Applications of the Combinatorial Nullstellensatz in Additive Combinatorics

Éric Balandraud

Additive Combinatorics in Bordeaux
Lundi 11 Avril 2016

The Combinatorial Nullstellensatz

Theorem (Alon, 1999)

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

The Combinatorial Nullstellensatz

Theorem (Alon, 1999)

$\mathbb{K}$ 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, 1999)

$\mathbb{K}$ 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:

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

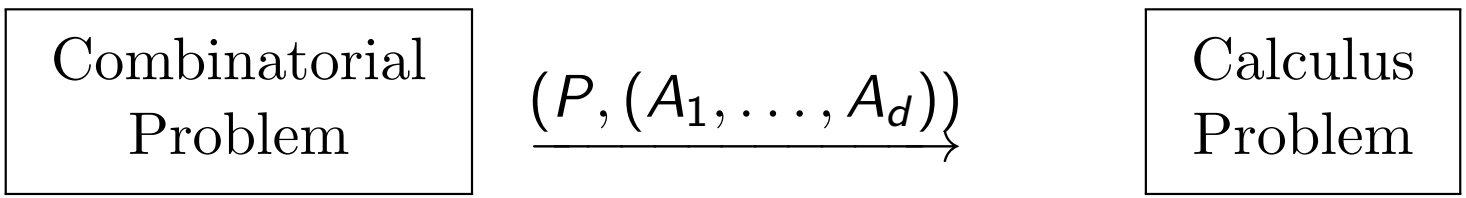
Another formulation

Theorem (Alon, 1999)

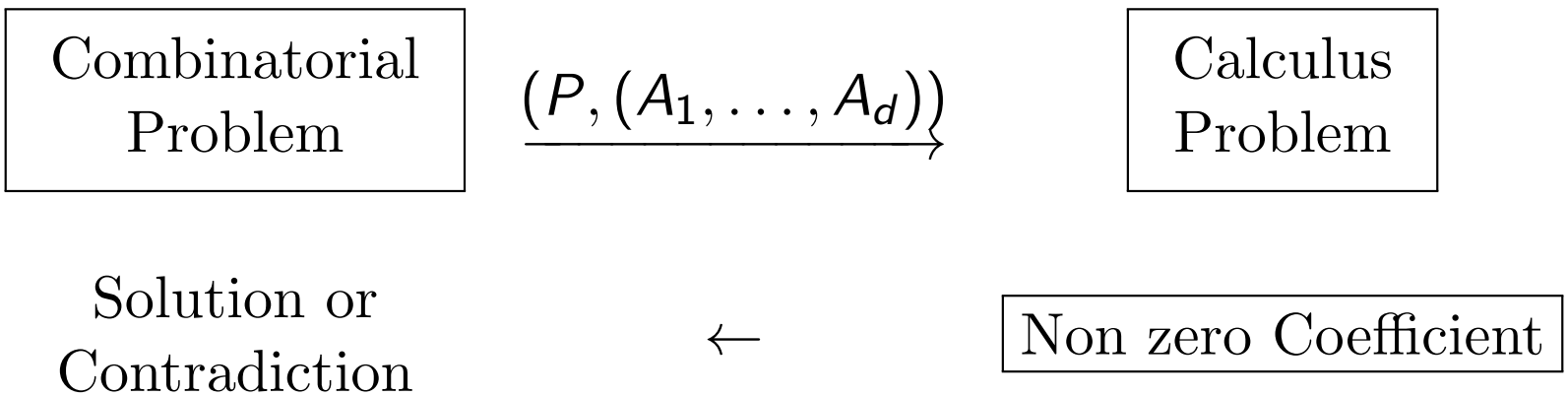
$\mathbb{K}$ a field and P a polynomial $\mathbb{K}[X_1, \ldots, X_d]$. Let $A_1, \ldots, A_d$ subsets of $\mathbb{K}$. Setting $g_i(X_i) = \prod_{a_i \in A_i}(X_i - a_i)$. If P vanishes on $A_1 \times \cdots \times A_d$, there exist $h_i \in \mathbb{K}[X_1, \ldots, X_d]$, with $\deg(h_i) \leqslant \deg(P)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

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

The polynomial method



The polynomial method



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:

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

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

Cauchy-Davenport

Theorem (Cauchy-Davenport - 1813, 1935)

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

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

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

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

Cauchy-Davenport

Theorem (Cauchy-Davenport - 1813, 1935)

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

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

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

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

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

Dias da Silva-Hamidoune

Conjecture (Erdős-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 (Erdős-Heilbronn - 1964)

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

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

Define:

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

Dias da Silva-Hamidoune

Conjecture (Erdős-Heilbronn - 1964)

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

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

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,

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

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

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

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

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

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

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 (B. - 2012)

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

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

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 (B. - 2012)

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

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

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

$(p > \frac{d(d+1)}{2} + 1)$, $A = \{2a_1, \ldots, 2a_d\}$:

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

$(p > \frac{d(d+1)}{2} + 1)$, $A = \{2a_1, \ldots, 2a_d\}$:

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

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

$(p > \frac{d(d+1)}{2} + 1)$, $A = \{2a_1, \ldots, 2a_d\}$:

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

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

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

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

$$\begin{pmatrix} a_1, \ldots, a_d \\ b_1, \ldots, b_d \end{pmatrix} = \begin{vmatrix} \binom{a_1}{b_1} & \binom{a_1}{b_2} & \cdots & \binom{a_1}{b_d} \\ \binom{a_2}{b_1} & \binom{a_2}{b_2} & \cdots & \binom{a_2}{b_d} \\ \vdots & \vdots & & \vdots \\ \binom{a_d}{b_1} & \binom{a_d}{b_2} & \cdots & \binom{a_d}{b_d)} \end{vmatrix}.$$

$$D_{n,h} = \begin{pmatrix} n-h, & n-h+1, & \ldots, & n-1 \\ 0, & 1, & \ldots, & (h-1) \end{pmatrix}$$

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

Binomial Determinants

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

$$D_{n,h} = \left(\begin{array}{ccccc} n-h, & n-h+1, & \ldots, & n-1 \\ 0, & 1, & \ldots, & (h-1) \end{array} \right) = 1 \neq 0,$$

$$D_d = \left(\begin{array}{ccccc} d, & d+1, & \ldots, & 2d-1 \\ 0, & 2, & \ldots, & 2(d-1) \end{array} \right) = 2^{d(d-1)/2} \neq 0$$

Additive results on sequences

- Erdős-Ginzburg-Ziv
- Snevily's conjecture (Arsovsky)
- Kemnitz' conjecture (Reiher)
- Problem "à la Vinatier"
- Nullstellensatz for sequences

The permanent Lemma

Theorem (Alon - 1999)

K a field, A an $n \times n$ matrix with non zero permanent, $b \in K^n$, 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 - 1999)

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 $Per(A) \neq 0$.

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.

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

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

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

Snevily's Conjecture

G a finite abelian group of odd order.

$a_1, \ldots, a_k$, distinct elements	
$b_1, \ldots, b_k$, distinct elements	

.

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 - 2001),
$\prod_{i=1}^{k} A_i = \{g^{a_i} \mid i = 1..k\}^k \subset \mathbb{F}_{2^d}^k$,

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

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

Kemnitz conjecture

Theorem (Rónyai - 2000)

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*:*

Kemnitz conjecture

Theorem (Rónyai - 2000)

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*:*

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

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

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

Problem "à la Vinatier"

Theorem (Gács, Héger, Nagy, Pálvögyi - 2010)

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 - 2010)

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, 2014)

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

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

Theorem (B.-Girard, 2014)

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

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

Theorem (B.-Girard, - 2014)

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

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

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

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

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

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

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

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