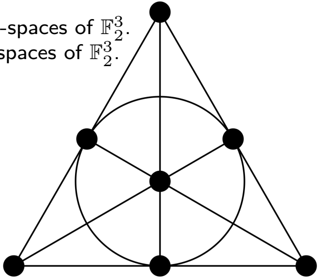
The proof **relies on ...**

1. **Structural Results:**
   - Drudge (1998): $f(x) = x_P$ locally $\longrightarrow$ $f(x) = x_P$ globally.
   - Drudge (1998): $f(x) = x_P + x_H$ locally $\longrightarrow$ $f(x) = x_P + x_H$ globally.
   - Metsch (2010): f not trivial $\longrightarrow$ far away from trivial.
2. **Ramsey for vector spaces:** Graham, Leeb, Rothschild (1972).
3. The case $k = 2$ suffices: Filmus, Ih. (2019).

My key insight was that we can use **Ramsey theory**.

Coloring the Fano Plane

Points of Fano plane $= 1$-spaces of $\mathbb{F}_2^3$.
Lines of Fano plane $= 2$-spaces of $\mathbb{F}_2^3$.



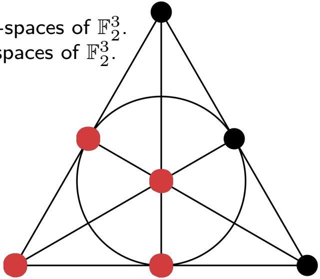
Question

*Can we color the points of the Fano plane black/red with **no monochromatic line**?*

Cf. Ex. 14.1.4 in *Discrete Mathematics: Elementary and Beyond* by L. Lovász, J. Pelikán, and K. Vesztergombi.

Coloring the Fano Plane

Points of Fano plane $= 1$-spaces of $\mathbb{F}_2^3$.
Lines of Fano plane $= 2$-spaces of $\mathbb{F}_2^3$.



Question

Can we color the points of the Fano plane black/red with ***no monochromatic line****?*

Cf. Ex. 14.1.4 in *Discrete Mathematics: Elementary and Beyond* by L. Lovász, J. Pelikán, and K. Vesztergombi.

No! This shows $R_2(2; 2) = 3$.

A formal definition of $R_q(s; m)$ follows on the next slide.

Ramsey Theory for Vector Spaces

Definition

A m-**coloring** of $\mathbb{F}_q^n$ is a coloring of the 1-spaces of $\mathbb{F}_q^n$ with m colors. The number $R_q(s;m)$ denotes the smallest integer n such that any m-coloring of $\mathbb{F}_q^n$ possesses a monochromatic s-space.

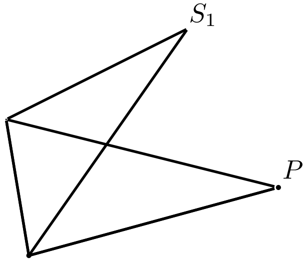
Theorem (Graham, Leeb, Rothschild (1972))

The number $R_q(s;m)$ is ***finite****.*

Theorem (Graham, Leeb, Rothschild (1972))

Analogous result for affine spaces.

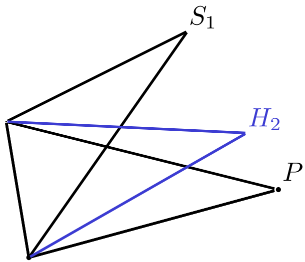
Applying Ramsey



How to apply **Ramsey**? Example for $q = 2$.

1. Fix a 1-space P.
2. **Goal:** the coefficient of x_P.
3. Say, **only** 896 **coefficients** can occur!
4. $n \geq R_2(s_1; 896)$: monochromatic s_1-space S_1.

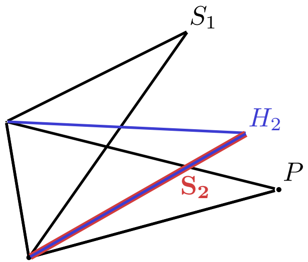
Applying Ramsey



How to apply **Ramsey**? Example for $q = 2$.

1. Fix a 1-space P.
2. **Goal:** the coefficient of x_P.
3. Say, **only 896 coefficients** can occur!
4. $n \geq R_2(s_1; 896)$: monochromatic s_1-space S_1.

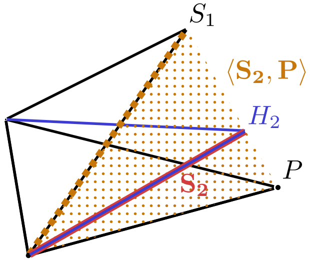
Applying Ramsey



How to apply **Ramsey**? Example for $q = 2$.

1. Fix a 1-space P.
2. **Goal:** the coefficient of x_P.
3. Say, **only** 896 **coefficients** can occur!
4. $n \geq R_2(s_1; 896)$: monochromatic s_1-space S_1.
5. $s_1 \geq R_2(s_2; 896)$: monochromatic affine s_2-sp. S_2 in $H_2 \cap \langle S_1, P \rangle$.

Applying Ramsey



How to apply **Ramsey**? Example for $q = 2$.

1. Fix a 1-space P.
2. **Goal:** the coefficient of x_P.
3. Say, **only** 896 **coefficients** can occur!
4. $n \geq R_2(s_1; 896)$: monochromatic s_1-space S_1.
5. $s_1 \geq R_2(s_2; 896)$: monochromatic affine s_2-sp. S_2 in $H_2 \cap \langle S_1, P \rangle$.
6. $s_2 \geq R_2(2; 896)$: monochromatic affine 2-space in $\langle S_2, P \rangle$.

Limited Weights

Ramsey gives us that any P has one of the coefficients

$$\{-\frac{q}{q+1}, -\frac{q-1}{q}, -\frac{1}{q^2+q}, 0, \frac{1}{q}, \frac{1}{q+1}, 1-\frac{1}{q^2+q}, 1\}.$$

Proposition

If ***all coefficients*** *are in* $[-1, -\frac{q-1}{q+1}) \cup \{-\frac{1}{q^2+q}, 0, \frac{1}{q+1}, \frac{1}{q}\} \cup (\frac{q}{q+1}, 1]$, *then* f *or* $1-f$ *is one of* 0, x_P, x_H, $x_P + x_H$.

Proof.

- Drudge (1998),
- Metsch (2010),
- Some easy calculations. $\square$

What is $c_0(k,q)$?

Other arguments: $c_0(2,2) = 2$.

Best known vector space Ramsey bound (I think):

Theorem (Frederickson, Yepremyan (2023, simplified))

$R_2(s;m) \leq 2 \uparrow\uparrow ms.$

[4] Also, I did not check the estimate below too carefully.

What is $c_0(k, q)$?

Other arguments: $c_0(2,2) = 2$.

Best known vector space Ramsey bound (I think):

Theorem (Frederickson, Yepremyan (2023, simplified))

$R_2(s; m) \leq 2 \uparrow\uparrow ms.$

Ignoring the difference between affine/projective, this gives[4]

$$\begin{aligned} 2 = c_0(2,2) &\leq R_2(R_2(R_2(2;896);896);896) - 2 \\ &\leq 2 \uparrow\uparrow (896 \cdot (2 \uparrow\uparrow (896 \cdot (2 \uparrow\uparrow 896 \cdot 2)))) - 2 \gg 2. \end{aligned}$$

Question

Does $c_0(2, q)$ grow in q?

[4] Also, I did not check the estimate below too carefully.

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 (2023, Annals of Mathematics))

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 (2023, Annals of Mathematics))

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 (2023, Annals of Mathematics))

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.

Two-Intersecting Sets

Problem: Pick a set of 1-spaces $\mathcal{P}$ in $\mathbb{F}_q^n$ such that $|L \cap \mathcal{P}| \in \{a, b\}$ for any k-space L. (two-intersecting set)

There are many examples for $(n, k) = (3, 2)$, e.g., **hyperovals**.

Always: take a 1-space or a hyperplane. (trivial examples)

Two-Intersecting Sets

Problem: Pick a set of 1-spaces $\mathcal{P}$ in $\mathbb{F}_q^n$ such that $|L \cap \mathcal{P}| \in \{a, b\}$ for any k-space L. (two-intersecting set)

There are many examples for $(n, k) = (3, 2)$, e.g., **hyperovals**.

Always: take a 1-space or a hyperplane. (trivial examples)

Theorem (Tallini Scafati (1976, simplified))

*For $(n, k) = (4, 2)$, if there is a non-trivial two-intersecting set, then q is an **odd square**.*

First open case is $q = 9$.

Theorem (Ih. (2024, AMS Proceedings, accepted))

*For k fixed and n sufficiently large, **all** two-intersecting sets are **trivial**.*

Future Work

Problem (Updated)

Investigate the behavior of $\mathbf{c_0(k, q)}$*. Does it grow in* q*?*

Problem (FKN)

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

Problem (Nisan-Szegedy)

On ***how many variables*** *can a Boolean degree* d *function depend?*

Problem

Can we improve the bounds for the ***Ramsey number*** $R_q(s; m)$*?*

Thank you for your attention!