Additive Combinatorics and the Polynomial Method

John R. Schmitt
Mathematics Department
Middlebury College

Vermont, USA

March 2022

What is Additive Combinatorics?

"(A)dditive combinatorics is a marriage of number theory, harmonic analysis, combinatorics, and ideas from ergodic theory, which aims to understand very *simple* systems: the operations of addition and multiplication and how they interact."

-Ben Green, Waynflete Professor of Pure Mathematics, U. Oxford

An *additive group* is any abelian group Z with group operation $+$. Examples: the integers $\mathbb{Z}$, a cyclic group $\mathbb{Z}_n$, Euclidean space $\mathbb{R}^n$, a finite field geometry $\mathbb{F}_p^n$. An *additive set* is a pair (A, Z), where Z is an additive group, and A is a finite non-empty subset of Z. Often we abbreviate as A.

Let A and B be additive sets in Z, then we define:

$$A + B := \{a + b : a \in A, b \in B\}$$

$$A - B := \{a - b : a \in A, B \in B\}$$

$$kA := \{a_1 + \cdots + a_k : a_i \in A\}$$

$$k \cdot A := \{ka : a \in A\}$$

$$A \cdot A := \{ab : a, b \in A\}$$

Examples of additive structure

- Arithmetic progressions:
  $a + [0, N) \cdot r := \{a, a + r, \ldots a + (N-1)r\}$
  where $a, r \in Z$ and $N \in \mathbb{Z}^+$
- d-dimensional arithmetic progressions:
  $a + [0, N) \cdot v := \{a + n_1 v_1 + \cdots n_d v_d : 0 \leq n_j < N_j \textit{ for all } 1 \leq j \leq d\}$
  where $a \in Z$, $v = (v_1, \ldots, v_d) \in Z^d$ and
  $N = (N_1, \ldots, N_d) \in (\mathbb{Z}^+)^d$
- d-dimensional cubes:
  $a + \{0, 1\}^d \cdot v := \{a + \epsilon_1 v_1 + \cdots + \epsilon_d v_d : \epsilon_i \in \{0, 1\}\}$
  where $v = (v_1, \ldots, v_d) \in Z^d$
- Subset sums: $FS(A) := \{\sum_{a \in B} a : B \subseteq A\}$

The goal is to give quantitative measures of additive structure in a set

"A has additive structure":

- $A + A$ is small
- $A - A$ is small
- $A - A$ can be covered by a small number of translates of A
- kA is small for any fixed k
- there are many quadruples $(a_1, a_2, a_3, a_4) \in A \times A \times A \times A$ such that $a_1 + a_2 = a_3 + a_4$
- the subset sums $FS(A) := \{\sum_{a \in B} a : B \subseteq A\}$ have high multiplicity
- A has a large intersection with (or is contained in) a generalized arithmetic progression of size comparable to A
- A contains a large generalized arithmetic progression

Cauchy-Davenport Theorem

Let $\mathbb{F}_p$ be the finite field of prime order p. Let A and B be two additive sets in $\mathbb{F}_p$, then

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

Proofs:

- Cauchy 1813
- Davenport 1935
- Alon via polynomial method in 1999
- Tao via Fourier transforms in 2005

Let $A \subseteq \mathbb{N}$ be a set of natural numbers. The *upper density of* A is defined as $\overline{\sigma}(A) := \limsup_{n\to\infty} \frac{|A\cap[0,n)|}{n}$.

Szemerédi's Theorem, 1975

Let A be a subset of the positive integers with positive upper density $\overline{\sigma}(A) > 0$. Then A contains arbitrarily long arithmetic progressions.

Let $A \subseteq \mathbb{N}$ be a set of natural numbers. The *upper density of* A is defined as $\overline{\sigma}(A) := \limsup_{n\to\infty} \frac{|A\cap[0,n)|}{n}$.

Szemerédi's Theorem, 1975

Let A be a subset of the positive integers with positive upper density $\overline{\sigma}(A) > 0$. Then A contains arbitrarily long arithmetic progressions.

- Original proof by Sz. in 1975 via Szemerédi's Regularity Lemma

Let $A \subseteq \mathbb{N}$ be a set of natural numbers. The *upper density of* A is defined as $\overline{\sigma}(A) := \limsup_{n\to\infty} \frac{|A\cap[0,n)|}{n}$.

Szemerédi's Theorem, 1975

Let A be a subset of the positive integers with positive upper density $\overline{\sigma}(A) > 0$. Then A contains arbitrarily long arithmetic progressions.

- Original proof by Sz. in 1975 via Szemerédi's Regularity Lemma
- Furstenberg via ergodic theory in 1977

Let $A \subseteq \mathbb{N}$ be a set of natural numbers. The *upper density of* A is defined as $\overline{\sigma}(A) := \limsup_{n\to\infty} \frac{|A\cap[0,n)|}{n}$.

Szemerédi's Theorem, 1975

Let A be a subset of the positive integers with positive upper density $\overline{\sigma}(A) > 0$. Then A contains arbitrarily long arithmetic progressions.

- Original proof by Sz. in 1975 via Szemerédi's Regularity Lemma
- Furstenberg via ergodic theory in 1977
- Gowers via additive combinatorial proof in 2001

Let $A \subseteq \mathbb{N}$ be a set of natural numbers. The *upper density of* A is defined as $\overline{\sigma}(A) := \limsup_{n\to\infty} \frac{|A\cap[0,n)|}{n}$.

Szemerédi's Theorem, 1975

Let A be a subset of the positive integers with positive upper density $\overline{\sigma}(A) > 0$. Then A contains arbitrarily long arithmetic progressions.

- Original proof by Sz. in 1975 via Szemerédi's Regularity Lemma
- Furstenberg via ergodic theory in 1977
- Gowers via additive combinatorial proof in 2001
- Gowers via hypergraph regularity method in 2006
- Nagle, Rödl, Schacht, Skokan via hypergraph regularity method in 2006

2012 Abel Prize citation for Szemerédi

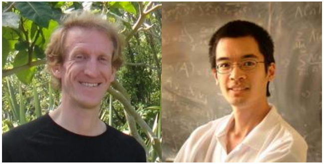
"for his fundamental contributions to discrete mathematics and theoretical computer science, and in recognition of the profound and lasting impact of these contributions on additive number theory and ergodic theory." Endre Szemerédi has revolutionized discrete mathematics by introducing ingenious and novel techniques, and by solving many fundamental problems. His work has brought combinatorics to the center-stage of mathematics, by revealing its deep connections to such fields as additive number theory, ergodic theory, theoretical computer science, and incidence geometry. In 1975, Endre Szemerédi first attracted the attention of many mathematicians with his solution of the famous Erdős–Turán conjecture, showing that in any set of integers with positive density, there are arbitrarily long arithmetic progressions. This was a surprise, since even the case of progressions of lengths 3 or 4 had earlier required substantial effort, by Klaus Roth and by Szemerédi himself, respectively. A bigger surprise lay ahead. Szemerédi's proof was a masterpiece of combinatorial reasoning, and was immediately recognized to be of exceptional depth and importance. A key step in the proof, now known as the Szemerédi Regularity Lemma, is a structural classification of large graphs. Over time, this lemma has become a central tool of both graph theory and theoretical computer science, leading to the solution of major problems in property testing, and giving rise to the theory of graph limits. Still other surprises lay in wait. Beyond its impact on discrete mathematics and additive number theory, Szemerédi's theorem inspired Hillel Furstenberg to develop ergodic theory in new

2020 Abel Prize citation for Furstenberg

Using ergodic theory and his multiple recurrence theorem, in 1977, Furstenberg gave a stunning new proof of Szemerédi's theorem about the existence of large arithmetic progressions in subsets of integers with positive density. In subsequent works with Yitzhak Kaztnelson, Benjamin Weiss and others, he found higher dimensional and far-reaching generalisations of Szemerédi's theorem and other applications of topological dynamics and ergodic theory to Ramsey theory and additive combinatorics. This work has influenced many later developments including the works of Ben Green, Terence Tao and Tamar Ziegler on the Hardy – Littlewood conjecture and arithmetic progressions of prime numbers.

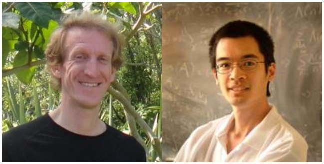
Green-Tao Theorem, 2004

The primes contain arbitrarily long arithmetic progressions.



Green-Tao Theorem, 2004

The primes contain arbitrarily long arithmetic progressions.



Tao's Fields Medal (2006) citation reads: "For his contributions to partial differential equations, combinatorics, harmonic analysis and additive number theory"

Erdős-Szemerédi Theorem, 1983

For any non-empty set $A \subseteq \mathbb{N}$, there exist positive constants c and ϵ such that

$$max\{|A+A|, |A \cdot A|\} \geq c|A|^{1+\epsilon}.$$

An example of the sum-product phenomenon.

Erdős-Szemerédi Conjecture

For any non-empty set $A \subseteq \mathbb{R}$, one has

$$max\{|A+A|, |A \cdot A|\} \geq c|A|^{2-o(1)}.$$

What is the polynomial method?

"The strategy is to capture (or at least partition) the arbitrary sets of objects (viewed as points in some configuration space) in the zero set of a polynomial whose degree (or other measure of complexity) is under control. One then use tools from algebraic geometry to understand the structure of this zero set, and thence to control the original sets of objects."

-T. Tao

Hilbert's Nullstellensatz

Let F be an algebraically closed field, let $g_1, \ldots, g_m \in F[\underline{t}]$, and let $f \in F[\underline{t}]$ be a polynomial which vanishes on all the common zeros of $g_1, \ldots, g_m$. Then there is $k \in \mathbb{Z}^+$ and $q_1, \ldots, q_m \in F[\underline{t}]$ such that

$$f^k = \sum_{i=1}^{m} q_i g_i .$$

Alon's Combinatorial Nullstellensatz I, 1999

Let F be a field, let $X_1, \ldots, X_n \subset F$ be nonempty and finite, and $X = \prod_{i=1}^{n} X_i$. For $1 \leq i \leq n$, put

$$\varphi_i(t_i) = \prod_{x_i \in X_i} (t_i - x_i) \in F[t_i] \subset F[\underline{t}]. \tag{1}$$

Let $f \in F[\underline{t}]$ be a polynomial which vanishes on all the common zeros of $\varphi_1, \ldots, \varphi_n$: that is, for all $x \in F^n$, if $\varphi_1(x) = \ldots = \varphi_n(x) = 0$, then $f(x) = 0$. Then:
a) (Combinatorial Nullstellensatz I) There are $q_1, \ldots, q_n \in F[\underline{t}]$ such that

$$f(t) = \sum_{i=1}^{n} q_i(t)\varphi_i(t). \tag{2}$$

Alon's Combinatorial Nullstellensatz I (continued)

b) (Supplementary Relations) Let R be the subring of F generated by the coefficients of f and $\varphi_1, \ldots, \varphi_n$. Then the $q_1, \ldots, q_n$ may be chosen to lie in $R[\underline{t}]$ and satisfy

$$\forall 1 \leq i \leq n, \;\; \deg q_i \leq \deg f - \deg \varphi_i. \tag{3}$$

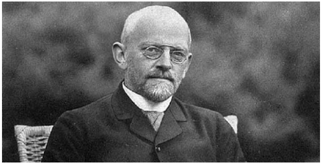
Alon's Combinatorial Nullstellensatz II

Let F be a field, $n \in \mathbb{Z}^+$, $d_1, \ldots, d_n \in \mathbb{N}$, and let $f \in F[\underline{t}] = F[t_1, \ldots, t_n]$. We suppose:
(i) $\deg f \leq d_1 + \ldots + d_n$.
(ii) The coefficient of $t_1^{d_1} \cdots t_n^{d_n}$ in f is nonzero.
Then, for any subsets $X_1, \ldots, X_n$ of F with $\# X_i = d_i + 1$ for $1 \leq i \leq n$, there is $x = (x_1, \ldots, x_n) \in X = \prod_{i=1}^{n} X_i$ such that $f(x) \neq 0$.

Alon's Nullstellensatz

- F any field
- $f = \sum_{i=1}^{n} q_i \varphi_i$
- Supplementary relations: Effective

Hilbert's Nullstellensatz

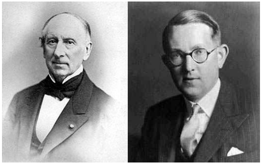


- F algebraically closed
- $f^{k} = \sum_{i=1}^{m} q_i g_i$.
- not effective

Cauchy-Davenport Theorem

Let $\mathbb{F}_p$ be the finite field of prime order p. Let A and B be two additive sets in $\mathbb{F}_p$, then

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



Proving Cauchy-Davenport with CN II

Proof.

If $|A|+|B|>p$, then for every $g\in\mathbb{F}_p$ we have $A\cap(g-B)\neq\emptyset$. Thus, $A+B=\mathbb{F}_p$.
Assume $|A|+|B|\leq p$ and assume the result false: $|A+B|\leq|A|+|B|-2$. Let $C\subseteq\mathbb{F}_p$ such that $A+B\subseteq C$ and $|C|=|A|+|B|-2$. Define

$$f(t_1,t_2)=\prod_{c\in C}(t_1+t_2-c).$$

Observe $f(a,b)=0$ for all $a\in A, b\in B$. For $d_1=|A|-1, d_2=|B|-1$, note that coefficient on $t_1^{d_1}t_2^{d_2}$ is the binomial coefficient $\binom{|A|+|B|-2}{|A|-1}$, which is nonzero in $\mathbb{F}_p$ since $|A|+|B|-2<p$. By CNII (with $n=2$, $X_1=A$, $X_2=B$), there exists $a\in A, b\in B$ such that $f(a,b)\neq 0$, contradicting the above. $\square$

Snevily's Conjecture

Let Z be an additive group of odd order and let A, B be two additive sets in Z with $|A| = |B|$. Then there is a bijection $\phi : A \to B$ such that the sums $\{a + \phi(a) : a \in A\}$ are all distinct.

Snevily's Conjecture

Let Z be an additive group of odd order and let A, B be two additive sets in Z with $|A| = |B|$. Then there is a bijection $\phi : A \to B$ such that the sums $\{a + \phi(a) : a \in A\}$ are all distinct.

Snevily's Conjecture holds for $Z = \mathbb{F}_p$ via CNII

MAIN PROOF IDEA:
APPLY CNII TO THE POLYNOMIAL

$$P(t_1, \ldots, t_{|A|}) = \prod_{1 \leq i \leq j \leq |A|} (t_j - t_i)((t_j - a_j) - (t_i - a_i)).$$

Chevalley-Warning Theorem

Let $n, r, d_1, \ldots, d_r \in \mathbb{Z}^+$ with

$$d_1 + \ldots + d_r < n. \tag{4}$$

For $1 \leq i \leq r$, let $P_i(t_1, \ldots, t_n) \in \mathbb{F}_q[t_1, \ldots, t_n]$ be a polynomial of degree d_i. Let

$$Z = Z(P_1, \ldots, P_r) = \{x \in \mathbb{F}_q^n \mid P_1(x) = \ldots = P_r(x) = 0\}$$

be the common zero set in $\mathbb{F}_q^n$ of the P_i's, and let $\mathbf{z} = \#Z$. Then:

a) (Chevalley's Theorem, 1935) We have $\mathbf{z} = 0$ or $\mathbf{z} \geq 2$.

b) (Warning's Theorem, 1935) We have $\mathbf{z} \equiv 0 \pmod{p}$.

Warning's Second Theorem

The same hypotheses as above: Let $n, r, d_1, \ldots, d_r \in \mathbb{Z}^+$ with

$$d_1 + \ldots + d_r < n. \tag{5}$$

For $1 \leq i \leq r$, let $P_i(t_1, \ldots, t_n) \in \mathbb{F}_q[t_1, \ldots, t_n]$ be a polynomial of degree d_i. Let

$$Z = Z(P_1, \ldots, P_r) = \{x \in \mathbb{F}_q^n \mid P_1(x) = \ldots = P_r(x) = 0\}$$

be the common zero set in $\mathbb{F}_q^n$ of the P_i's, and let $\mathbf{z} = \#Z$. Then:

$$\mathbf{z} = 0 \text{ or } \mathbf{z} \geq q^{n-d}. \tag{6}$$

Alon's Combinatorial Nullstellensatz: 300+ citations on MathSciNet

Following sharpening of CNII due to Schauz (2008), Lason(2010) and Karasev-Petrov(2012)

Coefficient Formula

Let F be a field, and let $f \in F[\underline{t}]$. Let $d_1, \ldots, d_n \in \mathbb{N}$ be such that $\deg f \leq d_1 + \ldots + d_n$. For each $1 \leq i \leq n$, let $X_i \subset F$ with $\#X_i = d_i + 1$, and let $X = \prod_{i=1}^n X_i$. Let $\mathbf{d} = (d_1, \ldots, d_n)$, and let $c_{\mathbf{d}}$ be the coefficient of $t_1^{d_1} \cdots t_n^{d_n}$ in f. Then

$$c_{\mathbf{d}} = \sum_{x=(x_1,\ldots,x_n)\in X} \frac{f(x)}{\prod_{i=1}^n \varphi_i'(x_i)}. \tag{7}$$

Question

Given a positive integer m, how many integers must we be given so as to guarantee a non-empty subset of these with sum divisible by m?

Question

Given a positive integer m, how many integers must we be given so as to guarantee a non-empty subset of these with sum divisible by m?

Extremal configuration(s): $\overbrace{1, \ldots, 1}^{m-1}$ or $\overbrace{m-1, \ldots, m-1}^{m-1}$

Question

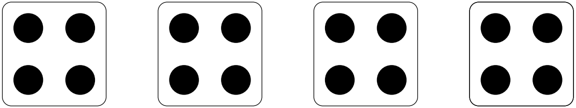
Given a positive integer m, how many integers must we be given so as to guarantee a non-empty subset of these with sum divisible by m?

Extremal configuration(s): $\overbrace{1,\ldots,1}^{m-1}$ or $\overbrace{m-1,\ldots,m-1}^{m-1}$

So, we must be given at least m integers. In fact, the pigeonhole principle shows that m is enough.

A different view

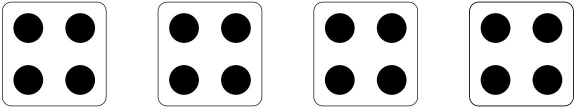
Let's say $m = 5$ and view given integers as sizes of sets.



We have here that $5 \nmid \#(\bigcup_{i \in J} \mathcal{F}_i)$ for any $\emptyset \neq J \subseteq \{1, 2, 3, 4\}$.

A different view

Let's say $m = 5$ and view given integers as sizes of sets.



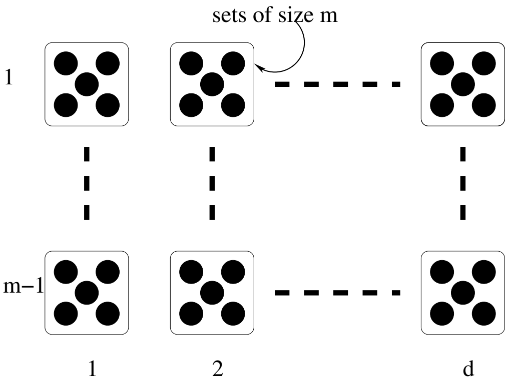
We have here that $5 \nmid \#(\bigcup_{i \in J} \mathcal{F}_i)$ for any $\emptyset \neq J \subseteq \{1, 2, 3, 4\}$.

And, if we had 5 sets, then regardless of what is given we have a $\emptyset \neq J \subseteq \{1, 2, 3, 4, 5\}$ such that $5 | \#(\bigcup_{i \in J} \mathcal{F}_i)$

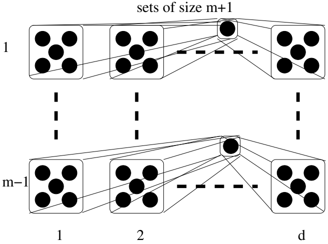
Question

What if we allow sets to overlap? That is, if we consider a set-system (i.e. a hypergraph) with maximum degree d, how many sets must we be given to guarantee the existence of a sub-collection (i.e. a subhypergraph) so that the cardinality of the union of these sets (edges) is divisible by m?

Extremal configuration

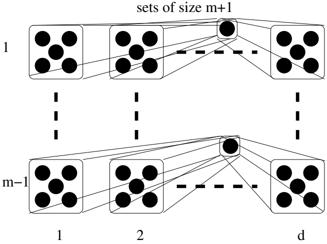


Extremal configuration



Sets have size $m+1$ and maximum degree is d.

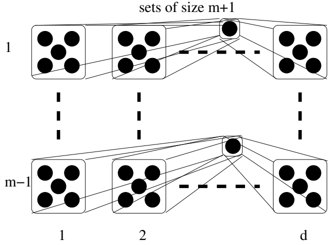
Extremal configuration



Sets have size $m+1$ and maximum degree is d.

We have $d(m-1)$ sets and there is no non-trivial sub-collection the cardinality of whose union is divisible by m.

Extremal configuration



Sets have size $m+1$ and maximum degree is d.

We have $d(m-1)$ sets and there is no non-trivial sub-collection the cardinality of whose union is divisible by m.

Proposition

$d(m-1)+1$ sets suffice.

For $\mathcal{F} = \{\mathcal{F}_1, \ldots, \mathcal{F}_n\}$ a set system of length n and maximal degree at most d, put

$$h(t_1, \ldots, t_n) = \sum_{\varnothing \neq J \subset \{1,\ldots,n\}} (-1)^{\#J+1} \#(\bigcap_{j \in J} \mathcal{F}_i) \prod_{j \in J} t_j.$$

John R. Schmitt

For $\mathcal{F} = \{\mathcal{F}_1, \ldots, \mathcal{F}_n\}$ a set system of length n and maximal degree at most d, put

$$h(t_1, \ldots, t_n) = \sum_{\emptyset \neq J \subset \{1,\ldots,n\}} (-1)^{\#J+1} \#\left(\bigcap_{j \in J} \mathcal{F}_i\right) \prod_{j \in J} t_j.$$

- $deg(h) \leq d$

For $\mathcal{F} = \{\mathcal{F}_1, \ldots, \mathcal{F}_n\}$ a set system of length n and maximal degree at most d, put

$$h(t_1, \ldots, t_n) = \sum_{\emptyset \neq J \subset \{1,\ldots,n\}} (-1)^{\#J+1} \#\left(\bigcap_{j \in J} \mathcal{F}_i\right) \prod_{j \in J} t_j.$$

- $deg(h) \leq d$
- $h(0, \ldots, 0) = 0$

For $\mathcal{F} = \{\mathcal{F}_1, \ldots, \mathcal{F}_n\}$ a set system of length n and maximal degree at most d, put

$$h(t_1, \ldots, t_n) = \sum_{\emptyset \neq J \subset \{1,\ldots,n\}} (-1)^{\#J+1} \#(\bigcap_{j \in J} \mathcal{F}_i) \prod_{j \in J} t_j.$$

- $deg(h) \leq d$
- $h(0, \ldots, 0) = 0$
- Seek $0, 1$-vectors of length n that evaluate to 0 – say $\mathbf{x} \in \{0,1\}^n$ and $J_{\mathbf{x}} = \{1 \leq j \leq n \mid x_j = 1\}$ – since the Inclusion-Exclusion Principle implies

$$h(\mathbf{x}) = \# \bigcup_{j \in J_x} \mathcal{F}_j.$$

Restricted Variable Warning's Second Theorem, P. Clark, A. Forrow, S. - 2017

Let p be a prime, let $n, r, v \in \mathbb{Z}^+$, and for $1 \leq i \leq r$, let $1 \leq v_j \leq v$. Let $A_1, \ldots, A_n$ be nonempty subsets of $\mathbb{Z}$ such that for each i, the elements of A_i are pairwise incongruent modulo p, and put $A = \prod_{i=1}^n A_i$. Let $P_1, \ldots, P_r \in \mathbb{Z}[t_1, \ldots, t_n]$. Let

$$Z_A = \{x \in A \mid P_j(x) \equiv 0 \pmod{p^{v_j}} \ \forall 1 \leq j \leq r\}, \ \mathbf{z}_A = \# Z_A.$$

a) $\mathbf{z}_A = 0$ or $\mathbf{z}_A \geq \mathfrak{m}\left(\#A_1, \ldots, \#A_n; \#A_1 + \ldots + \#A_n - \sum_{j=1}^r (p^{v_j} - 1)\deg(P_j)\right)$.

b) (**Boolean Case**) We have $\mathbf{z}_{\{0,1\}^n} = 0$ or $\mathbf{z}_{\{0,1\}^n} \geq 2^{n - \sum_{j=1}^r (p^{v_j} - 1)\deg(P_j)}$.

Recall: For $\mathcal{F} = \{\mathcal{F}_1, \ldots, \mathcal{F}_n\}$ a set system of length n and maximal degree at most d, put

$$h(t_1, \ldots, t_n) = \sum_{\varnothing \neq J \subset \{1,\ldots,n\}} (-1)^{\#J+1} \#(\bigcap_{j \in J} \mathcal{F}_i) \prod_{j \in J} t_j.$$

with $deg(h) \leq d$, $h(0, \ldots, 0) = 0$ and for $\mathbf{x} \in \{0,1\}^n$ and $J_{\mathbf{x}} = \{1 \leq j \leq n \mid x_j = 1\}$ we have

$$h(\mathbf{x}) = \# \bigcup_{j \in J_x} \mathcal{F}_j.$$

Recall: For $\mathcal{F} = \{\mathcal{F}_1, \ldots, \mathcal{F}_n\}$ a set system of length n and maximal degree at most d, put

$$h(t_1, \ldots, t_n) = \sum_{\varnothing \neq J \subset \{1,\ldots,n\}} (-1)^{\#J+1} \#(\bigcap_{j \in J} \mathcal{F}_i) \prod_{j \in J} t_j.$$

with $deg(h) \leq d$, $h(0, \ldots, 0) = 0$ and for $\mathbf{x} \in \{0,1\}^n$ and $J_{\mathbf{x}} = \{1 \leq j \leq n \mid x_j = 1\}$ we have

$$h(\mathbf{x}) = \# \bigcup_{j \in J_x} \mathcal{F}_j.$$

When $m = p^v$ apply the Boolean case of Warning's Second Theorem to h to obtain that there are $2^{n-d(p^v-1)}$ sub-(set systems) with cardinality of the union divisible by m.

Recall: For $\mathcal{F} = \{\mathcal{F}_1, \ldots, \mathcal{F}_n\}$ a set system of length n and maximal degree at most d, put

$$h(t_1, \ldots, t_n) = \sum_{\varnothing \neq J \subset \{1,\ldots,n\}} (-1)^{\#J+1} \#(\bigcap_{j \in J} \mathcal{F}_i) \prod_{j \in J} t_j.$$

with $deg(h) \leq d$, $h(0, \ldots, 0) = 0$ and for $\mathbf{x} \in \{0,1\}^n$ and $J_\mathbf{x} = \{1 \leq j \leq n \mid x_j = 1\}$ we have

$$h(\mathbf{x}) = \# \bigcup_{j \in J_x} \mathcal{F}_j.$$

When $m = p^v$ apply the Boolean case of Warning's Second Theorem to h to obtain that there are $2^{n-d(p^v-1)}$ sub-(set systems) with cardinality of the union divisible by m. Thus, when $n > d(p^v - 1)$ we have a non-trivial such sub-(set system). This refines a result of Alon, Kleitman, Lipton, Meshulam, Rabin and Spencer (1991).

Recall: For $\mathcal{F} = \{\mathcal{F}_1, \ldots, \mathcal{F}_n\}$ a set system of length n and maximal degree at most d, put

$$h(t_1, \ldots, t_n) = \sum_{\varnothing \neq J \subset \{1,\ldots,n\}} (-1)^{\#J+1} \#(\bigcap_{j \in J} \mathcal{F}_i) \prod_{j \in J} t_j.$$

with $deg(h) \leq d$, $h(0, \ldots, 0) = 0$ and for $\mathbf{x} \in \{0,1\}^n$ and $J_{\mathbf{x}} = \{1 \leq j \leq n \mid x_j = 1\}$ we have

$$h(\mathbf{x}) = \# \bigcup_{j \in J_x} \mathcal{F}_j.$$

When $m = p^v$ apply the Boolean case of Warning's Second Theorem to h to obtain that there are $2^{n-d(p^v-1)}$ sub-(set systems) with cardinality of the union divisible by m.
Thus, when $n > d(p^v - 1)$ we have a non-trivial such sub-(set system). This refines a result of Alon, Kleitman, Lipton, Meshulam, Rabin and Spencer (1991).
Our theorem helps one make good conjectures.

Thank you!