Problem posed by Ernie Croot at ICM Satellite Conference, 2010

January 23, 2011

The Problem. Show that the following holds for all $c > 0$ and $n > n_0(c)$: If $\{A_g\}_{g \in \mathbb{F}_2^n}$ is a collection of subsets of the vector space $\mathbb{F}_2^n$ satisfying

$$\text{for all } g \in \mathbb{F}_2^n,\ |A_g| \ \geq\ 2^n/n^c,$$

then

$$\cup_{g \in \mathbb{F}_2^n} (A_g \hat{+} A_g + g)$$

contains all but at most $o(2^n)$ elements of $\mathbb{F}_2^n$. Here, $A \hat{+} B$ is the restricted sumset, and denotes the set of all sums $\{a + b \ :\ a \in A,\ b \in B,\ a \neq b\}$ ('restricted' refers to the condition $a \neq b$).

Another way to state this problem, without resorting to restricted sumsets, is to just say that we want

$$\cup_{g \in \mathbb{F}_2^n} (A_g + A_g + g) \tag{1}$$

to cover all but $o(2^n)$ of the elements of $\mathbb{F}_2^n$ at least twice. Obviously, this union covers all of $\mathbb{F}_2^n$ at least once, since $0 \in A_g + A_g$ for all $g \in \mathbb{F}_2^n$.

1 Motivation and discussion

1.1 Progressions in $\mathbb{Z}_4^n$

This problem grew out of my attempts to improve upon a result of T. Sanders on the maximal subset $S \subseteq \mathbb{Z}_4^n$ having no three-term progressions – i.e. no solutions to the equation $a + b = 2c$, with $a, b, c \in S$.

In fact, if we could solve the above problem, assuming the slightly stronger conclusion that all but $2^n/n^c$ elements of $\mathbb{F}_2^n$ are double-covered by any union (1), then it would imply that if S is any largest set without 3APs, *satisfying a certain uniformity condition (3) listed below*, then

$$|S| \ll 4^n/n^c.$$

Here's how to see this: Let $G := \mathbb{Z}_4^n$ and let $H \cong \mathbb{F}_2^n$ be the additive subgroup given by $H = 2 * G$, and let T be any set of 2^n vectors, one in each coset of H; in other words, H is the set of vectors all of whose coordinates are 0 or 2, and we could choose $T \subseteq \mathbb{Z}_4^n$ to just be those vectors with coordinates 0 or 1. Write $S = \cup_{t \in T} S_t$, where S_t is the elements of S belonging to the coset $t + H$. In order that $a + b = 2c$ in $\mathbb{Z}_4^n$, we must have that a and b belong to the same set S_t for some t; of course, c could possibly lie in any set S_u (i.e. u and t need not be related in any way). So basically, in order for S to contain three-term progressions, we must have that

$$\cup_{t \in T}(S_t \hat{+} S_t) \ \cap \ (2 * S) \ \neq \ \emptyset, \tag{2}$$

where $2 * A$ denotes $\{2a : a \in A\}$. And now letting $A_t := S_t - t \subseteq H$, we have that (2) holds provided

$$|\cup_{t \in T} (A_t \hat{+} A_t + 2t)| \ > \ 2^n - |S|/2^n.$$

Of course, the left-hand-side can be re-expressed in terms of subsets $A_g \subseteq \mathbb{F}_2^n$, since the $A_t \subseteq H \cong \mathbb{F}_2^n$ and $2t \in H \cong \mathbb{F}_2^n$; and so, we are reduced to the problem in the previous section, *provided* we have that

$$|S_t| \ > \ 2^n/n^c, \text{ for every } t \in T. \tag{3}$$

1.2 Intrinsic appeal

Besides its connection to 3APs, I think the problem is also intrinsically interesting, because it highlights a new phenomenon; however, in vector spaces of characteristic 3 and higher, the analogous phenomenon uses the restricted difference set $A \hat{-} A$, instead of the restricted sumset $A \hat{+} A$. Consider, for example, the same problem in $\mathbb{F}_3^n$: Clearly, if we let V be any subspace of size 3^{n-1} we will have that $V + V = V$ also has size 3^{n-1}; and, if we let $V_g = V + g$, then $V_g + V_g + g = V$, making

$$\cup_{g \in \mathbb{F}_3^n}(V_g + V_g + g) \ = \ V,$$

which is only a positive fraction of $\mathbb{F}_3^n$; and we got this without even bothering with restricted sumsets.

So, in $\mathbb{F}_2^n$ (and in $\mathbb{F}_p^n$, $p \geq 3$, if differencesets are used) there is "not enough room" for the sumsets to move around and avoid covering most of $\mathbb{F}_2^n$ as we vary over translations g; but in other groups there *is* enough room.

1.3 Partial results

Seva Lev (and independently myself) found a nice elementary solution to the problem for $c < 1 + o(1)$; however, it gives nothing for $c > 1$ (which is really the case I am interested in). Here is the idea: Suppose that you have a family of sets A_g as described above so that $|A_g| \gg 2^n/n$, and our union fails to cover $\varepsilon 2^n$ elements of $\mathbb{F}_2^n$. Then, using the Szemeredi cube lemma, there exists an affine cube

$$C \;=\; t_0 + \{0, t_1\} + \cdots + \{t_k\},\ |C| \;\gg_\varepsilon n.$$

contained within this exceptional set of size $\varepsilon 2^n$. Now we show that C intersects $A_{t_0} \hat{+} A_{t_0} + t_0$ non-trivially: This is equivalent to showing that A_{t_0} contains two distinct elements that lie in the same coset of $D = C - t_0$. And indeed there is such a pair provided $|A_{t_0}| > 2^n/|D| = 2^n/|C|$.

It is also possible to give a fairly routine Fourier analytic proof. However, it also gets stuck at exponent $c = 1$.

1.4 An variant and a solution

In some ways the reason that some problems about sumsets are so difficult to resolve is that they are "unnatural (or artificial) objects" from an algebraic point of view (though perfectly natural from other perspectives) – so, one cannot easily apply the powerful methods of algebra to probelms about sumsets. The 'right' (or 'A right') sort of object from an algebraic perspective is "affine subspaces" (translates of subspaces), which then leads to the following Grassmannian special case variant of the above problem about sumsets:

Problem. Show that for every $c > 0$ and $n > n_0(c)$ we have that if $\{V_g\}_{g \in \mathbb{F}_2^n}$ is a family of subspaces of codimension at most $c \log n$, then

$$\cup_{g \in \mathbb{F}_2^n} (V_g + g)$$

covers $2^n(1-o(1))$ elements of $\mathbb{F}_2^n$ at least twice; obviously, by using the notation V_g^* to mean $V_g \setminus \{0\}$ we can reformulate this in terms of covering, rather than double-covering.

This problem feels like it involves some sort of Kakeya phenomena. To my great astonishment, like with the finite field Kakeya problem, it too has an elegant solution, though this one was provided by A. Blokhuis. His argument goes as follows: Form the $\mathbb{F}_2$ "incidence matrix" whose rows correspond to all the affine subspaces (translate $t+V$ of a subspace V) of $(\mathbb{F}_2)^n$ having codimension d, and let the columns correspond to the elements of $(\mathbb{F}_2)^n$ (placed in any order). Put a $1 \in \mathbb{F}_2$ in a particular row and column if the corresponding element is in the corresponding affine subspace; otherwise, put a $0 \in \mathbb{F}_2$ in that position. To bound the $\mathbb{F}_2$-rank of this matrix, one begins by observing that for a given affine subspace of codimension d (i.e. dimension $n-d$), one can easily construct a polynomial $f(x_1, ..., x_d)$ of degree $\leq d$, such that

$$v = (v_1, ..., v_n) \in V \iff f(x_1, ..., x_n) = 1.$$

We can assume that the monomials making up f are square-free by modding out by the ideal $(x_1^2 - x_1, ..., x_n^2 - x_n)$, and letting $g \equiv f$ modulo this ideal, where g is a sum of square-free monomials $x_{i_1} \cdots x_{i_k}$. Since there are at most $\binom{n}{d} + \binom{n}{d-1} + \cdots + 1$ monomials, there can be at most about $\binom{n}{d}$ (for $d = o(n)$, say) linearly independent polynomials corresponding to codimension d subspaces. It is a simple matter to show that a set of polynomials corresponding to some affine subspaces are independent if and only if the corresponding rows in the incidence matrix are independent; and so, the incidence matrix has rank at most about $\binom{n}{d}$, which is quite small relative to the number of rows or columns of the matrix.

Now suppose that S is the complement of the set $\cup_{g \in \mathbb{F}_2^n}(g + V_g^*)$, and that $|S|$ is "large". Then, we know that S can intersect $g + V_g$ at most at the point g (so, we use the element $0 \in V_g$ in the sum $g + V_g$ to get the element of S). Using this, one can show the matrix has a large identity submatrix, and therefore has large rank since we assumed $|S|$ was "large", and then this contradicts the rank upper bounds developed above.

Seva Lev has another proof that uses the polynomial method, and resembles Dvir's proof of the finite field Kakeya conjecture. It appears to be genuinely different from the proof above.

2 Acknowledgments

I would like to thank Seva Lev for comments and corrections.