Flat-Containing and Shift-Blocking Sets in $\mathbb{F}_2^n$

Vsevolod F. Lev
(Joint work with Aart Blokhuis)

The University of Haifa

Erdős Centennial – Budapest, July 2013

The Kakeya & Nikodym Problems

The Kakeya Problem in the Vector Space V

How small can a subset $C \subseteq V$ be, given that C contains a line in every direction?

The “Dual” Problem (Concept)

How small can a subset $C \subseteq V$ be, given that C contains a line through every point of V?

(We need $C = V$: for, if $v \notin C$, then C cannot contain a line through v.)

The *refined* dual problem(s):

The Nikodym Problem

How small can a subset $C \subseteq V$ be, given that C contains a line through every point of C?

We Study

How small can a subset $C \subseteq V$ be, given that through every $v \in V$ there is a line, entirely contained in C with the possible exception of the point v itself?

The Kakeya & Nikodym Problems

The Kakeya Problem in the Vector Space V

How small can a subset $C \subseteq V$ be, given that C contains a line *in every direction?*

The "Dual" Problem (Concept)

How small can a subset $C \subseteq V$ be, given that C contains a line *through every point of V?*

(We need $C = V$: for, if $v \notin C$, then C cannot contain a line through v.)

The *refined* dual problem(s):

The Nikodym Problem

How small can a subset $C \subseteq V$ be, given that C contains a line through every point of C?

We Study

How small can a subset $C \subseteq V$ be, given that through every $v \in V$ there is a line, entirely contained in C with the possible exception of the point v itself?

The Kakeya & Nikodym Problems

The Kakeya Problem in the Vector Space V

How small can a subset $C \subseteq V$ be, given that C contains a line *in every direction?*

The "Dual" Problem (Concept)

How small can a subset $C \subseteq V$ be, given that C contains a line *through every point of V?*

(We need $C = V$: for, if $v \notin C$, then C cannot contain a line through v.)

The *refined* dual problem(s):

The Nikodym Problem

How small can a subset $C \subseteq V$ be, given that C contains a line through every point of C?

We Study

How small can a subset $C \subseteq V$ be, given that through every $v \in V$ there is a line, entirely contained in C with the possible exception of the point v itself?

The Kakeya & Nikodym Problems

The Kakeya Problem in the Vector Space V

How small can a subset $C \subseteq V$ be, given that C contains a line *in every direction?*

The "Dual" Problem (Concept)

How small can a subset $C \subseteq V$ be, given that C contains a line *through every point of V?*

(We need $C = V$: for, if $v \notin C$, then C cannot contain a line through v.)

The *refined* dual problem(s):

The Nikodym Problem

How small can a subset $C \subseteq V$ be, given that C contains a line through every point of C?

We Study

How small can a subset $C \subseteq V$ be, given that through every $v \in V$ there is a line, entirely contained in C with the possible exception of the point v itself?

Complete Sets in $\mathbb{F}_2^n$

We focus on the case where $V = \mathbb{F}_2^n$, while working in the general settings of dimension-d subspaces (rather than just lines).

We want to color some of the points of $\mathbb{F}_2^n$ say, green, so that through every point $v \in \mathbb{F}_2^n$ there is a d-flat which is entirely green — save, perhaps, for v itself. What is the smallest number of points to color?

We call sets with this property *d-complete*, and denote by $\gamma_n(d)$ the smallest size of a d-complete set in $\mathbb{F}_2^n$.

Definition

For $0 \le d \le n$, a subset $C \subseteq \mathbb{F}_2^n$ is *d-complete* if for every $v \in \mathbb{F}_2^n$, there is a d-subspace $L_v \le \mathbb{F}_2^n$ with $v + (L_v \setminus \{0\}) \subseteq C$. We let

$$\gamma_n(d) := \min\{|C| : C \subseteq \mathbb{F}_2^n \text{ is } d\text{-complete}\}.$$

Since $v + (L_v \setminus \{0\}) \subseteq C$ can be written as $L_v \setminus \{0\} \subseteq C + v$, a set $C \subseteq \mathbb{F}_2^n$ is d-complete iff every translate of C contains all non-zero vectors of some d-subspace.

Complete Sets in $\mathbb{F}_2^n$

We focus on the case where $V = \mathbb{F}_2^n$, while working in the general settings of dimension-d subspaces (rather than just lines).

We want to color some of the points of $\mathbb{F}_2^n$ say, green, so that through every point $v \in \mathbb{F}_2^n$ there is a d-flat which is entirely green — save, perhaps, for v itself. What is the smallest number of points to color?

We call sets with this property *d-complete*, and denote by $\gamma_n(d)$ the smallest size of a d-complete set in $\mathbb{F}_2^n$.

Definition

For $0 \le d \le n$, a subset $C \subseteq \mathbb{F}_2^n$ is *d-complete* if for every $v \in \mathbb{F}_2^n$, there is a d-subspace $L_v \le \mathbb{F}_2^n$ with $v + (L_v \setminus \{0\}) \subseteq C$. We let

$$\gamma_n(d) := \min\{|C| : C \subseteq \mathbb{F}_2^n \text{ is } d\text{-complete}\}.$$

Since $v + (L_v \setminus \{0\}) \subseteq C$ can be written as $L_v \setminus \{0\} \subseteq C + v$, a set $C \subseteq \mathbb{F}_2^n$ is d-complete iff every translate of C contains all non-zero vectors of some d-subspace.

Complete Sets in $\mathbb{F}_2^n$

We focus on the case where $V = \mathbb{F}_2^n$, while working in the general settings of dimension-d subspaces (rather than just lines).

We want to color some of the points of $\mathbb{F}_2^n$ say, green, so that through every point $v \in \mathbb{F}_2^n$ there is a d-flat which is entirely green — save, perhaps, for v itself. What is the smallest number of points to color?

We call sets with this property *d-complete*, and denote by $\gamma_n(d)$ the smallest size of a d-complete set in $\mathbb{F}_2^n$.

Definition

For $0 \le d \le n$, a subset $C \subseteq \mathbb{F}_2^n$ is *d-complete* if for every $v \in \mathbb{F}_2^n$, there is a d-subspace $L_v \le \mathbb{F}_2^n$ with $v + (L_v \setminus \{0\}) \subseteq C$. We let

$$\gamma_n(d) := \min\{|C| : C \subseteq \mathbb{F}_2^n \text{ is } d\text{-complete}\}.$$

Since $v + (L_v \setminus \{0\}) \subseteq C$ can be written as $L_v \setminus \{0\} \subseteq C + v$, a set $C \subseteq \mathbb{F}_2^n$ is d-complete iff every translate of C contains all non-zero vectors of some d-subspace.

An Alternative Viewpoint

Clearly, the set $B \subseteq \mathbb{F}_2^n$ of all “black” points (those not colored green) has the property that every translate $B + v$ avoids with some punctured linear subspace $L_v \setminus \{0\}$. We call such sets *non-blocking*.

Definition

For $0 \le d \le n$, a subset $B \subseteq \mathbb{F}_2^n$ is *d-non-blocking* if for every $v \in \mathbb{F}_2^n$, there is a co-d-subspace $L_v \le \mathbb{F}_2^n$ with $(B + v) \cap (L_v \setminus \{0\}) = \varnothing$.
We let

$$\beta_n(d) := \max\{|B| \colon B \subseteq \mathbb{F}_2^n \text{ is } d\text{-non-blocking}\}.$$

Thus, every $B \subseteq \mathbb{F}_2^n$ with $|B| > \beta_n(d)$ is guaranteed to have a translate blocking all co-d-subspaces of $\mathbb{F}_2^n$.

From the definitions, we have

$$\beta_n(d) = 2^n - \gamma_n(n - d);$$

hence, all results can be equivalently stated in terms of either γ_n or β_n.

An Alternative Viewpoint

Clearly, the set $B \subseteq \mathbb{F}_2^n$ of all “black” points (those not colored green) has the property that every translate $B + v$ avoids with some punctured linear subspace $L_v \setminus \{0\}$. We call such sets *non-blocking*.

Definition

For $0 \le d \le n$, a subset $B \subseteq \mathbb{F}_2^n$ is *d-non-blocking* if for every $v \in \mathbb{F}_2^n$, there is a co-d-subspace $L_v \le \mathbb{F}_2^n$ with $(B + v) \cap (L_v \setminus \{0\}) = \varnothing$.
We let

$$\beta_n(d) := \max\{|B| \colon B \subseteq \mathbb{F}_2^n \text{ is } d\text{-non-blocking}\}.$$

Thus, every $B \subseteq \mathbb{F}_2^n$ with $|B| > \beta_n(d)$ is guaranteed to have a translate blocking all co-d-subspaces of $\mathbb{F}_2^n$.

From the definitions, we have

$$\beta_n(d) = 2^n - \gamma_n(n-d);$$

hence, all results can be equivalently stated in terms of either γ_n or β_n.

An Alternative Viewpoint

Clearly, the set $B \subseteq \mathbb{F}_2^n$ of all "black" points (those not colored green) has the property that every translate $B + v$ avoids with some punctured linear subspace $L_v \setminus \{0\}$. We call such sets *non-blocking*.

Definition

For $0 \le d \le n$, a subset $B \subseteq \mathbb{F}_2^n$ is *d-non-blocking* if for every $v \in \mathbb{F}_2^n$, there is a co-d-subspace $L_v \le \mathbb{F}_2^n$ with $(B + v) \cap (L_v \setminus \{0\}) = \varnothing$.
We let

$$\beta_n(d) := \max\{|B| : B \subseteq \mathbb{F}_2^n \text{ is } d\text{-non-blocking}\}.$$

Thus, every $B \subseteq \mathbb{F}_2^n$ with $|B| > \beta_n(d)$ is guaranteed to have a translate blocking all co-d-subspaces of $\mathbb{F}_2^n$.

From the definitions, we have

$$\beta_n(d) = 2^n - \gamma_n(n - d);$$

hence, all results can be equivalently stated in terms of either γ_n or β_n.

Basic Observations

$$\gamma_n(d) := \min\{|C| \colon C \subseteq \mathbb{F}_2^n \text{ is } d\text{-complete}\}$$
$$\beta_n(d) := \max\{|B| \colon B \subseteq \mathbb{F}_2^n \text{ is } d\text{-non-blocking}\}$$

$$\beta_n(d) = 2^n - \gamma_n(n-d)$$

$$0 = \gamma_n(0) < \gamma_n(1) \le \dots \le \gamma_n(n-1) < \gamma_n(n) = 2^n,$$
$$0 = \beta_n(0) < \beta_n(1) \le \dots \le \beta_n(n-1) < \beta_n(n) = 2^n.$$

- $\gamma_n(0) = 0$ because $C = \varnothing$ is 0-complete: every translate of $\varnothing$ contains the punctured 0-dimensional subspace.
- $\beta_n(0) = 0$ because no $B \ne \varnothing$ is 0-non-blocking: there exists $v \in \mathbb{F}_2^r$ such that $B + v$ is not disjoint with the punctured n-dimensional subspace.
- $\gamma_n(d+1) \ge \gamma_n(d)$ because containing a $(d+1)$-subspace requires a larger set C than containing a d-subspace.

Basic Observations

$$\gamma_n(d) := \min\{|C| \colon C \subseteq \mathbb{F}_2^n \text{ is } d\text{-complete}\}$$
$$\beta_n(d) := \max\{|B| \colon B \subseteq \mathbb{F}_2^n \text{ is } d\text{-non-blocking}\}$$

$$\beta_n(d) = 2^n - \gamma_n(n-d)$$

$$0 = \gamma_n(0) < \gamma_n(1) \le \cdots \le \gamma_n(n-1) < \gamma_n(n) = 2^n,$$
$$0 = \beta_n(0) < \beta_n(1) \le \cdots \le \beta_n(n-1) < \beta_n(n) = 2^n.$$

- $\gamma_n(0) = 0$ because $C = \varnothing$ is 0-complete: every translate of $\varnothing$ contains the punctured 0-dimensional subspace.
- $\beta_n(0) = 0$ because no $B \ne \varnothing$ is 0-non-blocking: there exists $v \in \mathbb{F}_2^r$ such that $B + v$ is not disjoint with the punctured n-dimensional subspace.
- $\gamma_n(d+1) \ge \gamma_n(d)$ because containing a $(d+1)$-subspace requires a larger set C than containing a d-subspace.

Basic Observations

$$\gamma_n(d) := \min\{|C| : C \subseteq \mathbb{F}_2^n \text{ is } d\text{-complete}\}$$
$$\beta_n(d) := \max\{|B| : B \subseteq \mathbb{F}_2^n \text{ is } d\text{-non-blocking}\}$$

$$\beta_n(d) = 2^n - \gamma_n(n-d)$$

$$0 = \gamma_n(0) < \gamma_n(1) \le \dots \le \gamma_n(n-1) < \gamma_n(n) = 2^n,$$
$$0 = \beta_n(0) < \beta_n(1) \le \dots \le \beta_n(n-1) < \beta_n(n) = 2^n.$$

- $\gamma_n(0) = 0$ because $C = \varnothing$ is 0-complete: every translate of $\varnothing$ contains the punctured 0-dimensional subspace.
- $\beta_n(0) = 0$ because no $B \ne \varnothing$ is 0-non-blocking: there exists $v \in \mathbb{F}_2^r$ such that $B + v$ is not disjoint with the punctured n-dimensional subspace.
- $\gamma_n(d+1) \ge \gamma_n(d)$ because containing a $(d+1)$-subspace requires a larger set C than containing a d-subspace.

Basic Observations

$$\gamma_n(d) := \min\{|C| \colon C \subseteq \mathbb{F}_2^n \text{ is } d\text{-complete}\}$$
$$\beta_n(d) := \max\{|B| \colon B \subseteq \mathbb{F}_2^n \text{ is } d\text{-non-blocking}\}$$

$$\beta_n(d) = 2^n - \gamma_n(n-d)$$

$$0 = \gamma_n(0) < \gamma_n(1) \le \dots \le \gamma_n(n-1) < \gamma_n(n) = 2^n,$$
$$0 = \beta_n(0) < \beta_n(1) \le \dots \le \beta_n(n-1) < \beta_n(n) = 2^n.$$

- $\gamma_n(0) = 0$ because $C = \varnothing$ is 0-complete: every translate of $\varnothing$ contains the punctured 0-dimensional subspace.
- $\beta_n(0) = 0$ because no $B \ne \varnothing$ is 0-non-blocking: there exists $v \in \mathbb{F}_2^r$ such that $B + v$ is not disjoint with the punctured n-dimensional subspace.
- $\gamma_n(d+1) \ge \gamma_n(d)$ because containing a $(d+1)$-subspace requires a larger set C than containing a d-subspace.

More Basics: Lines & Hyperplanes

Claim

We have $\gamma_n(1) = \beta_n(1) = 2$. *Thus,* $\gamma_n(n-1) = \beta_n(n-1) = 2^n - 2$.

$\gamma_n(1) = 2$: a singleton set does not contain a punctured 1-flat through its unique element; hence, is not 1-complete. For any *two*-element set $C \subseteq \mathbb{F}_2^n$ and any $v \in \mathbb{F}_2^n$, there is a punctured 1-flat through v, contained in C; hence, any 2-element set is 1-complete.

$\beta_n(1) = 2$: if $B = \{b_1, b_2, b_3\} \subseteq \mathbb{F}_2^n$, then the translate $B + (b_1 + b_2 + b_3) = \{b_1 + b_2, b_2 + b_3, b_3 + b_1\}$ blocks every linear co-1-subspace (hyperplane): for, its three elements add up to 0, so cannot be all contained in the complement of a hyperplane. Hence, $\beta_n(1) < 3$. On the other hand, for any *two*-element subset $B \subseteq \mathbb{F}_2^n$ there is a co-1-subspace, disjoint with $B \setminus \{0\}$; hence, every two-element set is 1-non-blocking and $\beta_n(1) \geq 2$.

More Basics: Lines & Hyperplanes

Claim

We have $\gamma_n(1) = \beta_n(1) = 2$*. Thus,* $\gamma_n(n-1) = \beta_n(n-1) = 2^n - 2$*.*

$\gamma_n(1) = 2$: a singleton set does not contain a punctured 1-flat through its unique element; hence, is not 1-complete. For any *two*-element set $C \subseteq \mathbb{F}_2^n$ and any $v \in \mathbb{F}_2^n$, there is a punctured 1-flat through v, contained in C; hence, any 2-element set is 1-complete.

$\beta_n(1) = 2$: if $B = \{b_1, b_2, b_3\} \subseteq \mathbb{F}_2^n$, then the translate $B + (b_1 + b_2 + b_3) = \{b_1 + b_2, b_2 + b_3, b_3 + b_1\}$ blocks every linear co-1-subspace (hyperplane): for, its three elements add up to 0, so cannot be all contained in the complement of a hyperplane. Hence, $\beta_n(1) < 3$. On the other hand, for any *two*-element subset $B \subseteq \mathbb{F}_2^n$ there is a co-1-subspace, disjoint with $B \setminus \{0\}$; hence, every two-element set is 1-non-blocking and $\beta_n(1) \geq 2$.

Yet More Basics: 2-flats & co-2-flats

Theorem 1

$\gamma_n(2)$ is the smallest cardinality of a subset $C \subseteq \mathbb{F}_2^n$ with the property that every element of $\mathbb{F}_2^n$ is a sum of three pairwise distinct elements of C. Consequently,

$$\gamma_n(2) = \Theta(2^{n/3}).$$

Proof.

A set $C \subseteq \mathbb{F}_2^n$ is 2-complete whenever for every $v \in \mathbb{F}_2^n$, there exist $c_1, c_2, c_3 \in C$ such that $\{v, c_1, c_2, c_3\}$ is a 2-flat. However, this is equivalent to $v = c_1 + c_2 + c_3$ and c_1, c_2, c_3 being pairwise distinct. □

For $\beta_n(2)$, we have the estimates

$$\frac{3}{8}(n^2 - 6n + 9) \leq \beta_n(2) \leq \frac{1}{2}(n^2 + n - 6)$$

(to be discussed later).

Yet More Basics: 2-flats & co-2-flats

Theorem 1

$\gamma_n(2)$ is the smallest cardinality of a subset $C \subseteq \mathbb{F}_2^n$ with the property that every element of $\mathbb{F}_2^n$ is a sum of three pairwise distinct elements of C. Consequently,

$$\gamma_n(2) = \Theta(2^{n/3}).$$

Proof.

A set $C \subseteq \mathbb{F}_2^n$ is 2-complete whenever for every $v \in \mathbb{F}_2^n$, there exist $c_1, c_2, c_3 \in C$ such that $\{v, c_1, c_2, c_3\}$ is a 2-flat. However, this is equivalent to $v = c_1 + c_2 + c_3$ and c_1, c_2, c_3 being pairwise distinct. □

For $\beta_n(2)$, we have the estimates

$$\frac{3}{8}(n^2 - 6n + 9) \leq \beta_n(2) \leq \frac{1}{2}(n^2 + n - 6)$$

(to be discussed later).

Submultiplicativity

Lemma

For any $n_1, n_2 \geq d \geq 0$ *we have*

$$\gamma_{n_1+n_2}(d) \leq \gamma_{n_1}(d)\gamma_{n_2}(d).$$

Sketch of the proof.

Let $n := n_1 + n_2$, write $\mathbb{F}_2^n = V_1 \oplus V_2$ where $\dim V_i = n_i$, and find $C_i \subseteq V_i$ so that $|C_i| = \gamma_i(d)$ and C_i is d-complete in V_i. Then $C_1 + C_2$ is d-complete in $\mathbb{F}_2^n$, whence

$$\gamma_{n_1+n_2}(d) \leq |C_1 + C_2| = |C_1||C_2| = \gamma_{n_1}(d)\gamma_{n_2}(d).$$

□

As a result, to any fixed $d \geq 1$ there corresponds some $\varkappa_d \in [0, 1]$ such that $\gamma_n(d) = 2^{(\varkappa_d + o(1))n}$ as $n \to \infty$. We know that

- $\varkappa_1 = 0,\ \varkappa_2 = 1/3$;
- $3/8 \leq \varkappa_3 \leq 3/7$;
- $\varkappa_d < 1/2$ for all d.

Submultiplicativity

Lemma

For any $n_1, n_2 \geq d \geq 0$ *we have*

$$\gamma_{n_1+n_2}(d) \leq \gamma_{n_1}(d)\gamma_{n_2}(d).$$

Sketch of the proof.

Let $n := n_1 + n_2$, write $\mathbb{F}_2^n = V_1 \oplus V_2$ where $\dim V_i = n_i$, and find $C_i \subseteq V_i$ so that $|C_i| = \gamma_i(d)$ and C_i is d-complete in V_i. Then $C_1 + C_2$ is d-complete in $\mathbb{F}_2^n$, whence

$$\gamma_{n_1+n_2}(d) \leq |C_1 + C_2| = |C_1||C_2| = \gamma_{n_1}(d)\gamma_{n_2}(d).$$

□

As a result, to any fixed $d \geq 1$ there corresponds some $\varkappa_d \in [0, 1]$ such that $\gamma_n(d) = 2^{(\varkappa_d + o(1))n}$ as $n \to \infty$. We know that

- $\varkappa_1 = 0,\ \varkappa_2 = 1/3;$
- $3/8 \leq \varkappa_3 \leq 3/7;$
- $\varkappa_d < 1/2$ for all d.

Lower Bounds for γ_n, Upper Bounds for β_n

(Non-Existence Results)

From the discussion above, $\gamma_n(3) \geq \gamma_n(2) = \Theta(2^{n/3})$.

Theorem 2

We have $\gamma_n(3) > c \cdot 2^{3n/8}$ with $c \approx 3.36$.

Consequently, $\gamma_n(d) > c \cdot 2^{3n/8}$ (and so $\varkappa_d \geq 3/8$) for $d \geq 3$.

For flats of dimension $d \gtrsim 0.073n$, we can give a better bound.

Theorem 3

We have

$$\gamma_n(d) \geq \sum_{j=0}^{d-1} \binom{n}{j}.$$

Equivalently,

$$\beta_n(d) \leq \sum_{j=0}^{d} \binom{n}{j}.$$

Thus, $\beta_n(2) \leq 1 + n + \binom{n}{2}$. (Further minor improvements are available.)

Lower Bounds for γ_n, Upper Bounds for β_n

(Non-Existence Results)

From the discussion above, $\gamma_n(3) \geq \gamma_n(2) = \Theta(2^{n/3})$.

Theorem 2

We have $\gamma_n(3) > c \cdot 2^{3n/8}$ with $c \approx 3.36$.

Consequently, $\gamma_n(d) > c \cdot 2^{3n/8}$ (and so $\varkappa_d \geq 3/8$) for $d \geq 3$.

For flats of dimension $d \gtrsim 0.073n$, we can give a better bound.

Theorem 3

We have

$$\gamma_n(d) \geq \sum_{j=0}^{d-1} \binom{n}{j}.$$

Equivalently,

$$\beta_n(d) \leq \sum_{j=0}^{d} \binom{n}{j}.$$

Thus, $\beta_n(2) \leq 1 + n + \binom{n}{2}$. (Further minor improvements are available.)

Upper Bounds for γ_n, Lower Bounds for β_n

Flats of Low Dimension

Theorem 4

We have

$$\gamma_n(d) < K_d \cdot 2^{(1/2-\varepsilon_d)n}.$$

where $\varepsilon_d = 1/(2(2^d - 1))$ and $K_d \approx 2^{2^d}$.

(As a particular case, $\gamma_n(3) = O(2^{3n/7})$; that is, $\varkappa_3 \leq 3/7$.)

The double-exponential dependence of K_d on d makes Theorem 3 trivial for $d \gtrsim \log n$. A non-trivial estimate in this regime:

Theorem 5

We have

$$\gamma_n(d) < 2^{0.5n+K(nd/\log n)^{2/3}}$$

(with K absolute). Hence, if $d = o(\sqrt{n}\log n)$, then $\gamma_n(d) < 2^{(0.5+o(1))n}$.

Upper Bounds for γ_n, Lower Bounds for β_n

Flats of Low Dimension

Theorem 4

We have

$$\gamma_n(d) < K_d \cdot 2^{(1/2-\varepsilon_d)n}.$$

where $\varepsilon_d = 1/(2(2^d - 1))$ and $K_d \approx 2^{2^d}$.

(As a particular case, $\gamma_n(3) = O(2^{3n/7})$; that is, $\varkappa_3 \leq 3/7$.)

The double-exponential dependence of K_d on d makes Theorem 3 trivial for $d \gtrsim \log n$. A non-trivial estimate in this regime:

Theorem 5

We have

$$\gamma_n(d) < 2^{0.5n+K(nd/\log n)^{2/3}}$$

(with K absolute). Hence, if $d = o(\sqrt{n}\log n)$, then $\gamma_n(d) < 2^{(0.5+o(1))n}$.

Upper Bounds for γ_n, Lower Bounds for β_n

Flats of Low Co-Dimension

Theorems 3 and 4 are of primary interest for flats of low dimension d. For flats of low *co*-dimension we have the following estimates.

Theorem 6

We have

$$\beta_n(d) \ge \binom{2d}{d} \left\lfloor \frac{n}{2d} \right\rfloor^d, \ 2 \le d \le n/2.$$

(In particular, $\beta_n(2) \ge \frac{3}{8}(n^2 - 6n + 9)$.)

Theorem 7

Suppose that $0 \le d_1 \le n_1 \le d_1 + d, \dots, 0 \le d_k \le n_k \le d_k + d$ are integers with $n_1 + \dots + n_k \le n$ and $d_1 + \dots + d_k \le d$. Then

$$\beta_n(d) \ge \binom{n_1}{d_1} \cdots \binom{n_k}{d_k}.$$

As a corollary, if $d/\sqrt{n} \to \infty$, then $\beta_n(d) > \binom{n}{d}^{1+o(1)}$.

▸ Theorem 3

Upper Bounds for γ_n, Lower Bounds for β_n

Flats of Low Co-Dimension

Theorems 3 and 4 are of primary interest for flats of low dimension d. For flats of low *co*-dimension we have the following estimates.

Theorem 6

We have

$$\beta_n(d) \geq \binom{2d}{d} \left\lfloor \frac{n}{2d} \right\rfloor^d, \; 2 \leq d \leq n/2.$$

(In particular, $\beta_n(2) \geq \frac{3}{8}(n^2 - 6n + 9)$.)

Theorem 7

Suppose that $0 \leq d_1 \leq n_1 \leq d_1 + d, \ldots, 0 \leq d_k \leq n_k \leq d_k + d$ are integers with $n_1 + \cdots + n_k \leq n$ and $d_1 + \cdots + d_k \leq d$. Then

$$\beta_n(d) \geq \binom{n_1}{d_1} \cdots \binom{n_k}{d_k}.$$

As a corollary, if $d/\sqrt{n} \to \infty$, then $\beta_n(d) > \binom{n}{d}^{1+o(1)}$.

Theorem 3

Upper Bounds for γ_n, Lower Bounds for β_n

Flats of Low Co-Dimension

Theorems 3 and 4 are of primary interest for flats of low dimension d. For flats of low *co*-dimension we have the following estimates.

Theorem 6

We have

$$\beta_n(d) \geq \binom{2d}{d} \left\lfloor \frac{n}{2d} \right\rfloor^d, \; 2 \leq d \leq n/2.$$

(In particular, $\beta_n(2) \geq \frac{3}{8}(n^2 - 6n + 9)$.)

Theorem 7

Suppose that $0 \leq d_1 \leq n_1 \leq d_1 + d, \dots, 0 \leq d_k \leq n_k \leq d_k + d$ are integers with $n_1 + \cdots + n_k \leq n$ and $d_1 + \cdots + d_k \leq d$. Then

$$\beta_n(d) \geq \binom{n_1}{d_1} \cdots \binom{n_k}{d_k}.$$

As a corollary, if $d/\sqrt{n} \to \infty$, then $\beta_n(d) > \binom{n}{d}^{1+o(1)}$.

▸ Theorem 3

Proof of Theorem 3

To prove: $\beta_n(d) \le \sum_{j=0}^{d} \binom{n}{j}$

Notation: $\mathcal{L}_{n,d} := \{P \in \mathbb{F}_2[x_1, \dots, x_n] \colon P \text{ is multilinear}, \deg P \le d\}$

Fix a d-non-blocking set $B \subseteq \mathbb{F}_2^n$ with $|B| = \beta_n(d)$. To every $b \in B$ there corresponds a co-d-flat $F_b \subseteq \mathbb{F}_2^n$ with $F_b \cap B = \{b\}$. For every such flat, find a polynomial $P_b \in \mathcal{L}_{n,d}$ with $P_b = 1_{F_b}$. These $|B|$ polynomials are linearly independent: for, if

$$\sum_{b \in B} \varepsilon_b P_b = 0,$$

then

$$\sum_{b \in B} \varepsilon_b 1_{F_b}(z) = 0, \; z \in \mathbb{F}_2^n,$$

and choosing $z \in B$ yields $\varepsilon_z = 0$ (as $z \notin F_b$ for $b \ne z$). It follows that

$$|B| \le \dim \mathcal{L}_{n,d} = \sum_{j=0}^{d} \binom{n}{j}.$$

□

Proof of Theorem 3

To prove: $\beta_n(d) \le \sum_{j=0}^{d} \binom{n}{j}$

Notation: $\mathcal{L}_{n,d} := \{P \in \mathbb{F}_2[x_1, \dots, x_n] \colon P \text{ is multilinear}, \deg P \le d\}$

Fix a d-non-blocking set $B \subseteq \mathbb{F}_2^n$ with $|B| = \beta_n(d)$. To every $b \in B$ there corresponds a co-d-flat $F_b \subseteq \mathbb{F}_2^n$ with $F_b \cap B = \{b\}$. For every such flat, find a polynomial $P_b \in \mathcal{L}_{n,d}$ with $P_b = 1_{F_b}$. These $|B|$ polynomials are linearly independent: for, if

$$\sum_{b \in B} \varepsilon_b P_b = 0,$$

then

$$\sum_{b \in B} \varepsilon_b 1_{F_b}(z) = 0, \ z \in \mathbb{F}_2^n,$$

and choosing $z \in B$ yields $\varepsilon_z = 0$ (as $z \notin F_b$ for $b \ne z$). It follows that

$$|B| \le \dim \mathcal{L}_{n,d} = \sum_{j=0}^{d} \binom{n}{j}.$$

□

Proof of Theorems 4 and 5

Wanted: a d-complete set $C \subseteq \mathbb{F}_2^n$ of size $|C| \lesssim 2^{(0.5+o(1))n}$

Fix a linear code $S < \mathbb{F}_2^m$ of dimension d so that its length m is small (as a function of d), while its minimum distance μ is $(0.5 + o(1))m$. Also, fix a decomposition $\mathbb{F}_2^n = \bigoplus_{i=1}^m V_i$ with $\dim V_i = n/m$, and set

$$C := \bigcup_{(s_1,\dots,s_m)\in S\setminus\{0\}} \bigoplus_{i:\ s_i=0} V_i;$$

thus, $|C| \le (|S| - 1)2^{(m-\mu)(n/m)} \lesssim 2^{(0.5+o(1))n}$. Why is C d-complete?

Given a vector $v = v_1 + \cdots + v_m \in \mathbb{F}_2^n$ (with $v_i \in V_i$), consider the linear subspace

$$L_v := \{s_1 v_1 + \cdots + s_m v_m : (s_1, \dots, s_m) \in S\}.$$

We have $v + (L_v \setminus \{0\}) \subseteq C$. Hence, if $\dim L_v = d$, then C contains a punctured d-flat through v, and we are done. But if $\dim L_v < d$, then there exists $(s_1, \dots, s_m) \in S \setminus \{0\}$ with $s_1 v_1 + \cdots + s_m v_m = 0$. In this case $v \in \bigoplus_{i:\ s_i=0} V_i$, the right-hand side being a subspace contained in C, and "normally" of dimension at least d. □

Proof of Theorems 4 and 5

Theorems 4 and 5

Wanted: a d-complete set $C \subseteq \mathbb{F}_2^n$ of size $|C| \lesssim 2^{(0.5+o(1))n}$

Fix a linear code $S < \mathbb{F}_2^m$ of dimension d so that its length m is small (as a function of d), while its minimum distance μ is $(0.5 + o(1))m$. Also, fix a decomposition $\mathbb{F}_2^n = \bigoplus_{i=1}^m V_i$ with $\dim V_i = n/m$, and set

$$C := \bigcup_{(s_1,\dots,s_m)\in S\setminus\{0\}} \bigoplus_{i:\ s_i=0} V_i;$$

thus, $|C| \le (|S|-1)2^{(m-\mu)(n/m)} \lesssim 2^{(0.5+o(1))n}$. Why is C d-complete?

Given a vector $v = v_1 + \dots + v_m \in \mathbb{F}_2^n$ (with $v_i \in V_i$), consider the linear subspace

$$L_v := \{s_1v_1 + \dots + s_mv_m \colon (s_1,\dots,s_m) \in S\}.$$

We have $v + (L_v \setminus \{0\}) \subseteq C$. Hence, if $\dim L_v = d$, then C contains a punctured d-flat through v, and we are done. But if $\dim L_v < d$, then there exists $(s_1,\dots,s_m) \in S\setminus\{0\}$ with $s_1v_1 + \dots + s_mv_m = 0$. In this case $v \in \bigoplus_{i:\ s_i=0} V_i$, the right-hand side being a subspace contained in C, and “normally” of dimension at least d. □

Proof of Theorem 6

▸ Theorem 6

Wanted: a d-non-blocking set $B \subseteq \mathbb{F}_2^n$ of size $|B| \ge \binom{2d}{d} \left\lfloor \frac{n}{2d} \right\rfloor^d$

Write $\mathbb{F}_2^n = V_1 \oplus \cdots \oplus V_{2d}$ with $\dim V_i = \frac{n}{2d}$, fix bases $\mathfrak{e}_i \subseteq V_i$, and let

$$B := \{e_{i_1} + \cdots + e_{i_d} : 1 \le i_1 < \cdots < i_d \le 2d,\ e_{i_j} \in \mathfrak{e}_{i_j}\};$$

thus, $|B| = \binom{2d}{d}\left(\frac{n}{2d}\right)^d$. Why is B a d-non-blocking set?

Consider $v = v_1 + \cdots + v_{2d} \in \mathbb{F}_2^n$ ($v_i \in V_i$):

- If $v \in B$, then we let $F_v := \{u \in \mathbb{F}_2^n \colon \operatorname{supp} v \subseteq \operatorname{supp} u\}$.
- if $|\operatorname{supp} v_i| \ge 2$ for some $i \in [1, 2d]$, then we find $E \subseteq \operatorname{supp} v_i$ with $|E| = 2$, and let $F_v := \{u \in \mathbb{F}_2^n \colon E \subseteq \operatorname{supp} u\}$.
- if $v \notin B$ and $|\operatorname{supp} v_i| \le 1$ for each $i \in [1, 2d]$, then there exists $I \in [1, 2d]$ with $|I| = d + 1$ and $|\operatorname{supp} v_i|$ being equal to each other for all $i \in I$. In this case, we let F_v be the subspace of all those $u \in \mathbb{F}_2^n$ with $|\operatorname{supp} v_i|$ ($i \in I$) all of the same parity.

In any case, we have $\operatorname{codim} F_v \le d$, $v \in F_v$, and $(F_v \setminus \{v\}) \cap B = \varnothing$.

Proof of Theorem 6

▸ Theorem 6

Wanted: a d-non-blocking set $B \subseteq \mathbb{F}_2^n$ of size $|B| \ge \binom{2d}{d} \left\lfloor \frac{n}{2d} \right\rfloor^d$

Write $\mathbb{F}_2^n = V_1 \oplus \dots \oplus V_{2d}$ with $\dim V_i = \frac{n}{2d}$, fix bases $\mathfrak{e}_i \subseteq V_i$, and let

$$B := \{e_{i_1} + \dots + e_{i_d} \colon 1 \le i_1 < \dots < i_d \le 2d,\ e_{i_j} \in \mathfrak{e}_{i_j}\};$$

thus, $|B| = \binom{2d}{d} \left(\frac{n}{2d}\right)^d$. Why is B a d-non-blocking set?

Consider $v = v_1 + \dots + v_{2d} \in \mathbb{F}_2^n$ ($v_i \in V_i$):

- If $v \in B$, then we let $F_v := \{u \in \mathbb{F}_2^n \colon \operatorname{supp} v \subseteq \operatorname{supp} u\}$.
- if $|\operatorname{supp} v_i| \ge 2$ for some $i \in [1, 2d]$, then we find $E \subseteq \operatorname{supp} v_i$ with $|E| = 2$, and let $F_v := \{u \in \mathbb{F}_2^n \colon E \subseteq \operatorname{supp} u\}$.
- if $v \notin B$ and $|\operatorname{supp} v_i| \le 1$ for each $i \in [1, 2d]$, then there exists $I \in [1, 2d]$ with $|I| = d + 1$ and $|\operatorname{supp} v_i|$ being equal to each other for all $i \in I$. In this case, we let F_v be the subspace of all those $u \in \mathbb{F}_2^n$ with $|\operatorname{supp} v_i|$ ($i \in I$) all of the same parity.

In any case, we have $\operatorname{codim} F_v \le d$, $v \in F_v$, and $(F_v \setminus \{v\}) \cap B = \varnothing$.

Proof of Theorem 6

▸ Theorem 6

Wanted: a d-non-blocking set $B \subseteq \mathbb{F}_2^n$ of size $|B| \geq \binom{2d}{d} \left\lfloor \frac{n}{2d} \right\rfloor^d$

Write $\mathbb{F}_2^n = V_1 \oplus \cdots \oplus V_{2d}$ with $\dim V_i = \frac{n}{2d}$, fix bases $\mathfrak{e}_i \subseteq V_i$, and let

$$B := \{e_{i_1} + \cdots + e_{i_d} \colon 1 \leq i_1 < \cdots < i_d \leq 2d,\ e_{i_j} \in \mathfrak{e}_{i_j}\};$$

thus, $|B| = \binom{2d}{d} \left(\frac{n}{2d}\right)^d$. Why is B a d-non-blocking set?

Consider $v = v_1 + \cdots + v_{2d} \in \mathbb{F}_2^n$ ($v_i \in V_i$):

- If $v \in B$, then we let $F_v := \{u \in \mathbb{F}_2^n \colon \operatorname{supp} v \subseteq \operatorname{supp} u\}$.
- if $|\operatorname{supp} v_i| \geq 2$ for some $i \in [1, 2d]$, then we find $E \subseteq \operatorname{supp} v_i$ with $|E| = 2$, and let $F_v := \{u \in \mathbb{F}_2^n \colon E \subseteq \operatorname{supp} u\}$.
- if $v \notin B$ and $|\operatorname{supp} v_i| \leq 1$ for each $i \in [1, 2d]$, then there exists $I \in [1, 2d]$ with $|I| = d + 1$ and $|\operatorname{supp} v_i|$ being equal to each other for all $i \in I$. In this case, we let F_v be the subspace of all those $u \in \mathbb{F}_2^n$ with $|\operatorname{supp} v_i|$ ($i \in I$) all of the same parity.

In any case, we have $\operatorname{codim} F_v \leq d$, $v \in F_v$, and $(F_v \setminus \{v\}) \cap B = \varnothing$.

Proof of Theorem 6

▸ Theorem 6

Wanted: a d-non-blocking set $B \subseteq \mathbb{F}_2^n$ of size $|B| \ge \binom{2d}{d} \left\lfloor \frac{n}{2d} \right\rfloor^d$

Write $\mathbb{F}_2^n = V_1 \oplus \cdots \oplus V_{2d}$ with $\dim V_i = \frac{n}{2d}$, fix bases $\mathfrak{e}_i \subseteq V_i$, and let

$$B := \{e_{i_1} + \cdots + e_{i_d} \colon 1 \le i_1 < \cdots < i_d \le 2d,\ e_{i_j} \in \mathfrak{e}_{i_j}\};$$

thus, $|B| = \binom{2d}{d} \left(\frac{n}{2d}\right)^d$. Why is B a d-non-blocking set?

Consider $v = v_1 + \cdots + v_{2d} \in \mathbb{F}_2^n$ ($v_i \in V_i$):

- If $v \in B$, then we let $F_v := \{u \in \mathbb{F}_2^n \colon \operatorname{supp} v \subseteq \operatorname{supp} u\}$.
- if $|\operatorname{supp} v_i| \ge 2$ for some $i \in [1, 2d]$, then we find $E \subseteq \operatorname{supp} v_i$ with $|E| = 2$, and let $F_v := \{u \in \mathbb{F}_2^n \colon E \subseteq \operatorname{supp} u\}$.
- if $v \notin B$ and $|\operatorname{supp} v_i| \le 1$ for each $i \in [1, 2d]$, then there exists $I \in [1, 2d]$ with $|I| = d + 1$ and $|\operatorname{supp} v_i|$ being equal to each other for all $i \in I$. In this case, we let F_v be the subspace of all those $u \in \mathbb{F}_2^n$ with $|\operatorname{supp} v_i|$ ($i \in I$) all of the same parity.

In any case, we have $\operatorname{codim} F_v \le d$, $v \in F_v$, and $(F_v \setminus \{v\}) \cap B = \varnothing$.

Proof of Theorem 6

▸ Theorem 6

Wanted: a d-non-blocking set $B \subseteq \mathbb{F}_2^n$ of size $|B| \ge \binom{2d}{d} \left\lfloor \frac{n}{2d} \right\rfloor^d$

Write $\mathbb{F}_2^n = V_1 \oplus \cdots \oplus V_{2d}$ with $\dim V_i = \frac{n}{2d}$, fix bases $\mathfrak{e}_i \subseteq V_i$, and let

$$B := \{e_{i_1} + \cdots + e_{i_d} \colon 1 \le i_1 < \cdots < i_d \le 2d,\ e_{i_j} \in \mathfrak{e}_{i_j}\};$$

thus, $|B| = \binom{2d}{d}\left(\frac{n}{2d}\right)^d$. Why is B a d-non-blocking set?

Consider $v = v_1 + \cdots + v_{2d} \in \mathbb{F}_2^n$ ($v_i \in V_i$):

- If $v \in B$, then we let $F_v := \{u \in \mathbb{F}_2^n \colon \operatorname{supp} v \subseteq \operatorname{supp} u\}$.
- if $|\operatorname{supp} v_i| \ge 2$ for some $i \in [1, 2d]$, then we find $E \subseteq \operatorname{supp} v_i$ with $|E| = 2$, and let $F_v := \{u \in \mathbb{F}_2^n \colon E \subseteq \operatorname{supp} u\}$.
- if $v \notin B$ and $|\operatorname{supp} v_i| \le 1$ for each $i \in [1, 2d]$, then there exists $I \in [1, 2d]$ with $|I| = d + 1$ and $|\operatorname{supp} v_i|$ being equal to each other for all $i \in I$. In this case, we let F_v be the subspace of all those $u \in \mathbb{F}_2^n$ with $|\operatorname{supp} v_i|$ ($i \in I$) all of the same parity.

In any case, we have $\operatorname{codim} F_v \le d$, $v \in F_v$, and $(F_v \setminus \{v\}) \cap B = \varnothing$.

Summary

A subset $C \subseteq V$ is *d-complete* if through every $v \in V$ passes a d-flat contained in $C \cup \{v\}$.

A subset $B \subseteq V$ is *d-non-blocking* if through every $v \in V$ passes is a co-d-flat disjoint with $B \setminus \{v\}$.

Letting

$$\gamma_n(d) := \min\{|C| \colon C \subseteq \mathbb{F}_2^n \text{ is } d\text{-complete}\},$$
$$\beta_n(d) := \max\{|B| \colon B \subseteq \mathbb{F}_2^n \text{ is } d\text{-non-blocking}\},$$

we have

$$\beta_n(d) = 2^n - \gamma_n(n-d),$$
$$0 = \gamma_n(0) < \gamma_n(1) \le \cdots \le \gamma_n(n-1) < \gamma_n(n) = 2^n,$$
$$0 = \beta_n(0) < \beta_n(1) \le \cdots \le \beta_n(n-1) < \beta_n(n) = 2^n.$$

A number of upper and lower bounds for these quantities are obtained.

The First Asymptotically Open Case

What is the smallest possible size of a 3-complete set?

We know that $\gamma_n(3) = 2^{(\varkappa_3 + o(1))n}$ with $3/8 \le \varkappa_3 \le 3/7$.
What is the exact value of $\varkappa_3$?

Stated notation-free way:

How large must a subset of $\mathbb{F}_2^n$ be
given that it contains a punctured 3-flat
through every point of $\mathbb{F}_2^n$?

Thank you!

Lower Bounds for γ_n, Upper Bounds for β_n

(Non-Existence Results)

From the discussion above, $\gamma_n(3) \ge \gamma_n(2) = \Theta(2^{n/3})$.

Theorem 2

We have $\gamma_n(3) > c \cdot 2^{3n/8}$ with $c \approx 3.36$.

Consequently, $\gamma_n(d) > c \cdot 2^{3n/8}$ (and so $\varkappa_d \ge 3/8$) for $d \ge 3$.

For flats of dimension $d \gtrsim 0.073n$, we can give a better bound.

Theorem 3 Back

We have

$$\gamma_n(d) \ge \sum_{j=0}^{d-1} \binom{n}{j}.$$

Equivalently,

$$\beta_n(d) \le \sum_{j=0}^{d} \binom{n}{j}.$$

Thus, $\beta_n(2) \le 1 + n + \binom{n}{2}$. (Further minor improvements are available.)

Theorem 4

Back

We have

$$\gamma_n(d) < K_d \cdot 2^{(1/2-\varepsilon_d)n},$$

where $\varepsilon_d = 1/(2(2^d - 1))$ and $K_d \approx 2^{2^d}$.

(As a particular case, $\gamma_n(3) = O(2^{3n/7})$; that is, $\varkappa_3 \le 3/7$.)

The double-exponential dependence of K_d on d makes Theorem 3 trivial for $d \gtrsim \log n$. A non-trivial estimate in this regime:

Theorem 5

Back

We have

$$\gamma_n(d) < 2^{0.5n+K(nd/\log n)^{2/3}}$$

(with K absolute). Hence, if $d = o(\sqrt{n}\log n)$, then $\gamma_n(d) < 2^{(0.5+o(1))n}$.

Upper Bounds for γ_n, Lower Bounds for β_n

Flats of Low Co-Dimension

Theorems 3 and 4 are of primary interest for flats of low dimension d. For flats of low *co*-dimension we have the following estimates.

Theorem 6 [Back]

We have

$$\beta_n(d) \geq \binom{2d}{d} \left\lfloor \frac{n}{2d} \right\rfloor^d, \; 2 \leq d \leq n/2.$$

(In particular, $\beta_n(2) \geq \frac{3}{8}(n^2 - 6n + 9)$.)

Theorem 7

Suppose that $0 \leq d_1 \leq n_1 \leq d_1 + d, \dots, 0 \leq d_k \leq n_k \leq d_k + d$ are integers with $n_1 + \dots + n_k \leq n$ and $d_1 + \dots + d_k \leq d$. Then

$$\beta_n(d) \geq \binom{n_1}{d_1} \cdots \binom{n_k}{d_k}.$$

As a corollary, if $d/\sqrt{n} \to \infty$, then $\beta_n(d) > \binom{n}{d}^{1+o(1)}$. [Theorem 3]