Set systems with no union of cardinality 0 modulo m

N. Alon, IBM Almaden and Tel Aviv University
D. Kleitman, MIT
R. Lipton, Princeton University
R. Meshulam, MIT
M. Rabin, Hebrew University and Harvard University
J. Spencer, Courant Institute

Abstract

Let q be a prime power. It is shown that for any hypergraph $\mathcal{F} = \{F_1, \ldots, F_{d(q-1)+1}\}$ whose maximal degree is d, there exists $\emptyset \neq \mathcal{F}_0 \subset \mathcal{F}$, such that $|\bigcup_{F \in \mathcal{F}_0} F| \equiv 0 \pmod{q}$.

For integers $d, m \geq 1$ let $f_d(m)$ denote the minimal t such that for any hypergraph $\mathcal{F} = \{F_1, \ldots, F_t\}$ whose maximal degree is d, there exists $\emptyset \neq \mathcal{F}_0 \subset \mathcal{F}$, such that $|\bigcup_{F \in \mathcal{F}_0} F| \equiv 0 \pmod{m}$.
Here we determine $f_d(m)$ when m is a prime power, and remark on the general case.

Example: Let $A_{ij} \quad 1 \leq i \leq m-1, \ 1 \leq j \leq d$, be pairwise disjoint sets, each of cardinality m, and let $\{v_1, \ldots, v_{m-1}\}$ be disjoint from all the A_{ij} 's. Now $\mathcal{F} = \{A_{ij} \cup \{v_i\} : \ 1 \leq i \leq m-1, \ 1 \leq j \leq d\}$ satisfies $|\mathcal{F}| = d(m-1)$ but $|\bigcup_{F \in \mathcal{F}_0}| \not\equiv 0 \pmod{m}$ for any $\emptyset \neq \mathcal{F}_0 \subset \mathcal{F}$. Hence $f_d(m) \geq d(m-1) + 1$.

Theorem 1: If q is a prime power then $f_d(q) = d(q-1) + 1$.

Proof: Let $\mathcal{F} = \{F_1, \ldots, F_t\}$, $t = d(q-1) + 1$, be a hypergraph of degree $\leq d$, and consider the polynomial:

$$p(x_1, \ldots, x_t) = \sum_{\emptyset \neq I \subset [t]} (-1)^{|I|+1} \cdot |\bigcap_{i \in I} F_i| \cdot \prod_{i \in I} x_i \ .$$

We shall need the following result of Baker and Schmidt [2]. We sketch a short proof based on a method of Alon, Friedland and Kalai [1]:

Theorem 2 (Baker-Schmidt [2]): Let $q = p^r$, p prime. If $t \geq d(q-1)+1$ and $h(x_1,\ldots,x_t) \in \mathbf{Z}[x_1,\ldots,x_t]$ satisfies $h(0)=0$, and $\deg h \leq d$, then there exists an $0 \neq \epsilon \in \{0,1\}^t$ such that $h(\epsilon) \equiv 0 \pmod{q}$.

Proof: Suppose $h(\epsilon) \not\equiv 0 \pmod{q}$ for all $0 \neq \epsilon \in \{0,1\}^t$, and let $u(x) = \prod_{i=1}^{q-1}(h(x)-i)$. Denote by s the smallest power of p that does not divide $(q-1)!$, i.e., $s = p \cdot max\{p^r : p^r \mid (q-1)!\}$.

The proof of the following simple fact is omitted:

Lemma 1: For every integer a, $\prod_{i=1}^{q-1}(a-i) \equiv 0 \pmod{s}$ iff $a \not\equiv 0 \pmod{q}$.

$\square$

By Lemma 1 $u(\epsilon) \equiv 0 \pmod{s}$ for all $0 \neq \epsilon \in \{0,1\}^t$, and $u(0) \not\equiv 0 \pmod{s}$. Let $\overline{u}(x)$ denote the multilinear polynomial obtained from $u(x)$ by replacing each monomial ${x_{i_1}}^{\alpha_1} \cdots {x_{i_j}}^{\alpha_j}$, $\alpha_1,\ldots,\alpha_j \geq 1$, by $x_{i_1}\cdots x_{i_j}$.

The following Lemma can be easily proved by induction on t:

Lemma 2 [1]: If $g(x_1,\ldots,x_t)$ is a multilinear polynomial in $\mathbf{Z}[x_1,\ldots,x_t]$ and $g(\epsilon) \equiv 0 \pmod{s}$ for all $\epsilon \in \{0,1\}^t$, then $g(x_1,\ldots,x_t) \equiv 0 \pmod{s}$

$\square$

Now $g(x) = \overline{u}(x) - u(0)\cdot\prod_{i=1}^{t}(1-x_i)$ satisfies the assumptions of Lemma 2, hence $\overline{u}(x) \equiv u(0)\cdot\prod_{i=1}^{t}(1-x_i) \pmod{s}$, and so $\deg \overline{u} \geq t$. But $\deg \overline{u} \leq \deg u = (\deg h)^{q-1} \leq d(q-1) < t$, a contradiction.

$\square$

Returning to the proof of Theorem 1, we note that $\deg p \leq d$ and $p(0)=0$. Hence by Theorem 2 $p(\epsilon) \equiv 0 \pmod{q}$ for some $0 \neq \epsilon \in \{0,1\}^t$. Now by Inclusion - Exclusion $p(\epsilon) = |\bigcup_{\{i:\epsilon_i=1\}} F_i|$, and so $|\bigcup_{\{i:\epsilon_i=1\}} F_i| \equiv 0 \pmod{q}$.

$\square$

Following [2] let $g_d(m)$ denote the minimal t such that for any $h \in \mathbf{Z}[x_1, \ldots, x_t]$ which satisfies $h(0) = 0$, and $\deg h \leq d$, there exists an $0 \neq \epsilon \in \{0,1\}^t$ such that $h(\epsilon) \equiv 0 \pmod{m}$. The proof of Theorem 1 shows that $f_d(m) \leq g_d(m)$. Hence Theorem 6 in [2], implies that for any m, $f_d(m) \leq C(d) \cdot m^{2^d d!}$.

We next prove the following proposition that shows that the number theoretic problem of determining $g_d(m)$ is equivalent to the combinatorial problem of determining $f_d(m)$.

Proposition: $f_d(m) = g_d(m)$.

Proof: It suffices to show that for any multilinear polynomial $h \in \mathbf{Z}_m[x_1, \ldots, x_t]$ of degree $\leq d$ which satisfies $h(0) = 0$, there exists a hypergraph $\mathcal{F} = \{F_1, \ldots, F_t\}$ of degree $\leq d$ such that h is *realized* by $\mathcal{F}$, i.e.,

$$h(x_1, \ldots, x_t) = \sum_{\emptyset \neq I \subset [t]} (-1)^{|I|+1} \cdot |\bigcap_{i \in I} F_i| \cdot \prod_{i \in I} x_i \pmod{m} .$$

For any $\emptyset \neq J \subset [t]$, the polynomial

$$u_J(x) = 1 - \prod_{j \in J}(1 - x_j) = \sum_{\emptyset \neq I \subset J} (-1)^{|I|+1} \cdot \prod_{i \in I} x_i$$

can clearly be realized by a hypergraph with maximal degree $|J|$. (Simply take $|J|$ pairwise disjoint sets of size m each and add a common point to all of them). To complete the proof it suffices to show that if h and g are realized by hypergraphs of degree $\leq d$, then so is $h + g$, and that any multilinear polynomial of degree $\leq d$ in $\mathbf{Z}_m[x_1, \ldots, x_t]$ that vanishes at 0 can be written as a linear combination (with $\mathbf{Z}_m$ coefficients) of u_J's with $J \subset [t]$ and $0 < |J| \leq d$

If h is realized by the hypergraph $\mathcal{H} = \{H_1, \ldots, H_{t_1}\}$ and g is realized by $\mathcal{G} = \{G_1, \ldots, G_{t_2}\}$ and the degrees of both hypergraphs are at most d we first observe that we may assume that $t_1 = t_2$ since otherwise we can add sufficiently many empty edges to one of the hypergraphs. Put $t = t_1 = t_2$, assume the hypergraphs are realized on pairwise disjoint sets of vertices, and consider the hypergraph $\mathcal{F} = \{H_1 \cup G_1, \ldots, H_t \cup G_t\}$. It is easy to check that this hypergraph realizes the polynomial $h + g$.

It remains to show that any multilinear polynomial of degree $\leq d$ in $\mathbf{Z}_m[x_1, \ldots, x_t]$ that vanishes at 0 can be written as a linear combination (with $\mathbf{Z}_m$ coefficients) of u_J's with $J \subset [t]$ and $0 < |J| \leq d$. Each such polynomial can obviously be written as a linear combination of the above polynomials u_J and 1. However, the coefficient of 1 must be 0 since our polynomial, as well as all the polynomials u_J vanish when all the variables are 0.

□

It is worth mentioning that some (very weak) upper bounds for $f_d(m)$ can be obtained by applying Ramsey Theory. By the last proposition the same bounds follow for $g_d(m)$. Although these estimates are (much) weaker than the best known bounds for $g_d(m)$ this shows that it is conceivable that the number theoretic function $g_d(m)$ can be studied by purely combinatorial methods.

We conclude the note mentioning that by considering the dual of our Theorem 1 (or by applying a similar proof) we can prove the follwing result, whose detailed proof is left to the reader.

Theorem 3: If q is a prime power then any hypergraph with $n > (q-1)d$ vertices and with e edges, each of size at most d, contains an induced sub-hypergraph on less than n vertices whose number of edges is congruent to e modulo q.

□

References

[1] N. Alon, S. Friedland and G. Kalai, Regular subgraphs of almost regular graphs, *J. Combinatorial Theory, Ser. B.* **37** (1980), 79-91.

[2] R. C. Baker and W. M. Schmidt, Diophantine problems in variables restricted to the values 0 and 1, *J. Number Theory* **12** (1980), 460-486.