ON CAP SETS AND THE GROUP-THEORETIC APPROACH TO MATRIX MULTIPLICATION

JONAH BLASIAK, THOMAS CHURCH, HENRY COHN, JOSHUA A. GROCHOW, AND CHRIS UMANS

Abstract. In 2003, Cohn and Umans described a framework for proving upper bounds on the exponent \( \omega \) of matrix multiplication by reducing matrix multiplication to group algebra multiplication. In 2005 Cohn, Kleinberg, Szegedy, and Umans proposed specific conjectures for how to obtain \( \omega = 2 \) in this framework. In this note we rule out obtaining \( \omega = 2 \) in this framework from the groups \( \mathbb{F}_p^n \), using the breakthrough results of Croot, Lev, Pach, Ellenberg, and Gijswijt on cap sets. These restrictions do not however rule out abelian groups in general, let alone nonabelian groups.

1. Introduction

A cap set is a subset of \( \mathbb{F}_3^n \) containing no lines; equivalently, if \( u, v, w \) belong to the set then \( u + v + w = 0 \) if and only if \( u = v = w \). In a remarkable development, Ellenberg [9] and Gijswijt [11] proved that cap sets in \( \mathbb{F}_3^n \) are bounded in size by \( O(c^n) \) with \( c < 3 \). These papers built on a technique developed by Croot, Lev, and Pach [6] to analyze subsets of \( (\mathbb{Z}/4\mathbb{Z})^n \) containing no three-term arithmetic progression.

Via the connections established by Alon, Shpilka, and Umans [1], the cap set bounds prove the Erdős–Szemerédi sunflower conjecture [10], which was proposed as a means to show that the exponent \( \omega \) of matrix multiplication is 2. Alon et al. also show that a multicolored version of the cap set conjecture would disprove the “strong Uniquely Solvable Puzzle (USP)” conjecture of Cohn, Kleinberg, Szegedy, and Umans [2], which was another proposed approach to prove \( \omega = 2 \) in the group-theoretic framework of Cohn and Umans [3]. The strong USP conjecture is situated in the context of a broader family of conjectures from [2], which are all potential means to prove \( \omega = 2 \).

These conjectures all assert the existence of certain large “simultaneous triple product property” (STPP) constructions. An STPP construction is a collection of triples of subsets \( A_i, B_i, C_i \subseteq H \) inside a group \( H \), satisfying certain conditions (see Definition 2.2). The approach of [2] shows that when \( H \) is abelian, any STPP construction implies the inequality

\[
\sum_i (|A_i||B_i||C_i|)^{\omega/3} \leq |H|.
\]

If the sets involved are large enough, this yields a nontrivial bound on \( \omega \), and [2] showed how a family of sufficiently large STPP constructions could imply \( \omega = 2 \).

The purpose of this note is twofold. First, we check that Ellenberg and Gijswijt’s proof works in the multicolored case [1] thus disproving the strong USP conjecture via [1]. Second, we generalize [1] by showing that every STPP construction yields a large multicolored sum-free set. Together these two facts show that it is impossible to prove \( \omega = 2 \) using sets satisfying the simultaneous triple product property in the abelian groups \( \mathbb{F}_p^n \) for any fixed \( p \), or more precisely:
Theorem A. For every prime $p$, there is an $\varepsilon_p > 0$ such that no STPP construction in $\mathbb{F}_p^n$ is large enough to yield a bound better than $\omega \leq 2 + \varepsilon_p$ via the inequality (1).

(Note that there would be no additional generality in considering finite fields of prime power order, because only the additive group structure matters.)

Our results do not rule out achieving $\omega = 2$ by using STPP constructions over abelian groups. Specifically, when the group has a large cyclic factor, it indeed contains a large sum-free subset and thus the constraints analyzed in this note are irrelevant. Furthermore, one can use non-abelian groups or even more general objects such as association schemes [4]. Thus, our results serve to focus the search for group-theoretic constructions, and certainly do not rule them out as an approach to achieving $\omega = 2$.

For comparison, all of the current best bounds on $\omega$ via the group theoretic approach (in [2]), as well as the current best bounds on $\omega$ which use the Coppersmith–Winograd approach [5, 7, 14, 12], yield STPP constructions whose underlying group is $(\mathbb{Z}/m\mathbb{Z})^n$ for $m$ fixed. We expect that Theorem A generalizes to these cases (and perhaps even to products of powers of $\mathbb{Z}/m\mathbb{Z}$ for bounded $m$), but we do not see how to handle the case when $m$ is not prime.

2. The simultaneous triple product property

In 2003, Cohn and Umans [3] described a framework for proving upper bounds on the exponent $\omega$ of matrix multiplication by reducing matrix multiplication to group algebra multiplication. This reduction is carried out by means of a triple of subsets $A, B, C \subseteq G$ satisfying the triple product property:

Definition 2.1. Subsets $A, B, C$ of a group $G$ satisfy the triple product property if

$$abc = 1 \iff a = b = c = 1$$

for all $a \in A^{-1}A$, $b \in B^{-1}B$, and $c \in C^{-1}C$.

Such a triple of subsets realizes $\langle |A|, |B|, |C| \rangle$ inside the group algebra of $G$. (Here $\langle m, n, p \rangle$ denotes the matrix multiplication tensor for multiplying an $m \times n$ matrix by an $n \times p$ matrix.) From this, letting $\{d_i\}$ be the character degrees of $G$ (i.e., the dimensions of its irreducible representations), we obtain the inequality

$$(|A| |B| |C|)^{\omega/3} \leq \sum d_i^{\omega/3}$$

by bounding the rank of group algebra multiplication [3, Theorem 4.1]. This inequality yields an upper bound for $\omega$ when $G$ and $A, B, C$ are chosen appropriately.

In the later paper [2] several concrete routes to proving $\omega = 2$ were proposed. These proposals go beyond the framework of the triple product property in various different ways; however as described in [2, §7], all of the constructions proposed there can be described in a uniform way as follows. Several independent matrix multiplications are realized via the triple product property in the group algebra of a wreath product $H \wr S_m = H^m \rtimes S_m$ using certain well-chosen subsets of a group $H$. This general formulation is captured by the simultaneous triple product property [2, Definition 5.1]:

Definition 2.2. An STPP construction is a collection of triples of subsets $A_i, B_i, C_i$ of a group $H$ satisfying the simultaneous triple product property (STPP), which states that

1. for each $i$ the sets $A_i, B_i, C_i$ satisfy the triple product property, and
2. setting $S_i = A_i B_i^{-1}$, $T_i = B_i C_i^{-1}$, and $U_i = C_i A_i^{-1}$,

$$s_i t_j u_k = 1 \Rightarrow i = j = k$$

for all $s_i \in S_i$, $t_j \in T_j$ and $u_k \in U_k$. 


Lemma 2.4. Any family of STPP constructions that does not meet the packing bound cannot imply \( \omega = 2 \) via the inequality (1).

Proof. In our usual notation, if \( \sum_i |A_i| |B_i| \leq |H|^{1-3\varepsilon} \) for some fixed \( \varepsilon > 0 \), then

\[
\sum_i (|A_i| |B_i| |C_i|)^{\omega/3} \leq \left( \sum_i (|A_i| |B_i| |C_i|)^{2/3} \right)^{\omega/2}
\leq \left( \sum_i \left( |A_i| |B_i| |H|^{2\varepsilon} \cdot |C_i| |H|^{-\varepsilon} \cdot |A_i| |H|^{-\varepsilon} \right) \right)^{1/3} \leq 3 \sum_i |A_i| |B_i| |H|^{2\varepsilon} + \sum_i |B_i| |C_i| |H|^{-\varepsilon} + \sum_i |C_i| |A_i| |H|^{-\varepsilon} \omega/2
\leq (|H|^{1-\varepsilon})^{\omega/2},
\]

and so the strongest bound that can be obtained from (1) is \( \omega \leq 2 \cdot \frac{1}{1-\varepsilon} \), which is bounded strictly away from the hoped-for \( \omega = 2 \). The same holds if either \( \sum_i |B_i| |C_i| \leq |H|^{1-3\varepsilon} \) or \( \sum_i |C_i| |A_i| \leq |H|^{1-3\varepsilon} \).
Both the strong USP conjecture \cite[Conjecture 3.4]{2} and the “two families” conjecture \cite[Conjecture 4.7]{2} would, if true, yield STPP constructions that meet the packing bound and moreover prove $\omega = 2$. However, the STPP constructions produced by the strong USP conjecture have underlying group $H = \mathbb{F}_3^3$. Thus, Theorem \ref{thm:A} disproves the strong USP conjecture; by contrast, it addresses only very special cases of the two families conjecture.

3. The proof of Theorem \ref{thm:A}

**Definition 3.1.** A multicolored sum-free set in an abelian group $H$ is a 3-dimensional perfect matching $M \subseteq S \times T \times U$ on a triple of sets $S,T,U \subseteq H$, such that $s+t+u = 0$ for all $(s,t,u) \in M$ and $s+t+u \neq 0$ for all $(s,t,u) \in (S \times T \times U) \setminus M$. The cardinality of a multicolored sum-free set is the cardinality of $M$.

By a perfect matching $M \subseteq S \times T \times U$ we mean a subset whose projection onto each of the three factors is a bijection. In other words, given $s \in S$ there exist unique $t \in T$ and $u \in U$ such that $(s,t,u) \in M$ (and similarly for the other factors); in this case we say that $s$, $t$, and $u$ are matched. The cardinality of the matching $M$ is therefore equal to $|S|$, $|T|$, and $|U|$. Note that any 3-dimensional matching $M \subseteq H^3$ (not necessarily perfect, i.e., replacing “bijection” above with “injection”) uniquely determines three sets $S,T,U \subseteq H$ such that $M$ is a 3-dimensional perfect matching on $S \times T \times U$.

If $S \subseteq \mathbb{F}_p^n$ contains no three-term arithmetic progressions, then $M = \{(s,s, -2s) : s \in S\}$ is a multicolored sum-free set. Similarly, for any $\alpha, \beta, \gamma \in \mathbb{F}_p^n$ with $\alpha + \beta + \gamma = 0$, we obtain a multicolored sum-free set $M = \{ (\alpha s, \beta s, \gamma s) : s \in S \}$ whenever $S$ avoids nontrivial solutions to $\alpha s + \beta t + \gamma u = 0$.

The remainder of the paper is devoted to the proof of Theorem \ref{thm:A}. In Section 3.1 we show how to obtain a multicolored sum-free set from any STPP construction in an abelian group. In Section 3.2 we show that the breakthroughs of Croot, Lev, and Pach \cite{6}, Ellenberg \cite{9}, and Gijswijt \cite{11} which prove the cap set conjecture allow us to rule out multicolored sum-free sets of size $p^{n(1-o(1))}$ in groups of the form $\mathbb{F}_p^n$ when $p$ is a fixed prime and $n \to \infty$. Finally, we combine these pieces in Section 3.3 to complete the proof of Theorem \ref{thm:A} Specifically, we show that if there were a family of STPP constructions meeting the packing bound in groups of the form $\mathbb{F}_p^n$ with $p$ a fixed prime, then there would be multicolored sum-free sets of size $p^{n(1-o(1))}$ in such groups.

3.1. STPP constructions imply multicolored sum-free sets. Our main new contribution in this note is the following construction:

**Theorem 3.2.** Let $A_i, B_i, C_i \subseteq H$ be an STPP construction in an abelian group $H$. Then there is a multicolored sum-free set in $H$ of cardinality at least

$$\sum_i \frac{|A_i||B_i||C_i|}{|A_i|+|B_i|+|C_i|}.$$ 

**Proof.** Fix an $i$ and let $n_i = |A_i|$, $m_i = |B_i|$, and $p_i = |C_i|$. Identify $A_i, B_i, C_i$ with $[n_i], [m_i], [p_i]$, respectively, via bijections $\alpha, \beta, \gamma$. Let $r_i$ be the most frequently occurring value in the multiset

$$\{x+y+z : (x,y,z) \in [n_i] \times [m_i] \times [p_i]\}.$$ 

Define $M_i \subseteq H^3$ as

$$M_i = \{(a - b, b - c, c - a) : a \in A_i, b \in B_i, c \in C_i \text{ such that } \alpha(a) + \beta(b) + \gamma(c) = r_i\}.$$ 

Then $M_i$ is a multicolored sum-free set in $H$: to see that it is a matching, note that given the first coordinate $a - b$, the triple product property determines $a$ and $b$ from $a - b$, and then $\alpha(a) + \beta(b) + \gamma(c) = r_i$ determines $c$, and the same is true for the other two coordinates. By construction, for
We have because the original STPP construction meets the packing bound. Expanding the left side gives \( \hat{A} \) construction

Lemma 3.3. necessary in the proof of Theorem A.

\[ \left( \sum_i |A_i| |B_i| |C_i| \right)^N \cdot \left( \sum_i |B_i| |C_i| \right)^N \cdot \left( \sum_i |C_i| |A_i| \right)^N \geq |H|^{3N(1-o(1))} \]

because the original STPP construction meets the packing bound. Expanding the left side gives

\[ \sum_u \prod_{\ell} |A_{u_{\ell}}| |B_{v_{\ell}}| \cdot \sum_v \prod_{\ell} |B_{v_{\ell}}| |C_{v_{\ell}}| \cdot \sum_w \prod_{\ell} |C_{w_{\ell}}| |A_{w_{\ell}}| = \sum_{u,v,w} \prod_{\ell} |A_{u_{\ell}}| |B_{v_{\ell}}| |C_{w_{\ell}}| |B_{u_{\ell}}| |C_{v_{\ell}}| |A_{w_{\ell}}| . \]

We have

\[ \left( \sum_i |A_i| |B_i| \right)^N \cdot \left( \sum_i |B_i| |C_i| \right)^N \cdot \left( \sum_i |C_i| |A_i| \right)^N \geq |H|^{3N(1-o(1))} \]

To control the size of the multicolored sum-free set resulting from Theorem 3.2, we will need the following notion. We say that an STPP construction is uniform if \( |A_i| \) is independent of \( i \), as are \( |B_i| \) and \( |C_i| \) (note that we do not require \( |A_i| = |B_i| = |C_i| \)). The following lemma will be necessary in the proof of Theorem A.

Lemma 3.3. If there is a family of STPP constructions in abelian groups \( H \) meeting the packing bound, then there is a family of uniform STPP constructions in powers of \( H \) meeting the packing bound.

Proof. Let the original STPP construction consist of \( n \) triples \( A_i, B_i, C_i \) of subsets of \( H \) indexed by \( i \in [n] \). Our new STPP construction will consist of subsets of \( H^{3N} \), where \( N \) is a large number to be chosen later; these subsets are indexed by triples \( (u,v,w) \in [n]^N \times [n]^N \times [n]^N \) and defined by

\[ \tilde{A}_{u,v,w} = \prod_{\ell} A_{u_{\ell}} \times \prod_{\ell} B_{v_{\ell}} \times \prod_{\ell} C_{w_{\ell}} \]

\[ \tilde{B}_{u,v,w} = \prod_{\ell} B_{u_{\ell}} \times \prod_{\ell} C_{v_{\ell}} \times \prod_{\ell} A_{w_{\ell}} \]

\[ \tilde{C}_{u,v,w} = \prod_{\ell} C_{u_{\ell}} \times \prod_{\ell} A_{v_{\ell}} \times \prod_{\ell} B_{w_{\ell}} \]

Finally, the sets \( S_i \) are pairwise disjoint, as are \( T_i \) and \( U_i \), and we set \( S = \bigcup_i S_i \), \( T = \bigcup_i T_i \), \( U = \bigcup_i U_i \), and \( M = \bigcup_i M_i \). Then \( M \) is a multicolored sum-free set in \( H \), because the simultaneous triple product property implies that if \( s_i + t_j + u_k = 0 \) with \( s_i \in S_i \), \( t_j \in T_j \), and \( u_k \in U_k \), then \( i = j = k \). Since the sets \( S_i \) are disjoint, so are the sets \( M_i \); thus \( |M| = \sum_i |M_i| \), and the theorem follows from the lower bound on \( |M_i| \) above.

To control the size of the multicolored sum-free set resulting from Theorem 3.2, we will need the following notion. We say that an STPP construction is uniform if \( |A_i| \) is independent of \( i \), as are \( |B_i| \) and \( |C_i| \) (note that we do not require \( |A_i| = |B_i| = |C_i| \)). The following lemma will be necessary in the proof of Theorem A.

Lemma 3.3. If there is a family of STPP constructions in abelian groups \( H \) meeting the packing bound, then there is a family of uniform STPP constructions in powers of \( H \) meeting the packing bound.

Proof. Let the original STPP construction consist of \( n \) triples \( A_i, B_i, C_i \) of subsets of \( H \) indexed by \( i \in [n] \). Our new STPP construction will consist of subsets of \( H^{3N} \), where \( N \) is a large number to be chosen later; these subsets are indexed by triples \( (u,v,w) \in [n]^N \times [n]^N \times [n]^N \) and defined by

\[ \tilde{A}_{u,v,w} = \prod_{\ell} A_{u_{\ell}} \times \prod_{\ell} B_{v_{\ell}} \times \prod_{\ell} C_{w_{\ell}} \]

\[ \tilde{B}_{u,v,w} = \prod_{\ell} B_{u_{\ell}} \times \prod_{\ell} C_{v_{\ell}} \times \prod_{\ell} A_{w_{\ell}} \]

\[ \tilde{C}_{u,v,w} = \prod_{\ell} C_{u_{\ell}} \times \prod_{\ell} A_{v_{\ell}} \times \prod_{\ell} B_{w_{\ell}} \]

Note that the products here are cartesian products of sets. It is not hard to verify that these sets satisfy the STPP in \( H^{3N} \) (see [2, Lemma 5.4]). The resulting STPP construction is not yet uniform, but will become so below when we restrict the choices of \( u, v, \) and \( w \). We first argue that the STPP construction \( \tilde{A}_{u,v,w}, \tilde{B}_{u,v,w}, \tilde{C}_{u,v,w} \) meets the packing bound if the original sets \( A_i, B_i, C_i \) did.

To check that this construction meets the packing bound, we observe that

\[ \left( \sum_i |A_i| |B_i| \right)^N \cdot \left( \sum_i |B_i| |C_i| \right)^N \cdot \left( \sum_i |C_i| |A_i| \right)^N \geq |H|^{3N(1-o(1))} \]

because the original STPP construction meets the packing bound. Expanding the left side gives

\[ \sum_{u,v,w} \prod_{\ell} |A_{u_{\ell}}| |B_{v_{\ell}}| |C_{w_{\ell}}| |A_{u_{\ell}}| |B_{v_{\ell}}| |C_{w_{\ell}}| |B_{u_{\ell}}| |C_{v_{\ell}}| |A_{w_{\ell}}| . \]

We have

\[ \sum_{u,v,w} \prod_{\ell} |A_{u_{\ell}}| |B_{v_{\ell}}| |C_{w_{\ell}}| |B_{u_{\ell}}| |C_{v_{\ell}}| |A_{w_{\ell}}| \]

(3) \[ |\tilde{A}_{u,v,w}| |\tilde{B}_{u,v,w}| = \prod_{\ell} |A_{u_{\ell}}| |B_{v_{\ell}}| |C_{w_{\ell}}| |B_{u_{\ell}}| |C_{v_{\ell}}| |A_{w_{\ell}}| \]
and hence
\[\sum_{u,v,w} |\hat{A}_{u,v,w}| |\hat{B}_{u,v,w}| \geq |H|^{3N(1-o(1))},\]
as desired; the same also holds for \(\sum_{u,v,w} |\hat{B}_{u,v,w}| |\hat{C}_{u,v,w}|\) and \(\sum_{u,v,w} |\hat{A}_{u,v,w}| |\hat{C}_{u,v,w}|\).

To enforce uniformity, we restrict our attention to only certain choices of \(u, v,\) and \(w\). Specifically, we look at their distributions (the distribution of \(u\) is the vector specifying the number of times each element of \([n]\) occurs in \(u\)). There are \(\binom{N+n-1}{n-1}\) possible distributions, but all we need is the crude upper bound \((N+1)^n\) from the fact that each element of \([n]\) occurs between 0 and \(N\) times. It follows that there is at least one triple \(\mu_1, \mu_2, \mu_3\) of distributions for which
\[(4) \quad \sum_{u \sim \mu_1} \prod_{\ell} |A_{u,\ell}| |B_{u,\ell}| \cdot \sum_{v \sim \mu_2} \prod_{\ell} |B_{v,\ell}| |C_{v,\ell}| \cdot \sum_{w \sim \mu_3} \prod_{\ell} |C_{w,\ell}| |A_{w,\ell}| \geq \frac{1}{(N+1)^{3n}} |H|^{3N(1-o(1))},\]
where \(u \sim \mu_1\) means \(u\) has distribution \(\mu_1\).

The sets \(\hat{A}_{u,v,w}, \hat{B}_{u,v,w},\) and \(\hat{C}_{u,v,w}\) with \(u \sim \mu_1, v \sim \mu_2,\) and \(w \sim \mu_3\) are uniform, because
\[|\hat{A}_{u,v,w}| = \prod_{\ell} |A_{u,\ell}| |B_{v,\ell}| |C_{w,\ell}|\]
depends only on the distributions (not the choice of \(u, v, w\)) and the same holds for \(\hat{B}_{u,v,w}\) and \(\hat{C}_{u,v,w}\). Combining (3) and (4) we obtain
\[\sum_{u \sim \mu_1, v \sim \mu_2, w \sim \mu_3} |\hat{A}_{u,v,w}| |\hat{B}_{u,v,w}| \geq \frac{1}{(N+1)^{3n}} |H|^{3N(1-o(1))},\]
which is again \(|H|^{3N(1-o(1))}\) as long as \(N\) is chosen sufficiently large relative to \(n\) and \(|H|\), and the same holds for the other two conditions in the packing bound.

Choosing \(N\) and \(\mu_1, \mu_2, \mu_3\) in this way thus yields a family of uniform STPP constructions meeting the packing bound in powers of \(|H|\), as desired. \(\square\)

3.2. Upper bound on multicolored sum-free sets. We reproduce the proof of Ellenberg and Gijswijt in order to demonstrate that it extends to the multicolored case. That the proof extends to this case was also observed independently by Noga Alon and by Eric Naslund. We follow Ellenberg’s proof in [9] closely, although we phrase some things slightly differently.

**Theorem 3.4.** For any prime \(p\), every multicolored sum-free set in \(\mathbb{F}_p^n\) has cardinality at most \(5p^n e^{-n/18}\). In other words, every multicolored sum-free set in an abelian group \(H\) of exponent \(p\) has cardinality at most \(5|H|^{1-1/18\log p}\).

As Alon has noted in personal communication, the Salem–Spencer subsets of \(\mathbb{F}_p^n\) without three-term arithmetic progressions have size \((2+o(1))^{-n} p^n\) as \(n \to \infty\) with \(p\) fixed (see, for example, the proof of Theorem 2.13 in [1]), and thus the exponential factor \(e^{-n/18}\) in Theorem 3.4 is tight up to the constant 18.

**Proof.** Let \(M_n\) denote the set of \(n\)-variate \(p\)-power-free monomials (i.e., the degree in each variable is less than \(p\)). There are \(p^n\) such monomials, and interpreting them as functions on \(\mathbb{F}_p^n\), they span the \(p^n\)-dimensional space of \(\mathbb{F}_p\)-valued functions on \(\mathbb{F}_p^n\). As in [1], for any \(c \in \mathbb{R}\) let \(M_n^c\) denote the set of \(n\)-variate \(p\)-power-free monomials with total degree at most \(c\). Writing \(D = (p-1)n\), every monomial has degree at most \(D\), i.e., \(M_n = M_n^D\). Moreover the bijection \(m \mapsto (x_1^{p-1} \cdots x_{n-1}^{p-1})/m\) shows \(|M_n^c| = p^n - |M_n^{D-c-1}|\). (When \(c \in \mathbb{N}\), this is not correct; in that case \(|M_n^c| = p^n - |M_n^{D-c-1}|\) instead. However we will be able to ignore this tiny discrepancy, because the bounds we obtain below depend continuously on \(d\), so it suffices that they hold whenever \(d\) is perturbed by an arbitrarily small amount.)
For our proof we set \( d = \frac{3}{2} D \) and consider \( M_n^d \), which has size

\[
|M_n^d| = p^n - |M_n^{D-d}| = p^n - |M_n^d| = p^n - |M_n^{d/2}|.
\]

Let us estimate the size of \( M_n^{d/2} = M_n^{\frac{d}{2}} \). The degree of a random monomial in \( M_n \) is the sum of \( n \) independent random variables uniformly distributed on \( 0, 1, \ldots, p-1 \). The mean is \( \frac{1}{2} D \), and the chance that this sum deviates on one side from the mean by at least \( \varepsilon D \) is at most \( e^{-2n\varepsilon^2} \) (a special case of Hoeffding’s inequality). We want to know how many polynomials have degree at most \( \frac{1}{2} D \), so \( \varepsilon = \frac{1}{6} \) and

\[
|M_n^{d/2}| = |M_n^{\frac{d}{2}}| \leq p^n e^{-n/18}.
\]

Let \( M \) be a multicolored sum-free set in \( \mathbb{F}_p^n \), which is a 3-dimensional perfect matching \( M \subseteq S \times T \times U \) on a triple of sets \( S, T, U \subseteq H \). Our goal is to prove that \( |M| = |U| \) is at most \( 5p^n e^{-n/18} \). Assume therefore that \( |U| \geq 5|M_n^{d/2}| \). Consider the subspace \( V \) of \( \text{span}_{\mathbb{F}_p} M_n^d \) consisting of polynomials that vanish on the complement of \( -U \). Note that \( \dim V \) must be at least \( |M_n^d| - (p^n - |U|) = |U| - |M_n^{d/2}| \), so our assumption guarantees that \( \dim V \geq \frac{4}{5} |U| \).

A random polynomial in \( V \) is expected to be non-zero on at least \( (1 - \frac{1}{p}) \dim V \) distinct points in \( -U \); indeed, each point in \( -U \) at which some element of \( V \) is non-zero contributes \( 1 - \frac{1}{p} \) to this expectation, and there are at least \( \dim V \) such points. Substituting \( 1 - \frac{1}{p} \geq \frac{4}{5} \) for simplicity, we conclude that there exists some polynomial \( P \in V \) which is non-zero on at least \( \frac{1}{2} \dim V \geq \frac{2}{5} |U| \) distinct points in \( -U \).

Fix this polynomial \( P \) and consider the \( |S| \times |T| \) matrix with entries \( P_M[s, t] = P(s + t) \) indexed by \( S \) and \( T \), and with matched terms on the diagonal. We will bound the rank of \( M_P \) from first beyond and then from above. The properties of multicolored sum-free sets imply that \( P(s + t) = 0 \) if \( s \) and \( t \) are not matched (since in that case \( s + t \notin -U \), and \( P \) vanishes off \( -U \) by definition), so the off-diagonal entries of \( M_P \) vanish. The diagonal entries correspond to matched terms \((s, t, u)\) with \( s + t = -u \), and we know that \( P(s + t) = P(-u) \) is nonzero for at least \( \frac{2}{3} |U| \) of the points in \( -U \), so at least \( \frac{2}{5} |U| \) of the diagonal entries are nonzero. Therefore the rank of \( M_P \) is at least \( \frac{2}{5} |U| \).

To conclude we need to bound the rank of \( M_P \) from above. Since \( P \in \text{span}_{\mathbb{F}_p} M_n^d \) the rank of \( M_P \) is trivially at most \( |M_n^d| \), but the insight of Croot, Lev, and Pach was that it is actually much smaller (for any \( P \in M_n^d \), not just our chosen polynomial). As in [9], we can expand \( P(x + y) \) and gather terms; noting that each monomial in \( P(x + y) \) has degree at most \( d/2 \) in either \( x \) or \( y \), we can write \( P(x + y) \) as

\[
P(x + y) = \sum_{m \in M_n^{d/2}} m(x) F_m(y) + \sum_{m \in M_n^{d/2}} G_m(x)m(y),
\]

where the \( F_m \) and \( G_m \) are two families of polynomials indexed by monomials \( m \in M_n^{d/2} \). In other words, if

\[
A \text{ is the } |S| \times 2|M_n^{d/2}| \text{ matrix with } A[s, (m, 0)] = m(s) \text{ and } A[s, (m, 1)] = G_m(s), \text{ and}
\]

\[
B \text{ is the } 2|M_n^{d/2}| \times |T| \text{ matrix with } B[(m, 0), t] = F_m(t) \text{ and } B[(m, 1), t] = m(t),
\]

then \( M_P = AB \), so the rank of \( M_P \) is at most \( 2|M_n^{d/2}| \). Combined with the previous paragraph, we conclude that \( \frac{2}{5} |U| \leq 2|M_n^{d/2}| \); in other words, \( |U| \leq 5|M_n^{d/2}| \leq 5p^n e^{-n/18} \), as desired. \( \square \)

As in [9], one can obtain a slightly better bound via a more careful analysis, such as the upper bound of \( 2.756^n \) obtained for cap sets in \( \mathbb{F}_3^n \) in [9]. It is worth noting that attempts to improve the upper bound in Theorem 3.4 must contend with the fact that the known lower bound for
multicolored sum-free sets in $\mathbb{F}_3^n$ is $(2^{4/3} - o(1))^n = (2.519\ldots - o(1))^n$ from [1], p. 238], which is substantially larger than the cap set construction of $(2.217\ldots - o(1))^n$ obtained by Edel [8] or the refinement of Edel’s construction obtained by Naslund (personal communication).

3.3. Concluding the proof. Fix a prime $p$, and suppose that for each $\varepsilon > 0$ there is an STPP construction in a group of exponent $p$ that proves $\omega \leq 2 + \varepsilon$. Choosing a sequence with $\varepsilon$ tending to zero, we obtain a family of STPP constructions that meets the packing bound by Lemma 2.4. Furthermore, by Lemma 3.3 we can inflate these constructions to make them uniform, while still meeting the packing bound and remaining in groups of exponent $p$.

Consider one of these uniform STPP constructions, in a group $H$ of exponent $p$. By Theorem 3.2, there exists a multicolored sum-free set in $H$ of cardinality $\sum |A_i||B_i||C_i|$. Since $|A_i|$, $|B_i|$, and $|C_i|$ are each independent of $i$, without loss of generality we may assume that $|C_i|$ is the largest of these, in which case

$$\sum |A_i||B_i||C_i|/|A_i|+|B_i|+|C_i| \geq \frac{1}{3} \sum |A_i||B_i| \geq |H|^{1-o(1)}.$$  

This contradicts Theorem 3.3, which states that the cardinality of any multicolored sum-free set in $H$ is at most $5|H|^{-\frac{1}{8} \log p}$, and thus completes the proof of Theorem A.

ACKNOWLEDGEMENTS

We thank the AIM SQuaRE program, the Santa Fe Institute, and Microsoft Research for hosting visits.

REFERENCES

[1] N. Alon, A. Shpilka, and C. Umans, On sunflowers and matrix multiplication, Computational Complexity 22 (2013), 219–243.
[2] H. Cohn, R. Kleinberg, B. Szegedy, and C. Umans, Group-theoretic algorithms for matrix multiplication, Proceedings of the 46th Annual Symposium on Foundations of Computer Science, 23–25 October 2005, Pittsburgh, PA, IEEE Computer Society, pp. 379–388, arXiv:math.GR/0511460.
[3] H. Cohn and C. Umans, A group-theoretic approach to fast matrix multiplication, Proceedings of the 44th Annual Symposium on Foundations of Computer Science, 11–14 October 2003, Cambridge, MA, IEEE Computer Society, pp. 438–449, arXiv:math.GR/0307321.
[4] H. Cohn and C. Umans, Fast matrix multiplication using coherent configurations, Proceedings of the 24th Annual ACM-SIAM Symposium on Discrete Algorithms, 6–8 January 2013, New Orleans, LA, Society for Industrial and Applied Mathematics, pp. 1074–1087, arXiv:1207.6528.
[5] D. Coppersmith and S. Winograd, Matrix multiplication via arithmetic progressions, J. Symbolic Computation 9 (1990), 251–280.
[6] E. Croot, V. Lev, and P. Pach, Progression-free sets in $\mathbb{Z}_4^n$ are exponentially small, preprint, 2016, arXiv:1605.01506.
[7] A. M. Davie and A. J. Stothers, Improved bound for complexity of matrix multiplication, Proc. Roy. Soc. Edinburgh Sect. A 143 (2013), 351–369.
[8] Y. Edel, Extensions of generalized product caps, Des. Codes Cryptogr. 31 (2004), 5–14.
[9] J. Ellenberg, On large subsets of $\mathbb{F}_p^n$ with no three-term arithmetic progression, preprint, 2016.
[10] P. Erdős and E. Szemerédi, Combinatorial properties of systems of sets, J. Combinatorial Theory Ser. A 24 (1978), 308–313.
[11] D. Gijswijt, Asymptotic upper bounds on progression-free sets in $\mathbb{Z}_4^n$, preprint, 2016, arXiv:1605.05492.
[12] F. Le Gall, Powers of tensors and fast matrix multiplication, Proceedings of the 39th International Symposium on Symbolic and Algebraic Computation, 23–25 July 2014, Kobe, Japan, ACM, pp. 296–303, full version at arXiv:1407.7713.
[13] A. Schönhage, Partial and total matrix multiplication, SIAM J. Comp. 10 (1981), 434–455.
[14] V. Vassilevska Williams, Multiplying matrices faster than Coppersmith–Winograd, Proceedings of the 44th ACM Symposium on Theory of Computing, 19–22 May 2012, New York, NY, Association for Computing Machinery, pp. 887–898.
