Applications of the Combinatorial Nullstellensatz

Éric Balandraud
Université de Bordeaux

IPMCCC
April 16, 2019

Plan

The Combinatorial Nullstellensatz and the polynomial method

Applications in various fields

Additive results on sequences

Sequences or geometry in finite fields

Addition Theorems in $\mathbb{F}_p$

Plan

The Combinatorial Nullstellensatz

Theorem (Alon 1999)

K a field and P a polynomial from $K[X_1, \ldots, X_d]$.
If $\deg(P) = \sum_{i=1}^{d} k_i$ and its coefficient of $\prod_{i=1}^{d} X_i^{k_i}$ is not zero,

The Combinatorial Nullstellensatz

Theorem (Alon 1999)

K a field and P a polynomial from $K[X_1, \ldots, X_d]$.
If $\deg(P) = \sum_{i=1}^{d} k_i$ and its coefficient of $\prod_{i=1}^{d} X_i^{k_i}$ is not zero,
Then whatever $A_1, \ldots, A_d$ subsets of $\mathbb{K}$ satisfying $|A_i| > k_i$, there is $(a_1, \ldots, a_d) \in A_1 \times \cdots \times A_d$ such that :

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

Another formulation

Theorem

K a field and P a polynomial from $K[X_1, \ldots, X_d]$. Let $A_1, \ldots, A_d$ a family of subsets of K.
Denoting $g_i(X_i) = \prod_{a_i \in A_i}(X_i - a_i)$.

Another formulation

Theorem

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

$$P(\underline{X}) = \sum_{i=1}^{d} h_i(\underline{X}) g_i(X_i).$$

The coefficient formula

Theorem (Schauz, Karasev-Petrov, Lasoń)

K a field and P a polynomial from $K[X_1, \ldots, X_d]$.
If $\deg(P) = \sum_{i=1}^{d} k_i$ then whatever the family of subsets $A_1, \ldots, A_d$, such that $|A_i| = k_i + 1$, the coefficient of $\prod_{i=1}^{d} X_i^{k_i}$ in P is:

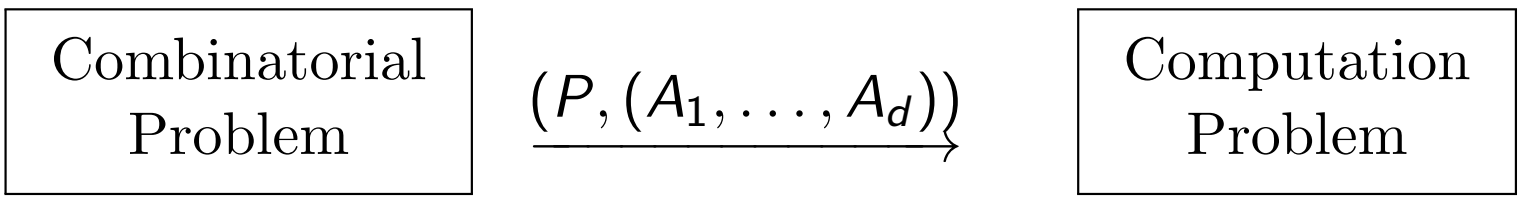
The coefficient formula

Theorem (Schauz, Karasev-Petrov, Lasoń)

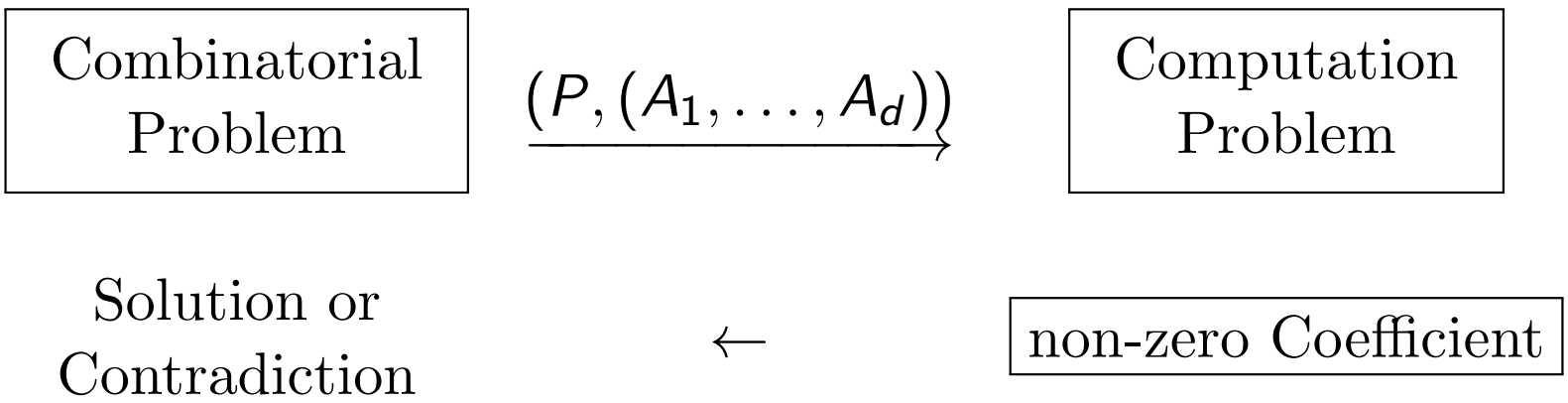
K a field and P a polynomial from $K[X_1, \ldots, X_d]$.
If $\deg(P) = \sum_{i=1}^{d} k_i$ then whatever the family of subsets $A_1, \ldots, A_d$, such that $|A_i| = k_i + 1$, the coefficient of $\prod_{i=1}^{d} X_i^{k_i}$ in P is:

$$c = \sum_{\underline{a} \in \prod A_i} \frac{P(\underline{a})}{\prod g_i'(a_i)}.$$

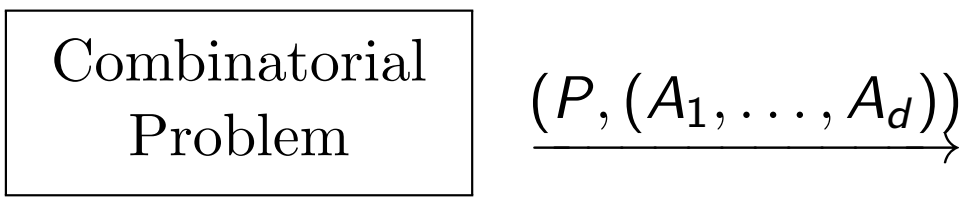
The polynomial method



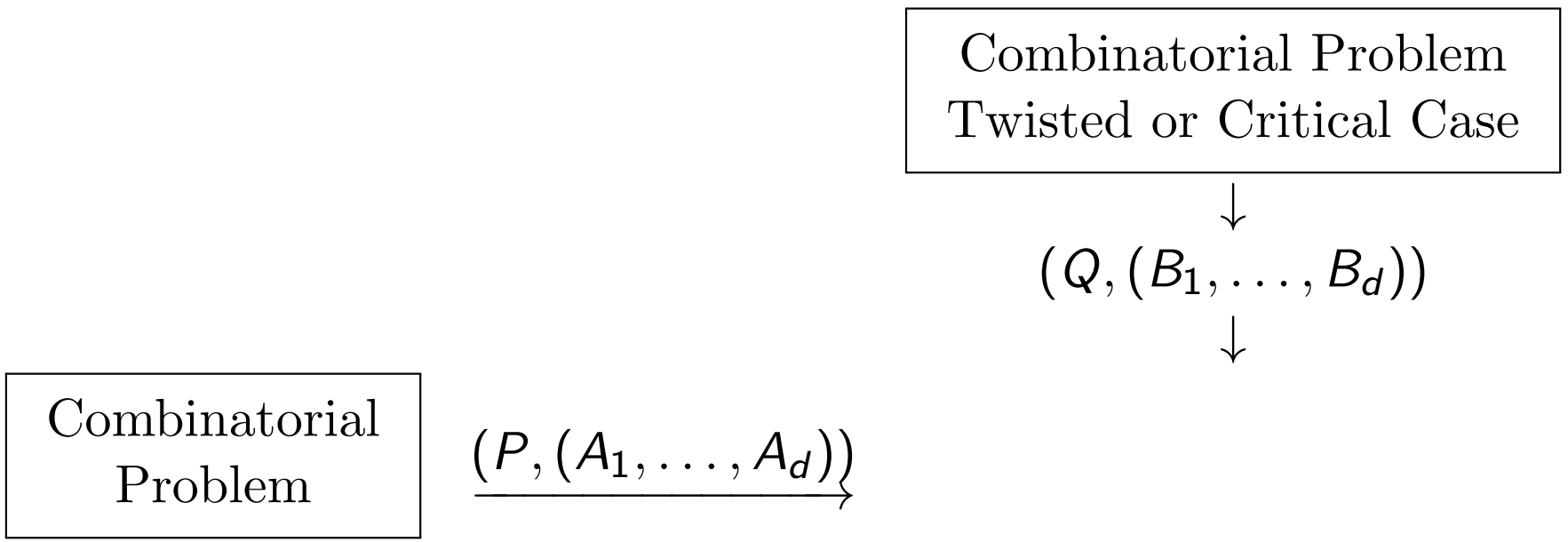
The polynomial method



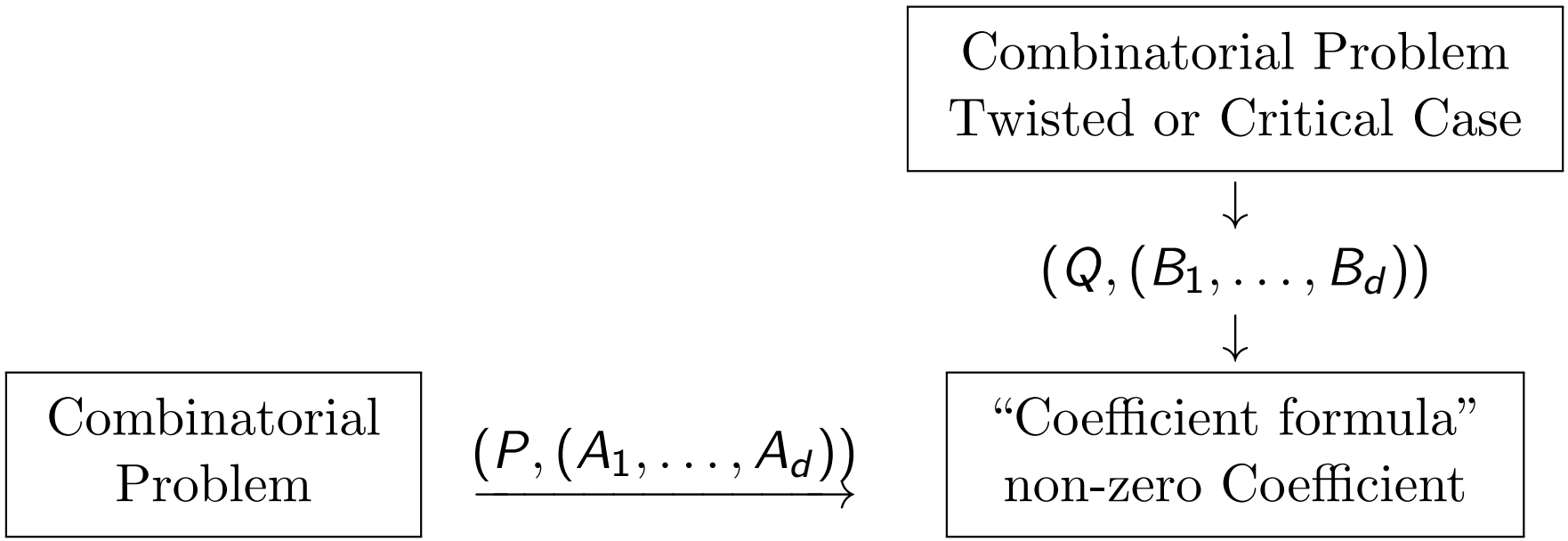
The polynomial method revisited



The polynomial method revisited



The polynomial method revisited



Plan

Theorem (Alon, Friedland, Kalai)

$p \in \mathbb{P}$, $G = (V, E)$ simple graph with average degre $\bar{d} > 2p - 2$ and max degre $\Delta \leqslant 2p - 1$, then G admits a p-regular subgraph.

Theorem (Alon, Friedland, Kalai)

$p \in \mathbb{P}$, $G = (V, E)$ simple graph with average degre $\bar{d} > 2p - 2$ and max degre $\Delta \leqslant 2p - 1$, then G admits a p-regular subgraph.

In $\mathbb{F}_p$, $\forall e \in E$, $A_e = \{0, 1\}$

$$P((X_e)_{e\in E}) = \prod_{v\in V}\left(1 - \left(\sum_{e\in E} a_{ve}X_e\right)^{p-1}\right) - \prod_{e\in E}(1 - X_e).$$

Theorem (Komjáth's conjecture, Alon-Furedi)

In $\mathbb{R}^d$, *to cover* $\{0,1\}^d \setminus (0,\ldots,0)$ *by hyperplanes not containing* $(0,\ldots,0)$, *one needs at least* d *hyperplanes.*

Theorem (Komjáth's conjecture, Alon-Furedi)

In $\mathbb{R}^d$, *to cover* $\{0,1\}^d \setminus (0,\ldots,0)$ *by hyperplanes not containing* $(0,\ldots,0)$, *one needs at least* d *hyperplanes.*

Given $m \leq d$ hyperplanes, $A_i = \{0,1\}$:

$$P(X_1,\ldots,X_d) = \prod_{i=1}^{m} \underbrace{\left(\sum_{j=1}^{d} a_{ij}X_j - 1\right)}_{\text{normalised equation}} - (-1)^{m-d} \prod_{j=1}^{d} (X_j - 1).$$

Theorem (Chevalley-Warning)

In $\mathbb{F}_p$*, whenever* $\sum \deg(P_i) < d$ *the number of solutions to*

$$\begin{cases} P_i(X_1, \ldots, X_d) = 0 \end{cases}$$

is a multiple of p*.*

Theorem (Chevalley-Warning)

In $\mathbb{F}_p$, *whenever* $\sum \deg(P_i) < d$ *the number of solutions to*

$$\begin{cases} P_i(X_1, \ldots, X_d) = 0 \end{cases}$$

is a multiple of p.

$\prod_{i=1}^{d} A_i = \mathbb{F}_p^d$,

$$\prod \left(1 - P_i^{p-1}(X_1, \ldots, X_d)\right) - \sum_{\underline{s} \in S} L_{\underline{s}}(X_1, \ldots, X_d).$$

Theorem (Conjecture de Dyson, Karasev-Petrov)

Given integers $a_1, \ldots, a_n$, *the fraction*

$$\prod_{1 \leq i \neq j \leq n} \left(1 - \frac{X_i}{X_j}\right)^{a_i}$$

has constant term $\binom{\Sigma a_i}{a_1, \ldots, a_n}$.

Theorem (Conjecture de Dyson, Karasev-Petrov)

Given integers $a_1, \ldots, a_n$, *the fraction*

$$\prod_{1 \leq i \neq j \leq n} \left(1 - \frac{X_i}{X_j}\right)^{a_i}$$

has constant term $\binom{\Sigma a_i}{a_1, \ldots, a_n}$.

Coefficient of $\prod_{i=1}^{n} X_i^{a-a_i}$ in $\prod_{1 \leq i < j \leq n} (-1)^{a_j} (X_j - X_i)^{a_j + a_i}$.
Consider the sets $A_i = [0, (\Sigma a_j) - a_i]$ and

$$\prod_{1 \leq i < j \leq n} \prod_{s=-a_i+1}^{a_j} (X_j - X_i + s).$$

Plan

The permanent Lemma

Theorem (Alon)

K a field, A an $n \times n$ matrix with non zero permanent, $b \in K^n$, and $S_i \subset \mathbb{K}$, $i = 1..n$, $|S_i| = 2$. There exists $s = (s_1, \ldots, s_n) \in S_1 \times \cdots \times S_n$, such that As and b are coordinatewise distincts.

The permanent Lemma

Theorem (Alon)

K a field, A an $n \times n$ matrix with non zero permanent, $b \in K^n$, and $S_i \subset \mathbb{K}$, $i = 1..n$, $|S_i| = 2$. There exists $s = (s_1, \ldots, s_n) \in S_1 \times \cdots \times S_n$, such that As and b are coordinatewise distincts.

$\prod_{i=1}^{n} A_i = \prod_{i=1}^{n} S_i$,

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

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

Theorem (Erdős, Ginzburg, Ziv)

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.

Theorem (Erdős, Ginzburg, Ziv)

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.

$\prod_{i=1}^{p-1} A_i = \prod_{i=1}^{p-1} \{g_i, g_{i+p-1}\}$

$$A = \underbrace{\begin{pmatrix} 1 & \ldots & 1 \\ \vdots & & \vdots \\ 1 & \ldots & 1 \end{pmatrix}}_{p-1},$$

$$\underline{b} = (-g_{2p-1} + 1, \ldots, -g_{2p-1} + (p-1)).$$

Snevily's conjecture

G a finite abelian group of odd order.

$a_1, \ldots, a_k$, distinct elements	There is π, such that
$b_1, \ldots, b_k$, distinct elements	$a_1 + b_{\pi(1)}, \ldots, a_k + b_{\pi(k)}$
	are pairwise distincts.

Snevily's conjecture

G a finite abelian group of odd order.

$a_1, \ldots, a_k$, distinct elements	There is π, such that
$b_1, \ldots, b_k$, distinct elements	$a_1 + b_{\pi(1)}, \ldots, a_k + b_{\pi(k)}$
	are pairwise distincts.

$G = \mathbb{Z}/n\mathbb{Z}$ (Dasgupta, Karolyi, Serra, Szegedy),
$\prod_{i=1}^{k} A_i = \{g^{a_i} \mid i = 1..k\}^k \subset \mathbb{F}_{2^d}^k$,

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

with $\alpha_i = g^{b_i}$.

Theorem (Kemnitz conjecture - Rónyai)

In a sequence of $4p-2$ *elements* $((a_i, b_i))$ *of* $\mathbb{F}_p^2$, *there is a* 0*-sum subsequence of length* p*:*

Theorem (Kemnitz conjecture - Rónyai)

In a sequence of $4p-2$ *elements* $((a_i, b_i))$ *of* $\mathbb{F}_p^2$*, there is a* 0*-sum subsequence of length* p*:*

$\prod_{i=1}^{4p-2} A_i = \{0,1\}^{4p-2}$,

$$\left(1-\left(\sum_{i=1}^{4p-2} a_i X_i\right)^{p-1}\right)\left(1-\left(\sum_{i=1}^{4p-2} b_i X_i\right)^{p-1}\right)$$

$$\times\left(1-\left(\sum_{i=1}^{4p-2} X_i\right)^{p-1}\right)\left(\sum_{\substack{I\in[1,4p-2]\\|I|=p}}\prod_{i\in I} X_i - 2\right) + (2L_{\underline{0}}(\underline{X})).$$

Plan

Problem "à la Vinatier"

Theorem (Gács, Héger, Nagy, Pálvögyi)

In $\mathbb{F}_q^n$, $n \leqslant q$, $H_{i,j} = \{\underline{X} | X_i = X_j\}$, *whenever* $H \subset \bigcup_{i \neq j} H_{i,j}$.

Problem "à la Vinatier"

Theorem (Gács, Héger, Nagy, Pálvögyi)

In $\mathbb{F}_q^n$, $n \leqslant q$, $H_{i,j} = \{\underline{X} | X_i = X_j\}$, *whenever* $H \subset \bigcup_{i \neq j} H_{i,j}$.

- $H = H_{i,j}$,
- $n = q$, $H = \{\underline{X} | \alpha(X_i - X_j) + \sum X_k = 0\}$,
- $n = q - 1$, $H = \{\underline{X} | X_j + \sum X_k = 0\}$.

Theorem

$(a_1, \ldots, a_q) \in \mathbb{F}_q^q$

There is no pairwise distinct $(b_1, \ldots, b_q) \in \mathbb{F}_q^q$ *such that* $\sum_{i=1}^{q} a_i b_i = 0$.

$\iff$ *There are* $(a, b) \in \mathbb{F}_q$, $b \neq 0$ *such that* $a_i = a + b$, $a_j = a - b$, *and* $k \neq i, j$, $a_k = a$.

Theorem

$(a_1, \ldots, a_q) \in \mathbb{F}_q^q$

There is no pairwise distinct $(b_1, \ldots, b_q) \in \mathbb{F}_q^q$ *such that* $\sum_{i=1}^q a_i b_i = 0$.

$\iff$ *There are* $(a, b) \in \mathbb{F}_q$, $b \neq 0$ *such that* $a_i = a + b$, $a_j = a - b$, *and* $k \neq i, j$, $a_k = a$.

$\prod_{i=1}^q A_i = \mathbb{F}_q^q$,

$$G(\underline{Y}) = \left(\left(\sum_{i=1}^{k} Y_i \right)^{q-1} - 1 \right) \begin{vmatrix} a_1^{k-1} & a_1^{k-1} Y_1 & \ldots & Y_1^{k-1} \\ a_2^{k-1} & a_2^{k-1} Y_2 & \ldots & Y_2^{k-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_k^{k-1} & a_k^{k-1} Y_k & \ldots & Y_k^{k-1} \end{vmatrix}.$$

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

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

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

Set

$$\dim(A) = \dim(< \mathcal{S}_A >).$$

Theorem (B.-Girard)

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

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

Theorem (B.-Girard)

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

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

Theorem (B.-Girard)

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

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

$\mathcal{S}_A \subset \mathcal{S}_B$,

$$\Sigma_i = \Sigma(S_i),\ \ S_i = (a_j \in A : b_j/a_j = \lambda_i)$$

$$\mathcal{S}_A \subset \mathcal{S}_B,$$

$$\Sigma_i = \Sigma(S_i),\ \ S_i = (a_j \in A : b_j/a_j = \lambda_i)$$

$$\prod A_i = \prod \Sigma_i,$$

$$P(X_1, \ldots, X_d) = \left(\underbrace{\sum_{i=1}^{d} \lambda_i X_i}_{\sum_{i\in I} b_i} \right) \left(\left(\underbrace{\sum_{i=1}^{d} X_i}_{\sum_{i\in I} a_i} \right)^{p-1} - 1 \right).$$

Plan

Theorem (Cauchy-Davenport)

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

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

Theorem (Cauchy-Davenport)

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

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

$(p > (|A|-1)+|B-1|)$
$A \times B$,

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

The coefficient of $X^{|A|-1}Y^{|B|-1}$ is $\binom{(|A|-1)+(|B|-1)}{|A|-1} \neq 0$.

Conjecture (Erdős-Heilbronn)

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

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

Conjecture (Erdős-Heilbronn)

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

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

Define:

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

Theorem (Dias da Silva, Hamidoune)

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

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

$$(p > h(|A| - h))$$

$$\left|\begin{array}{lll} A_1 & = \left\{a_1, \ldots, a_{|A|-h}, a_{|A|-h+1}\right\} & \\ \vdots & \vdots & \ddots \\ A_{h-1} & = \left\{a_1, \quad \cdots \quad , a_{|A|-1}\right\} & \\ A_h & = \left\{a_1, \quad \cdots \quad , a_{|A|-1}, a_{|A|}\right\}, & \end{array}\right.$$

$$\prod_{c \in h^{\wedge} A} (X_1 + \cdots + X_h - c) \left(\prod_{1 \leqslant i < j \leqslant h} (X_j - X_i) \right).$$

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

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

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 (B.)

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

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

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

$$(p > \tfrac{d(d+1)}{2} + 1)$$

$$A = \{2a_1, \ldots, 2a_d\},\ \Sigma(A) = \left(\sum_{i=1}^{d} a_i\right) + \sum_{i=1}^{d} \{-a_i, a_i\}$$

$$\left|\begin{array}{ll} A_1 & = \{a_1, \ldots, a_d, -a_1\} \\ \vdots & \qquad\qquad\qquad\quad \ddots \\ A_d & = \{a_1, \ldots, a_d, -a_1, \ldots, -a_d\}, \end{array}\right.$$

$$\prod_{c \in \Sigma(A)} (X_1 + \cdots + X_d - c) \left(\prod_{1 \leqslant i < j \leqslant d} (X_j^2 - X_i^2) \right)$$

Define

$$\Sigma_\alpha(A) = \{a_1 + \cdots + a_k \mid a_i \in A,\ \alpha \leq k \leq |A|,\ a_i \neq a_j\}$$
$$\Sigma^\alpha(A) = \{a_1 + \cdots + a_k \mid a_i \in A,\ 0 \leq k \leq |A| - \alpha,\ a_i \neq a_j\}.$$

Define

$$\Sigma_\alpha(A) = \{a_1 + \cdots + a_k \mid a_i \in A,\ \alpha \le k \le |A|,\ a_i \neq a_j\}$$
$$\Sigma^\alpha(A) = \{a_1 + \cdots + a_k \mid a_i \in A,\ 0 \le k \le |A| - \alpha,\ a_i \neq a_j\}.$$

Theorem (B.)

$A \subset \mathbb{F}_p$ such that $A \cap (-A) = \emptyset$, then:

$$|\Sigma_\alpha(A)| = |\Sigma^\alpha(A)| \ge \min\left\{p, \frac{|A|(|A|+1)}{2} - \frac{\alpha(\alpha+1)}{2} + 1\right\}$$

Set $A = \{2a_1, 2a_2, \ldots, 2a_d\}$ et $m = \sum_{i=1}^{d} a_i$.
Let C such that $\Sigma^{\alpha}(A) \subset C$ and
$|C| = \min\left\{p-1, \frac{d(d+1)}{2} - \frac{\alpha(\alpha+1)}{2}\right\}$

$$P_{d,\alpha}(\underline{X}) = \prod_{x \in C}(X_1+\cdots+X_d+m-x) \prod_{1 \le i < j \le d}(X_j - X_i) \prod_{\substack{1 \le i < j \le d \\ \text{and } j > \alpha}}(X_j + X_i)$$

$$
\begin{array}{lcl}
A_1 & = & \{-a_d, \ldots, -a_\alpha\} \\
\vdots & & \vdots \qquad\qquad \ddots \\
A_\alpha & = & \{-a_d, \quad \ldots \quad , -a_1\} \\
A_{\alpha+1} & = & \{-a_d, \quad \ldots \quad , -a_1, \quad a_1, \ldots, a_{\alpha+1}\} \\
\vdots & & \vdots \qquad\qquad\qquad \vdots \quad \vdots \qquad\qquad \ddots \\
A_d & = & \{-a_d, \quad \ldots \quad , -a_1, \quad a_1, \quad \ldots \quad , a_d\}
\end{array}
$$

$$
\begin{array}{lcl}
B_1 & = & \{-d, \ldots, -\alpha\} \\
\vdots & & \vdots \qquad\qquad \ddots \\
B_\alpha & = & \{-d, \quad \ldots \quad , -1\} \\
B_{\alpha+1} & = & \{-d, \quad \ldots \quad , -1, \quad 1, \ldots, \alpha+1\} \\
\vdots & & \vdots \qquad\qquad\qquad \vdots \quad \vdots \qquad\qquad \ddots \\
B_d & = & \{-d, \quad \ldots \quad , -1, \quad 1, \qquad \ldots \qquad , d\}
\end{array}
$$