Additive combinatorics in $\mathbb{F}_p$ and the polynomial method

Éric Balandraud

Journées estivales de la Méthode Polynomiale

The Combinatorial Nullstellensatz

Theorem (Alon)

$\mathbb{K}$ *a field and* P *a polynomial* $\mathbb{K}[X_1, \ldots, X_d]$.

The Combinatorial Nullstellensatz

Theorem (Alon)

$\mathbb{K}$ a field and P a polynomial $\mathbb{K}[X_1, \ldots, X_d]$.
If $\deg(P) = \sum_{i=1}^{d} k_i$ and P has a non zero coefficient for $\prod_{i=1}^{d} X_i^{k_i}$,

The Combinatorial Nullstellensatz

Theorem (Alon)

$\mathbb{K}$ a field and P a polynomial $\mathbb{K}[X_1, \ldots, X_d]$.
If $\deg(P) = \sum_{i=1}^{d} k_i$ and P has a non zero coefficient for $\prod_{i=1}^{d} X_i^{k_i}$, then whatever $A_1, \ldots, A_d$, subsets of $\mathbb{K}$ such that $|A_i| > k_i$, there exists $(a_1, \ldots, a_d) \in A_1 \times \cdots \times A_d$ so that:

$$P(a_1, \ldots, a_d) \neq 0.$$

Another formulation

Theorem

$\mathbb{K}$ a field and P a polynomial $\mathbb{K}[X_1, \ldots, X_d]$. Let $A_1, \ldots, A_d$ subsets of $\mathbb{K}$. Setting $g_i(X_i) = \prod_{a_i \in A_i}(X_i - a_i)$. If P vanishes on $A_1 \times \cdots \times A_d$, there exist $h_i \in \mathbb{K}[X_1, \ldots, X_d]$, with $\deg(h_i) \leqslant \deg(P) - deg(g_i)$ such that:

$$P = \sum_{i=1}^{d} h_i g_i.$$

Three Addition Theorems in $\mathbb{F}_p$

- Cauchy-Davenport
- Dias da Silva-Hamidoune (Erdős-Heilbronn)
- Set of Subsums

Cauchy-Davenport

Theorem (Cauchy-Davenport - 1813, 1935)

p a prime number, A and B two subsets of $\mathbb{F}_p$, then:

$$|A+B| \geqslant \min\{p, |A|+|B|-1\}.$$

Cauchy-Davenport

Theorem (Cauchy-Davenport - 1813, 1935)

p a prime number, A and B two subsets of $\mathbb{F}_p$, then:

$$|A+B| \geqslant \min\left\{p, 1+(|A|-1)+(|B|-1)\right\}.$$

Cauchy-Davenport

Theorem (Cauchy-Davenport - 1813, 1935)

p a prime number, A and B two subsets of $\mathbb{F}_p$, then:

$$|A+B| \geqslant \min\{p, 1+(|A|-1)+(|B|-1)\}.$$

proof: If $A+B \subset C$, with $|C| = \min\{p-1, |A|+|B|-2\}$, the polynomial

$$\prod_{c\in C}(X+Y-c)$$

would vanish on $A \times B$ and the coefficient of $X^{|A|-1}Y^{|C|-|A|-1}$ is $\binom{|C|}{|A|-1} \neq 0$.

Dias da Silva-Hamidoune

Conjecture (Erdös-Heilbronn - 1964)

p a prime number, $A \subset \mathbb{F}_p$, then:

$$|\{a_1 + a_2 \mid a_i \in A,\ a_1 \neq a_2\}| \geqslant \min\{p, 2|A| - 3\}$$

Dias da Silva-Hamidoune

Conjecture (Erdös-Heilbronn - 1964)

p a prime number, $A \subset \mathbb{F}_p$, then:

$$|\{a_1 + a_2 \mid a_i \in A,\ a_1 \neq a_2\}| \geqslant \min\{p, 2(|A| - 2) + 1\}$$

Dias da Silva-Hamidoune

Conjecture (Erdös-Heilbronn - 1964)

p a prime number, $A \subset \mathbb{F}_p$, then:

$$|\{a_1 + a_2 \mid a_i \in A,\ a_1 \neq a_2\}| \geqslant \min\{p, 2(|A| - 2) + 1\}$$

Define:

$$h^{\wedge}A = \{a_1 + \cdots + a_h \mid a_i \in A,\ a_i \neq a_j\}$$

Dias da Silva-Hamidoune

Conjecture (Erdös-Heilbronn - 1964)

p a prime number, $A \subset \mathbb{F}_p$, then:

$$|\{a_1 + a_2 \mid a_i \in A,\ a_1 \neq a_2\}| \geqslant \min\{p, 2(|A| - 2) + 1\}$$

Define:

$$h^{\wedge}A = \{a_1 + \cdots + a_h \mid a_i \in A,\ a_i \neq a_j\}$$

Theorem (Dias da Silva, Hamidoune - 1994)

Let p be a prime number and $A \subset \mathbb{F}_p$. Let $h \in [1, |A|]$, one has,

$$|h^{\wedge}A| \geqslant \min\{p, 1 + h(|A| - h)\}.$$

Proof: Setting $i_0 = \max\{0, h(|A| - h) - p + 1\}$,
$(h(|A| - h) - p + 1 < h)$. one considers the polynomial

$$(X_0 + \cdots + X_{h-1})^{h(|A|-h)-i_0} \left(\prod_{0 \leqslant i < j \leqslant h-1} (X_j - X_i) \right),$$

it has degree $h(|A| - h) - i_0 + \frac{h(h-1)}{2}$,

Proof: Setting $i_0 = \max\{0, h(|A|-h)-p+1\}$, $(h(|A|-h)-p+1 < h)$. one considers the polynomial

$$(X_0 + \cdots + X_{h-1})^{h(|A|-h)-i_0}\left(\prod_{0\leqslant i<j\leqslant h-1}(X_j - X_i)\right),$$

it has degree $h(|A|-h) - i_0 + \frac{h(h-1)}{2}$, and the sets:

$$\begin{array}{lll}
A_0 & = & \{a_1,\dots,a_{|A|-h}\} \\
A_1 & = & \{a_1,\dots,a_{|A|-h},a_{|A|-h+1}\} \\
\vdots & \vdots & \ddots \\
A_{i_0-1} & = & \{a_1,\dots,a_{|A|-h},\dots,a_{|A|-h+i_0-1}\} \\
A_{i_0} & = & \{a_1,\dots,a_{|A|-h},\dots,a_{|A|-h+i_0-1},a_{|A|-h+i_0},a_{|A|-h+i_0+1}\} \\
\vdots & & \ddots \\
A_{h-2} & = & \{a_1, \quad \dots \quad ,a_{|A|-1}\} \\
A_{h-1} & = & \{a_1, \quad \dots \quad ,a_{|A|-1},a_{|A|}\},
\end{array}$$

Set of Subsums

Let A be a subset of $\mathbb{F}_p$, define

$$\Sigma(A) = \left\{ \sum_{x \in I} x \mid \emptyset \subset I \subset A \right\}$$

Set of Subsums

Let A be a subset of $\mathbb{F}_p$, define

$$\Sigma^*(A) = \left\{ \sum_{x \in I} x \mid \emptyset \subsetneq I \subset A \right\}$$

Set of Subsums

Let A be a subset of $\mathbb{F}_p$, define

$$\Sigma^*(A) = \left\{ \sum_{x \in I} x \mid \emptyset \subsetneq I \subset A \right\}$$

Theorem (Olson - 1968)

Let $A \subset \mathbb{F}_p$. If $A \cap (-A) = \emptyset$, then

$$|\Sigma(A)| \geqslant \min \left\{ \frac{p+3}{2}, \frac{|A|(|A|+1)}{2} \right\}.$$

Theorem (B.)

p a odd prime number, $A \subset \mathbb{F}_p$, such that $A \cap (-A) = \emptyset$. One has

$$|\Sigma(A)| \geqslant \min\left\{p, 1 + \frac{|A|(|A|+1)}{2}\right\},$$

Theorem (B.)

p a odd prime number, $A \subset \mathbb{F}_p$, such that $A \cap (-A) = \emptyset$. One has

$$|\Sigma(A)| \geqslant \min\left\{p, 1 + \frac{|A|(|A|+1)}{2}\right\},$$

$$|\Sigma^*(A)| \geqslant \min\left\{p, \frac{|A|(|A|+1)}{2}\right\}.$$

Theorem (B.)

p a odd prime number, $A \subset \mathbb{F}_p$, such that $A \cap (-A) = \emptyset$. One has

$$|\Sigma(A)| \geqslant \min\left\{p, 1 + \frac{|A|(|A|+1)}{2}\right\},$$

$$|\Sigma^*(A)| \geqslant \min\left\{p, \frac{|A|(|A|+1)}{2}\right\}.$$

Conjecture (Selfridge - 1976)

p a prime number, A a maximal zerosum free subset of $\mathbb{Z}/p\mathbb{Z}$, then:

$$|A| = \max\left\{k \mid \frac{k(k+1)}{2} < p\right\}.$$

Theorem (B.)

p a odd prime number, $A \subset \mathbb{F}_p$, such that $A \cap (-A) = \emptyset$. One has

$$|\Sigma(A)| \geqslant \min\left\{p, 1 + \frac{|A|(|A|+1)}{2}\right\},$$

$$|\Sigma^*(A)| \geqslant \min\left\{p, \frac{|A|(|A|+1)}{2}\right\}.$$

Theorem (B.)

p a odd prime number, $A \subset \mathbb{F}_p$, such that $A \cap (-A) = \emptyset$. One has

$$|\Sigma(A)| \geqslant \min\left\{p, 1 + \frac{|A|(|A|+1)}{2}\right\},$$
$$|\Sigma^*(A)| \geqslant \min\left\{p, \frac{|A|(|A|+1)}{2}\right\}.$$

Denote $A = \{2a_1, \ldots, 2a_d\}$.

$$\Sigma(A) = \sum_{i\in[1,d]} \{0, 2a_i\} = \left(\sum_{i\in[1,d]} a_i\right) + \underbrace{\sum_{i\in[1,d]} \{-a_i, a_i\}}_{d \text{ terms}}.$$

Let $i_0 = \max\{0, \frac{d(d+1)}{2} - p + 1\}$, one has
$t = \frac{d(d+1)}{2} - i_0 = \min\{\frac{d(d+1)}{2}, p-1\}$

$$(X_0 + \cdots + X_{d-1})^t \left(\prod_{0 \leqslant i < j \leqslant d-1} (X_j^2 - X_i^2) \right)$$

Let $i_0 = \max\{0, \frac{d(d+1)}{2} - p + 1\}$, one has
$t = \frac{d(d+1)}{2} - i_0 = \min\{\frac{d(d+1)}{2}, p-1\}$

$$(X_0 + \cdots + X_{d-1})^t \left(\prod_{0 \leqslant i < j \leqslant d-1} (X_j^2 - X_i^2) \right)$$

$$\begin{aligned}
A_0 &= \{a_1, \ldots, a_d\} \\
A_1 &= \{a_1, \ldots, a_d, -a_1\} \\
&\vdots \qquad\qquad\qquad \ddots \\
A_{i_0-1} &= \{a_1, \ldots, a_d, -a_1, \ldots, -a_{i_0-1}\} \\
A_{i_0} &= \{a_1, \ldots, a_d, -a_1, \ldots, -a_{i_0-1}, -a_{i_0}, -a_{i_0+1}\} \\
&\vdots \qquad\qquad\qquad\qquad\qquad\qquad \ddots \\
A_{d-1} &= \{a_1, \ldots, a_d, -a_1, \qquad \ldots \qquad \ldots \qquad , -a_d\}.
\end{aligned}$$

Let $i_0 = \max\{0, \frac{d(d+1)}{2} - p + 1\}$, one has
$t = \frac{d(d+1)}{2} - i_0 = \min\{\frac{d(d+1)}{2}, p-1\}$

$$(X_0 + \cdots + X_{d-1})^t \left(\prod_{0 \leqslant i < j \leqslant d-1} (X_j^2 - X_i^2) \right)$$

$$\begin{aligned}
A_0 &= \{a_1, \ldots, a_d\} \\
A_1 &= \{a_1, \ldots, a_d, -a_1\} \\
&\vdots \qquad\qquad\qquad \ddots \\
A_{i_0-1} &= \{a_1, \ldots, a_d, -a_1, \ldots, -a_{i_0-1}\} \\
A_{i_0} &= \{a_1, \ldots, a_d, -a_1, \ldots, -a_{i_0-1}, -a_{i_0}, -a_{i_0+1}\} \\
&\vdots \qquad\qquad\qquad\qquad\qquad\qquad \ddots \\
A_{d-1} &= \{a_1, \ldots, a_d, -a_1, \qquad \ldots \qquad\qquad \ldots \qquad\qquad , -a_d\}.
\end{aligned}$$

$$(X_0 + \cdots + X_{d-1})^t \left(\prod_{0 \leqslant i < j \leqslant d-1} (X_j^2 - X_i^2) \right)$$

$$(X_0 + \cdots + X_{d-1})^t \left(\prod_{0 \leqslant i < j \leqslant d-1} (X_j^2 - X_i^2) \right)$$

$$= \left(\sum_{\substack{(t_0,\ldots,t_{d-1}) \\ \sum_{i=0}^{d-1} t_i = t}} \frac{t!}{\prod_{i=0}^{d-1} t_i!} \prod_{i=0}^{d-1} X_i^{t_i} \right) \begin{vmatrix} 1 & X_0^2 & \cdots & X_0^{2(d-1)} \\ 1 & X_1^2 & \cdots & X_1^{2(d-1)} \\ \vdots & \vdots & & \vdots \\ 1 & X_{d-1}^2 & \cdots & X_{d-1}^{2(d-1)} \end{vmatrix}$$

$$(X_0 + \cdots + X_{d-1})^t \left(\prod_{0 \leqslant i < j \leqslant d-1} (X_j^2 - X_i^2) \right)$$

$$= \left(\sum_{\substack{(t_0,\ldots,t_{d-1}) \\ \sum_{i=0}^{d-1} t_i = t}} \frac{t!}{\prod_{i=0}^{d-1} t_i!} \prod_{i=0}^{d-1} X_i^{t_i} \right) \left(\sum_{\sigma \in \mathfrak{S}_d} sign(\sigma) \prod_{i=0}^{d-1} X_i^{2\sigma(i)} \right)$$

$$(X_0 + \cdots + X_{d-1})^t \left(\prod_{0 \leqslant i < j \leqslant d-1} (X_j^2 - X_i^2) \right)$$

$$= t! \sum_{\sigma \in \mathfrak{S}_d} sign(\sigma) \sum_{\substack{(t_0,\ldots,t_{d-1}) \\ \sum_{i=0}^{d-1} t_i = t}} \frac{1}{\prod_{i=0}^{d-1} t_i!} \prod_{i=0}^{d-1} X_i^{t_i + 2\sigma(i)}$$

$$(X_0 + \cdots + X_{d-1})^t \left(\prod_{0 \leqslant i < j \leqslant d-1} (X_j^2 - X_i^2) \right)$$

$$= t! \sum_{\sigma \in \mathfrak{S}_d} sign(\sigma) \sum_{\substack{(b_0,\ldots,b_{d-1}) \\ 0 \leqslant b_i - 2\sigma(i) \leqslant t \\ \sum_{i=0}^{d-1} b_i = t + d(d-1)}} \frac{1}{\prod_{i=0}^{d-1} (b_i - 2\sigma(i))!} \prod_{i=0}^{d-1} X_i^{b_i}$$

$$(X_0 + \cdots + X_{d-1})^t \left(\prod_{0 \leqslant i < j \leqslant d-1} (X_j^2 - X_i^2) \right)$$

$$= \sum_{\substack{(b_0,\ldots,b_{d-1}) \\ \sum_{i=0}^{d-1} b_i = t + d(d-1) \\ \max\{b_i\} < p}} \left(\frac{t! \prod_{i=0}^{d-1} (2i)!}{\prod_{i=0}^{d-1} b_i!} \left(\sum_{\sigma \in \mathfrak{S}_d} sign(\sigma) \prod_{i=0}^{d-1} \binom{b_i}{2\sigma(i)} \right) \right) \prod_{i=0}^{d-1} X_i^{b_i} + S_p$$

$$(X_0 + \cdots + X_{d-1})^t \left(\prod_{0 \leqslant i < j \leqslant d-1} (X_j^2 - X_i^2) \right)$$

$$= \sum_{\substack{(b_0,\ldots,b_{d-1}) \\ \sum_{i=0}^{d-1} b_i = t + d(d-1) \\ \max\{b_i\} < p}} \left(\frac{t! \prod_{i=0}^{d-1} (2i)!}{\prod_{i=0}^{d-1} b_i!} \binom{b_0, b_1, \ldots, b_{d-1}}{0, 2, \ldots, 2(d-1)} \right) \prod_{i=0}^{d-1} X_i^{b_i} + S_p$$

$$(X_0 + \cdots + X_{d-1})^t \left(\prod_{0 \leqslant i < j \leqslant d-1} (X_j^2 - X_i^2) \right)$$

$$= \sum_{\substack{(b_0,\ldots,b_{d-1}) \\ \sum_{i=0}^{d-1} b_i = t + d(d-1) \\ \max\{b_i\} < p}} \left(\frac{t! \prod_{i=0}^{d-1} (2i)!}{\prod_{i=0}^{d-1} b_i!} \begin{pmatrix} b_0, b_1, \ldots, b_{d-1} \\ 0, 2, \ldots, 2(d-1) \end{pmatrix} \right) \prod_{i=0}^{d-1} X_i^{b_i} + S_p$$

It suffices to prove that the following binomial determinant is non zero:

$$D_{d,i_0} = \begin{pmatrix} d-1, & d, & \ldots, & d-2+i_0, & d+i_0, & \ldots, & 2d-1 \\ 0, & 2, & \ldots, & 2(i_0-1), & 2i_0, & \ldots, & 2(d-1) \end{pmatrix}.$$

Binomial Determinants

$$\left(\begin{array}{c} a_1, \ldots, a_d \\ b_1, \ldots, b_d \end{array} \right) = \begin{vmatrix} \binom{a_1}{b_1} & \binom{a_1}{b_2} & \cdots & \binom{a_1}{b_d} \\ \binom{a_2}{b_1} & \binom{a_2}{b_2} & \cdots & \binom{a_2}{b_d} \\ \vdots & \vdots & & \vdots \\ \binom{a_d}{b_1} & \binom{a_d}{b_2} & \cdots & \binom{a_d}{b_d)} \end{vmatrix}.$$

Binomial Determinants

$$\left(\begin{array}{c} a_1, \ldots, a_d \\ b_1, \ldots, b_d \end{array} \right) = \begin{vmatrix} \binom{a_1}{b_1} & \binom{a_1}{b_2} & \cdots & \binom{a_1}{b_d} \\ \binom{a_2}{b_1} & \binom{a_2}{b_2} & \cdots & \binom{a_2}{b_d} \\ \vdots & \vdots & & \vdots \\ \binom{a_d}{b_1} & \binom{a_d}{b_2} & \cdots & \binom{a_d}{b_d)} \end{vmatrix}.$$

$$D_{n,h,i} = \binom{n-h-1, n-h, \ldots, n-h+i-2, n-h+i, \ldots, n-1}{0 \ , \ 1 \ , \ \ldots \ , \ (i-1) \ , \ i \ , \ \ldots \ , \ (h-1)}$$

$$D_{d,i} = \left(\begin{array}{ccccccc} d-1, & d, & \ldots, & d-2+i, & d+i, & \ldots, & 2d-1 \\ 0, & 2, & \ldots, & 2(i-1), & 2i, & \ldots, & 2(d-1) \end{array} \right).$$

$$D_{n,h,i} = \binom{h}{i},$$

This proves Dias da Silva-Hamidoune Theorem.

$$D_{n,h,i} = \binom{h}{i},$$

This proves Dias da Silva-Hamidoune Theorem.

Proposition

Let $d \geqslant 1$, one has:

$$D_{d,0} = 2^{d(d-1)/2},$$

$$D_{d,d} = 2^{(d-1)(d-2)/2}.$$

$$D_{n,h,i} = \binom{h}{i},$$

This proves Dias da Silva-Hamidoune Theorem.

Proposition

Let $d \geqslant 1$, one has:

$$D_{d,0} = 2^{d(d-1)/2},$$

$$D_{d,d} = 2^{(d-1)(d-2)/2}.$$

$$D_{d,i} = 2^{d-1}\frac{d-1}{d-2+i}D_{d-1,i-1} + 2^{d-1}\frac{d-1}{d-1+i}D_{d-1,i}.$$

$$D_{n,h,i} = \binom{h}{i},$$

This proves Dias da Silva-Hamidoune Theorem.

Proposition

Let $d \geqslant 1$, one has:

$$D_{d,0} = 2^{d(d-1)/2},$$

$$D_{d,d} = 2^{(d-1)(d-2)/2}.$$

$$D_{d,i} = 2^{d-1}\frac{d-1}{d-2+i}D_{d-1,i-1} + 2^{d-1}\frac{d-1}{d-1+i}D_{d-1,i}.$$

$$D_{d,i} = 2^{\frac{d(d-1)}{2}-i}\binom{d}{i}\frac{d+i}{d}.$$

Three Additive results on sequences in $\mathbb{F}_p$

- Erdős-Ginzburg-Ziv
- Snevily's conjecture (Arsovsky)
- Nullstellensatz for sequences

The permanent Lemma

Theorem (Alon - 1999)

K a field, A an $n \times n$ matrix with non zero permanent, $b \in K^n$. If one considers some sets S_i, $i = 1..n$, $|S_i| = 2$. There exists $s = (s_1, \ldots, s_n) \in S_1 \times \cdots \times S_n$, such that As and b are coordoninatewise distincts.

The permanent Lemma

Theorem (Alon - 1999)

K a field, A an $n \times n$ matrix with non zero permanent, $b \in K^n$. If one considers some sets S_i, $i = 1..n$, $|S_i| = 2$. There exists $s = (s_1, \ldots, s_n) \in S_1 \times \cdots \times S_n$, such that As and b are coordoninatewise distincts.

proof: The polynomial

$$\prod_{i=1}^{n} \left(\sum_{j=1}^{n} a_{i,j} X_j - b_i \right)$$

has degree n and the coefficient of $\prod_{i=1}^{n} X_i$ is $Per(A) \neq 0$.

Erdős Ginzburg Ziv

Theorem (Erdős Ginzburg Ziv - 1961)

G abelian finite group, $|G| = n$. Whathever $(g_1, g_2, \ldots, g_{2n-1})$ elements of G. There exists a zerosum subsequence of length n.

Erdős Ginzburg Ziv

Theorem (Erdős Ginzburg Ziv - 1961)

G abelian finite group, $|G| = n$. Whathever $(g_1, g_2, \ldots, g_{2n-1})$ elements of G. There exists a zerosum subsequence of length n.

In [0,p-1], $\bar{g}_1 \leqslant \bar{g}_2 \leqslant \cdots \leqslant \bar{g}_{2p-1}$.

Erdős Ginzburg Ziv

Theorem (Erdős Ginzburg Ziv - 1961)

G abelian finite group, $|G| = n$. Whathever $(g_1, g_2, \ldots, g_{2n-1})$ elements of G. There exists a zerosum subsequence of length n.

In [0,p-1], $\bar{g}_1 \leqslant \bar{g}_2 \leqslant \cdots \leqslant \bar{g}_{2p-1}$.

- If $g_i = g_{i+p-1}$, one has p equal elements.

Erdős Ginzburg Ziv

Theorem (Erdős Ginzburg Ziv - 1961)

G abelian finite group, $|G| = n$. Whathever $(g_1, g_2, \ldots, g_{2n-1})$ elements of G. There exists a zerosum subsequence of length n.

In [0,p-1], $\bar{g}_1 \leqslant \bar{g}_2 \leqslant \cdots \leqslant \bar{g}_{2p-1}$.

- If $g_i = g_{i+p-1}$, one has p equal elements.
- Otherwise, one considers the $(p-1) \times (p-1)$ matrix with only 1's, its permanent is $(p-1)! \neq 0$. Define $S_i = \{g_i, g_{i+p-1}\}$, for $i \in [1, p-1]$, of cardinality 2, and b containing all values but $-g_{2p-1}$.

Snevily's Conjecture

G a finite group of odd order.

$a_1, \ldots, a_k$, k distinct elements and $b_1, \ldots, b_k$, k distincts elements.

then there exists a permutation π of $[1, k]$ such that

$a_1 + b_{\pi(1)}, \ldots, a_k + b_{\pi(k)}$ are pairwise distincts.

Snevily's Conjecture

G a finite group of odd order.

$a_1, \ldots, a_k$, k distinct elements and $b_1, \ldots, b_k$, k distincts elements.

then there exists a permutation π of $[1, k]$ such that

$a_1 + b_{\pi(1)}, \ldots, a_k + b_{\pi(k)}$ are pairwise distincts.

- $G = \mathbb{Z}/p\mathbb{Z}$ (Alon - 2000)

Snevily's Conjecture

G a finite group of odd order.
$a_1, \ldots, a_k$, k distinct elements and $b_1, \ldots, b_k$, k distincts elements.
then there exists a permutation π of $[1, k]$ such that
$a_1 + b_{\pi(1)}, \ldots, a_k + b_{\pi(k)}$ are pairwise distincts.

- $G = \mathbb{Z}/p\mathbb{Z}$ (Alon - 2000)
- $G = \mathbb{Z}/n\mathbb{Z}$ (Dasgupta, Karolyi, Serra, Szegedy - 2001),
  in $\mathbb{F}_{2^d}$ (with $n \mid 2^d - 1$), g of order n in $\mathbb{F}_{2^d}^{\times}$, the polynomial:

$$P(X_1, \ldots, X_k) = \prod_{1 \leqslant j < i \leqslant k} (X_i - X_j)(\alpha_i X_i - \alpha_j X_j).$$

has degree $k(k-1)$, where $\alpha_i = g^{b_i}$ and
$A_1 = \cdots = A_k = \{g^{a_i} \mid i = 1..k\}$.

Snevily's Conjecture

G a finite group of odd order.
$a_1, \ldots, a_k$, k distinct elements and $b_1, \ldots, b_k$, k distincts elements.
then there exists a permutation π of $[1, k]$ such that
$a_1 + b_{\pi(1)}, \ldots, a_k + b_{\pi(k)}$ are pairwise distincts.

- $G = \mathbb{Z}/p\mathbb{Z}$ (Alon - 2000)
- $G = \mathbb{Z}/n\mathbb{Z}$ (Dasgupta, Karolyi, Serra, Szegedy - 2001), in $\mathbb{F}_{2^d}$ (with $n \mid 2^d - 1$), g of order n in $\mathbb{F}_{2^d}^{\times}$, the polynomial:

$$P(X_1, \ldots, X_k) = \prod_{1 \leqslant j < i \leqslant k} (X_i - X_j)(\alpha_i X_i - \alpha_j X_j).$$

has degree $k(k-1)$, where $\alpha_i = g^{b_i}$ and
$A_1 = \cdots = A_k = \{g^{a_i} \mid i = 1..k\}$.
Coefficient of $\prod_{i=1}^{k} X_i^{k-1}$ is the Van der Monde permanent of the α_i's. In $\mathbb{F}_{2^d}$, permanent and determinant are equal.

A question of Erdős

$A = (a_1, \ldots, a_\ell)$ a sequence of $\mathbb{F}_p^\times$.
$\mathcal{S}_A$: set of $(0-1)$-solutions of

$$a_1 x_1 + \cdots + a_\ell x_\ell = 0.$$

$$\mathcal{S}_A = A^\perp \cap \{0,1\}^\ell$$

A question of Erdős

$A = (a_1, \ldots, a_\ell)$ a sequence of $\mathbb{F}_p^\times$.
$\mathcal{S}_A$: set of $(0-1)$-solutions of

$$a_1 x_1 + \cdots + a_\ell x_\ell = 0.$$

$$\mathcal{S}_A = A^\perp \cap \{0,1\}^\ell$$

One considers:

$$\dim(A) = \dim(\langle S_A \rangle).$$

Theorem (B.-Girard)

p a prime number, $A = (a_1, \ldots, a_\ell)$ a sequence of $\ell > p$ elements of $\mathbb{F}_p^\times$:

Theorem (B.-Girard)

p a prime number, $A = (a_1, \ldots, a_\ell)$ a sequence of $\ell > p$ elements of $\mathbb{F}_p^\times$:

$$\dim(A) = \ell - 1.$$

Theorem (B.-Girard)

p a prime number, $A = (a_1, \ldots, a_\ell)$ a sequence of $\ell > p$ elements of $\mathbb{F}_p^\times$:

$$\dim(A) = \ell - 1.$$

Method: $\mathcal{S}_A \subset \mathcal{S}_B$, $I_\lambda = \{i \in [1, \ell] : b_i/a_i = \lambda\}$.

Theorem (B.-Girard)

p a prime number, $A = (a_1, \ldots, a_\ell)$ a sequence of $\ell > p$ elements of $\mathbb{F}_p^\times$:

$$\dim(A) = \ell - 1.$$

Method: $\mathcal{S}_A \subset \mathcal{S}_B$, $I_\lambda = \{i \in [1, \ell] : b_i/a_i = \lambda\}$.
$\lambda_1, \ldots, \lambda_d$ ratios associated to (A, B) and $S_i = (a_j : j \in I_{\lambda_i})$ and $\Sigma_i = \Sigma(S_i)$.

Theorem (B.-Girard)

p a prime number, $A = (a_1, \ldots, a_\ell)$ a sequence of $\ell > p$ elements of $\mathbb{F}_p^\times$:

$$\dim(A) = \ell - 1.$$

Method: $\mathcal{S}_A \subset \mathcal{S}_B$, $I_\lambda = \{i \in [1, \ell] : b_i/a_i = \lambda\}$.
$\lambda_1, \ldots, \lambda_d$ ratios associated to (A, B) and $S_i = (a_j : j \in I_{\lambda_i})$ and $\Sigma_i = \Sigma(S_i)$. The polynomial

$$P(X_1, \ldots, X_d) = \left(\sum_{i=1}^{d} \lambda_i X_i\right)\left(\left(\sum_{i=1}^{d} X_i\right)^{p-1} - 1\right),$$

vanishes on $\prod_{i=1}^{d} \Sigma_i$, coefficient of $\prod X_i^{t_i}$ is $c \sum \lambda_i t_i$.

Theorem (B.-Girard)

p a prime number, $A = (a_1, \ldots, a_p)$ a sequence of p elements of $\mathbb{F}_p^\times$:

Theorem (B.-Girard)

p a prime number, $A = (a_1, \ldots, a_p)$ a sequence of p elements of $\mathbb{F}_p^\times$:

- $\dim(A) = 1$,

$$(a_1, \ldots, a_p) = (r, \ldots, r).$$

Theorem (B.-Girard)

p a prime number, $A = (a_1, \ldots, a_p)$ a sequence of p elements of $\mathbb{F}_p^\times$:

- $\dim(A) = 1$,
$$(a_1, \ldots, a_p) = (r, \ldots, r).$$
- $\dim(A) = p-2$, $\exists t \in [1, p-3]$,
$$(a_{\sigma(1)}, \ldots, a_{\sigma(p)}) = (\underbrace{r, \ldots, r}_{t}, \underbrace{-r, \ldots, -r}_{p-2-t}, -(t+1)r, -(t+1)r).$$

Theorem (B.-Girard)

p a prime number, $A = (a_1, \ldots, a_p)$ a sequence of p elements of $\mathbb{F}_p^\times$:

- $\dim(A) = 1$,
$$(a_1, \ldots, a_p) = (r, \ldots, r).$$
- $\dim(A) = p-2$, $\exists t \in [1, p-3]$,
$$(a_{\sigma(1)}, \ldots, a_{\sigma(p)}) = (\underbrace{r, \ldots, r}_{t}, \underbrace{-r, \ldots, -r}_{p-2-t}, -(t+1)r, -(t+1)r).$$
- $\dim(A) = p-1$.

The polynomial

$$P(X_1, \ldots, X_d) = \left(\sum_{i=1}^{d} \lambda_i X_i\right) \left(\left(\sum_{i=1}^{d} X_i\right)^{p-1} - 1\right),$$

vanishes on $\prod_{i=1}^{d} \Sigma_i$, the coefficient of $\prod X_i^{t_i}$ is $c \sum \lambda_i t_i$.

The polynomial

$$P(X_1, \ldots, X_d) = \left(\sum_{i=1}^{d} \lambda_i X_i\right) \left(\left(\sum_{i=1}^{d} X_i\right)^{p-1} - 1\right),$$

vanishes on $\prod_{i=1}^{d} \Sigma_i$, the coefficient of $\prod X_i^{t_i}$ is $c \sum \lambda_i t_i$.

- $$\sum_{i=1}^{d} (|\Sigma_i| - 1) \geq p$$

The polynomial

$$P(X_1, \ldots, X_d) = \left(\sum_{i=1}^{d} \lambda_i X_i\right) \left(\left(\sum_{i=1}^{d} X_i\right)^{p-1} - 1\right),$$

vanishes on $\prod_{i=1}^{d} \Sigma_i$, the coefficient of $\prod X_i^{t_i}$ is $c \sum \lambda_i t_i$.

- $$\sum_{i=1}^{d} (|\Sigma_i| - 1) \geq p$$
- If $\sum (|\Sigma_i| - 1) = p$, one has:

$$\sum \lambda_i (|\Sigma_i| - 1) = 0$$

The polynomial

$$P(X_1, \ldots, X_d) = \left(\sum_{i=1}^{d} \lambda_i X_i\right)\left(\left(\sum_{i=1}^{d} X_i\right)^{p-1} - 1\right),$$

vanishes on $\prod_{i=1}^{d} \Sigma_i$, the coefficient of $\prod X_i^{t_i}$ is $c \sum \lambda_i t_i$.

- $$\sum_{i=1}^{d} (|\Sigma_i| - 1) \geq p$$
- If $\sum(|\Sigma_i| - 1) = p$, one has:

$$\sum \lambda_i (|\Sigma_i| - 1) = 0$$

- And $|\Sigma_i| - 1 = |S_i|$, Σ_i arithmetic progression.

$i_0, j_0 \in [1, d]$ and $r_{i_0} \in S_{i_0}$

$$\Sigma'_{i_0} = \Sigma(S_{i_0} \setminus (r_{i_0})),\ \Sigma'_{j_0} = \Sigma(S_{j_0} \cup (r_{i_0})) = \Sigma_{j_0} + \{0, r_{i_0}\}$$

$i_0, j_0 \in [1, d]$ and $r_{i_0} \in S_{i_0}$

$$\Sigma'_{i_0} = \Sigma(S_{i_0} \smallsetminus (r_{i_0})),\ \Sigma'_{j_0} = \Sigma(S_{j_0} \cup (r_{i_0})) = \Sigma_{j_0} + \{0, r_{i_0}\}$$

$$Q_{i_0,j_0}(X_1, \ldots, X_d) = \left(\sum_{i=1}^{d} \lambda_i X_i\right)\left(\sum_{i=1}^{d} \lambda_i X_i - \chi\right)\left(\left(\sum_{i=1}^{d} X_i\right)^{p-1} - 1\right),$$

vanishes on $\prod_{i=1}^{d} \Sigma'_i$, $\chi = (\lambda_{j_0} - \lambda_{i_0}) r_{i_0}$.

$i_0, j_0 \in [1, d]$ and $r_{i_0} \in S_{i_0}$

$$\Sigma'_{i_0} = \Sigma(S_{i_0} \setminus (r_{i_0})),\ \Sigma'_{j_0} = \Sigma(S_{j_0} \cup (r_{i_0})) = \Sigma_{j_0} + \{0, r_{i_0}\}$$

$$Q_{i_0,j_0}(X_1, \ldots, X_d) = \left(\sum_{i=1}^{d} \lambda_i X_i\right)\left(\sum_{i=1}^{d} \lambda_i X_i - \chi\right)\left(\left(\sum_{i=1}^{d} X_i\right)^{p-1} - 1\right),$$

vanishes on $\prod_{i=1}^{d} \Sigma'_i$, $\chi = (\lambda_{j_0} - \lambda_{i_0}) r_{i_0}$. $|\Sigma'_{i_0}| = |\Sigma_{i_0}| - 1$ et $|\Sigma'_{j_0}| \geq |\Sigma_{j_0}| + 2$

$i_0, j_0 \in [1, d]$ and $r_{i_0} \in S_{i_0}$

$$\Sigma'_{i_0} = \Sigma(S_{i_0} \setminus (r_{i_0})),\ \Sigma'_{j_0} = \Sigma(S_{j_0} \cup (r_{i_0})) = \Sigma_{j_0} + \{0, r_{i_0}\}$$

$$Q_{i_0,j_0}(X_1, \ldots, X_d) = \left(\sum_{i=1}^{d} \lambda_i X_i\right)\left(\sum_{i=1}^{d} \lambda_i X_i - \chi\right)\left(\left(\sum_{i=1}^{d} X_i\right)^{p-1} - 1\right),$$

vanishes on $\prod_{i=1}^{d} \Sigma'_i$, $\chi = (\lambda_{j_0} - \lambda_{i_0}) r_{i_0}$. $|\Sigma'_{i_0}| = |\Sigma_{i_0}| - 1$ et $|\Sigma'_{j_0}| \geq |\Sigma_{j_0}| + 2$
For $t_{i_0} = |\Sigma_{i_0}| - 2$, $t_{j_0} = |\Sigma_{j_0}| + 1$, one has $t_i \leq |\Sigma'_i| - 1$, the coefficient is

$i_0, j_0 \in [1, d]$ and $r_{i_0} \in S_{i_0}$

$$\Sigma'_{i_0} = \Sigma(S_{i_0} \setminus (r_{i_0})),\ \Sigma'_{j_0} = \Sigma(S_{j_0} \cup (r_{i_0})) = \Sigma_{j_0} + \{0, r_{i_0}\}$$

$$Q_{i_0,j_0}(X_1, \ldots, X_d) = \left(\sum_{i=1}^{d} \lambda_i X_i\right)\left(\sum_{i=1}^{d} \lambda_i X_i - \chi\right)\left(\left(\sum_{i=1}^{d} X_i\right)^{p-1} - 1\right),$$

vanishes on $\prod_{i=1}^{d} \Sigma'_i$, $\chi = (\lambda_{j_0} - \lambda_{i_0}) r_{i_0}$. $|\Sigma'_{i_0}| = |\Sigma_{i_0}| - 1$ et $|\Sigma'_{j_0}| \geq |\Sigma_{j_0}| + 2$
For $t_{i_0} = |\Sigma_{i_0}| - 2$, $t_{j_0} = |\Sigma_{j_0}| + 1$, one has $t_i \leq |\Sigma'_i| - 1$, the coefficient is

$$2(\lambda_{j_0} - \lambda_{i_0})^2 - \sum_{i=1}^{d} \lambda_i^2 (|\Sigma_i| - 1)$$

Theorem (B.-Girard)

p a prime number, $A = (a_1, \ldots, a_{p-1})$ a zerosum sequence of $p-1$ elements of $\mathbb{F}_p^\times$:

- $\dim(A) = 1$,

$$(a_{\sigma(1)}, \ldots, a_{\sigma(p-1)}) = (r, \ldots, r, 2r).$$

Theorem (B.-Girard)

p a prime number, $A = (a_1, \ldots, a_{p-1})$ a zerosum sequence of $p-1$ elements of $\mathbb{F}_p^\times$:

- $\dim(A) = 1$, $(r, \ldots, r, 2r)$.
- $\dim(A) = p-4$,

$$(a_{\sigma(1)}, \ldots, a_{\sigma(p-1)}) = (\underbrace{r, \ldots, r}_{p-5}, -r, 2r, 2r, 2r).$$

Theorem (B.-Girard)

p a prime number, $A = (a_1, \ldots, a_{p-1})$ a zerosum sequence of $p-1$ elements of $\mathbb{F}_p^\times$:

- $\dim(A) = 1$, $(r, \ldots, r, 2r)$.
- $\dim(A) = p-4$, $(\underbrace{r, \ldots, r}_{p-5}, -r, 2r, 2r, 2r)$.
- $\dim(A) = p-3$, $\exists t \in [0, p-6]$,

$$(a_{\sigma(1)}, \ldots, a_{\sigma(p-1)}) = (\underbrace{r, \ldots, r}_{t}, \underbrace{-r, \ldots, -r}_{p-4-t}, 2r, -(t+3)r, -(t+3)r).$$

Theorem (B.-Girard)

p a prime number, $A = (a_1, \ldots, a_{p-1})$ a zerosum sequence of $p-1$ elements of $\mathbb{F}_p^\times$:

- $\dim(A) = 1$, $(r, \ldots, r, 2r)$.
- $\dim(A) = p-4$, $(\underbrace{r, \ldots, r}_{p-5}, -r, 2r, 2r, 2r)$.
- $\dim(A) = p-3$, $\exists t \in [0, p-6]$,
  $(\underbrace{r, \ldots, r}_{t}, \underbrace{-r, \ldots, -r}_{p-4-t}, 2r, -(t+3)r, -(t+3)r)$.
- $\dim(A) = p-3$, $\exists t \in [1, p-4]$,

$$(a_{\sigma(1)}, \ldots, a_{\sigma(p-1)}) = (\underbrace{r, \ldots, r}_{t}, \underbrace{-r, \ldots, -r}_{p-3-t}, -(t+1)r, -(t+2)r).$$

Theorem (B.-Girard)

p a prime number, $A = (a_1, \ldots, a_{p-1})$ a zerosum sequence of $p-1$ elements of $\mathbb{F}_p^\times$:

- $\dim(A) = 1$, $(r, \ldots, r, 2r)$.
- $\dim(A) = p-4$, $(\underbrace{r, \ldots, r}_{p-5}, -r, 2r, 2r, 2r)$.
- $\dim(A) = p-3$, $\exists t \in [0, p-6]$,
  $(\underbrace{r, \ldots, r}_{t}, \underbrace{-r, \ldots, -r}_{p-4-t}, 2r, -(t+3)r, -(t+3)r)$.
- $\dim(A) = p-3$, $\exists t \in [1, p-4]$,
  $(\underbrace{r, \ldots, r}_{t}, \underbrace{-r, \ldots, -r}_{p-3-t}, -(t+1)r, -(t+2)r)$.
- $p = 7$, $\dim(A) = p-3 = 4$,

$$(a_{\sigma(1)}, \ldots, a_{\sigma(6)}) = (-1, 1, -2, 2, -3, 3).$$

Theorem (B.-Girard)

p a prime number, $A = (a_1, \ldots, a_{p-1})$ a zerosum sequence of $p-1$ elements of $\mathbb{F}_p^\times$:

- $\dim(A) = 1$, $(r, \ldots, r, 2r)$.
- $\dim(A) = p-4$, $(\underbrace{r, \ldots, r}_{p-5}, -r, 2r, 2r, 2r)$.
- $\dim(A) = p-3$, $\exists t \in [0, p-6]$,
  $(\underbrace{r, \ldots, r}_{t}, \underbrace{-r, \ldots, -r}_{p-4-t}, 2r, -(t+3)r, -(t+3)r)$.
- $\dim(A) = p-3$, $\exists t \in [1, p-4]$,
  $(\underbrace{r, \ldots, r}_{t}, \underbrace{-r, \ldots, -r}_{p-3-t}, -(t+1)r, -(t+2)r)$.
- $p = 7$, $\dim(A) = p-3 = 4$, $(-1, 1, -2, 2, -3, 3)$.
- $\dim(A) = p-2$.