SUMSETS AS UNIONS OF SUMSETS OF SUBSETS

JORDAN S. ELLENBERG

The novel approach to the polynomial method introduced by Croot, Lev, and Pach in [CLP17] has led to rapid progress in a range of problems in extremal combinatorics: for instance, a new upper bound for the cap set probem [EG17], bounds for complexity of matrix-multiplication methods based on elementary abelian groups [BCC+16], bounds for the Erdős-Szemeredi sunflower conjecture [NS16], and polynomial bounds for the arithmetic triangle removal lemma [FL16]. In many of the applications, the original bound on cap sets in [EG17] does not suffice for applications: for instance, in [BCC+16] and [FL16] one needs to bound the size of a *multi-colored sum-free set*, a somewhat more general object.

In the present note, we show how to use the polynomial method to prove a still more general lemma on sumsets which implies the combinatorial bounds used in applications so far. Loosely speaking, we show that the sumset $S+T$ of two large subsets S and T of $\mathbb{F}_q^n$ can be expressed "more efficiently" as a union of sumsets of smaller subsets.

Write $M(\mathbb{F}_q^n)$ for the upper bound proved in [EG17] for the size of a subset of $\mathbb{F}_q^n$ with no three-term arithmetic progressions; to be precise, $M(\mathbb{F}_q^n)$ is three times the number of monomials in $x_1, \ldots, x_n$ with degree at most $(q-1)$ in each variable and total degree at most $(q-1)n/3$. For each q, the bound $M(\mathbb{F}_q^n)$ is bounded above by c^n for some $c < q$. (We note that for the sake of the present argument there is no need to consider prime powers q other than primes.)

Theorem 1. *Let $\mathbb{F}_q$ be a finite field and let S, T be subsets of $\mathbb{F}_q^n$. Then there is a subset S' of S and a subset T' of T such that*

- $|S'| + |T'| \leq M(\mathbb{F}_q^n)$;
- $(S' + T) \cup (S + T') = S + T$.

Applying Theorem 1 to the symmetric case $S = T$, we get the following corollary:

Corollary 2. *Let S be a subset of $\mathbb{F}_q^n$. Then S has a subset S' of size at most $M(\mathbb{F}_q^n)$ such that $S' + S = S + S$.*

Proof. By Theorem 1 there are subsets S_1 and S_2 of S such that $S + S = (S_1 + S) \cup (S + S_2)$ and $|S_1| + |S_2| \leq M(\mathbb{F}_q^n)$. Taking S' to be $S_1 \cup S_2$ we are done. □

This immediately implies the bound proved in [EG17] on subsets of $\mathbb{F}_q^n$ with no three terms in arithmetic progression:

Corollary 3 ([EG17]). *A subset S of $\mathbb{F}_q^n$ containing no three-term arithmetic progression has size at most $M(\mathbb{F}_q^n)$.*

Proof. If S has no 3-term arithmetic progression, then $S' + S$ is strictly smaller than $S + S$ for every *proper* subset $S' \subset S$ (because $S' + S$ fails to contain $2s$ if s lies in the complement

Date: 1 Dec 2016.

of S'.) Thus, the subset S' guaranteed by Corollary 2 must be equal to S, whence $|S| = |S'| \leq M(\mathbb{F}_q^n)$. $\square$

Theorem 1 also implies the bounds on mutli-colored sum-free sets proved in [Kle16] and [BCC$^+$16]. (We note that [BCC$^+$16] proves a substantially more general result which applies, for example, to arbitrary abelian groups of bounded exponent.)

Corollary 4 (Th 1, [Kle16])**.** *Let S, T be subsets of $\mathbb{F}_q^n$ of the same cardinality N, assigned an ordering $s_1, \dots s_N$ and $t_1, \dots, t_N$ such that the equation $s_i + t_i = s_j + t_k$ holds only when $(j, k) = (i, i)$. Then $N \leq M(\mathbb{F}_q^n)$.*

Proof. Let S', T' be chosen as in Theorem 1. Each sum $s_i + t_i$ therefore lies in either $S + T'$ or $S' + T$. But since $s_i + t_i$ can't be expressed as $s_j + t_k$ for any other j, k, this implies that either $s_i \in S'$ or $t_i \in T'$. It follows that $N \leq |S'| + |T'| \leq M(\mathbb{F}_q^n)$. $\square$

We now prove Theorem 1. The proof is in essence no different from the arguments in the papers cited, but there is one new ingredient: a result of Meshulam [Mes85] on linear spaces of matrices of low rank.

Proof. Let V be the space of polynomials in $\mathbb{F}_q[x_1, \dots, x_n]$ with degree at most $(q-1)$ in each variable and total degree at most d, which vanish on the complement of $S + T$. Then $\dim V$ is at least $m_d - q^n + |S + T|$. Write $\mathcal{M}$ for the space of of $|S| \times |T|$ matrices, where the rows are understood to be indexed by S and the columns by T.

For each $P \in V$ we may consider $M(P) \in \mathcal{M}$ whose entries are $P(s + t)_{s \in S, t \in T}$. By the argument of the Croot-Lev-Pach lemma [CLP17] this matrix has rank at most $2m_{d/2}$.

Note that M is an homomorphism from V to $\mathcal{M}$, which is injective: if P lies in the kernel, it vanishes at $S + T$, but P vanishes on the complement of $S + T$, so P vanishes on every point of $\mathbb{F}_q^n$ and is 0.

We thus can, and do, think of V as a vector subspace of $\mathcal{M}$ of dimension at least $m_d - q^n + |S + T|$, each of whose members has rank at most $2m_{d/2}$.

In order to derive the desired conclusion, we use a theorem of Meshulam [Mes85], which gives lower bounds for the maximum rank attained in a linear space of matrices. Choose an ordering on S and an ordering on T. These choices endow the entries of a matrix in $\mathcal{M}$ with a lexicographic order. If $A \in \mathcal{M}$ is a matrix, we denote by $p(A) \in S \times T$ the location of the lexicographically first nonzero entry of A.

We note that $p(M(P))$ cannot be an arbitrary element of $S \times T$, since $M(P)$ has equal entries at (s, t) and (s', t') whenever $s + t = s' + t'$. In particular, this means that (s, t) and (s', t') cannot both be $p(M(P))$ for polynomials $P \in V$; only the lexicographically prior of these two pairs can appear.

By Gaussian elimination, there is a basis $A_1, \dots, A_{\dim V}$ for V such that $p(A_1), \dots, p(A_{\dim V})$ are distinct. Now apply Meshulam's theorem [Mes85, Theorem 1], which shows that there is a set of $2m_{d/2}$ lines (a line being a row or a column) whose union contains $p(A_i)$ for all i.

This set of lines consists of a subset of S, which we call S_0, and a subset of T, which we call T_0, satisfying $|S_0| + |T_0| = 2m_{d/2}$.

We now have, for $i = 1, \dots, \dim V$,

$$p(A_i) = (s_i, t_i)$$

with either $s_i \in S_0$ or $t_i \in T_0$. What's more, $s_i + t_i$ and $s_j + t_j$ are distinct whenever i and j are. So the union of $S_0 + T$ with $S + T_0$ contains at least $\dim V$ elements of $S + T$.

Since $\dim V \geq m_d - q_n + |S+T|$, the set W of elements of $S+T$ *not* contained in $(S_0+T)\cup(S+T_0)$ has cardinality at most $q_n - m_d$. Let S_1 be a subset of S of size $q_n - m_d$ such that each $w \in W$ is represented as $s+t$ for some $s \in S_1$. Then taking $S' = S_0 \cup S_1$ and $T' = T_0$, we have that $S'+T \cup S+T'$ contains all of $S+T$; moreover,

$$|S'| + |T'| \leq 2m_{d/2} + q^n - m_d$$

and minimizing over d we get the desired result. □

Remark 5. The bound on $|S'|+|T'|$ in Theorem 1 is essentially sharp, since Corollary 4, the consequent bound on multi-colored sum-free sets, is now known to be essentially sharp ([KSS16],[Nor16],[Peb16].)

Question 6. One naturally wonders whether Theorem 1 has an analogue for cyclic groups. That is: let $g(N)$ be the smallest integer such that, for any subsets S and T of $\mathbb{Z}/N\mathbb{Z}$, there are always $S' \subset S$ and $T' \subset T$ with $(S+T')\cup(S'+T) = S+T$ and $|S'|+|T'| \leq g(N)$. What can we say about the growth of $g(N)$? Behrend's example [Beh46] of a large subset of $\mathbb{Z}/N\mathbb{Z}$ with no three-term arithmetic progressions shows that $g(N)$ would have to be at least $N^{1-\epsilon}$. Jacob Fox and Will Sawin explained to me that $g(N) = o(N)$ follows from known bounds for arithmetic triangle removal.

Acknowledgments

The author is supported by NSF Grant DMS-1402620 and a Guggenheim Fellowship. He thanks Jacob Fox and the readers of Quomodocumque for useful discussions about the subject of this paper.

References

[BCC+16] J. Blasiak, T. Church, H. Cohn, J. A Grochow, E. Naslund, W. F. Sawin, and C. Umans, *On cap sets and the group-theoretic approach to matrix multiplication*, arXiv preprint arXiv:1605.06702, to appear, Discrete Analysis (2016).

[Beh46] F. A Behrend, *On sets of integers which contain no three terms in arithmetical progression*, Proceedings of the National Academy of Sciences **32** (1946), no. 12, 331–332.

[CLP17] E. Croot, V. Lev, and P. P. Pach, *Progression-free sets in $\mathbf{Z}_4^n$ are exponentially small*, Ann. of Math. **185** (2017), no. 1, 331-337.

[EG17] J. S. Ellenberg and D. Gijswijt, *On large subsets of $\mathbb{F}_q^n$ with no three-term arithmetic progression*, Ann. of Math. **185** (2017), no. 1, 339-343.

[FL16] J. Fox and L. M. Lovász, *A tight bound for Green's boolean removal lemma*, arXiv preprint arXiv:1606.01230 (2016).

[Kle16] R. Kleinberg, *A nearly tight upper bound on tri-colored sum-free sets in characteristic 2*, arXiv preprint arXiv:1605.08416 (2016).

[KSS16] R. Kleinberg, W. F. Sawin, and D. E. Speyer, *The Growth Rate of Tri-Colored Sum-Free Sets*, arXiv preprint arXiv:1607.00047 (2016).

[Mes85] R. Meshulam, *On the maximal rank in a subspace of matrices*, The Quarterly Journal of Mathematics **36** (1985), no. 2, 225–229.

[NS16] E. Naslund and W. F. Sawin, *Upper bounds for sunflower-free sets*, arXiv preprint arXiv:1606.09575 (2016).

[Nor16] S. Norin, *A distribution on triples with maximum entropy marginal*, arXiv preprint arXiv:1608.00243 (2016).

[Peb16] L. Pebody, *Proof of a Conjecture of Kleinberg-Sawin-Speyer*, arXiv preprint arXiv:1608.05740 (2016).