# Combinatorial Nullstellensatz

Richard (Evan) Chen

SPARC 2013
Summer Program for Applied Rationality and Cognition

August 28, 2013

# The Theorem Statement



Let $F$ be a field (e.g. $\mathbb{R}$ or $\mathbb{Z}_p$).

**Theorem (A Trivial Theorem)**

*Let $f \in F[x]$ be a polynomial of degree $t$. If $S \subseteq F$ satisfies $|S| > t$, then*

$$\exists s \in S : f(s) \neq 0.$$

# The Theorem Statement



Let $F$ be a field (e.g. $\mathbb{R}$ or $\mathbb{Z}_p$).

**Theorem (Combinatorial Nullstellensatz)**

*Let $f \in F[x_1, x_2, \ldots, x_n]$ be a polynomial of degree $t_1 + \cdots + t_n$. If $S_1, S_2, \ldots, S_n \subseteq F$ satisfies $|S_i| > t_i$ for all $i$,*

$$\exists s_i \in S_i : f(s_1, s_2, \ldots, s_n) \neq 0$$

*whenever the coefficient of $x_1^{t_1} x_2^{t_2} \ldots x_n^{t_n}$ is nonzero.*

# Small Fry



**Problem (Russia 2007, Day 2, Problem 1)**

Two distinct numbers are written on each vertex of a convex 100-gon. Prove one can remove a number from each vertex so that the remaining numbers on any two adjacent vertices differ.

**Proof.**

Define $P(x_1, \ldots, x_{100})$ by

$$(x_1 - x_2)(x_2 - x_3)(x_3 - x_4)\ldots(x_{99} - x_{100})(x_{100} - x_1).$$

The coefficient of $x_1 x_2 \ldots x_{100}$ is 2. □

# Small Fry



**Problem (Russia 2007, Day 2, Problem 1)**

Two distinct numbers are written on each vertex of a convex 100-gon. Prove one can remove a number from each vertex so that the remaining numbers on any two adjacent vertices differ.

**Proof.**

Define $P(x_1, \ldots, x_{100})$ by

$$(x_1 - x_2)(x_2 - x_3)(x_3 - x_4)\ldots(x_{99} - x_{100})(x_{100} - x_1).$$

The coefficient of $x_1 x_2 \ldots x_{100}$ is $2$. □

# #1's are easy, let's kill IMO #6's



## Problem (IMO 2007 Problem 6)

Let $n$ be a positive integer. Consider

$$S = \{(x, y, z) \mid x, y, z \in \{0, 1, \ldots, n\}, (x, y, z) \neq (0, 0, 0)\}$$

as a set of $(n+1)^3 - 1$ points in the three-dimensional space. Determine the smallest possible number of planes, the union of which contains $S$ but does not include $(0, 0, 0)$.

## Answer

$3n$. Use the planes $x = 1, 2, \ldots, n$, $y = 1, 2, \ldots, n$ and $z = 1, 2, \ldots, n$.

# #1's are easy, let's kill IMO #6's



## Problem (IMO 2007 Problem 6)

Let $n$ be a positive integer. Consider

$$S = \{(x, y, z) \mid x, y, z \in \{0, 1, \ldots, n\}, (x, y, z) \neq (0, 0, 0)\}$$

as a set of $(n+1)^3 - 1$ points in the three-dimensional space. Determine the smallest possible number of planes, the union of which contains $S$ but does not include $(0, 0, 0)$.

## Answer

$3n$. Use the planes $x = 1, 2, \ldots, n$, $y = 1, 2, \ldots, n$ and $z = 1, 2, \ldots, n$.

# Solution to IMO 2007/6



Suppose for contradiction we have $k < 3n$ planes. Let them be $a_i x + b_i y + c_i z + d_i = 0$.

$$A(x,y,z) \stackrel{\text{def}}{=} \prod_{i=1}^{k} (a_i x + b_i y + c_i z + d_i)$$

$$B(x,y,z) \stackrel{\text{def}}{=} \prod_{i=1}^{n} (x-i) \prod_{i=1}^{n} (y-i) \prod_{i=1}^{n} (z-i)$$

- The coefficient of $x^n y^n z^n$ in $A$ is $0$.
- The coefficient of $x^n y^n z^n$ in $B$ is $1$.

# Solution to IMO 2007/6



Suppose for contradiction we have $k < 3n$ planes. Let them be $a_i x + b_i y + c_i z + d_i = 0$.

$$A(x,y,z) \stackrel{\text{def}}{=} \prod_{i=1}^{k} (a_i x + b_i y + c_i z + d_i)$$

$$B(x,y,z) \stackrel{\text{def}}{=} \prod_{i=1}^{n} (x-i) \prod_{i=1}^{n} (y-i) \prod_{i=1}^{n} (z-i)$$

- The coefficient of $x^n y^n z^n$ in $A$ is $0$.
- The coefficient of $x^n y^n z^n$ in $B$ is $1$.

# Solution to IMO 2007/6



Suppose for contradiction we have $k < 3n$ planes. Let them be $a_i x + b_i y + c_i z + d_i = 0$.

$$A(x,y,z) \stackrel{\text{def}}{=} \prod_{i=1}^{k} (a_i x + b_i y + c_i z + d_i)$$

$$B(x,y,z) \stackrel{\text{def}}{=} \prod_{i=1}^{n} (x-i) \prod_{i=1}^{n} (y-i) \prod_{i=1}^{n} (z-i)$$

- The coefficient of $x^n y^n z^n$ in $A$ is $0$.
- The coefficient of $x^n y^n z^n$ in $B$ is $1$.

# Solution to IMO 2007/6, continued



$$P(x,y,z) \stackrel{\text{def}}{=} A(x,y,z) - \frac{A(0,0,0)}{B(0,0,0)} B(x,y,z).$$

- Now $P(x,y,z) = 0$ for any $x, y, z \in \{0, 1, \ldots, n\}^3$.
- But the coefficient of $x^n y^n z^n$ is $-\frac{A(0,0,0)}{B(0,0,0)}$.
- This is a contradiction of the nullstellensatz.

# Solution to IMO 2007/6, continued



$$P(x,y,z) \stackrel{\text{def}}{=} A(x,y,z) - \frac{A(0,0,0)}{B(0,0,0)} B(x,y,z).$$

- Now $P(x,y,z) = 0$ for any $x, y, z \in \{0, 1, \ldots, n\}^3$.
- But the coefficient of $x^n y^n z^n$ is $-\frac{A(0,0,0)}{B(0,0,0)}$.
- This is a contradiction of the nullstellensatz.

# Taking mod $p$



Let $p$ denote an odd prime.

Let $\mathbb{Z}_p$ denote the integers modulo $p$; this is a field.

# Cauchy-Davenport



**Theorem (Cauchy-Davenport)**

*If $A$ and $B$ are subsets of $\mathbb{Z}_p$, where $p$ is prime, then*

$$|A+B| \geq \min(p, |A|+|B|-1).$$

**Proof.**

- If $|A|+|B|>p$ you can just use Pigeonhole.
- Otherwise, take any set $C$ with $|C| = |A|+|B|-2$. We want to show $\exists (a,b) \in A \times B$ for which $a+b \notin C$.

$$f(a,b) \stackrel{\text{def}}{=} \prod_{c \in C} (a+b-c).$$

The coefficient of $a^{|A|-1}b^{|B|-1}$ is $\binom{|A|+|B|-2}{|A|-1} \not\equiv 0 \pmod{p}$. $\square$

# Cauchy-Davenport



## Theorem (Cauchy-Davenport)

*If $A$ and $B$ are subsets of $\mathbb{Z}_p$, where $p$ is prime, then*

$$|A+B| \geq \min(p, |A|+|B|-1).$$

## Proof.

- If $|A|+|B| > p$ you can just use Pigeonhole.
- Otherwise, take any set $C$ with $|C| = |A|+|B|-2$. We want to show $\exists (a,b) \in A \times B$ for which $a+b \notin C$.

$$f(a,b) \stackrel{\text{def}}{=} \prod_{c \in C} (a+b-c).$$

The coefficient of $a^{|A|-1}b^{|B|-1}$ is $\binom{|A|+|B|-2}{|A|-1} \not\equiv 0 \pmod{p}$. $\square$

# Cauchy-Davenport



## Theorem (Cauchy-Davenport)

*If $A$ and $B$ are subsets of $\mathbb{Z}_p$, where $p$ is prime, then*

$$|A+B| \geq \min(p, |A|+|B|-1).$$

## Proof.

- If $|A|+|B| > p$ you can just use Pigeonhole.
- Otherwise, take any set $C$ with $|C| = |A|+|B|-2$. We want to show $\exists (a,b) \in A \times B$ for which $a+b \notin C$.

$$f(a,b) \stackrel{\text{def}}{=} \prod_{c \in C} (a+b-c).$$

The coefficient of $a^{|A|-1}b^{|B|-1}$ is $\binom{|A|+|B|-2}{|A|-1} \not\equiv 0 \pmod{p}$. $\square$

# Cauchy-Davenport



## Theorem (Cauchy-Davenport)

*If $A$ and $B$ are subsets of $\mathbb{Z}_p$, where $p$ is prime, then*

$$|A+B| \geq \min(p, |A|+|B|-1).$$

## Proof.

- If $|A|+|B| > p$ you can just use Pigeonhole.
- Otherwise, take any set $C$ with $|C| = |A|+|B|-2$. We want to show $\exists (a,b) \in A \times B$ for which $a+b \notin C$.

$$f(a,b) \stackrel{\text{def}}{=} \prod_{c \in C} (a+b-c).$$

The coefficient of $a^{|A|-1}b^{|B|-1}$ is $\binom{|A|+|B|-2}{|A|-1} \not\equiv 0 \pmod{p}$. $\square$

# Cauchy-Davenport



## Theorem (Cauchy-Davenport)

*If $A$ and $B$ are subsets of $\mathbb{Z}_p$, where $p$ is prime, then*

$$|A+B| \geq \min(p, |A|+|B|-1).$$

## Proof.

- If $|A|+|B| > p$ you can just use Pigeonhole.
- Otherwise, take any set $C$ with $|C| = |A|+|B|-2$. We want to show $\exists (a,b) \in A \times B$ for which $a+b \notin C$.

$$f(a,b) \stackrel{\text{def}}{=} \prod_{c \in C} (a+b-c).$$

The coefficient of $a^{|A|-1}b^{|B|-1}$ is $\binom{|A|+|B|-2}{|A|-1} \not\equiv 0 \pmod{p}$. $\square$

# A 30-year Conjecture



**Theorem (Erdős-Heilbronn Conjecture)**

*Let $A$ be a subset of $\mathbb{Z}_p$. Then*

$$|\{x+y \mid x,y \in A, x \neq y\}| \geq \min(p, 2|A|-3).$$

**Proof.**

Similarly, suppose $|C| = 2|A| - 4 < p$. Define

$$f(x,y) = (x-y)\prod_{c\in C}(x+y-c).$$

The coefficient of $x^{|A|-1}y^{|A|-2}$ is

$$\binom{2|A|-4}{|A|-2} - \binom{2|A|-4}{|A|-3} = \left(\frac{|A|-3}{|A|-1} - 1\right)\binom{2|A|-4}{|A|-3} \neq 0.$$

□

# A 30-year Conjecture



**Theorem (Erdős-Heilbronn Conjecture)**

*Let $A$ be a subset of $\mathbb{Z}_p$. Then*

$$|\{x+y \mid x,y \in A, x \neq y\}| \geq \min(p, 2|A|-3).$$

**Proof.**

Similarly, suppose $|C| = 2|A| - 4 < p$. Define

$$f(x,y) = (x-y)\prod_{c\in C}(x+y-c).$$

The coefficient of $x^{|A|-1}y^{|A|-2}$ is

$$\binom{2|A|-4}{|A|-2} - \binom{2|A|-4}{|A|-3} = \left(\frac{|A|-3}{|A|-1} - 1\right)\binom{2|A|-4}{|A|-3} \neq 0.$$

□

# A 30-year Conjecture



**Theorem (Erdős-Heilbronn Conjecture)**

*Let $A$ be a subset of $\mathbb{Z}_p$. Then*

$$|\{x+y \mid x,y \in A, x \neq y\}| \geq \min(p, 2|A|-3).$$

**Proof.**

Similarly, suppose $|C| = 2|A| - 4 < p$. Define

$$f(x,y) = (x-y)\prod_{c\in C}(x+y-c).$$

The coefficient of $x^{|A|-1}y^{|A|-2}$ is

$$\binom{2|A|-4}{|A|-2} - \binom{2|A|-4}{|A|-3} = \left(\frac{|A|-3}{|A|-1} - 1\right)\binom{2|A|-4}{|A|-3} \neq 0.$$

□

# Chevalley's Theorem



## Corollary (Chevalley, 1935)

*Let $f_1, f_2, \cdots, f_k \in \mathbb{Z}_p[X_1, X_2, \cdots, X_n]$ satisfy $\sum_{i=1}^{k} \deg f_i < n$. If the polynomials $f_i$ have a common zero $(c_1, c_2, \cdots, c_n)$, then they have another common zero.*

## Proof.

$$A(x_1, x_2, \ldots, x_n) \stackrel{\text{def}}{=} \prod_{i=1}^{k} \left(f(x_1, x_2, \ldots, x_n)^{p-1} - 1\right)$$

$$B(x_1, x_2, \ldots, x_n) \stackrel{\text{def}}{=} \prod_{i=1}^{n} \left((x_i - c_i)^{p-1} - 1\right)$$

$$F(x_1, \ldots, x_n) \stackrel{\text{def}}{=} A(x_1, \ldots, x_n) - \delta B(x_1, \ldots, x_n)$$

where $\delta = \frac{A(c_1,\ldots,c_n)}{B(c_1,\ldots,c_n)}$. $[x_1^{p-1} x_2^{p-1} \ldots x_n^{p-1}]\, F = -\delta \neq 0$. □

# Chevalley's Theorem



## Corollary (Chevalley, 1935)

*Let $f_1, f_2, \cdots, f_k \in \mathbb{Z}_p[X_1, X_2, \cdots, X_n]$ satisfy $\sum_{i=1}^{k} \deg f_i < n$. If the polynomials $f_i$ have a common zero $(c_1, c_2, \cdots, c_n)$, then they have another common zero.*

## Proof.

$$A(x_1, x_2, \ldots, x_n) \stackrel{\text{def}}{=} \prod_{i=1}^{k} \left(f(x_1, x_2, \ldots, x_n)^{p-1} - 1\right)$$

$$B(x_1, x_2, \ldots, x_n) \stackrel{\text{def}}{=} \prod_{i=1}^{n} \left((x_i - c_i)^{p-1} - 1\right)$$

$$F(x_1, \ldots, x_n) \stackrel{\text{def}}{=} A(x_1, \ldots, x_n) - \delta B(x_1, \ldots, x_n)$$

where $\delta = \frac{A(c_1,\ldots,c_n)}{B(c_1,\ldots,c_n)}$. $[x_1^{p-1} x_2^{p-1} \ldots x_n^{p-1}]\, F = -\delta \neq 0.$ □

# Chevalley's Theorem



## Corollary (Chevalley, 1935)

*Let $f_1, f_2, \cdots, f_k \in \mathbb{Z}_p[X_1, X_2, \cdots, X_n]$ satisfy $\sum_{i=1}^{k} \deg f_i < n$. If the polynomials $f_i$ have a common zero $(c_1, c_2, \cdots, c_n)$, then they have another common zero.*

## Proof.

$$A(x_1, x_2, \ldots, x_n) \stackrel{\text{def}}{=} \prod_{i=1}^{k} \left(f(x_1, x_2, \ldots, x_n)^{p-1} - 1\right)$$

$$B(x_1, x_2, \ldots, x_n) \stackrel{\text{def}}{=} \prod_{i=1}^{n} \left((x_i - c_i)^{p-1} - 1\right)$$

$$F(x_1, \ldots, x_n) \stackrel{\text{def}}{=} A(x_1, \ldots, x_n) - \delta B(x_1, \ldots, x_n)$$

where $\delta = \frac{A(c_1,\ldots,c_n)}{B(c_1,\ldots,c_n)}$. $[x_1^{p-1} x_2^{p-1} \ldots x_n^{p-1}]\ F = -\delta \neq 0$. □

# More Treats



## Theorem (Troi-Zannier)

*Let $p$ be a prime and let $S_1, S_2, \cdots, S_k \subseteq \mathbb{Z}_{\geq 0}$, each containing $0$ and having pairwise distinct elements modulo $p$. Suppose that $\sum_i (|S_i| - 1) \geq p$. Then for any elements $a_1, \cdots, a_k \in \mathbb{Z}_p$, the equation $\sum_i x_i a_i = 0$ has a solution $(x_1, \cdots, x_k) \in S_1 \times \cdots \times S_k$ other than the all-zero solution.*

## Problem (TSTST 2011/9)

Let $n \in \mathbb{Z}^+$. Suppose we're given $2^n + 1$ distinct sets, each containing finitely many objects. Place each set into one of two categories, the red sets and the blue sets, with at least one set in each category. We define the *symmetric difference* of two sets as the set of objects belonging to exactly one of the two sets. Prove that there are at least $2^n$ different sets which can be obtained as the symmetric difference of a red and blue set.

# And More Treats...



**Theorem**

*Let $H_1, H_2, \ldots, H_m$ be a family of hyperplanes in $R^n$ that cover all vertices of the unit cube $\{0,1\}^n$ but one. Then $m \leq n$.*

**Theorem (Alon)**

*For any prime $p$, any loopless graph $G = (V, E)$ with average degree at least $2p-2$ and maximum degree at most $2p-1$ contains a $p$-regular subgraph.*

Corollary of above is the Berge-Saurer Conjecture: any simple $4$-regular graph contains a $3$-regular subgraph.

# And Even More Treats...



## Theorem (Alon)

*A graph $G = (V, E)$ on the vertices $\{1, 2, \ldots, n\}$ is not $k$-colorable if and only if the graph polynomial[a] $f_G$ lies in the ideal generated by the polynomials $x_i^k - 1$, where $1 \le i \le n$.*

[a] The graph polynomial
$f_G = f_G(x_1, x_2, \ldots, x_n) = \prod\{(x_i - x_j) : i < j, \{v_i, v_j\} \in E\}$.

## Theorem (Alon)

*Let $p$ be a prime, and let $G = (V, E)$ be a graph on a set of $|V| > d(p-1)$ vertices. Then there is a nonempty subset $U$ of vertices of $G$ such that the number of cliques of $d$ vertices of $G$ that intersect $U$ is $0$ modulo $p$.*

# Summary



1. Encode condition in a polynomial.
2. Check a coefficient is nonzero.
3. Profit.