Chevalley-Warning Meets Hypergraphs: Counting Sub-hypergraphs with Union Cardinality 0 Modulo q

John Schmitt

Middlebury College
Vermont, USA

Joint work with Pete L. Clark (U. Georgia) and Aden Forrow (M.I.T.)

A warm-up exercise

Exercise: 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?

A warm-up exercise

Exercise: 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): $\overbrace{1, \dots, 1}^{m-1}$ or $\overbrace{m-1, \dots, m-1}^{m-1}$

A warm-up exercise

Exercise: 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.

A warm-up exercise

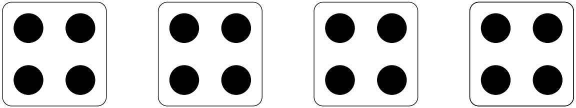
Exercise: Given a positive integer m, how many integers must we be given so as to guarantee a non-empty subset of these with sum divisible by m?

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 of the warm-up

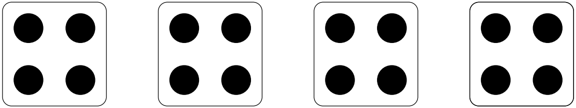
Let's say $m = 5$ and view given integers as sizes of sets.



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 of the warm-up

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



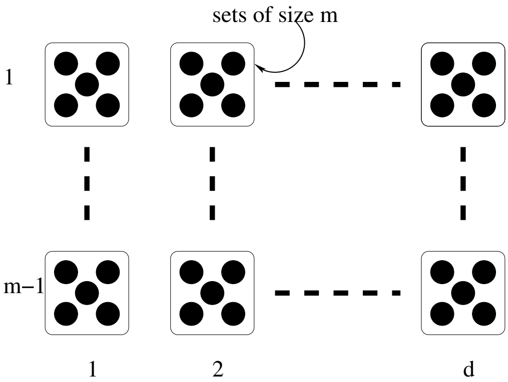
We have here that $5 \nmid \#(\bigcup_{i \in J} \mathcal{F}_i)$ for any $\emptyset \neq J \subseteq \{1, 2, 3, 4\}$.

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 $5 | \#(\bigcup_{i \in J} \mathcal{F}_i)$

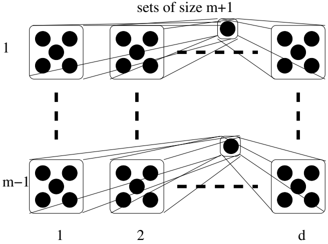
Generalizing the basic question

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

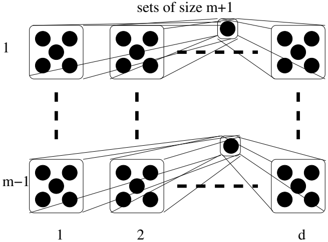


Extremal configuration



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

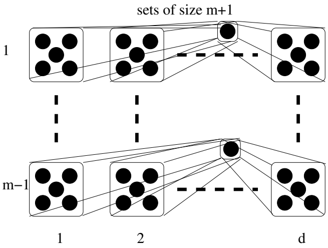
Extremal configuration



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.
Question: Does $d(m - 1) + 1$ sets suffice?

Encode combinatorial problems via a polynomial so that zeros of polynomial correspond to solutions of the combinatorial problem.

Encode combinatorial problems via a polynomial so that zeros of polynomial correspond to solutions of the combinatorial problem.

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

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

Encode combinatorial problems via a polynomial so that zeros of polynomial correspond to solutions of the combinatorial problem.

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

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

- $deg(h) \leq d$

Encode combinatorial problems via a polynomial so that zeros of polynomial correspond to solutions of the combinatorial problem.

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

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

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

Encode combinatorial problems via a polynomial so that zeros of polynomial correspond to solutions of the combinatorial problem.

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

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

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

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

Encode combinatorial problems via a polynomial so that zeros of polynomial correspond to solutions of the combinatorial problem.

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

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

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

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

We now need algebraic statements about the zeros of a polynomial.

Theorem

(Chevalley- Theorem) Let $n, r, d_1, \ldots, d_r \in \mathbb{Z}^+$ *with*

$$d := d_1 + \ldots + d_r < n.$$

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* $\mathbf{z} \geq 2$*.*

Theorem

(Chevalley-Warning Theorem) Let $n, r, d_1, \ldots, d_r \in \mathbb{Z}^+$ *with*

$$d := d_1 + \ldots + d_r < n.$$

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

Theorem

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

$$d := d_1 + \ldots + d_r < n.$$

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:*

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

Theorem

(Restricted Variable Warning's Second Theorem, P. Clark, A. Forrow, S. - 2014+) *Let K be a number field with ring of integers R, let $\mathfrak{p}$ be a nonzero prime ideal of R, and let $q = p^{\ell}$ be the prime power such that $R/\mathfrak{p} \cong \mathbb{F}_q$. Let $A_1, \ldots, A_n$ be nonempty subsets of R such that for each i, the elements of A_i are pairwise incongruent modulo $\mathfrak{p}$, and put $A = \prod_{i=1}^{n} A_i$. Let $r, v_1, \ldots, v_r \in \mathbb{Z}^+$. Let $P_1, \ldots, P_r \in R[t_1, \ldots, t_n]$. Let*

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

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

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

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

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

with $deg(h) \leq d$, $h(0, \dots, 0) = 0$ 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

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

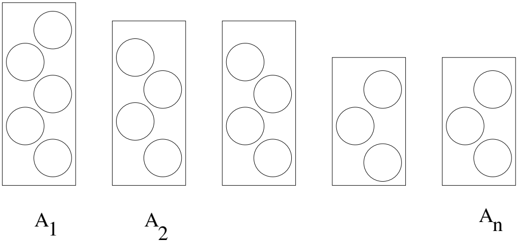
with $deg(h) \leq d$, $h(0, \ldots, 0) = 0$ and for $\mathbf{x} \in \{0,1\}^n$ and $J_{\mathbf{x}} = \{1 \leq j \leq n \mid x_j = 1\}$ we have

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

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.

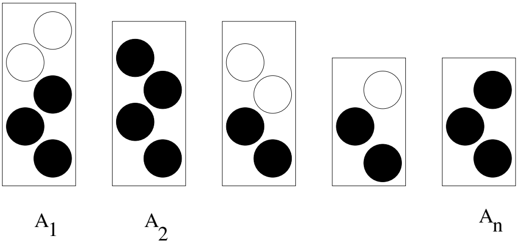
Thank you!

Balls in bins



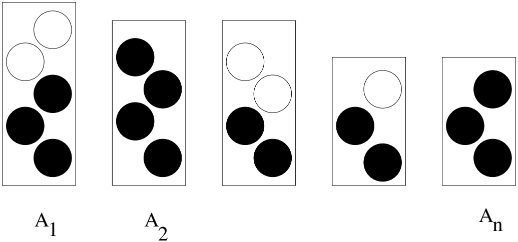
Bin A_i holds at most a_i balls.

Balls in bins lemma



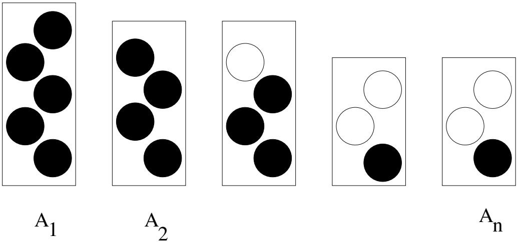
Bin A_i holds at most a_i balls. Distribution of N balls is an n-tuple $y = (y_1, \ldots, y_n)$ with $y_1 + \ldots + y_n = N$ and $1 \leq y_i \leq a_i$ for all i.

Balls in bins lemma



Let $P(y) = y_1 \cdots y_n$. If $n \leq N \leq a_1 + \ldots + a_n$, let $\mathfrak{m}(a_1, \ldots, a_n; N)$ be the minimum value of $P(y)$ as y ranges over all distributions of N balls into bins $A_1, \ldots, A_n$.

Balls in bins lemma



Let $P(y) = y_1 \cdots y_n$. If $n \leq N \leq a_1 + \ldots + a_n$, let $\mathfrak{m}(a_1, \ldots, a_n; N)$ be the minimum value of $P(y)$ as y ranges over all distributions of N balls into bins $A_1, \ldots, A_n$. To minimize the product, serve the largest bins first.

Alon-Füredi Theorem

Theorem

(Alon-Füredi Theorem) Let F be a field, let $A_1, \ldots, A_n$ be nonempty finite subsets of F. Put $A = \prod_{i=1}^{n} A_i$ and $a_i = \# A_i$ for all $1 \leq i \leq n$. Let $P \in F[t] = F[t_1, \ldots, t_n]$ be a polynomial. Let

$$\mathcal{U}_A = \{x \in A \mid P(x) \neq 0\}, \ \mathfrak{u}_A = \#\mathcal{U}_A.$$

Then $\mathfrak{u}_A = 0$ or $\mathfrak{u}_A \geq \mathfrak{m}(a_1, \ldots, a_n; a_1 + \ldots + a_n - \deg P)$.

Proof.

Induction on n. $\square$

Warning's Second Theorem

Theorem

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

$$d := d_1 + \ldots + d_r < n.$$

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:*

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

Proof of Warning's Second Theorem via Alon-Füredi Theorem

Put

$$P(\mathbf{t}) = \prod_{i=1}^{r}(1 - P_i(\mathbf{t})^{q-1}).$$

Proof of Warning's Second Theorem via Alon-Füredi Theorem

Put

$$P(\mathbf{t}) = \prod_{i=1}^{r}(1 - P_i(\mathbf{t})^{q-1}).$$

Then $\deg P = (q-1)(\deg(P_1) + \ldots + \deg(P_r))$, and

$$\mathcal{U}_A = \{x \in A \mid P(x) \neq 0\} = Z_A,$$

so

$$z_A = \# Z_A = \# \mathcal{U}_A = \mathfrak{u}_A.$$

Proof of Warning's Second Theorem via Alon-Füredi Theorem

Put

$$P(\mathbf{t}) = \prod_{i=1}^{r}(1 - P_i(\mathbf{t})^{q-1}).$$

Then $\deg P = (q-1)(\deg(P_1) + \ldots + \deg(P_r))$, and

$$\mathcal{U}_A = \{x \in A \mid P(x) \neq 0\} = Z_A,$$

so

$$z_A = \# Z_A = \# \mathcal{U}_A = \mathfrak{u}_A.$$

Applying the Alon-Füredi Theorem we get $\mathbf{z}_A = 0$ or

$$\mathbf{z}_A \geq \mathfrak{m}(\# A_1 + \ldots + \# A_n; \# A_1 + \ldots + \# A_n - (q-1)d).$$