Avoiding arithmetic progressions or certain geometric configurations

Péter Pál Pach

MTA-BME Lendület Arithmetic Combinatorics Research Group
Budapest University of Technology and Economics

23 February 2021

This research was supported by the Lendület (Momentum) Grant of the Hungarian Academy of Sciences and the Hungarian Scientific Research Funds (Grant Nr. OTKA NKFIH K124171 and NKFIH K129335).

Avoiding arithmetic progressions or right angles

Joint work with Richárd Palincza and with Balázs Bursics, Dávid Matolcsi and Jakab Schrettner.

Different types of forbidden configurations in $\mathbb{F}_p^n$ (or $\mathbb{Z}_m^n$)

- k-AP: $a, a+d, \ldots, a+(k-1)d$ (nontrivial, if the elements are distinct)
- corner: $(a,b),(a+d,b),(a,b+d) \in \mathbb{F}_p^n \times \mathbb{F}_p^n$ (and $d \neq 0$)
- right angle: $(x,y,z) \in \mathbb{F}_p^n$ such that $\langle x-y, x-z \rangle = 0$ (and x,y,z are distinct)
- $(a,b),(a,b+d),(a+d,c),(a+d,c+d) \in \mathbb{F}_2^n \times \mathbb{F}_2^n$ (and $d \neq 0$)

What is the size of the largest set avoiding the given configuration?
Is it $(p-o(1))^n$ (or $(m-o(1))^n$)?
Is it $\leq (p-\varepsilon)^n$?
Is it $\leq n^{O(1)}$?

Different types of forbidden configurations in $\mathbb{F}_p^n$ (or $\mathbb{Z}_m^n$)

- k-AP: $a, a+d, \ldots, a+(k-1)d$ (nontrivial, if the elements are distinct)
- corner: $(a,b),(a+d,b),(a,b+d) \in \mathbb{F}_p^n \times \mathbb{F}_p^n$ (and $d \neq 0$)
- right angle: $(x,y,z) \in \mathbb{F}_p^n$ such that $\langle x-y, x-z\rangle = 0$ (and x,y,z are distinct)
- $(a,b),(a,b+d),(a+d,c),(a+d,c+d) \in \mathbb{F}_2^n \times \mathbb{F}_2^n$ (and $d \neq 0$)

What is the size of the largest set avoiding the given configuration?
Is it $(p-o(1))^n$ (or $(m-o(1))^n$)?
Is it $\leq (p-\varepsilon)^n$?
Is it $\leq n^{O(1)}$?

Different types of forbidden configurations in $\mathbb{F}_p^n$ (or $\mathbb{Z}_m^n$)

- k-AP: $a, a+d, \ldots, a+(k-1)d$ (nontrivial, if the elements are distinct)
- corner: $(a,b),(a+d,b),(a,b+d) \in \mathbb{F}_p^n \times \mathbb{F}_p^n$ (and $d \neq 0$)
- right angle: $(x,y,z) \in \mathbb{F}_p^n$ such that $\langle x-y, x-z\rangle = 0$ (and x,y,z are distinct)
- $(a,b),(a,b+d),(a+d,c),(a+d,c+d) \in \mathbb{F}_2^n \times \mathbb{F}_2^n$ (and $d \neq 0$)

What is the size of the largest set avoiding the given configuration?
Is it $(p-o(1))^n$ (or $(m-o(1))^n$)?
Is it $\leq (p-\varepsilon)^n$?
Is it $\leq n^{O(1)}$?

Different types of forbidden configurations in $\mathbb{F}_p^n$ (or $\mathbb{Z}_m^n$)

- k-AP: $a, a+d, \ldots, a+(k-1)d$ (nontrivial, if the elements are distinct)
- corner: $(a,b),(a+d,b),(a,b+d) \in \mathbb{F}_p^n \times \mathbb{F}_p^n$ (and $d \neq 0$)
- right angle: $(x,y,z) \in \mathbb{F}_p^n$ such that $\langle x-y, x-z\rangle = 0$ (and x,y,z are distinct)
- $(a,b),(a,b+d),(a+d,c),(a+d,c+d) \in \mathbb{F}_2^n \times \mathbb{F}_2^n$ (and $d \neq 0$)

What is the size of the largest set avoiding the given configuration?
Is it $(p-o(1))^n$ (or $(m-o(1))^n$)?
Is it $\leq (p-\varepsilon)^n$?
Is it $\leq n^{O(1)}$?

k-AP-free sets in $\mathbb{Z}_m^n$

$r_k(\mathbb{Z}_m^n) := \max\{|A| : \ A \subseteq \mathbb{Z}_m^n \text{ is } k\text{-AP-free}\}$

$k = 3$, $m = 3, 4$

$$2.217\ldots^n \leq r_3(\mathbb{Z}_3^n) \leq 2.755\ldots^n$$

$$3^n/\sqrt{n} \ll r_3(\mathbb{Z}_4^n) \leq 3.61\ldots^n$$

$k = 3$

For $m > 2$ we have $r_3(\mathbb{Z}_m^n) < (0.92m)^n$.

$m \geq k \geq 4$

Not known whether $r_k(\mathbb{Z}_m^n) = (m - o(1))^n$ or $r_k(\mathbb{Z}_m^n) \leq (m - \varepsilon)^n$ for some $\varepsilon > 0$.

k-AP-free sets in $\mathbb{Z}_m^n$

$r_k(\mathbb{Z}_m^n) := \max\{|A| : \ A \subseteq \mathbb{Z}_m^n \text{ is } k\text{-AP-free}\}$

$k = 3$, $m = 3, 4$

$$2.217\ldots^n \leq r_3(\mathbb{Z}_3^n) \leq 2.755\ldots^n$$

$$3^n/\sqrt{n} \ll r_3(\mathbb{Z}_4^n) \leq 3.61\ldots^n$$

$k = 3$

For $m > 2$ we have $r_3(\mathbb{Z}_m^n) < (0.92m)^n$.

$m \geq k \geq 4$

Not known whether $r_k(\mathbb{Z}_m^n) = (m - o(1))^n$ or $r_k(\mathbb{Z}_m^n) \leq (m - \varepsilon)^n$ for some $\varepsilon > 0$.

k-AP-free sets in $\mathbb{Z}_m^n$

$r_k(\mathbb{Z}_m^n) := \max\{|A| : \ A \subseteq \mathbb{Z}_m^n \text{ is } k\text{-AP-free}\}$

$k = 3$, $m = 3, 4$

$$2.217\ldots^n \leq r_3(\mathbb{Z}_3^n) \leq 2.755\ldots^n$$

$$3^n/\sqrt{n} \ll r_3(\mathbb{Z}_4^n) \leq 3.61\ldots^n$$

$k = 3$

For $m > 2$ we have $r_3(\mathbb{Z}_m^n) < (0.92m)^n$.

$m \geq k \geq 4$

Not known whether $r_k(\mathbb{Z}_m^n) = (m - o(1))^n$ or $r_k(\mathbb{Z}_m^n) \leq (m - \varepsilon)^n$ for some $\varepsilon > 0$.

3AP-free sets in $\mathbb{Z}_m^n$

- easy: For every $2 < m$ we have $r_3(\mathbb{Z}_m^n) \leq (m - c_m)^n$ (since m is either divisible by 4 or has an odd prime divisor), for instance, $r_3(\mathbb{Z}_{15}^n) \leq 5^n r_3(\mathbb{Z}_3^n)$ and also $r_3(\mathbb{Z}_{15}^n) \leq 3^n r_3(\mathbb{Z}_5^n)$
- $r_3(\mathbb{Z}_9^n) \leq 3^n r_3(\mathbb{Z}_3^n) \leq 8.268^n$, but from the method even better upper bounds can be obtained: $r_3(\mathbb{Z}_9^n) \leq 7.847^n$, furthermore, in the even case, $r_3(\mathbb{Z}_8^n) \leq 2^n r_3(\mathbb{Z}_4^n) \leq 7.222^n$ can be improved to $r_3(\mathbb{Z}_8^n) \leq 7.09^n$ (Petrov-Pohoata, 2020)
- $r_3(\mathbb{Z}_6^n) = 2^n r_3(\mathbb{Z}_3^n)$, the case $m \equiv 2 \pmod 4$ is equivalent to the odd case

3AP-free sets in $\mathbb{Z}_m^n$

- easy: For every $2 < m$ we have $r_3(\mathbb{Z}_m^n) \leq (m - c_m)^n$ (since m is either divisible by 4 or has an odd prime divisor), for instance, $r_3(\mathbb{Z}_{15}^n) \leq 5^n r_3(\mathbb{Z}_3^n)$ and also $r_3(\mathbb{Z}_{15}^n) \leq 3^n r_3(\mathbb{Z}_5^n)$
- $r_3(\mathbb{Z}_9^n) \leq 3^n r_3(\mathbb{Z}_3^n) \leq 8.268^n$, but from the method even better upper bounds can be obtained: $r_3(\mathbb{Z}_9^n) \leq 7.847^n$, furthermore, in the even case, $r_3(\mathbb{Z}_8^n) \leq 2^n r_3(\mathbb{Z}_4^n) \leq 7.222^n$ can be improved to $r_3(\mathbb{Z}_8^n) \leq 7.09^n$ (Petrov-Pohoata, 2020)
- $r_3(\mathbb{Z}_6^n) = 2^n r_3(\mathbb{Z}_3^n)$, the case $m \equiv 2 \pmod 4$ is equivalent to the odd case

3AP-free sets in $\mathbb{Z}_m^n$

- easy: For every $2 < m$ we have $r_3(\mathbb{Z}_m^n) \leq (m - c_m)^n$ (since m is either divisible by 4 or has an odd prime divisor), for instance, $r_3(\mathbb{Z}_{15}^n) \leq 5^n r_3(\mathbb{Z}_3^n)$ and also $r_3(\mathbb{Z}_{15}^n) \leq 3^n r_3(\mathbb{Z}_5^n)$
- $r_3(\mathbb{Z}_9^n) \leq 3^n r_3(\mathbb{Z}_3^n) \leq 8.268^n$, but from the method even better upper bounds can be obtained: $r_3(\mathbb{Z}_9^n) \leq 7.847^n$, furthermore, in the even case, $r_3(\mathbb{Z}_8^n) \leq 2^n r_3(\mathbb{Z}_4^n) \leq 7.222^n$ can be improved to $r_3(\mathbb{Z}_8^n) \leq 7.09^n$ (Petrov-Pohoata, 2020)
- $r_3(\mathbb{Z}_6^n) = 2^n r_3(\mathbb{Z}_3^n)$, the case $m \equiv 2 \pmod 4$ is equivalent to the odd case

3AP-free sets in $\mathbb{Z}_m^n$

- easy: For every $2 < m$ we have $r_3(\mathbb{Z}_m^n) \leq (m - c_m)^n$ (since m is either divisible by 4 or has an odd prime divisor), for instance, $r_3(\mathbb{Z}_{15}^n) \leq 5^n r_3(\mathbb{Z}_3^n)$ and also $r_3(\mathbb{Z}_{15}^n) \leq 3^n r_3(\mathbb{Z}_5^n)$
- $r_3(\mathbb{Z}_9^n) \leq 3^n r_3(\mathbb{Z}_3^n) \leq 8.268^n$, but from the method even better upper bounds can be obtained: $r_3(\mathbb{Z}_9^n) \leq 7.847^n$, furthermore, in the even case, $r_3(\mathbb{Z}_8^n) \leq 2^n r_3(\mathbb{Z}_4^n) \leq 7.222^n$ can be improved to $r_3(\mathbb{Z}_8^n) \leq 7.09^n$ (Petrov-Pohoata, 2020)
- $r_3(\mathbb{Z}_6^n) = 2^n r_3(\mathbb{Z}_3^n)$, the case $m \equiv 2 \pmod 4$ is equivalent to the odd case

3AP-free sets in $\mathbb{Z}_m^n$

- easy: For every $2 < m$ we have $r_3(\mathbb{Z}_m^n) \leq (m - c_m)^n$ (since m is either divisible by 4 or has an odd prime divisor), for instance, $r_3(\mathbb{Z}_{15}^n) \leq 5^n r_3(\mathbb{Z}_3^n)$ and also $r_3(\mathbb{Z}_{15}^n) \leq 3^n r_3(\mathbb{Z}_5^n)$
- $r_3(\mathbb{Z}_9^n) \leq 3^n r_3(\mathbb{Z}_3^n) \leq 8.268^n$, but from the method even better upper bounds can be obtained: $r_3(\mathbb{Z}_9^n) \leq 7.847^n$, furthermore, in the even case, $r_3(\mathbb{Z}_8^n) \leq 2^n r_3(\mathbb{Z}_4^n) \leq 7.222^n$ can be improved to $r_3(\mathbb{Z}_8^n) \leq 7.09^n$ (Petrov-Pohoata, 2020)
- $r_3(\mathbb{Z}_6^n) = 2^n r_3(\mathbb{Z}_3^n)$, the case $m \equiv 2 \pmod 4$ is equivalent to the odd case

3AP-free sets in $\mathbb{Z}_m^n$

- easy: For every $2 < m$ we have $r_3(\mathbb{Z}_m^n) \leq (m - c_m)^n$ (since m is either divisible by 4 or has an odd prime divisor), for instance, $r_3(\mathbb{Z}_{15}^n) \leq 5^n r_3(\mathbb{Z}_3^n)$ and also $r_3(\mathbb{Z}_{15}^n) \leq 3^n r_3(\mathbb{Z}_5^n)$
- $r_3(\mathbb{Z}_9^n) \leq 3^n r_3(\mathbb{Z}_3^n) \leq 8.268^n$, but from the method even better upper bounds can be obtained: $r_3(\mathbb{Z}_9^n) \leq 7.847^n$, furthermore, in the even case, $r_3(\mathbb{Z}_8^n) \leq 2^n r_3(\mathbb{Z}_4^n) \leq 7.222^n$ can be improved to $r_3(\mathbb{Z}_8^n) \leq 7.09^n$ (Petrov-Pohoata, 2020)
- $r_3(\mathbb{Z}_6^n) = 2^n r_3(\mathbb{Z}_3^n)$, the case $m \equiv 2 \pmod 4$ is equivalent to the odd case

3AP-free sets in $\mathbb{Z}_m^n$

- easy: For every $2 < m$ we have $r_3(\mathbb{Z}_m^n) \leq (m - c_m)^n$ (since m is either divisible by 4 or has an odd prime divisor), for instance, $r_3(\mathbb{Z}_{15}^n) \leq 5^n r_3(\mathbb{Z}_3^n)$ and also $r_3(\mathbb{Z}_{15}^n) \leq 3^n r_3(\mathbb{Z}_5^n)$

- $r_3(\mathbb{Z}_9^n) \leq 3^n r_3(\mathbb{Z}_3^n) \leq 8.268^n$, but from the method even better upper bounds can be obtained: $r_3(\mathbb{Z}_9^n) \leq 7.847^n$, furthermore, in the even case, $r_3(\mathbb{Z}_8^n) \leq 2^n r_3(\mathbb{Z}_4^n) \leq 7.222^n$ can be improved to $r_3(\mathbb{Z}_8^n) \leq 7.09^n$ (Petrov-Pohoata, 2020)

- $r_3(\mathbb{Z}_6^n) = 2^n r_3(\mathbb{Z}_3^n)$, the case $m \equiv 2 \pmod 4$ is equivalent to the odd case

6AP-free sets in $\mathbb{Z}_6^n$

What can we say about $\lim \sqrt[n]{r_6(\mathbb{Z}_6^n)}$?

- Is it 6 or less than 6?
- Does this limit exist?

The product construction doesn't work here.

$\{0,1,2,3,4\} \subseteq \mathbb{Z}_6$ is 6AP-free, but
$\{0,1,2,3,4\} \times \{0,1,2,3,4\} \subseteq \mathbb{Z}_6^2$ contains (e.g.) the following 6AP:

$$(0,0), (2,3), (4,0), (0,3), (2,0), (4,3)$$

$r_6(\mathbb{Z}_6^2) = ?$

6AP-free sets in $\mathbb{Z}_6^n$

What can we say about $\lim \sqrt[n]{r_6(\mathbb{Z}_6^n)}$?

- Is it 6 or less than 6?
- Does this limit exist?

The product construction doesn't work here.

$\{0,1,2,3,4\} \subseteq \mathbb{Z}_6$ is 6AP-free, but
$\{0,1,2,3,4\} \times \{0,1,2,3,4\} \subseteq \mathbb{Z}_6^2$ contains (e.g.) the following 6AP:

$$(0,0), (2,3), (4,0), (0,3), (2,0), (4,3)$$

$r_6(\mathbb{Z}_6^2) = ?$

6AP-free sets in $\mathbb{Z}_6^n$

What can we say about $\lim \sqrt[n]{r_6(\mathbb{Z}_6^n)}$?

- Is it 6 or less than 6?
- Does this limit exist?

The product construction doesn't work here.

$\{0,1,2,3,4\} \subseteq \mathbb{Z}_6$ is 6AP-free, but
$\{0,1,2,3,4\} \times \{0,1,2,3,4\} \subseteq \mathbb{Z}_6^2$ contains (e.g.) the following 6AP:

$$(0,0), (2,3), (4,0), (0,3), (2,0), (4,3)$$

$r_6(\mathbb{Z}_6^2) =?$

6AP-free sets in $\mathbb{Z}_6^n$

What can we say about $\lim \sqrt[n]{r_6(\mathbb{Z}_6^n)}$?

- Is it 6 or less than 6?
- Does this limit exist?

The product construction doesn't work here.

$\{0,1,2,3,4\} \subseteq \mathbb{Z}_6$ is 6AP-free, but
$\{0,1,2,3,4\} \times \{0,1,2,3,4\} \subseteq \mathbb{Z}_6^2$ contains (e.g.) the following 6AP:

$$(0,0), (2,3), (4,0), (0,3), (2,0), (4,3)$$

$r_6(\mathbb{Z}_6^2) = ?$

6AP-free sets in $\mathbb{Z}_6^n$

What can we say about $\lim \sqrt[n]{r_6(\mathbb{Z}_6^n)}$?

- Is it 6 or less than 6?
- Does this limit exist?

The product construction doesn't work here.

$\{0,1,2,3,4\} \subseteq \mathbb{Z}_6$ is 6AP-free, but
$\{0,1,2,3,4\} \times \{0,1,2,3,4\} \subseteq \mathbb{Z}_6^2$ contains (e.g.) the following 6AP:

$$(0,0), (2,3), (4,0), (0,3), (2,0), (4,3)$$

$r_6(\mathbb{Z}_6^2) = ?$

6AP-free sets in $\mathbb{Z}_6^n$

What can we say about $\lim \sqrt[n]{r_6(\mathbb{Z}_6^n)}$?

- Is it 6 or less than 6?
- Does this limit exist?

The product construction doesn't work here.

$\{0,1,2,3,4\} \subseteq \mathbb{Z}_6$ is 6AP-free, but
$\{0,1,2,3,4\} \times \{0,1,2,3,4\} \subseteq \mathbb{Z}_6^2$ contains (e.g.) the following 6AP:

$$(0,0),(2,3),(4,0),(0,3),(2,0),(4,3)$$

$r_6(\mathbb{Z}_6^2) =?$

6AP-free sets in $\mathbb{Z}_6^n$

What can we say about $\lim \sqrt[n]{r_6(\mathbb{Z}_6^n)}$?

- Is it 6 or less than 6?
- Does this limit exist?

The product construction doesn't work here.

$\{0,1,2,3,4\} \subseteq \mathbb{Z}_6$ is 6AP-free, but
$\{0,1,2,3,4\} \times \{0,1,2,3,4\} \subseteq \mathbb{Z}_6^2$ contains (e.g.) the following 6AP:

$$(0,0),(2,3),(4,0),(0,3),(2,0),(4,3)$$

$r_6(\mathbb{Z}_6^2) = ?$

6AP-free sets in $\mathbb{Z}_6^n$

What can we say about $\lim \sqrt[n]{r_6(\mathbb{Z}_6^n)}$?

- Is it 6 or less than 6?
- Does this limit exist?

The product construction doesn't work here.

$\{0,1,2,3,4\} \subseteq \mathbb{Z}_6$ is 6AP-free, but
$\{0,1,2,3,4\} \times \{0,1,2,3,4\} \subseteq \mathbb{Z}_6^n$ contains (e.g.) the following 6AP:

$$(0,0),(2,3),(4,0),(0,3),(2,0),(4,3)$$

Proposition (P., Palincza, 2020+)

$r_6(\mathbb{Z}_6^2) = 25$

6AP-free sets in $\mathbb{Z}_6^n$

Proposition (P., Palincza, 2020+)

$r_6(\mathbb{Z}_6^2) = 25$

Reformulation

The maximal total size of 2^n subsets $A_i \subseteq \mathbb{Z}_3^n$ such that each 3AP is contained in at most one of these subsets is $r_6(\mathbb{Z}_6^n)$.

$A_1, A_2, A_3, A_4 \subseteq \mathbb{Z}_3^2$ such that $A_i \cap A_j$ is 3AP-free for every $i \neq j$.

Construction

A_1 A_2 A_3 A_4

6AP-free sets in $\mathbb{Z}_6^n$

Proposition (P., Palincza, 2020+)

$r_6(\mathbb{Z}_6^2) = 25$

Reformulation

The maximal total size of 2^n subsets $A_i \subseteq \mathbb{Z}_3^n$ such that each 3AP is contained in at most one of these subsets is $r_6(\mathbb{Z}_6^n)$.

$A_1, A_2, A_3, A_4 \subseteq \mathbb{Z}_3^2$ such that $A_i \cap A_j$ is 3AP-free for every $i \neq j$.

Construction

6AP-free sets in $\mathbb{Z}_6^n$

Proposition (P., Palincza, 2020+)

$r_6(\mathbb{Z}_6^2) = 25$

Reformulation

The maximal total size of 2^n subsets $A_i \subseteq \mathbb{Z}_3^n$ such that each 3AP is contained in at most one of these subsets is $r_6(\mathbb{Z}_6^n)$.

$A_1, A_2, A_3, A_4 \subseteq \mathbb{Z}_3^2$ such that $A_i \cap A_j$ is 3AP-free for every $i \neq j$.

Construction

6AP-free sets in $\mathbb{Z}_6^n$

Proposition (P., Palincza, 2020+)

$r_6(\mathbb{Z}_6^2) = 25$

Reformulation

The maximal total size of 2^n subsets $A_i \subseteq \mathbb{Z}_3^n$ such that each 3AP is contained in at most one of these subsets is $r_6(\mathbb{Z}_6^n)$.

$A_1, A_2, A_3, A_4 \subseteq \mathbb{Z}_3^2$ such that $A_i \cap A_j$ is 3AP-free for every $i \neq j$.

Construction

o	o	
o	o	
o	o	o

A_1

o	o	o
o	o	o

A_2

o		o
	o	o
o	o	

A_3

	o	o
o		o
o	o	

A_4

6AP-free sets in $\mathbb{Z}_6^n$

Proposition

$r_6(\mathbb{Z}_6^2) = 25$

$A_1, A_2, A_3, A_4 \subseteq \mathbb{Z}_3^2$ such that $A_i \cap A_j$ is 3AP-free for every $i \neq j$.

size of A	0	1	2	3	4	5	6	7	8	9
min #3AP in A	0	0	0	0	0	1	2	5	8	12

IP (x_i: number of i-element subsets)

$$\max x_1 + 2x_2 + 3x_3 + 4x_4 + 5x_5 + 6x_6 + 7x_7 + 8x_8 + 9x_9$$

subject to

$$x_0 + x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 + x_8 + x_9 = 4$$

$$x_5 + 2x_6 + 5x_7 + 8x_8 + 12x_9 \leq 12$$

$x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9$: nonnegative integers

6AP-free sets in $\mathbb{Z}_6^n$

Proposition

$r_6(\mathbb{Z}_6^2) = 25$

$A_1, A_2, A_3, A_4 \subseteq \mathbb{Z}_3^2$ such that $A_i \cap A_j$ is 3AP-free for every $i \neq j$.

size of A	0	1	2	3	4	5	6	7	8	9
min #3AP in A	0	0	0	0	0	1	2	5	8	12

IP (x_i: number of i-element subsets)

$$\max x_1 + 2x_2 + 3x_3 + 4x_4 + 5x_5 + 6x_6 + 7x_7 + 8x_8 + 9x_9$$

subject to

$$x_0 + x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 + x_8 + x_9 = 4$$

$$x_5 + 2x_6 + 5x_7 + 8x_8 + 12x_9 \leq 12$$

$x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9$: nonnegative integers

6AP-free sets in $\mathbb{Z}_6^n$

Proposition

$r_6(\mathbb{Z}_6^2) = 25$

$A_1, A_2, A_3, A_4 \subseteq \mathbb{Z}_3^2$ such that $A_i \cap A_j$ is 3AP-free for every $i \neq j$.

size of A	0	1	2	3	4	5	6	7	8	9
min #3AP in A	0	0	0	0	0	1	2	5	8	12

IP (x_i: number of i-element subsets)

$$\max x_1 + 2x_2 + 3x_3 + 4x_4 + 5x_5 + 6x_6 + 7x_7 + 8x_8 + 9x_9$$

subject to

$$x_0 + x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 + x_8 + x_9 = 4$$

$$x_5 + 2x_6 + 5x_7 + 8x_8 + 12x_9 \leq 12$$

$x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9$: nonnegative integers

6AP-free sets in $\mathbb{Z}_6^n$

Proposition

$r_6(\mathbb{Z}_6^2) = 25$

$A_1, A_2, A_3, A_4 \subseteq \mathbb{Z}_3^2$ such that $A_i \cap A_j$ is 3AP-free for every $i \neq j$.

size of A	0	1	2	3	4	5	6	7	8	9
min #3AP in A	0	0	0	0	0	1	2	5	8	12

IP (x_i: number of i-element subsets)

$$\max x_1 + 2x_2 + 3x_3 + 4x_4 + 5x_5 + 6x_6 + 7x_7 + 8x_8 + 9x_9$$

subject to

$$x_0 + x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 + x_8 + x_9 = 4$$

$$x_5 + 2x_6 + 5x_7 + 8x_8 + 12x_9 \leq 12$$

$x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9$: nonnegative integers

6AP-free sets in $\mathbb{Z}_6^n$

Proposition (P., Palincza, 2020+)

$r_6(\mathbb{Z}_6^2) = 25$

IP (x_i: the number of i-element subsets)

$$\max x_1 + 2x_2 + 3x_3 + 4x_4 + 5x_5 + 6x_6 + 7x_7 + 8x_8 + 9x_9$$

subject to

$$x_0 + x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 + x_8 + x_9 = 4$$

$$x_5 + 2x_6 + 5x_7 + 8x_8 + 12x_9 \leq 12$$

$x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9$: nonnegative integers

Optimum=25

$x_6 = 3, x_7 = 1$

6AP-free sets in $\mathbb{Z}_6^n$

Proposition (P., Palincza, 2020+)

$r_6(\mathbb{Z}_6^2) = 25$

Optimum=25

$x_6 = 3, x_7 = 1$

Construction (unique)

o	o	
o	o	
o	o	o

A_1

o	o	o
o	o	o

A_2

o		o
	o	o
o	o	

A_3

	o	o
o		o
o	o	

A_4

6AP-free sets in $\mathbb{Z}_6^n$

- $r_6(\mathbb{Z}_6) = 5$
- $r_6(\mathbb{Z}_6^2) = 25$
- $116 \leq r_6(\mathbb{Z}_6^3) \leq 124$

Theorem (P., Palincza, 2020+)

$r_6(\mathbb{Z}_6^n) \leq 5.709^n$

$r_6(\mathbb{Z}_6^n) \leq 2^{n+1}\sqrt{3^n r_3(\mathbb{Z}_3^n)}$

$r_6(\mathbb{Z}_6^n) \geq r_3(\mathbb{Z}_6^n) \geq 4.434^n$

Sketch: $\sum |A(x)|$ is large $\longrightarrow$ $\exists$ lot of large $A(x)$ $\longrightarrow$ these contain too many 3AP's

6AP-free sets in $\mathbb{Z}_6^n$

- $r_6(\mathbb{Z}_6) = 5$
- $r_6(\mathbb{Z}_6^2) = 25$
- $116 \leq r_6(\mathbb{Z}_6^3) \leq 124$

Theorem (P., Palincza, 2020+)

$r_6(\mathbb{Z}_6^n) \leq 5.709^n$

$r_6(\mathbb{Z}_6^n) \leq 2^{n+1}\sqrt{3^n r_3(\mathbb{Z}_3^n)}$

$r_6(\mathbb{Z}_6^n) \geq r_3(\mathbb{Z}_6^n) \geq 4.434^n$

Sketch: $\sum |A(x)|$ is large $\longrightarrow$ $\exists$ lot of large $A(x)$ $\longrightarrow$ these contain too many 3AP's

6AP-free sets in $\mathbb{Z}_6^n$

- $r_6(\mathbb{Z}_6) = 5$
- $r_6(\mathbb{Z}_6^2) = 25$
- $116 \leq r_6(\mathbb{Z}_6^3) \leq 124$

Theorem (P., Palincza, 2020+)

$r_6(\mathbb{Z}_6^n) \leq 5.709^n$

$r_6(\mathbb{Z}_6^n) \leq 2^{n+1}\sqrt{3^n r_3(\mathbb{Z}_3^n)}$

$r_6(\mathbb{Z}_6^n) \geq r_3(\mathbb{Z}_6^n) \geq 4.434^n$

Sketch: $\sum |A(x)|$ is large $\longrightarrow$ $\exists$ lot of large $A(x)$ $\longrightarrow$ these contain too many 3AP's

6AP-free sets in $\mathbb{Z}_6^n$

- $r_6(\mathbb{Z}_6) = 5$
- $r_6(\mathbb{Z}_6^2) = 25$
- $116 \leq r_6(\mathbb{Z}_6^3) \leq 124$

Theorem (P., Palincza, 2020+)

$r_6(\mathbb{Z}_6^n) \leq 5.709^n$

$r_6(\mathbb{Z}_6^n) \leq 2^{n+1}\sqrt{3^n r_3(\mathbb{Z}_3^n)}$

$r_6(\mathbb{Z}_6^n) \geq r_3(\mathbb{Z}_6^n) \geq 4.434^n$

Sketch: $\sum |A(x)|$ is large $\longrightarrow$ $\exists$ lot of large $A(x)$ $\longrightarrow$ these contain too many 3AP's

6AP-free sets in $\mathbb{Z}_6^n$

- $r_6(\mathbb{Z}_6) = 5$
- $r_6(\mathbb{Z}_6^2) = 25$
- $116 \leq r_6(\mathbb{Z}_6^3) \leq 124$

Theorem (P., Palincza, 2020+)

$r_6(\mathbb{Z}_6^n) \leq 5.709^n$

$r_6(\mathbb{Z}_6^n) \leq 2^{n+1}\sqrt{3^n r_3(\mathbb{Z}_3^n)}$

$r_6(\mathbb{Z}_6^n) \geq r_3(\mathbb{Z}_6^n) \geq 4.434^n$

Sketch: $\sum |A(x)|$ is large $\Longrightarrow$ $\exists$ lot of large $A(x)$ $\Longrightarrow$ these contain too many 3AP's

6AP-free sets in $\mathbb{Z}_6^n$

- $r_6(\mathbb{Z}_6) = 5$
- $r_6(\mathbb{Z}_6^2) = 25$
- $116 \leq r_6(\mathbb{Z}_6^3) \leq 124$

Theorem (P., Palincza, 2020+)

$r_6(\mathbb{Z}_6^n) \leq 5.709^n$

$r_6(\mathbb{Z}_6^n) \leq 2^{n+1}\sqrt{3^n r_3(\mathbb{Z}_3^n)}$

$r_6(\mathbb{Z}_6^n) \geq r_3(\mathbb{Z}_6^n) \geq 4.434^n$

Sketch: $\sum |A(x)|$ is large $\Longrightarrow$ $\exists$ lot of large $A(x)$ $\Longrightarrow$ these contain too many 3AP's

6AP-free sets in $\mathbb{Z}_6^n$

- $r_6(\mathbb{Z}_6) = 5$
- $r_6(\mathbb{Z}_6^2) = 25$
- $116 \leq r_6(\mathbb{Z}_6^3) \leq 124$

Theorem (P., Palincza, 2020+)

$r_6(\mathbb{Z}_6^n) \leq 5.709^n$
$r_6(\mathbb{Z}_6^n) \leq 2^{n+1}\sqrt{3^n r_3(\mathbb{Z}_3^n)}$
$r_6(\mathbb{Z}_6^n) \geq r_3(\mathbb{Z}_6^n) \geq 4.434^n$

Sketch: $\sum |A(x)|$ is large $\Longrightarrow$ $\exists$ lot of large $A(x)$ $\Longrightarrow$ these contain too many 3AP's

6AP-free sets in $\mathbb{Z}_6^n$

- $r_6(\mathbb{Z}_6) = 5$
- $r_6(\mathbb{Z}_6^2) = 25$
- $116 \leq r_6(\mathbb{Z}_6^3) \leq 124$

Theorem (P., Palincza, 2020+)

$r_6(\mathbb{Z}_6^n) \leq 5.709^n$
$r_6(\mathbb{Z}_6^n) \leq 2^{n+1}\sqrt{3^n r_3(\mathbb{Z}_3^n)}$
$r_6(\mathbb{Z}_6^n) \geq r_3(\mathbb{Z}_6^n) \geq 4.434^n$

Sketch: $\sum |A(x)|$ is large $\implies$ $\exists$ lot of large $A(x)$ $\implies$ these contain too many 3AP's

k-AP-free sets in $\mathbb{Z}_m^n$

Corollary

For $6 \mid m$ and $k \in \{4, 5, 6\}$ we have $r_k(\mathbb{Z}_m^n) \leq (0.948m)^n$.

$m \geq k \geq 3$

$r_k(\mathbb{Z}_m^n)$ is exponentially smaller than m^n for:

- $k = 3, 3 \leq m$ arbitrary
- $k \in \{4, 5, 6\}, 6 \mid m$
- ???

$r_k(\mathbb{Z}_m^n) = (m - o(1))^n$ for:

- ???

k-AP-free sets in $\mathbb{Z}_m^n$

Corollary

For $6 \mid m$ and $k \in \{4, 5, 6\}$ we have $r_k(\mathbb{Z}_m^n) \leq (0.948m)^n$.

$m \geq k \geq 3$

$r_k(\mathbb{Z}_m^n)$ is exponentially smaller than m^n for:

- $k = 3$, $3 \leq m$ arbitrary
- $k \in \{4, 5, 6\}$, $6 \mid m$
- ???

$r_k(\mathbb{Z}_m^n) = (m - o(1))^n$ for:

- ???

k-AP-free sets in $\mathbb{Z}_m^n$

Corollary

For $6 \mid m$ and $k \in \{4, 5, 6\}$ we have $r_k(\mathbb{Z}_m^n) \leq (0.948m)^n$.

$m \geq k \geq 3$

$r_k(\mathbb{Z}_m^n)$ is exponentially smaller than m^n for:

- $k = 3$, $3 \leq m$ arbitrary
- $k \in \{4, 5, 6\}$, $6 \mid m$
- ???

$r_k(\mathbb{Z}_m^n) = (m - o(1))^n$ for:

- ???

k-AP-free sets in $\mathbb{Z}_m^n$

Corollary

For $6 \mid m$ and $k \in \{4, 5, 6\}$ we have $r_k(\mathbb{Z}_m^n) \leq (0.948m)^n$.

$m \geq k \geq 3$

$r_k(\mathbb{Z}_m^n)$ is exponentially smaller than m^n for:

- $k = 3$, $3 \leq m$ arbitrary
- $k \in \{4, 5, 6\}$, $6 \mid m$
- ???

$r_k(\mathbb{Z}_m^n) = (m - o(1))^n$ for:

- ???

k-AP-free sets in $\mathbb{Z}_m^n$

Corollary

For $6 \mid m$ and $k \in \{4, 5, 6\}$ we have $r_k(\mathbb{Z}_m^n) \leq (0.948m)^n$.

$m \geq k \geq 3$

$r_k(\mathbb{Z}_m^n)$ is exponentially smaller than m^n for:

- $k = 3$, $3 \leq m$ arbitrary
- $k \in \{4, 5, 6\}$, $6 \mid m$
- ???

$r_k(\mathbb{Z}_m^n) = (m - o(1))^n$ for:

- ???

k-AP-free sets in $\mathbb{Z}_m^n$

Corollary

For $6 \mid m$ and $k \in \{4, 5, 6\}$ we have $r_k(\mathbb{Z}_m^n) \leq (0.948m)^n$.

$m \geq k \geq 3$

$r_k(\mathbb{Z}_m^n)$ is exponentially smaller than m^n for:

- $k = 3$, $3 \leq m$ arbitrary
- $k \in \{4, 5, 6\}$, $6 \mid m$
- ???

$r_k(\mathbb{Z}_m^n) = (m - o(1))^n$ for:

- ???

Right angles in $\mathbb{F}_q^n$

How large can $A \subseteq \mathbb{F}_q^n$ be if A does not contain a right angle, i.e. a triple x, y, z of distinct vectors such that $\langle x - z, y - z \rangle = 0$? Extremal size: $R(n, q)$. From now on, q: odd prime.

Theorem (Bennett, 2018)

$$R(n, q) \ll q^{\frac{n+2}{3}}$$

Theorem (Ge-Shangguan, 2019)

$$R(n, q) \leq \binom{n+q}{q-1} + 3$$

Conjecture (Ge-Shangguan)

$$R(n, q) = \Theta(n^{q-1})$$

Theorem (Naslund, 2020)

$$R(n, q) \leq \binom{n+q}{q-1} + 2 - \binom{n+q}{q-3}$$

Right angles in $\mathbb{F}_q^n$

How large can $A \subseteq \mathbb{F}_q^n$ be if A does not contain a right angle, i.e. a triple x, y, z of distinct vectors such that $\langle x - z, y - z \rangle = 0$? Extremal size: $R(n, q)$. From now on, q: odd prime.

Theorem (Bennett, 2018)

$$R(n, q) \ll q^{\frac{n+2}{3}}$$

Theorem (Ge-Shangguan, 2019)

$$R(n, q) \leq \binom{n+q}{q-1} + 3$$

Conjecture (Ge-Shangguan)

$$R(n, q) = \Theta(n^{q-1})$$

Theorem (Naslund, 2020)

$$R(n, q) \leq \binom{n+q}{q-1} + 2 - \binom{n+q}{q-3}$$

Right angles in $\mathbb{F}_q^n$

How large can $A \subseteq \mathbb{F}_q^n$ be if A does not contain a right angle, i.e. a triple x, y, z of distinct vectors such that $\langle x - z, y - z \rangle = 0$?
Extremal size: $R(n, q)$. From now on, q: odd prime.

Theorem (Bennett, 2018)

$$R(n, q) \ll q^{\frac{n+2}{3}}$$

Theorem (Ge-Shangguan, 2019)

$$R(n, q) \leq \binom{n+q}{q-1} + 3$$

Conjecture (Ge-Shangguan)

$$R(n, q) = \Theta(n^{q-1})$$

Theorem (Naslund, 2020)

$$R(n, q) \leq \binom{n+q}{q-1} + 2 - \binom{n+q}{q-3}$$

Right angles in $\mathbb{F}_q^n$

How large can $A \subseteq \mathbb{F}_q^n$ be if A does not contain a right angle, i.e. a triple x, y, z of distinct vectors such that $\langle x - z, y - z \rangle = 0$? Extremal size: $R(n, q)$. From now on, q: odd prime.

Theorem (Bennett, 2018)

$$R(n, q) \ll q^{\frac{n+2}{3}}$$

Theorem (Ge-Shangguan, 2019)

$$R(n, q) \leq \binom{n+q}{q-1} + 3$$

Conjecture (Ge-Shangguan)

$$R(n, q) = \Theta(n^{q-1})$$

Theorem (Naslund, 2020)

$$R(n, q) \leq \binom{n+q}{q-1} + 2 - \binom{n+q}{q-3}$$

Right angles in $\mathbb{F}_q^n$

Conjecture (Ge-Shangguan)

$R(n,q) = \Theta(n^{q-1})$

Theorem (Naslund, 2020)

$R(n,q) \leq \binom{n+q}{q-1} + 2 - \binom{n+q}{q-3}$

Lower bound: $R(n,q) \geq n$.

Theorem (Bursics, Matolcsi, P., Schrettner, 2020+)

$R(n,q) \ll n^{q-2}$

Theorem (Bursics, Matolcsi, P., Schrettner, 2020+)

$R(n,q) \geq (1-o(1)) \cdot \binom{n}{\lceil \frac{1}{2}\lfloor \frac{2}{3}q \rfloor \rceil} \Big/ \binom{\lfloor \frac{2}{3}q \rfloor}{\lceil \frac{1}{2}\lfloor \frac{2}{3}q \rfloor \rceil}$, that is,

$R(n,q) \gg n^{(q-1)/3}$

Right angles in $\mathbb{F}_q^n$

Conjecture (Ge-Shangguan)

$R(n,q) = \Theta(n^{q-1})$

Theorem (Naslund, 2020)

$R(n,q) \leq \binom{n+q}{q-1} + 2 - \binom{n+q}{q-3}$

Lower bound: $R(n,q) \geq n$.

Theorem (Bursics, Matolcsi, P., Schrettner, 2020+)

$R(n,q) \ll n^{q-2}$

Theorem (Bursics, Matolcsi, P., Schrettner, 2020+)

$R(n,q) \geq (1-o(1)) \cdot \binom{n}{\lceil \frac{1}{2}\lfloor \frac{2}{3}q \rfloor \rceil} \Big/ \binom{\lfloor \frac{2}{3}q \rfloor}{\lceil \frac{1}{2}\lfloor \frac{2}{3}q \rfloor \rceil}$, that is,

$R(n,q) \gg n^{(q-1)/3}$

Right angles in $\mathbb{F}_q^n$

Conjecture (Ge-Shangguan)

$R(n,q) = \Theta(n^{q-1})$

Theorem (Naslund, 2020)

$R(n,q) \leq \binom{n+q}{q-1} + 2 - \binom{n+q}{q-3}$

Lower bound: $R(n,q) \geq n$.

Theorem (Bursics, Matolcsi, P., Schrettner, 2020+)

$R(n,q) \ll n^{q-2}$

Theorem (Bursics, Matolcsi, P., Schrettner, 2020+)

$R(n,q) \geq (1-o(1)) \cdot \binom{n}{\lceil \frac{1}{2}\lfloor \frac{2}{3}q \rfloor \rceil} \Big/ \binom{\lfloor \frac{2}{3}q \rfloor}{\lceil \frac{1}{2}\lfloor \frac{2}{3}q \rfloor \rceil}$, that is,

$R(n,q) \gg n^{(q-1)/3}$

Right angles in $\mathbb{F}_q^n$

Conjecture (Ge-Shangguan)

$R(n,q) = \Theta(n^{q-1})$

Theorem (Naslund, 2020)

$R(n,q) \leq \binom{n+q}{q-1} + 2 - \binom{n+q}{q-3}$

Lower bound: $R(n,q) \geq n$.

Theorem (Bursics, Matolcsi, P., Schrettner, 2020+)

$R(n,q) \ll n^{q-2}$

Theorem (Bursics, Matolcsi, P., Schrettner, 2020+)

$R(n,q) \geq (1-o(1)) \cdot \binom{n}{\lceil \frac{1}{2}\lfloor \frac{2}{3}q \rfloor \rceil} \Big/ \binom{\lfloor \frac{2}{3}q \rfloor}{\lceil \frac{1}{2}\lfloor \frac{2}{3}q \rfloor \rceil}$, that is,

$R(n,q) \gg n^{(q-1)/3}$

Right angles in $\mathbb{F}_q^n$

Theorem (Bursics, Matolcsi, P., Schrettner, 2020+)

$R(n,q) \ll n^{q-2}$

Theorem (Bursics, Matolcsi, P., Schrettner, 2020+)

$R(n,q) \geq (1-o(1)) \cdot \binom{n}{\lceil \frac{1}{2}\lfloor \frac{2}{3}q \rfloor \rceil} \Big/ \binom{\lfloor \frac{2}{3}q \rfloor}{\lceil \frac{1}{2}\lfloor \frac{2}{3}q \rfloor \rceil}$, that is,

$R(n,q) \gg n^{(q-1)/3}$

Construction

- $S = (q/3, 2q/3) \subseteq \mathbb{F}_q$: sum-free
- $A \subseteq \mathbb{F}_q^n$ satisfies $\langle a,a \rangle = 0$ for every $a \in A$ and $\langle a,b \rangle \in S$ for every $a \neq b$, $a,b \in A$
- Then A is free of right angles:
  $\langle x-z, y-z \rangle = \langle x,y \rangle - (\langle x,z \rangle + \langle z,y \rangle) \neq 0.$

Right angles in $\mathbb{F}_q^n$

Theorem (Bursics, Matolcsi, P., Schrettner, 2020+)

$R(n,q) \ll n^{q-2}$

Theorem (Bursics, Matolcsi, P., Schrettner, 2020+)

$R(n,q) \geq (1-o(1)) \cdot \binom{n}{\left\lceil \frac{1}{2}\left\lfloor \frac{2}{3}q \right\rfloor \right\rceil} \Big/ \binom{\left\lfloor \frac{2}{3}q \right\rfloor}{\left\lceil \frac{1}{2}\left\lfloor \frac{2}{3}q \right\rfloor \right\rceil}$, that is,

$R(n,q) \gg n^{(q-1)/3}$

Construction

- $S = (q/3, 2q/3) \subseteq \mathbb{F}_q$: sum-free
- $A \subseteq \mathbb{F}_q^n$ satisfies $\langle a,a \rangle = 0$ for every $a \in A$ and $\langle a,b \rangle \in S$ for every $a \neq b$, $a,b \in A$
- Then A is free of right angles:
  $\langle x-z, y-z \rangle = \langle x,y \rangle - (\langle x,z \rangle + \langle z,y \rangle) \neq 0.$

Right angles in $\mathbb{F}_q^n$

Theorem (Bursics, Matolcsi, P., Schrettner, 2020+)

$R(n,q) \ll n^{q-2}$

Theorem (Bursics, Matolcsi, P., Schrettner, 2020+)

$R(n,q) \geq (1-o(1)) \cdot \binom{n}{\lceil \frac{1}{2}\lfloor \frac{2}{3}q \rfloor \rceil} \Big/ \binom{\lfloor \frac{2}{3}q \rfloor}{\lceil \frac{1}{2}\lfloor \frac{2}{3}q \rfloor \rceil}$, that is,

$R(n,q) \gg n^{(q-1)/3}$

Construction

- $S = (q/3, 2q/3) \subseteq \mathbb{F}_q$: sum-free
- $A \subseteq \mathbb{F}_q^n$ satisfies $\langle a,a \rangle = 0$ for every $a \in A$ and $\langle a,b \rangle \in S$ for every $a \neq b$, $a,b \in A$
- Then A is free of right angles:
  $\langle x-z, y-z \rangle = \langle x,y \rangle - (\langle x,z \rangle + \langle z,y \rangle) \neq 0.$

Right angles in $\mathbb{F}_q^n$

Theorem (Bursics, Matolcsi, P., Schrettner, 2020+)

$R(n,q) \ll n^{q-2}$

Theorem (Bursics, Matolcsi, P., Schrettner, 2020+)

$R(n,q) \geq (1-o(1)) \cdot \binom{n}{\lceil \frac{1}{2}\lfloor \frac{2}{3}q \rfloor \rceil} \Big/ \binom{\lfloor \frac{2}{3}q \rfloor}{\lceil \frac{1}{2}\lfloor \frac{2}{3}q \rfloor \rceil}$, that is,

$R(n,q) \gg n^{(q-1)/3}$

Construction

- $S = (q/3, 2q/3) \subseteq \mathbb{F}_q$: sum-free
- $A \subseteq \mathbb{F}_q^n$ satisfies $\langle a,a \rangle = 0$ for every $a \in A$ and $\langle a,b \rangle \in S$ for every $a \neq b$, $a,b \in A$
- Then A is free of right angles:
  $\langle x-z, y-z \rangle = \langle x,y \rangle - (\langle x,z \rangle + \langle z,y \rangle) \neq 0.$

Right angles in $\mathbb{F}_q^n$

Theorem (Bursics, Matolcsi, P., Schrettner, 2020+)

$R(n,q) \ll n^{q-2}$

Theorem (Bursics, Matolcsi, P., Schrettner, 2020+)

$R(n,q) \geq (1-o(1)) \cdot \binom{n}{\lceil \frac{1}{2}\lfloor \frac{2}{3}q \rfloor \rceil} \Big/ \binom{\lfloor \frac{2}{3}q \rfloor}{\lceil \frac{1}{2}\lfloor \frac{2}{3}q \rfloor \rceil}$, that is,

$R(n,q) \gg n^{(q-1)/3}$

Construction

- $S = (q/3, 2q/3) \subseteq \mathbb{F}_q$: sum-free
- $A \subseteq \mathbb{F}_q^n$ satisfies $\langle a,a \rangle = 0$ for every $a \in A$ and $\langle a,b \rangle \in S$ for every $a \neq b$, $a,b \in A$
- Then A is free of right angles:
  $\langle x-z, y-z \rangle = \langle x,y \rangle - (\langle x,z \rangle + \langle z,y \rangle) \neq 0.$

Right angles in $\mathbb{F}_q^n$

Theorem (Bursics, Matolcsi, P., Schrettner, 2020+)

$R(n,q) \ll n^{q-2}$

Theorem (Bursics, Matolcsi, P., Schrettner, 2020+)

$R(n,q) \geq (1-o(1)) \cdot \binom{n}{\lceil \frac{1}{2}\lfloor \frac{2}{3}q \rfloor \rceil} \Big/ \binom{\lfloor \frac{2}{3}q \rfloor}{\lceil \frac{1}{2}\lfloor \frac{2}{3}q \rfloor \rceil}$, that is,

$R(n,q) \gg n^{(q-1)/3}$

Construction

- $S = (q/3, 2q/3) \subseteq \mathbb{F}_q$: sum-free
- $A \subseteq \mathbb{F}_q^n$ satisfies $\langle a,a \rangle = 0$ for every $a \in A$ and $\langle a,b \rangle \in S$ for every $a \neq b$, $a,b \in A$
- Then A is free of right angles:
  $\langle x-z, y-z \rangle = \langle x,y \rangle - (\langle x,z \rangle + \langle z,y \rangle) \neq 0$.

k-right corner-free sets in $\mathbb{F}_q^n$

k-right corner: distinct $x_0, x_1, \ldots, x_k$ such that
$\langle x_i - x_0, x_j - x_0 \rangle = 0$ for all $1 \leq i < j \leq k$
(2-right corner: right angle)

Theorem (Naslund, 2020)

If $k < p$ and $|A| > \binom{n+(k-1)q}{(k-1)(q-1)}$, then A contains a k-right corner.

Theorem (Bursics, Matolcsi, P., Schrettner, 2020)

There exists a subset $A \subset \mathbb{F}_q^n$ of size

$$|A| \geq (1 - o(1)) \cdot \binom{n}{\lceil \frac{k-1}{k} \lfloor \frac{k}{2k-1} q \rfloor \rceil} \Big/ \binom{\lfloor \frac{k}{2k-1} q \rfloor}{\lceil \frac{k-1}{k} \lfloor \frac{k}{2k-1} q \rfloor \rceil}$$

which does not contain any k-right corner.

k-right corner-free sets in $\mathbb{F}_q^n$

k-right corner: distinct $x_0, x_1, \ldots, x_k$ such that $\langle x_i - x_0, x_j - x_0 \rangle = 0$ for all $1 \leq i < j \leq k$
(2-right corner: right angle)

Theorem (Naslund, 2020)

If $k < p$ and $|A| > \binom{n+(k-1)q}{(k-1)(q-1)}$, then A contains a k-right corner.

Theorem (Bursics, Matolcsi, P., Schrettner, 2020)

There exists a subset $A \subset \mathbb{F}_q^n$ of size

$$|A| \geq (1 - o(1)) \cdot \binom{n}{\left\lceil \frac{k-1}{k} \left\lfloor \frac{k}{2k-1} q \right\rfloor \right\rceil} \Big/ \binom{\left\lfloor \frac{k}{2k-1} q \right\rfloor}{\left\lceil \frac{k-1}{k} \left\lfloor \frac{k}{2k-1} q \right\rfloor \right\rceil}$$

which does not contain any k-right corner.

Triangles with all right angles in $\mathbb{F}_q^n$

Triangle with *all* right angles: distinct vectors x, y, z with $\langle x-y, y-z\rangle = \langle y-z, z-x\rangle = \langle z-x, x-y\rangle = 0$.

Theorem (Bursics, Matolcsi, P., Schrettner, 2020)

If $A \subseteq \mathbb{F}_q^n$ contains no triangle with *all* right angles, then

$$|A| \leq \binom{n+2q-1}{2q-2} + 2\binom{n+q}{q-1}.$$

Triangles with all right angles in $\mathbb{F}_q^n$

$$\langle x-y, y-z\rangle = \langle y-z, z-x\rangle = \langle z-x, x-y\rangle = 0$$

$$\Updownarrow$$

$$\langle x-y, x-y\rangle = \langle y-z, y-z\rangle = \langle z-x, z-x\rangle = 0$$

$S(n,q)$: maximal size of a set in $\mathbb{F}_q^n$ which does not contain distinct vectors x, y such that $\langle x-y, x-y\rangle = 0$.

No self-orthogonal difference

$S(n,q)$: maximal size of a set in $\mathbb{F}_q^n$ which does not contain distinct vectors x, y such that $\langle x-y, x-y\rangle = 0$.

Theorem (Bursics, Matolcsi, P., Schrettner, 2020)

$$\binom{n}{q-1} \leq S(n,q) \leq \binom{n+q}{q-1} - \binom{n+q-2}{q-3}$$

Moreover, whenever $n \not\equiv -2 \pmod q$ or $q \equiv 1 \pmod 4$, then

$$S(n,q) \geq \binom{n}{q-1} + \binom{n}{q-2}.$$

Theorem (Bursics, Matolcsi, P., Schrettner, 2020)

For $n \equiv 2 \pmod 3$ we have

$$S(n,3) = \binom{n+3}{2} - 1.$$

No self-orthogonal difference

$S(n,q)$: maximal size of a set in $\mathbb{F}_q^n$ which does not contain distinct vectors x, y such that $\langle x-y, x-y\rangle = 0$.

Theorem (Bursics, Matolcsi, P., Schrettner, 2020)

$$\binom{n}{q-1} \leq S(n,q) \leq \binom{n+q}{q-1} - \binom{n+q-2}{q-3}$$

Moreover, whenever $n \not\equiv -2 \pmod q$ or $q \equiv 1 \pmod 4$, then

$$S(n,q) \geq \binom{n}{q-1} + \binom{n}{q-2}.$$

Theorem (Bursics, Matolcsi, P., Schrettner, 2020)

For $n \equiv 2 \pmod 3$ we have

$$S(n,3) = \binom{n+3}{2} - 1.$$

No self-orthogonal difference

Theorem (Bursics, Matolcsi, P., Schrettner, 2020)

For $n \equiv 2 \pmod 3$ we have

$$S(n,3) = \binom{n+3}{2} - 1.$$

For $x, y \in \mathbb{F}_3^n$ we have $\langle x-y, x-y \rangle = d(x,y)$.

$T(n,q)$: maximum size of a binary code of length n if the Hamming distance of two different codewords is never divisible by a fixed prime q

Theorem (Delsarte, 1973)

$T(n,q) \leq \binom{n}{q-1} + \binom{n}{q-2} + \cdots + \binom{n}{1} + \binom{n}{0}$

New proofs by Frankl (1986) and Babai-Snevily-Wilson (1995).

No self-orthogonal difference

Theorem (Bursics, Matolcsi, P., Schrettner, 2020)

For $n \equiv 2 \pmod 3$ we have

$$S(n,3) = \binom{n+3}{2} - 1.$$

For $x, y \in \mathbb{F}_3^n$ we have $\langle x-y, x-y \rangle = d(x,y)$.

$T(n,q)$: maximum size of a binary code of length n if the Hamming distance of two different codewords is never divisible by a fixed prime q

Theorem (Delsarte, 1973)

$T(n,q) \leq \binom{n}{q-1} + \binom{n}{q-2} + \cdots + \binom{n}{1} + \binom{n}{0}$

New proofs by Frankl (1986) and Babai-Snevily-Wilson (1995).

No self-orthogonal difference

Theorem (Bursics, Matolcsi, P., Schrettner, 2020)

For $n \equiv 2 \pmod 3$ we have

$$S(n,3) = \binom{n+3}{2} - 1.$$

For $x, y \in \mathbb{F}_3^n$ we have $\langle x-y, x-y \rangle = d(x,y)$.

$T(n,q)$: maximum size of a binary code of length n if the Hamming distance of two different codewords is never divisible by a fixed prime q

Theorem (Delsarte, 1973)

$$T(n,q) \leq \binom{n}{q-1} + \binom{n}{q-2} + \cdots + \binom{n}{1} + \binom{n}{0}$$

New proofs by Frankl (1986) and Babai-Snevily-Wilson (1995).

No self-orthogonal difference

Theorem (Bursics, Matolcsi, P., Schrettner, 2020)

For $n \equiv 2 \pmod 3$ we have

$$S(n,3) = \binom{n+3}{2} - 1.$$

For $x, y \in \mathbb{F}_3^n$ we have $\langle x-y, x-y \rangle = d(x,y)$.

$T(n,q)$: maximum size of a binary code of length n if the Hamming distance of two different codewords is never divisible by a fixed prime q

Theorem (Delsarte, 1973)

$T(n,q) \leq \binom{n}{q-1} + \binom{n}{q-2} + \cdots + \binom{n}{1} + \binom{n}{0}$

New proofs by Frankl (1986) and Babai-Snevily-Wilson (1995).

Avoiding Hamming-distances divisible by q

Theorem (Delsarte, 1973)

$$T(n,q) \leq \binom{n}{q-1} + \binom{n}{q-2} + \cdots + \binom{n}{1} + \binom{n}{0}$$

New proofs by Frankl (1986) and Babai-Snevily-Wilson (1995).

Theorem (Bursics, Matolcsi, P., Schrettner, 2020+)

$$T(n,q) \leq \binom{n}{q-1} + \binom{n}{q-2} + \cdots + \binom{n}{1} + \binom{n}{0}$$

$$T(n,q) \geq \binom{n}{q-1} + \binom{n}{q-3} + \cdots + \binom{n}{2} + \binom{n}{0}$$

Avoiding Hamming-distances divisible by q

Theorem (Delsarte, 1973)

$$T(n,q) \leq \binom{n}{q-1} + \binom{n}{q-2} + \cdots + \binom{n}{1} + \binom{n}{0}$$

New proofs by Frankl (1986) and Babai-Snevily-Wilson (1995).

Theorem (Bursics, Matolcsi, P., Schrettner, 2020+)

$$T(n,q) \leq \binom{n}{q-1} + \binom{n}{q-2} + \cdots + \binom{n}{1} + \binom{n}{0}$$

$$T(n,q) \geq \binom{n}{q-1} + \binom{n}{q-3} + \cdots + \binom{n}{2} + \binom{n}{0}$$

Avoiding Hamming-distances divisible by q

Theorem (Delsarte, 1973)

$$T(n,q) \leq \binom{n}{q-1} + \binom{n}{q-2} + \cdots + \binom{n}{1} + \binom{n}{0}$$

New proofs by Frankl (1986) and Babai-Snevily-Wilson (1995).

Theorem (Bursics, Matolcsi, P., Schrettner, 2020+)

$$T(n,q) \leq \binom{n}{q-1} + \binom{n}{q-2} + \cdots + \binom{n}{1} + \binom{n}{0}$$

$$T(n,q) \geq \binom{n}{q-1} + \binom{n}{q-3} + \cdots + \binom{n}{2} + \binom{n}{0}$$

Avoiding Hamming-distances divisible by q

Theorem (Delsarte, 1973)

$$T(n,q) \leq \binom{n}{q-1} + \binom{n}{q-2} + \cdots + \binom{n}{1} + \binom{n}{0}$$

New proofs by Frankl (1986) and Babai-Snevily-Wilson (1995).

Theorem (Bursics, Matolcsi, P., Schrettner, 2020+)

$$T(n,q) \leq \binom{n}{q-1} + \binom{n}{q-2} + \cdots + \binom{n}{1} + \binom{n}{0}$$

$$T(n,q) \geq \binom{n}{q-1} + \binom{n}{q-3} + \cdots + \binom{n}{2} + \binom{n}{0}$$

Avoiding Hamming-distances divisible by q

Theorem (Delsarte, 1973)

$$T(n,q) \leq \binom{n}{q-1} + \binom{n}{q-2} + \cdots + \binom{n}{1} + \binom{n}{0}$$

New proofs by Frankl (1986) and Babai-Snevily-Wilson (1995).

Theorem (Bursics, Matolcsi, P., Schrettner, 2020+)

$$T(n,q) \leq \binom{n}{q-1} + \binom{n}{q-2} + \cdots + \binom{n}{1} + \binom{n}{0}$$

$$T(n,q) \geq \binom{n}{q-1} + \binom{n}{q-3} + \cdots + \binom{n}{2} + \binom{n}{0}$$

the lower bound is tight for $n \equiv 0 \pmod{q}$

Avoiding Hamming-distances divisible by q

Theorem (Delsarte, 1973)

$$T(n,q) \leq \binom{n}{q-1} + \binom{n}{q-2} + \cdots + \binom{n}{1} + \binom{n}{0}$$

New proofs by Frankl (1986) and Babai-Snevily-Wilson (1995).

Theorem (Bursics, Matolcsi, P., Schrettner, 2020+)

$$T(n,q) \leq \binom{n}{q-1} + \binom{n}{q-2} + \cdots + \binom{n}{1} + \binom{n}{0}$$

$$T(n,q) \geq \binom{n}{q-1} + \binom{n}{q-3} + \cdots + \binom{n}{2} + \binom{n}{0}$$

the lower bound is tight for $n \equiv 0 \pmod{q}$

the upper bound is tight for $n \equiv -1 \pmod{q}$

Proof (upper bound)

Let $A \subseteq \{-1,1\}^q \subseteq \mathbb{F}_q^n$.

$\langle x-y, x-y\rangle = \sum (x_i - y_i)^2 = 4d(x,y)$

$A := \{a_1, a_2, \ldots, a_r\}$

$p_i(x) := 1 - \langle x - a_i, x - a_i\rangle^{q-1}$

$f_i := p_i|_A$

$f_i(a_j) = \delta_{ij}$

$\Longrightarrow$ $f_1, f_2, \ldots, f_r$ are linearly independent

Proof (upper bound)

Let $A \subseteq \{-1,1\}^q \subseteq \mathbb{F}_q^n$.

$\langle x-y, x-y\rangle = \sum (x_i - y_i)^2 = 4d(x,y)$

$A := \{a_1, a_2, \ldots, a_r\}$

$p_i(x) := 1 - \langle x - a_i, x - a_i\rangle^{q-1}$

$f_i := p_i|_A$

$f_i(a_j) = \delta_{ij}$

$\Longrightarrow$ $f_1, f_2, \ldots, f_r$ are linearly independent

Proof (upper bound)

Let $A \subseteq \{-1,1\}^q \subseteq \mathbb{F}_q^n$.
$\langle x-y, x-y\rangle = \sum (x_i - y_i)^2 = 4d(x,y)$
$A := \{a_1, a_2, \ldots, a_r\}$
$p_i(x) := 1 - \langle x - a_i, x - a_i\rangle^{q-1}$
$f_i := p_i\big|_A$
$f_i(a_j) = \delta_{ij}$
$\Longrightarrow$ $f_1, f_2, \ldots, f_r$ are linearly independent

Proof (upper bound)

Let $A \subseteq \{-1,1\}^q \subseteq \mathbb{F}_q^n$.
$\langle x-y, x-y\rangle = \sum (x_i - y_i)^2 = 4d(x,y)$
$A := \{a_1, a_2, \ldots, a_r\}$
$p_i(x) := 1 - \langle x - a_i, x - a_i\rangle^{q-1}$
$f_i := p_i|_A$
$f_i(a_j) = \delta_{ij}$
$\Longrightarrow$ $f_1, f_2, \ldots, f_r$ are linearly independent

Proof (upper bound)

Let $A \subseteq \{-1,1\}^q \subseteq \mathbb{F}_q^n$.
$\langle x-y, x-y\rangle = \sum (x_i - y_i)^2 = 4d(x,y)$
$A := \{a_1, a_2, \ldots, a_r\}$
$p_i(x) := 1 - \langle x - a_i, x - a_i\rangle^{q-1}$
$f_i := p_i|_A$
$f_i(a_j) = \delta_{ij}$
$\implies$ $f_1, f_2, \ldots, f_r$ are linearly independent

Proof (upper bound)

Let $A \subseteq \{-1,1\}^q \subseteq \mathbb{F}_q^n$.
$\langle x-y, x-y\rangle = \sum (x_i - y_i)^2 = 4d(x,y)$
$A := \{a_1, a_2, \ldots, a_r\}$
$p_i(x) := 1 - \langle x - a_i, x - a_i\rangle^{q-1}$
$f_i := p_i\big|_A$
$f_i(a_j) = \delta_{ij}$
$\Longrightarrow$ $f_1, f_2, \ldots, f_r$ are linearly independent

Proof (upper bound)

Let $A \subseteq \{-1,1\}^q \subseteq \mathbb{F}_q^n$.
$\langle x-y, x-y\rangle = \sum (x_i - y_i)^2 = 4d(x,y)$
$A := \{a_1, a_2, \ldots, a_r\}$
$p_i(x) := 1 - \langle x - a_i, x - a_i\rangle^{q-1}$
$f_i := p_i\big|_A$
$f_i(a_j) = \delta_{ij}$
$\Longrightarrow$ $f_1, f_2, \ldots, f_r$ are linearly independent

Proof (upper bound)

Let $A \subseteq \{-1,1\}^q \subseteq \mathbb{F}_q^n$.
$\langle x-y, x-y\rangle = \sum (x_i - y_i)^2 = 4d(x,y)$
$A := \{a_1, a_2, \ldots, a_r\}$
$p_i(x) := 1 - \langle x - a_i, x - a_i\rangle^{q-1}$
$f_i := p_i\big|_A$
$f_i(a_j) = \delta_{ij}$
$\implies$ $f_1, f_2, \ldots, f_r$ are linearly independent

Proof (upper bound)

$f_1, \dots, f_r : A \to \mathbb{F}_q$
$f_i(x) = 1 - \langle x - a_i, x - a_i \rangle^{q-1}$

Observe that for $x \in A$ and $1 \le i \le r$ we have $\langle x - a_i, x - a_i \rangle = \sum_{j=1}^{n} (x_j - a_{i,j})^2 = \sum_{j=1}^{n} x_j^2 - \sum_{j=1}^{n} 2a_{i,j}x_j + \sum_{j=1}^{n} a_{i,j}^2 = 2n - \sum_{j=1}^{n} 2a_{i,j}x_j$, since $a_{i,j} \in \{\pm 1\}$ and $x \in A \subseteq \{\pm 1\}^n$.

Therefore, $f_i(x) = 1 - \left(2n - \sum_{j=1}^{n} 2a_{i,j}x_j\right)^{q-1}$ is a polynomial of $x_1, x_2, \dots, x_n$ of degree $q - 1$.

Since $x_j^2 = 1$ for every $x \in A$ we can reduce the exponent of x_j to 0 or 1, according to the parity of the original exponent. This way each f_i is represented as a multilinear polynomial of degree at most $q - 1$.

Proof (upper bound)

$f_1, \dots, f_r : A \to \mathbb{F}_q$
$f_i(x) = 1 - \langle x - a_i, x - a_i \rangle^{q-1}$

Observe that for $x \in A$ and $1 \le i \le r$ we have $\langle x - a_i, x - a_i \rangle = \sum_{j=1}^{n} (x_j - a_{i,j})^2 = \sum_{j=1}^{n} x_j^2 - \sum_{j=1}^{n} 2a_{i,j}x_j + \sum_{j=1}^{n} a_{i,j}^2 = 2n - \sum_{j=1}^{n} 2a_{i,j}x_j$, since $a_{i,j} \in \{\pm 1\}$ and $x \in A \subseteq \{\pm 1\}^n$.

Therefore, $f_i(x) = 1 - \left(2n - \sum_{j=1}^{n} 2a_{i,j}x_j\right)^{q-1}$ is a polynomial of $x_1, x_2, \dots, x_n$ of degree $q - 1$.

Since $x_j^2 = 1$ for every $x \in A$ we can reduce the exponent of x_j to 0 or 1, according to the parity of the original exponent. This way each f_i is represented as a multilinear polynomial of degree at most $q - 1$.

Proof (upper bound)

$f_1, \dots, f_r : A \to \mathbb{F}_q$
$f_i(x) = 1 - \langle x - a_i, x - a_i \rangle^{q-1}$

Observe that for $x \in A$ and $1 \le i \le r$ we have $\langle x - a_i, x - a_i \rangle = \sum_{j=1}^{n} (x_j - a_{i,j})^2 = \sum_{j=1}^{n} x_j^2 - \sum_{j=1}^{n} 2a_{i,j}x_j + \sum_{j=1}^{n} a_{i,j}^2 = 2n - \sum_{j=1}^{n} 2a_{i,j}x_j$, since $a_{i,j} \in \{\pm 1\}$ and $x \in A \subseteq \{\pm 1\}^n$.

Therefore, $f_i(x) = 1 - \left(2n - \sum_{j=1}^{n} 2a_{i,j}x_j\right)^{q-1}$ is a polynomial of $x_1, x_2, \dots, x_n$ of degree $q - 1$.

Since $x_j^2 = 1$ for every $x \in A$ we can reduce the exponent of x_j to 0 or 1, according to the parity of the original exponent. This way each f_i is represented as a multilinear polynomial of degree at most $q - 1$.

Proof (upper bound)

$f_1, \dots, f_r : A \to \mathbb{F}_q$
$f_i(x) = 1 - \langle x - a_i, x - a_i \rangle^{q-1}$

Observe that for $x \in A$ and $1 \le i \le r$ we have $\langle x - a_i, x - a_i \rangle = \sum_{j=1}^{n} (x_j - a_{i,j})^2 = \sum_{j=1}^{n} x_j^2 - \sum_{j=1}^{n} 2a_{i,j}x_j + \sum_{j=1}^{n} a_{i,j}^2 = 2n - \sum_{j=1}^{n} 2a_{i,j}x_j$, since $a_{i,j} \in \{\pm 1\}$ and $x \in A \subseteq \{\pm 1\}^n$.

Therefore, $f_i(x) = 1 - \left(2n - \sum_{j=1}^{n} 2a_{i,j}x_j\right)^{q-1}$ is a polynomial of $x_1, x_2, \dots, x_n$ of degree $q-1$.

Since $x_j^2 = 1$ for every $x \in A$ we can reduce the exponent of x_j to 0 or 1, according to the parity of the original exponent. This way each f_i is represented as a multilinear polynomial of degree at most $q-1$.

Proof (upper bound)

$f_i(x) = 1 - \langle x - a_i, x - a_i \rangle^{q-1}$

Each f_i is represented as a multilinear polynomial of degree at most $q-1$:

$$f_1, \ldots, f_r \in \langle \prod_{i \in I} x_i : I \subseteq [n], |I| \leq q-1 \rangle.$$

$$\implies |A| = r \leq \binom{n}{q-1} + \binom{n}{q-2} + \cdots + \binom{n}{1} + \binom{n}{0}.$$

Proof (upper bound)

Improvement for $q \mid n$:

$$f_i(x) = 1 - \left(2n - \sum_{j=1}^{n} 2a_{i,j}x_j\right)^{q-1} = 1 - \left(\sum_{j=1}^{n} 2a_{i,j}x_j\right)^{q-1}$$

After reducing the exponents, we get monomials with even total degree. Hence, $|A| = r \leq \binom{n}{q-1} + \binom{n}{q-3} + \cdots + \binom{n}{2} + \binom{n}{0}$.

(So for $q \mid n$ this is the exact answer.)

Proof (lower bound)

Let A consist of those elements of $\{a, b\}^n$ in which the number of characters a is even and at most $q - 1$.

Then $|A| = \binom{n}{q-1} + \binom{n}{q-3} + \cdots + \binom{n}{2} + \binom{n}{0}$.

Let x and y be two distinct elements of A.
Let k resp. ℓ denote the number of characters a in x resp. y, and denote by m the number of those entries where both x and y have a.

$$m = \#\text{ indices such that } (x_i, y_i) = (a, a)$$

$$k - m = \#\text{ indices such that } (x_i, y_i) = (a, b)$$

$$\ell - m = \#\text{ indices such that } (x_i, y_i) = (b, a)$$

$$d(x, y) = k + \ell - 2m.$$

Observe that k and ℓ are even and $k, \ell \leq q - 1$, thus $d(x, y) = k + \ell - 2m \in (0, 2q)$ is even, which implies that $d(x, y)$ is not divisible by q.

Proof (lower bound)

Let A consist of those elements of $\{a,b\}^n$ in which the number of characters a is even and at most $q-1$.

Then $|A| = \binom{n}{q-1} + \binom{n}{q-3} + \cdots + \binom{n}{2} + \binom{n}{0}$.

Let x and y be two distinct elements of A.
Let k resp. ℓ denote the number of characters a in x resp. y, and denote by m the number of those entries where both x and y have a.

$$m = \#\text{ indices such that } (x_i, y_i) = (a,a)$$

$$k - m = \#\text{ indices such that } (x_i, y_i) = (a,b)$$

$$\ell - m = \#\text{ indices such that } (x_i, y_i) = (b,a)$$

$$d(x,y) = k + \ell - 2m.$$

Observe that k and ℓ are even and $k, \ell \leq q-1$, thus $d(x,y) = k + \ell - 2m \in (0, 2q)$ is even, which implies that $d(x,y)$ is not divisible by q.

Proof (lower bound)

Let A consist of those elements of $\{a, b\}^n$ in which the number of characters a is even and at most $q-1$.

Then $|A| = \binom{n}{q-1} + \binom{n}{q-3} + \cdots + \binom{n}{2} + \binom{n}{0}$.

Let x and y be two distinct elements of A.
Let k resp. ℓ denote the number of characters a in x resp. y, and denote by m the number of those entries where both x and y have a.

$$m = \#\text{ indices such that } (x_i, y_i) = (a, a)$$

$$k - m = \#\text{ indices such that } (x_i, y_i) = (a, b)$$

$$\ell - m = \#\text{ indices such that } (x_i, y_i) = (b, a)$$

$$d(x, y) = k + \ell - 2m.$$

Observe that k and ℓ are even and $k, \ell \leq q-1$, thus $d(x, y) = k + \ell - 2m \in (0, 2q)$ is even, which implies that $d(x, y)$ is not divisible by q.

Proof (lower bound)

Let A consist of those elements of $\{a,b\}^n$ in which the number of characters a is even and at most $q-1$.

Then $|A| = \binom{n}{q-1} + \binom{n}{q-3} + \cdots + \binom{n}{2} + \binom{n}{0}$.

Let x and y be two distinct elements of A.
Let k resp. ℓ denote the number of characters a in x resp. y, and denote by m the number of those entries where both x and y have a.

$$m = \#\text{ indices such that } (x_i, y_i) = (a,a)$$

$$k - m = \#\text{ indices such that } (x_i, y_i) = (a,b)$$

$$\ell - m = \#\text{ indices such that } (x_i, y_i) = (b,a)$$

$$d(x,y) = k + \ell - 2m.$$

Observe that k and ℓ are even and $k, \ell \leq q-1$, thus $d(x,y) = k + \ell - 2m \in (0, 2q)$ is even, which implies that $d(x,y)$ is not divisible by q.

Proof (lower bound)

Let A consist of those elements of $\{a, b\}^n$ in which the number of characters a is even and at most $q-1$.

Then $|A| = \binom{n}{q-1} + \binom{n}{q-3} + \cdots + \binom{n}{2} + \binom{n}{0}$.

Let x and y be two distinct elements of A.
Let k resp. ℓ denote the number of characters a in x resp. y, and denote by m the number of those entries where both x and y have a.

$$m = \#\text{ indices such that } (x_i, y_i) = (a, a)$$

$$k - m = \#\text{ indices such that } (x_i, y_i) = (a, b)$$

$$\ell - m = \#\text{ indices such that } (x_i, y_i) = (b, a)$$

$$d(x, y) = k + \ell - 2m.$$

Observe that k and ℓ are even and $k, \ell \leq q-1$, thus $d(x, y) = k + \ell - 2m \in (0, 2q)$ is even, which implies that $d(x, y)$ is not divisible by q.

Proof (lower bound)

Improvement for $n \equiv -1 \pmod{q}$:

Previous construction:
those elements of $\{a, b\}^n$ in which $\#\, a$ is even and at most $q - 1$

add "new" elements: $\#\, b$ is odd and at most $q - 2$

Size: $\binom{n}{q-1} + \binom{n}{q-2} + \cdots + \binom{n}{1} + \binom{n}{0}$

x, y are original elements: done

x, y are new elements: similar

x: original, y: new

Proof (lower bound)

Improvement for $n \equiv -1 \pmod{q}$:

Previous construction:
those elements of $\{a, b\}^n$ in which $\#\, a$ is even and at most $q-1$

add "new" elements: $\#\, b$ is odd and at most $q-2$

Size: $\binom{n}{q-1} + \binom{n}{q-2} + \cdots + \binom{n}{1} + \binom{n}{0}$

x, y are original elements: done

x, y are new elements: similar

x: original, y: new

Proof (lower bound)

Improvement for $n \equiv -1 \pmod{q}$:

Previous construction:
those elements of $\{a, b\}^n$ in which $\#\, a$ is even and at most $q-1$

add "new" elements: $\#\, b$ is odd and at most $q-2$

Size: $\binom{n}{q-1} + \binom{n}{q-2} + \cdots + \binom{n}{1} + \binom{n}{0}$

x, y are original elements: done

x, y are new elements: similar

x: original, y: new

Proof (lower bound)

Improvement for $n \equiv -1 \pmod{q}$:

Previous construction:
those elements of $\{a, b\}^n$ in which $\#\, a$ is even and at most $q-1$

add "new" elements: $\#\, b$ is odd and at most $q-2$

Size: $\binom{n}{q-1} + \binom{n}{q-2} + \cdots + \binom{n}{1} + \binom{n}{0}$

x, y are original elements: done

x, y are new elements: similar

x: original, y: new

Proof (lower bound)

Improvement for $n \equiv -1 \pmod{q}$:

Previous construction:
those elements of $\{a, b\}^n$ in which $\#\, a$ is even and at most $q-1$

add "new" elements: $\#\, b$ is odd and at most $q-2$

Size: $\binom{n}{q-1} + \binom{n}{q-2} + \cdots + \binom{n}{1} + \binom{n}{0}$

x, y are original elements: done

x, y are new elements: similar

x: original, y: new

Proof (lower bound)

Improvement for $n \equiv -1 \pmod{q}$:

Previous construction:
those elements of $\{a, b\}^n$ in which $\#\, a$ is even and at most $q-1$

add "new" elements: $\#\, b$ is odd and at most $q-2$

Size: $\binom{n}{q-1} + \binom{n}{q-2} + \cdots + \binom{n}{1} + \binom{n}{0}$

x, y are original elements: done

x, y are new elements: similar

x: original, y: new

Proof (lower bound)

x: original, y: new

Then $\#a$ in $x = k \leq q-1$ is even and $\#b$ in $y = n - \ell \leq q-2$ is odd. Observe that

$$d(x,y) = k + \ell - 2m = n + 2(k-m) - k - (n-\ell),$$

thus

$$n - 2q + 3 \leq n + 2(k-m) - k - (n-\ell) = d(x,y) \leq n.$$

$2 \mid k,\ 2 \nmid n-\ell \implies d(x,y) = k + \ell - 2m$ has the same parity as $n+1$

$q \mid n+1 \implies$ in $[n-2q+3, n]$ only $n-q+1$ is divisible by q, however, its parity is different from the parity of $n+1$.
Hence, $q \nmid d(x,y)$, as we claimed.

Proof (lower bound)

x: original, y: new

Then $\#a$ in $x = k \leq q-1$ is even and $\#b$ in $y = n - \ell \leq q-2$ is odd. Observe that

$$d(x,y) = k + \ell - 2m = n + 2(k-m) - k - (n-\ell),$$

thus

$$n - 2q + 3 \leq n + 2(k-m) - k - (n-\ell) = d(x,y) \leq n.$$

$2 \mid k,\ 2 \nmid n-\ell \implies d(x,y) = k + \ell - 2m$ has the same parity as $n+1$

$q \mid n+1 \implies$ in $[n-2q+3, n]$ only $n-q+1$ is divisible by q, however, its parity is different from the parity of $n+1$.
Hence, $q \nmid d(x,y)$, as we claimed.

Proof (lower bound)

x: original, y: new

Then $\#a$ in $x = k \leq q-1$ is even and $\#b$ in $y = n - \ell \leq q-2$ is odd. Observe that

$$d(x,y) = k + \ell - 2m = n + 2(k-m) - k - (n-\ell),$$

thus

$$n - 2q + 3 \leq n + 2(k-m) - k - (n-\ell) = d(x,y) \leq n.$$

$2 \mid k,\ 2 \nmid n-\ell \implies d(x,y) = k + \ell - 2m$ has the same parity as $n+1$

$q \mid n+1 \implies$ in $[n-2q+3, n]$ only $n-q+1$ is divisible by q, however, its parity is different from the parity of $n+1$.
Hence, $q \nmid d(x,y)$, as we claimed.