

On Cap Sets and the Group-theoretic Approach to Matrix Multiplication

Jonah Blasiak* Thomas Church[†] Henry Cohn Joshua A. Grochow[‡]
Eric Naslund[§] William F. Sawin[¶] Chris Umans^{||}

Received 17 August 2016; Revised 5 January 2017; Published 16 January 2017

Abstract: In 2003, Cohn and Umans described a framework for proving upper bounds on the exponent ω of matrix multiplication by reducing matrix multiplication to group algebra multiplication, and in 2005 Cohn, Kleinberg, Szegedy, and Umans proposed specific conjectures for how to obtain $\omega = 2$. In this paper we rule out obtaining $\omega = 2$ in this framework from abelian groups of bounded exponent. To do this we bound the size of tricolored sum-free sets in such groups, extending the breakthrough results of Croot, Lev, Pach, Ellenberg, and Gijswijt on cap sets. As a byproduct of our proof, we show that a variant of tensor rank due to Tao gives a quantitative understanding of the notion of unstable tensor from geometric invariant theory.

1 Introduction

A *cap set* is a subset of \mathbb{F}_3^n containing no lines; equivalently, if u , v , and w belong to the set, then $u + v + w = 0$ if and only if $u = v = w$. In a remarkable pair of recent papers [9, 11], Croot, Lev, and

*Supported by NSF grant DMS-14071174.

[†]Supported by NSF grant DMS-1350138, the Alfred P. Sloan Foundation, and the Frederick E. Terman Fellowship.

[‡]Supported by a Santa Fe Institute Omidyar Fellowship.

[§]Supported by Ben Green's ERC Starting Grant 279438, Approximate Algebraic Structure and Applications.

[¶]Supported by NSF grant DGE-1148900, Dr. Max Rössler, the Walter Haefner Foundation, and the ETH Zürich Foundation.

^{||}Supported by NSF grant CCF-1423544 and a Simons Foundation Investigator grant.

Pach [9] introduced a powerful new technique, which Ellenberg and Gijswijt [11] used to prove that cap sets in \mathbb{F}_3^n are bounded in size by $O(c^n)$ with $c < 3$, thus settling a long-standing open question. The results of Ellenberg and Gijswijt similarly bound the size of subsets of \mathbb{F}_p^n that contain no three-term arithmetic progressions, as well as certain more general sum-free sets.

Via the connections established earlier by Alon, Shpilka, and Umans [1], the cap set bounds prove the Erdős–Szemerédi sunflower conjecture [12] and disprove the Coppersmith–Winograd “no three disjoint equivoluminous subsets” conjecture [7], which was proposed as a means to show that the exponent ω of matrix multiplication is 2. Alon *et al.* also showed that a *tricolored* version of the cap set bounds would disprove the “strong Uniquely Solvable Puzzle (USP)” conjecture of Cohn, Kleinberg, Szegedy, and Umans [4], which was another proposed approach to prove $\omega = 2$ in the group-theoretic framework of Cohn and Umans [5]. The strong USP conjecture is situated in the context of a broader family of conjectures from [4], 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 [4] shows that when H is abelian, any STPP construction implies the inequality

$$\sum_i (|A_i| |B_i| |C_i|)^{\omega/3} \leq |H|. \tag{1.1}$$

If the sets involved are large enough, this yields a nontrivial bound on ω , and [4] showed how a family of sufficiently large STPP constructions would imply $\omega = 2$.

This paper contains two main results. The first is a bound on the size of tricolored sum-free sets in abelian groups of bounded exponent. A tricolored sum-free set is a generalization of a three-term progression-free set (a set whose elements satisfy $u + v = 2w \iff u = v = w$) in which the elements u , v , and w range over three *different* subsets (see Definition 3.1). The *exponent* of a finite group is the least common multiple of the orders of all its elements; if a finite abelian group is generated by elements of order at most m , then its exponent is at most $\text{lcm}(1, 2, \dots, m) = e^{m(1+o(1))}$. (This asymptotic formula for $\text{lcm}(1, 2, \dots, m)$ is a variant of the prime number theorem. See, for example, Theorem 11 in [23] for a stronger bound on $\psi(m) = \log \text{lcm}(1, 2, \dots, m)$.)

Theorem A. *There exists an absolute constant $\varepsilon = \frac{1}{2} \log((2/3)2^{2/3}) = 0.02831\dots$ such that if H is an abelian group generated by elements of order at most m , then every tricolored sum-free set in H has size at most $3 \cdot |H|^{1-\frac{\varepsilon}{m}}$.*

In the case when H is a power of a single cyclic group $\mathbb{Z}/p^k\mathbb{Z}$, we obtain a sharper bound.

Theorem A’. *There exists an absolute constant $\delta = 2\varepsilon = 0.05663\dots$ such that if $H \cong (\mathbb{Z}/q\mathbb{Z})^n$ for some prime power q , then every tricolored sum-free set in H has size at most $3 \cdot |H|^{1-\frac{\delta}{\log q}}$.*

These theorems extend the Ellenberg–Gijswijt [11] result in two directions: from progression-free sets to tricolored sum-free sets¹ and from abelian groups of prime exponent to abelian groups of bounded exponent. In particular, Theorem A disproves the strong USP conjecture via [1]. Note that when H has prime exponent p , the bound in Theorem A’ of $3 \cdot |H|^{1-\frac{\delta}{\log p}}$ agrees with the bound for progression-free

¹Noga Alon independently observed that the Ellenberg–Gijswijt result extends to tricolored sum-free sets in \mathbb{F}_p^n .

sets obtained in [11], but with a slightly worse exponent as we have stated it uniformly in p . It remains to be seen whether $\frac{\varepsilon}{m}$ can be improved to $\frac{c}{\log m}$ for general abelian groups of bounded exponent. A generalization of the Ellenberg–Gijswijt result that handles progression-free sets in abelian p -groups of bounded exponent was also obtained by Petrov in [20].

In the proof of Theorem A, we study a variant of tensor rank due to Tao [22], which we call slice rank, and we show how slice rank is related to a quantitative version of the notion of instability from geometric invariant theory. We show that functions with low slice rank are unstable, and conversely prove that a quantitative bound on instability yields a bound on slice rank of tensor powers (see Section 4.2).

Our second main result generalizes [1] by showing that every STPP construction yields a large tricolored 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 abelian groups of bounded exponent:

Theorem B. *For every $\ell \in \mathbb{N}$, there is an $\varepsilon_\ell > 0$ such that no STPP construction in any abelian group of exponent at most ℓ is large enough to yield a bound better than $\omega \leq 2 + \varepsilon_\ell$ via the inequality (1.1).*

Note that all of the current best bounds on ω via the group-theoretic approach (in [4]), as well as the current best bounds on ω which use the Coppersmith–Winograd approach [7, 10, 24, 15], yield STPP constructions whose underlying group is $(\mathbb{Z}/m\mathbb{Z})^n$ for m fixed.

However, 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 here are irrelevant. Furthermore, one can use non-abelian groups or even more general objects such as association schemes [6]. Thus, our results serve to focus the search for group-theoretic constructions, and certainly *do not* rule them out as an approach to achieving $\omega = 2$.

2 The simultaneous triple product property

Recall that the *exponent of matrix multiplication* is defined as

$$\omega = \inf\{c : \text{the tensor rank of } n \times n \text{ matrix multiplication is at most } O(n^c) \text{ as } n \rightarrow \infty\}.$$

In 2003, Cohn and Umans [5] described a framework for proving upper bounds on ω by reducing matrix multiplication to group algebra multiplication. This reduction is carried out by means of a triple of subsets satisfying the *triple product property*:

Definition 2.1 ([5, 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 $c \in C^{-1}C$, where $S^{-1}S$ denotes $\{s^{-1}s' : s, s' \in S\}$ for $S \subseteq G$.

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_1, d_2, \dots be the character degrees of G (i.e., the dimensions of its irreducible representations), we obtain the inequality

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

by bounding the rank of group algebra multiplication [5, Theorem 4.1]. This inequality yields an upper bound for ω when G and A, B, C are chosen appropriately.

In the later paper [4] several concrete routes to proving $\omega = 2$ were proposed. These proposals seemingly go beyond the framework of the triple product property in various different ways; however as described in [4, §7], all of these constructions can be uniformly described using the triple product property 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:

Definition 2.2 ([4, Definition 5.1]). *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 $S_i = A_i B_i^{-1}$, $T_j = B_j C_j^{-1}$, and $U_k = C_k A_k^{-1}$,*

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

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

Equivalently, $A_i, B_i, C_i \subseteq H$ satisfy the STPP if for all i, j, k and $s \in A_k$, $s' \in A_i$, $t \in B_i$, $t' \in B_j$, $u \in C_j$, and $u' \in C_k$, we have

$$s^{-1} s' t^{-1} t' u^{-1} u' = 1 \quad \Leftrightarrow \quad i = j = k, \quad s = s', \quad t = t', \quad u = u'.$$

An STPP construction in H realizes the tensor $\bigoplus_i \langle |A_i|, |B_i|, |C_i| \rangle$ and, via the asymptotic sum inequality [21] or the use of a wreath product [4, §7], yields the fundamental inequality

$$\sum_i (|A_i| |B_i| |C_i|)^{\omega/3} \leq \sum_i d_i^\omega, \tag{2.1}$$

where d_1, d_2, \dots are the character degrees of H . For the rest of this paper we will take H to be abelian (with additive notation), in which case this bound becomes the inequality (1.1) of the introduction:

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

All of the analysis of STPP constructions in the framework of [4] is based on this inequality.

No single STPP construction can achieve $\omega = 2$ via (2.1) (more generally, see [8]), so we must consider families of constructions in groups of growing size. To simplify the notation we typically do not index such families explicitly (i.e., we refer to a group H rather than, say, $\{H_\alpha\}_{\alpha \in A}$).

Any STPP construction satisfies some simple “packing bound” inequalities, which reflect the fact that the sets S_i must be disjoint from each other, as must T_i and U_i . This disjointness follows immediately from the second condition in the definition of the simultaneous triple product property. Furthermore, since the sets A_i, B_i, C_i satisfy the triple product property we must have $|S_i| = |A_i| |B_i|$, $|T_i| = |B_i| |C_i|$, and $|U_i| = |C_i| |A_i|$. Together these give the packing bounds:

$$\sum_i |A_i| |B_i| \leq |H|, \quad \sum_i |B_i| |C_i| \leq |H|, \quad \text{and} \quad \sum_i |C_i| |A_i| \leq |H|.$$

Definition 2.3. We say that a family of STPP constructions with $|H| \rightarrow \infty$ meets the packing bound if

$$\sum_i |A_i| |B_i| \geq |H|^{1-o(1)}, \quad \sum_i |B_i| |C_i| \geq |H|^{1-o(1)}, \quad \text{and} \quad \sum_i |C_i| |A_i| \geq |H|^{1-o(1)}.$$

A key observation is that meeting the packing bound is necessary for achieving $\omega = 2$:

Lemma 2.4. Any family of STPP constructions that does not meet the packing bound cannot imply $\omega = 2$ via the inequality (1.1).

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

$$\begin{aligned} \sum_i (|A_i| |B_i| |C_i|)^{\omega/3} &\leq \left(\sum_i (|A_i| |B_i| |C_i|)^{2/3} \right)^{\omega/2} \\ &= \left(\sum_i \left(|A_i| |B_i| |H|^{2\varepsilon} \cdot |B_i| |C_i| |H|^{-\varepsilon} \cdot |C_i| |A_i| |H|^{-\varepsilon} \right)^{1/3} \right)^{\omega/2} \\ &\leq \left(\frac{\sum_i |A_i| |B_i| |H|^{2\varepsilon} + \sum_i |B_i| |C_i| |H|^{-\varepsilon} + \sum_i |C_i| |A_i| |H|^{-\varepsilon}}{3} \right)^{\omega/2} \\ &\leq (|H|^{1-\varepsilon})^{\omega/2}, \end{aligned}$$

and so the strongest bound that can be obtained from (1.1) 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 $\sum_i |C_i| |A_i| \leq |H|^{1-3\varepsilon}$. \square

Both the strong USP conjecture [4, Conjecture 3.4] and the “two families” conjecture [4, Conjecture 4.7] 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 $H = \mathbb{F}_3^n$, while the groups in the two families conjecture need not have bounded exponent. Thus although Theorem B disproves the strong USP conjecture, it addresses only very special cases of the two families conjecture.

3 STPP constructions and tricolored sum-free sets

Definition 3.1. A tricolored 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

$$s + t + u = 0 \text{ for all } (s, t, u) \in M$$

and

$$s + t + u \neq 0 \text{ for all } (s, t, u) \in (S \times T \times U) \setminus M.$$

The cardinality of a tricolored 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. 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 tricolored sum-free set. Similarly, for any nonzero $\alpha, \beta, \gamma \in \mathbb{F}_p$ with $\alpha + \beta + \gamma = 0$, we obtain a tricolored sum-free set $M = \{(\alpha s, \beta s, \gamma s) : s \in S\}$ whenever S avoids nontrivial solutions to $\alpha s + \beta t + \gamma u = 0$.

In this section, we show how to obtain a tricolored sum-free set from any STPP construction in an abelian group. This allows us to prove that Theorem A implies Theorem B; we then prove Theorem A in Section 4.

3.1 STPP constructions imply tricolored sum-free sets

We will first construct slightly weaker objects we call border tricolored sum-free sets, which are motivated by the notion of combinatorial degeneration in the theory of border rank (see Definition 15.29 in [2]). We will then use border tricolored sum-free sets to construct genuine tricolored sum-free sets.

Definition 3.2. A border tricolored 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 $S, T, U \subseteq H$ together with functions $\alpha : S \rightarrow \mathbb{Z}$, $\beta : T \rightarrow \mathbb{Z}$, and $\gamma : U \rightarrow \mathbb{Z}$ such that

$$s + t + u = 0 \quad \text{and} \quad \alpha(s) + \beta(t) + \gamma(u) = 0$$

for all $(s, t, u) \in M$, while

$$s + t + u \neq 0 \quad \text{or} \quad \alpha(s) + \beta(t) + \gamma(u) > 0$$

for all $(s, t, u) \in (S \times T \times U) \setminus M$. The cardinality of a border tricolored sum-free set is the cardinality of M , and its range is the maximum of $|\alpha(s)|$, $|\beta(t)|$, and $|\gamma(u)|$ over $s \in S$, $t \in T$, and $u \in U$.

One can reformulate the definition as follows: the sets $\{(s, \alpha(s)) : s \in S\}$, $\{(t, \beta(t)) : t \in T\}$, and $\{(u, \gamma(u)) : u \in U\}$ form a tricolored sum-free set in $H \times \mathbb{Z}$ (under the obvious 3-dimensional matching extending M), and they satisfy the positivity condition that $\alpha(s) + \beta(t) + \gamma(u) \geq 0$ whenever $s + t + u = 0$.

One of our main new contributions in this paper is the following construction:

Theorem 3.3. Let $A_i, B_i, C_i \subseteq H$ be an STPP construction in an abelian group H . Then there is a border tricolored 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. As in Definition 2.2 (but using additive notation), we will set $S_i = A_i - B_i = \{a - b : a \in A_i, b \in B_i\}$, and similarly $T_i = B_i - C_i$ and $U_i = C_i - A_i$.

We will first construct a matching M out of smaller matchings M_i on subsets of S_i , T_i , and U_i . This matching will not quite be a tricolored sum-free set in general, but we will define functions α , β , and γ that repair any problems with it, so that it becomes a border tricolored sum-free set.

To begin, let $n_i = |A_i|$, $m_i = |B_i|$, and $p_i = |C_i|$, and identify A_i, B_i, C_i with $[n_i], [m_i], [p_i]$, respectively, via bijections $\alpha_i, \beta_i, \gamma_i$. 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

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

The size of M_i is the number of times r_i occurs in the multiset above. The number of distinct elements of the multiset is $n_i + m_i + p_i - 2$; we can ignore the 2 and bound this by $|A_i| + |B_i| + |C_i|$. Since r_i was chosen to be the most frequent value,

$$|M_i| \geq \frac{|A_i| |B_i| |C_i|}{|A_i| + |B_i| + |C_i|}.$$

Each M_i is a 3-dimensional perfect matching: given the first coordinate $a - b$, the triple product property determines a and b from $a - b$, and then $\alpha_i(a) + \beta_i(b) + \gamma_i(c) = r_i$ determines c , and the same is true for the other two coordinates. We combine these matchings by setting $M = \bigcup_i M_i$. Note that the sets M_i are disjoint from each other (since the sets S_i are, for example), so $|M| = \sum_i |M_i|$. All that remains is to define the functions α, β, γ so as to obtain a border tricolored sum-free set.

Let S'_i, T'_i, U'_i be the projections of M_i onto the three factors of H^3 . In other words,

$$S'_i = \{a - b : a \in A_i, b \in B_i, \text{ and there exists } c \in C_i \text{ such that } \alpha_i(a) + \beta_i(b) + \gamma_i(c) = r_i\} \subseteq S_i,$$

and T'_i and U'_i can be expressed similarly. Let $S = \bigcup_i S'_i$, $T = \bigcup_i T'_i$, and $U = \bigcup_i U'_i$, so that M is a perfect matching between S , T , and U .

To complete the proof, we must analyze when $s + t + u = 0$ with $s \in S$, $t \in T$, and $u \in U$. First, note that 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 $i = j = k$. Thus, we cannot obtain a sum of zero from S'_i, T'_j , and U'_k unless $i = j = k$, so we can analyze each matching M_i individually, without worrying about how they might interact with each other. More specifically, if for each i we can find functions on S'_i, T'_i , and U'_i that make M_i into a border tricolored sum-free set, then this yields functions on S, T , and U that make M into a border tricolored sum-free set.

Now consider $(s, t, u) \in S'_i \times T'_i \times U'_i$, with $s = a - b' \in A_i - B_i$, $t = b - c' \in B_i - C_i$, and $u = c - a' \in C_i - A_i$. Note that s determines a and b' , t determines b and c' , and u determines c and a' since A_i, B_i, C_i satisfy the triple product property. Furthermore, the triple product property tells us that

$$s + t + u = 0 \quad \text{implies} \quad a = a', \quad b = b', \quad c = c'.$$

However, that is not enough to conclude that $(s, t, u) \in M_i$, because it is not necessarily the case that $\alpha_i(a) + \beta_i(b) + \gamma_i(c) = r_i$. To address this issue, we will define functions α, β , and γ on S'_i, T'_i , and U'_i , respectively, so that

$$\alpha(s) + \beta(t) + \gamma(u) = (\alpha_i(a) + \beta_i(b) + \gamma_i(c) - r_i)^2$$

whenever $s + t + u = 0$. Specifically, we can take

$$\begin{aligned}\alpha(s) &= \alpha_i(a)^2 + 2\alpha_i(a)\beta_i(b') - 2\alpha_i(a)r_i + r_i^2, \\ \beta(t) &= \beta_i(b)^2 + 2\beta_i(b)\gamma_i(c') - 2\beta_i(b)r_i, \quad \text{and} \\ \gamma(u) &= \gamma_i(c)^2 + 2\gamma_i(c)\alpha_i(a') - 2\gamma_i(c)r_i.\end{aligned}$$

(We simply expand the square and assign each term to one of $\alpha(s), \beta(t), \gamma(u)$ so that $\alpha(s)$ depends only on a and b' , $\beta(t)$ depends only on b and c' , and $\gamma(u)$ depends only on c and a' .)

By construction, $\alpha(s) + \beta(t) + \gamma(u) \geq 0$ whenever $s + t + u = 0$, and $\alpha(s) + \beta(t) + \gamma(u) = 0$ exactly when $(s, t, u) \in M_i$. Thus, we have constructed a border tricolored sum-free set, as desired. \square

Lemma 3.4. *Let H be an abelian group in which there is a border tricolored sum-free set of cardinality $|M|$ and range t . Then for each natural number N , there exists a tricolored sum-free set in H^N of cardinality at least $|M|^N / (2Nt + 1)^3$.*

In particular, as $N \rightarrow \infty$ there are tricolored sum-free sets in H^N of cardinality $|M|^{(1-o(1))N}$.

Proof. We will use the notation from Definition 3.2 for the border tricolored sum-free set in H : let M be the perfect matching on sets $S, T, U \subseteq H$, with functions $\alpha: S \rightarrow \mathbb{Z}$, $\beta: T \rightarrow \mathbb{Z}$, and $\gamma: U \rightarrow \mathbb{Z}$.

Define $M' \subseteq (S^N \times T^N \times U^N)$ in the natural way, so that $((s_1, \dots, s_N), (t_1, \dots, t_N), (u_1, \dots, u_N)) \in M'$ if and only if $(s_i, t_i, u_i) \in M$ for all i , and define $\alpha(s_1, \dots, s_N) = \alpha(s_1) + \dots + \alpha(s_N)$ and similarly for β and γ . This construction yields a border tricolored sum-free set of cardinality $|M|^N$ and range Nt in H^N .

To obtain a genuine tricolored sum-free set, we will shrink M' by a small amount. Because the functions α, β, γ for M' have range Nt (and thus each take on at most $2Nt + 1$ values), there exist integers $\alpha^*, \beta^*, \gamma^*$ such that for at least a $1/(2Nt + 1)^3$ fraction of the triples $(s', t', u') \in M'$, we have $\alpha(s') = \alpha^*$, $\beta(t') = \beta^*$, and $\gamma(u') = \gamma^*$. Furthermore, $\alpha^* + \beta^* + \gamma^* = 0$ because $\alpha(s') + \beta(t') + \gamma(u') = 0$ whenever $(s', t', u') \in M'$.

Let M'' be the subset of M' consisting of these triples with $\alpha(s') = \alpha^*$, $\beta(t') = \beta^*$, and $\gamma(u') = \gamma^*$, and let S'', T'', U'' be the sets on which M'' is a perfect matching. Then $|M''| \geq |M'| / (2Nt + 1)^3 = |M|^N / (2Nt + 1)^3$, and M'' is trivially a border tricolored sum-free set. Furthermore,

$$\alpha(s'') + \beta(t'') + \gamma(u'') = \alpha^* + \beta^* + \gamma^* = 0$$

whenever $s'' \in S'', t'' \in T'',$ and $u'' \in U''$, by construction. Because $\alpha(s'') + \beta(t'') + \gamma(u'')$ vanishes identically, the functions $\alpha, \beta,$ and γ serve no purpose in the definition of a border tricolored sum-free set. Thus, M'' reduces to an actual tricolored sum-free set, as desired. \square

To control the size of the tricolored sum-free sets resulting from Theorem 3.3 and Lemma 3.4, 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 $|A_i| = |B_i| = |C_i|$).

Lemma 3.5. *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

$$\begin{aligned}\widehat{A}_{u,v,w} &= \prod_{\ell} A_{u_{\ell}} \times \prod_{\ell} B_{v_{\ell}} \times \prod_{\ell} C_{w_{\ell}}, \\ \widehat{B}_{u,v,w} &= \prod_{\ell} B_{u_{\ell}} \times \prod_{\ell} C_{v_{\ell}} \times \prod_{\ell} A_{w_{\ell}}, \\ \widehat{C}_{u,v,w} &= \prod_{\ell} C_{u_{\ell}} \times \prod_{\ell} A_{v_{\ell}} \times \prod_{\ell} B_{w_{\ell}}.\end{aligned}$$

(The products here are cartesian products of sets.) It is not hard to verify that these sets satisfy the STPP in H^{3N} (see [4, 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 $\widehat{A}_{u,v,w}, \widehat{B}_{u,v,w}, \widehat{C}_{u,v,w}$ 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

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

We have

$$|\widehat{A}_{u,v,w}| |\widehat{B}_{u,v,w}| = \prod_{\ell} |A_{u_{\ell}}| |B_{v_{\ell}}| |C_{w_{\ell}}| |B_{u_{\ell}}| |C_{v_{\ell}}| |A_{w_{\ell}}| \tag{3.1}$$

and hence

$$\sum_{u,v,w} |\widehat{A}_{u,v,w}| |\widehat{B}_{u,v,w}| \geq |H|^{3N(1-o(1))},$$

as desired; the same also holds for $\sum_{u,v,w} |\widehat{B}_{u,v,w}| |\widehat{C}_{u,v,w}|$ and $\sum_{u,v,w} |\widehat{A}_{u,v,w}| |\widehat{C}_{u,v,w}|$.

To enforce uniformity, we restrict our attention to only certain choices of u, v , and w by observing that the cardinality

$$|\widehat{A}_{u,v,w}| = \prod_{\ell} |A_{u_{\ell}}| |B_{v_{\ell}}| |C_{w_{\ell}}|$$

depends only on the *distributions* of u, v, w (where the distribution of u is the vector specifying the number of times each element of $[n]$ occurs in u). The same is true for $|\widehat{B}_{u,v,w}|$ and $|\widehat{C}_{u,v,w}|$. 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 μ_1, μ_2, μ_3 of distributions for which

$$\sum_{u \sim \mu_1} \prod_{\ell} |A_{u_{\ell}}| |B_{u_{\ell}}| \cdot \sum_{v \sim \mu_2} \prod_{\ell} |B_{v_{\ell}}| |C_{v_{\ell}}| \cdot \sum_{w \sim \mu_3} \prod_{\ell} |C_{w_{\ell}}| |A_{w_{\ell}}| \geq \frac{1}{(N+1)^{3n}} |H|^{3N(1-o(1))}, \tag{3.2}$$

where $u \sim \mu_1$ means u has distribution μ_1 .

Restricting to only those sets $\widehat{A}_{u,v,w}$, $\widehat{B}_{u,v,w}$, and $\widehat{C}_{u,v,w}$ with $u \sim \mu_1$, $v \sim \mu_2$, and $w \sim \mu_3$ thus gives a uniform STPP construction. Combining (3.1) and (3.2) we obtain

$$\sum_{u \sim \mu_1, v \sim \mu_2, w \sim \mu_3} |\widehat{A}_{u,v,w}| |\widehat{B}_{u,v,w}| \geq \frac{1}{(N+1)^{3n}} |H|^{3N(1-o(1))},$$

which is again $|H|^{3N(1-o(1))}$ as long as N is chosen sufficiently large relative to n and $|H|$. The same holds for the other two conditions in the packing bound.

Choosing N and μ_1, μ_2, μ_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 Theorem A implies Theorem B

We conclude this section by proving that Theorem A implies Theorem B; we will then prove Theorem A in Section 4.

Fix $\ell \in \mathbb{N}$, and suppose that for each $\delta > 0$ there is an STPP construction in a group of exponent at most ℓ that proves $\omega \leq 2 + \delta$. Choosing a sequence with δ tending to zero, we obtain a family of STPP constructions that meets the packing bound by Lemma 2.4. Furthermore Lemma 3.5 lets us inflate these constructions to make them uniform, while still meeting the packing bound, in powers of the original groups; in particular, the exponent of all our groups is still at most ℓ .

Consider one of these uniform STPP constructions in a group H of exponent at most ℓ , thus generated by elements of order at most ℓ . By Theorem 3.3 there exists a border tricolored sum-free set in H of cardinality $|M| = \sum_i \frac{|A_i||B_i||C_i|}{|A_i|+|B_i|+|C_i|}$. 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

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

Finally, Lemma 3.4 converts the border tricolored sum-free set to a genuine tricolored sum-free set, at the cost of raising H to a high power (which of course does not change the exponent of this group). This contradicts Theorem A, which states that the cardinality of any tricolored sum-free set in H^N is at most $3|H|^{N(1-\frac{\epsilon}{\ell})}$, and thus completes the proof of Theorem B.

4 Tricolored sum-free sets in abelian groups of bounded exponent via rank and instability of tensors

The remainder of the paper is devoted to the proof of Theorems A and A'. Our approach builds on the symmetric formulation presented by Tao [22], although an earlier version of this paper contained a more direct application of the original methods [9, 11] to the \mathbb{F}_p^n case.

We begin here by outlining the main ideas of the proof, giving a road map for the remaining sections. In order to formulate the symmetric version, we develop the notion of *slice rank* (in Section 4.1), which is a weakening of tensor rank. For tricolored sum-free sets in \mathbb{F}_p^n , the upper bound is then a consequence of the following three facts about slice rank:

1. Just as the ordinary matrix rank of an $m \times m$ diagonal matrix is equal to m if all the diagonal entries are nonzero, the same holds for the slice rank of an $m \times m \times m$ diagonal tensor (over any field; see Lemma 4.7 or [22, Lemma 1]).
2. A tricolored sum-free set of cardinality m in a group G implies that the multiplication tensor of the group algebra $\mathbb{F}G$ restricts to an $m \times m \times m$ diagonal tensor with nonzero diagonal entries. It follows that the slice rank of the multiplication tensor of $\mathbb{F}G$ is at least the size of any tricolored sum-free set in G (see Proposition 4.8).
3. Over a field of characteristic p , the slice rank of the \mathbb{F}_p^n -multiplication tensor is at most the number of vectors in $[p]^n$ with coordinate sum at most $pn/3$, which is at most $(p - \varepsilon_p)^n$ for some $\varepsilon_p > 0$. By a remarkable observation [9, 11, 22], this upper bound on the slice rank follows almost immediately from the fact that the (x, y, z) entry of the tensor in question equals $\delta_0(x + y + z)$, and the delta function $\delta_0(x + y + z)$ (indeed every function of $x + y + z$) is expressible as an n -variate polynomial of degree $(p - 1)n$; see Observation 4.11.

These three statements give an upper bound of $(p - \varepsilon_p)^n$ on the cardinality of a tricolored sum-free set in \mathbb{F}_p^n . Expressed a different way, the upper bound for $H = \mathbb{F}_p^n$ is $|H|^{1 - \alpha_p}$ for some constant $\alpha_p > 0$. In Section 4.4, we prove an upper bound of the same form for tricolored sum-free sets in any group of the form $G = (\mathbb{Z}/p^k\mathbb{Z})^n$ with p prime, using a similar argument but using binomial coefficients instead of polynomials to describe the delta function.

We then extend this bound to any abelian group H of bounded exponent by arguing that such a group must decompose as $H \cong G \times K$ where $G \cong (\mathbb{Z}/p^k\mathbb{Z})^n$ and $|G| \geq |H|^c$ for a constant $c > 0$. Such a decomposition expresses the H -multiplication tensor D_H as a tensor product $D_G \otimes D_K$. We establish a simple but powerful property of slice rank: the slice rank of $T \otimes T'$ is at most the slice rank of T times the side length of T' (Proposition 4.2). This allows us to reduce to the $(\mathbb{Z}/p^k\mathbb{Z})^n$ case, because the slice rank of D_H is at most $|G|^{1 - \alpha} |K| = |H|^{1 - \alpha'}$ for some constant $\alpha' > 0$. As before, this bound on slice rank also bounds the cardinality of tricolored sum-free sets in G .

In the presentation below, we draw connections to *(in)stability* of tensors, a notion coming from geometric invariant theory (GIT). This broader context seems powerful, and potentially useful beyond the results in this paper. However, the reader who is interested only in the proofs of Theorems A and B can skip all of Section 4.2 except Lemma 4.7 and Proposition 4.8 and skip Theorem 4.10 since we only need the sharper bound on slice rank stated in Proposition 4.13, coming from triangle rank.

4.1 Tensor rank and its variants

Throughout this section, X, Y , and Z will denote finite sets. A function $F : X \times Y \rightarrow \mathbb{F}$ with values in a field \mathbb{F} has an unambiguous *rank*; $\text{rank}(F)$ is the smallest k for which we can write $F(x, y) = \sum_{i=1}^k f_i(x)g_i(y)$, and this coincides with the rank of the $|X| \times |Y|$ matrix described by F .

A common way to define the rank of a function $F : X \times Y \times Z \rightarrow \mathbb{F}$ is *tensor rank*: $\text{tensor-rank}(F)$ is the smallest k for which we can write

$$F(x, y, z) = \sum_{i=1}^k f_i(x)g_i(y)h_i(z).$$

In this paper, we make use of another notion of rank which we call *slice rank*: $\text{slice-rank}(F)$ is the smallest k for which we can write

$$F(x, y, z) = \sum_{i=1}^a f_i(x, y)g_i(z) + \sum_{i=a+1}^b f_i(x, z)g_i(y) + \sum_{i=b+1}^k f_i(y, z)g_i(x). \quad (4.1)$$

As far as we know, this notion of rank was first used by Tao in [22]; here we take this study a bit further by establishing some basic properties of slice rank (Section 4.1) and connections to GIT (Section 4.2).

Since any sum $\sum_i f_i(x)g_i(y)h_i(z)$ automatically fits the form (4.1), we always have

$$\text{slice-rank}(F) \leq \text{tensor-rank}(F) \leq |\text{support}(F)|.$$

Similarly, directly from the definition (4.1) we immediately conclude that

$$\text{slice-rank}(F) \leq \min(|X|, |Y|, |Z|) \quad (4.2)$$

and

$$\text{tensor-rank}(F) \leq \text{slice-rank}(F) \cdot \max(|X|, |Y|, |Z|). \quad (4.3)$$

Remark 4.1. Slice rank and tensor rank can be quite different. For example, if $|X| = N$ the function $F : X \times X \times X \rightarrow \mathbb{F}$ given by $F(x, y, z) = \delta_{x,y}$ has $\text{slice-rank}(F) = 1$ while $\text{tensor-rank}(F) = N$. (Note that this is the largest possible separation by (4.3).)

As another example of the difference between slice and tensor rank, every function $F : X \times X \times X \rightarrow \mathbb{F}$ has slice rank at most N (and this bound is sharp; see Lemma 4.7 or [22, Lemma 1]). However, tensor rank can be much larger: the tensor rank of a generic² F is $\lceil \frac{N^3}{3N-2} \rceil \approx N^2/3$ if $N \neq 3$ and \mathbb{F} is algebraically closed [16].

Given functions $F : X' \times Y' \times Z' \rightarrow \mathbb{F}$ and $G : X'' \times Y'' \times Z'' \rightarrow \mathbb{F}$, set $X = X' \times X''$, $Y = Y' \times Y''$, and $Z = Z' \times Z''$, and let $F \otimes G$ denote the function $F \otimes G : X \times Y \times Z \rightarrow \mathbb{F}$ given by

$$((x', x''), (y', y''), (z', z'')) \mapsto F(x', y', z')G(x'', y'', z'').$$

The inequality $\text{tensor-rank}(F \otimes G) \leq \text{tensor-rank}(F) \cdot \text{tensor-rank}(G)$ is well-known; it has the following two variants, which bound the slice rank of a tensor product:

Proposition 4.2. *For any F, G as above, $\text{slice-rank}(F \otimes G) \leq \text{slice-rank}(F) \cdot \text{tensor-rank}(G)$ and $\text{slice-rank}(F \otimes G) \leq \text{slice-rank}(F) \cdot \max(|X''|, |Y''|, |Z''|)$.*

Proof. Set $k = \text{slice-rank}(F)$ and choose functions f'_i and g'_i for $1 \leq i \leq k$ as in (4.1). Similarly, set $\ell = \text{tensor-rank}(G)$ and write $G(x'', y'', z'') = \sum_{j=1}^{\ell} \alpha_j(x'')\beta_j(y'')\gamma_j(z'')$. If we then define

$$\begin{aligned} f_{ij}(x, y) &:= f'_i(x', y')\alpha_j(x'')\beta_j(y''), & g_{ij}(z) &:= g'_i(z')\gamma_j(z'') && \text{for } 1 \leq i \leq a, 1 \leq j \leq \ell, \\ f_{ij}(x, z) &:= f'_i(x', z')\alpha_j(x'')\gamma_j(z''), & g_{ij}(y) &:= g'_i(y')\beta_j(y'') && \text{for } a < i \leq b, 1 \leq j \leq \ell, \text{ and} \\ f_{ij}(y, z) &:= f'_i(y', z')\beta_j(y'')\gamma_j(z''), & g_{ij}(x) &:= g'_i(x')\alpha_j(x'') && \text{for } b < i \leq k, 1 \leq j \leq \ell, \end{aligned}$$

²That is, the set of functions F with this tensor rank is non-empty and Zariski-open.

then

$$(F \otimes G)(x, y, z) = \sum_{\substack{1 \leq i \leq a \\ 1 \leq j \leq \ell}} f_{ij}(x, y) g_{ij}(z) + \sum_{\substack{a < i \leq b \\ 1 \leq j \leq \ell}} f_{ij}(x, z) g_{ij}(y) + \sum_{\substack{b < i \leq k \\ 1 \leq j \leq \ell}} f_{ij}(y, z) g_{ij}(x).$$

This demonstrates that $\text{slice-rank}(F \otimes G) \leq k \cdot \ell$, which verifies the first claim. For the second claim, we instead define

$$\begin{aligned} f_{i\zeta}(x, y) &:= f'_i(x', y') G(x'', y'', \zeta), & g_{i\zeta}(z) &:= g_i(z') \delta_\zeta(z'') && \text{for } 1 \leq i \leq a, \zeta \in Z'', \\ f_{i\psi}(x, z) &:= f'_i(x', z') G(x'', \psi, z''), & g_{i\psi}(y) &:= g_i(y') \delta_\psi(y'') && \text{for } a < i \leq b, \psi \in Y'', \text{ and} \\ f_{i\xi}(y, z) &:= f'_i(y', z') G(\xi, y'', z''), & g_{i\xi}(x) &:= g_i(x') \delta_\xi(x'') && \text{for } b < i \leq k, \xi \in X'', \end{aligned}$$

so that

$$(F \otimes G)(x, y, z) = \sum_{\substack{1 \leq i \leq a \\ \zeta \in Z''}} f_{i\zeta}(x, y) g_{i\zeta}(z) + \sum_{\substack{a < i \leq b \\ \psi \in Y''}} f_{i\psi}(x, z) g_{i\psi}(y) + \sum_{\substack{b < i \leq k \\ \xi \in X''}} f_{i\xi}(y, z) g_{i\xi}(x).$$

This shows that $\text{slice-rank}(F \otimes G) \leq k \cdot \max(|X''|, |Y''|, |Z''|)$, which verifies the second claim. □

4.2 Unstable tensors and slice rank

In this section we relate slice rank to the notion of an unstable tensor from geometric invariant theory. We show that functions with low slice rank are unstable and prove that a quantitative bound on instability yields a bound on slice rank of tensor powers.

Definition 4.3. *A function $F: X \times Y \times Z \rightarrow \mathbb{F}$ is unstable if there exist*

1. *a basis $\{f_a\}$ for the functions $X \rightarrow \mathbb{F}$, and similarly bases $\{g_b: Y \rightarrow \mathbb{F}\}$ and $\{h_c: Z \rightarrow \mathbb{F}\}$,*
2. *weights $u_a, v_b, w_c \in \mathbb{R}$ with arithmetic means $u_{\text{avg}}, v_{\text{avg}}, w_{\text{avg}}$, and*
3. *coefficients $r_{a,b,c} \in \mathbb{F}$ such that*

$$F(x, y, z) = \sum_{\substack{u_a + v_b + w_c < \\ u_{\text{avg}} + v_{\text{avg}} + w_{\text{avg}}}} r_{a,b,c} f_a(x) g_b(y) h_c(z).$$

This terminology comes from geometric invariant theory (when \mathbb{F} is algebraically closed). Consider the action of the group $G = \text{SL}_{|X|} \times \text{SL}_{|Y|} \times \text{SL}_{|Z|}$ on the vector space of functions $F: X \times Y \times Z \rightarrow \mathbb{F}$. A function F is said to be unstable in the sense of GIT if the zero function is contained in the Zariski closure of the G -orbit of F , or equivalently if every G -invariant homogeneous polynomial of positive degree vanishes on F . The Hilbert–Mumford criterion [17, §1] is a concrete condition for a function to be unstable: it says that a function F is unstable in the sense of GIT if and only if there exist functions and weights making F unstable according to Definition 4.3.

However, geometric invariant theory only deals with algebraically closed fields \mathbb{F} , which is why for general \mathbb{F} we take Definition 4.3 as the *definition* of unstable. To make our bounds explicit we will also need to introduce a *quantitative* version of this condition.

Definition 4.4. *The instability of a function $F : X \times Y \times Z \rightarrow \mathbb{F}$ is the supremum of all $\varepsilon \geq 0$ such that there exist bases f_a, g_b, h_c , nontrivial weights $u_a, v_b, w_c \in \mathbb{R}$, and coefficients $r_{a,b,c} \in \mathbb{F}$ such that*

$$F(x, y, z) = \sum_{u_a + v_b + w_c \leq R} r_{a,b,c} f_a(x) g_b(y) h_c(z) \tag{4.4}$$

where

$$R = (u_{\text{avg}} + v_{\text{avg}} + w_{\text{avg}}) - \varepsilon(u_{\text{max}} - u_{\text{min}} + v_{\text{max}} - v_{\text{min}} + w_{\text{max}} - w_{\text{min}}). \tag{4.5}$$

By “nontrivial weights” we mean that the weights u_a , v_b , and w_c should not all be constant (since in that case our definition of R becomes degenerate). Note that a function F is unstable if and only if $\text{instability}(F) > 0$. By convention, if for some F there is no nonnegative ε satisfying the hypotheses of the definition, we define $\text{instability}(F) = -\infty$. For readers familiar with the terminology of GIT, we remark that (assuming \mathbb{F} is algebraically closed) the function F is *semi-stable* if and only if $\text{instability}(F) \in \{-\infty, 0\}$, and F is *stable* if and only if $\text{instability}(F) = -\infty$. For consistency with this terminology, we are careful to use the term “not unstable” where appropriate (which is not the same, in GIT, as “stable”).

Remark 4.5 (Notes on the definition of instability).

1. Translating all the weights u_a (or all the v_b , or all the w_c) by a constant translates the quantity R of (4.5) by the same amount, so the condition $u_a + v_b + w_c \leq R$ is invariant under translation. Therefore if we like we may assume that $u_{\text{avg}} = v_{\text{avg}} = w_{\text{avg}} = 0$, or that $u_{\text{min}} = v_{\text{min}} = w_{\text{min}} = 0$, without loss of generality. Similarly, scaling all of the weights u_a , v_b , w_c by the same constant does not change the definition of instability nor the value of $\text{instability}(F)$.

2. It does not matter whether we require the weights to lie in \mathbb{R} , \mathbb{Q} , or \mathbb{Z} . Indeed, the supremum defining instability could be taken over rational $\varepsilon \geq 0$ without affecting the definition. For any given rational ε , the inequalities relating the u_a , v_b , and w_c are a system of homogeneous linear inequalities with rational coefficients, so they have rational solutions if and only if they have real solutions. We can then transform rational weights to integer weights by scaling. (In particular, this justifies our earlier claim that the Hilbert–Mumford criterion is equivalent to Definition 4.3 when over an algebraically closed field; the usual statement of the Hilbert–Mumford criterion would require integer weights with $u_{\text{avg}} = v_{\text{avg}} = w_{\text{avg}} = 0$.)

3. The definition of instability would be the same if the f_a , g_b , and h_c were arbitrary functions not required to form bases, as long as $|A| \leq |X|$, $|B| \leq |Y|$, and $|C| \leq |Z|$, where A, B, C denote index sets for the f_a, g_b, h_c , respectively. Indeed, if one function f_a is a linear combination of previous functions $f_{a'}$ with $u_{a'} \leq u_a$, then the terms $f_a \otimes g_b \otimes h_c$ appearing in (4.4) can be replaced with a linear combination of terms $f_{a'} \otimes g_b \otimes h_c$, still satisfying $u_{a'} + v_b + w_c \leq u_a + v_b + w_c \leq R$. Repeating this, we may assume that the set of functions $\{f_a\}_{a \in A'}$ (with $A' \subseteq A$) appearing is linearly independent. Then extend this set to a basis arbitrarily, giving $|X| - |A'|$ of these new functions the weight u_{avg} and giving $|A| - |A'|$ of them the weights $\{u_a\}_{a \in A \setminus A'}$. The other tensor factors are handled similarly.

Recall from (4.2) that any function $F : X \times Y \times Z \rightarrow \mathbb{F}$ has $\text{slice-rank}(F) \leq \min(|X|, |Y|, |Z|)$. It turns out that there is a close relationship between F being unstable and this inequality being *strict*. More

precisely, the latter implies the former (Theorem 4.6), and the former implies that the latter holds for sufficiently large tensor powers when $|X| = |Y| = |Z|$ (Theorem 4.10).

Theorem 4.6. *If $\text{slice-rank}(F) < \min(|X|, |Y|, |Z|)$, then F is unstable.*

Proof. Given an arbitrary F , choose a decomposition

$$F(x, y, z) = \sum_{i=1}^p \alpha_i(y, z) f_i(x) + \sum_{j=1}^q \beta_j(x, z) g_j(y) + \sum_{k=1}^r \gamma_k(x, y) h_k(z) \quad (4.6)$$

with $p + q + r = \text{slice-rank}(F)$. Note that this implies that the p functions f_1, \dots, f_p are linearly independent (otherwise we could find a smaller decomposition of F), so extend them to a basis $f_1, \dots, f_{|X|}$ for the functions $X \rightarrow \mathbb{F}$. Do the same for the other factors, and define weights by

$$u_i = \begin{cases} -1 & \text{for } 1 \leq i \leq p, \\ 0 & \text{for } p < i \leq |X|, \end{cases} \quad v_j = \begin{cases} -1 & \text{for } 1 \leq j \leq q, \\ 0 & \text{for } q < j \leq |Y|, \end{cases} \quad w_k = \begin{cases} -1 & \text{for } 1 \leq k \leq r, \\ 0 & \text{for } r < k \leq |Z|. \end{cases}$$

Expanding $\alpha_i(y, z)$ as a linear combination of $g_j(y)h_k(z)$ and so on, the decomposition (4.6) says that F is a linear combination of functions $f_i \cdot g_j \cdot h_k$ where at least *one* of $1 \leq i \leq p$, $1 \leq j \leq q$, or $1 \leq k \leq r$ holds. From the definition of our weight functions, these are precisely the cases when $u_i + v_j + w_k \leq -1$.

On the other hand $u_{\text{avg}} = -\frac{p}{|X|}$, $v_{\text{avg}} = -\frac{q}{|Y|}$, and $w_{\text{avg}} = -\frac{r}{|Z|}$, from which it follows that

$$u_{\text{avg}} + v_{\text{avg}} + w_{\text{avg}} = -\frac{p}{|X|} - \frac{q}{|Y|} - \frac{r}{|Z|} \geq -\frac{p+q+r}{\min(|X|, |Y|, |Z|)} = -\frac{\text{slice-rank}(F)}{\min(|X|, |Y|, |Z|)}.$$

Our hypothesis that $\text{slice-rank}(F) < \min(|X|, |Y|, |Z|)$ thus guarantees that these weights satisfy $u_{\text{avg}} + v_{\text{avg}} + w_{\text{avg}} > -1$. In this case, F is a linear combination of functions $f_i \cdot g_j \cdot h_k$ where $u_i + v_j + w_k \leq -1 < u_{\text{avg}} + v_{\text{avg}} + w_{\text{avg}}$, so F is unstable. \square

Theorem 4.6 implies that any tensor F that is not unstable has

$$\text{slice-rank}(F) = \min(|X|, |Y|, |Z|).$$

This lets us compute the slice rank of any diagonal. Say that a function $F : X \times Y \times Z \rightarrow \mathbb{F}$ is a *diagonal* if its support $\{(x, y, z) : F(x, y, z) \neq 0\}$ is a perfect matching on X , Y , and Z . Note that this implies $|X| = |Y| = |Z| = |\text{support}(F)|$, and that we require all the diagonal entries in F (i.e., those corresponding to the perfect matching) to be nonzero.

The following lemma was introduced to great effect by Tao [22, Lemma 1]. We first reproduce Tao's elementary proof for completeness, and then include a second proof inspired by the GIT perspective.

Lemma 4.7. *If $F : X \times Y \times Z \rightarrow \mathbb{F}$ is a diagonal, then*

$$\text{slice-rank}(F) = \text{tensor-rank}(F) = |X|.$$

Tao's proof from [22]. Suppose that $\text{slice-rank}(F) < |X|$. Then there exist $k < |X|$ and functions f_i, g_i such that

$$F(x, y, z) = \sum_{i=1}^j f_i(x)g_i(y, z) + \sum_{i=j+1}^{\ell} f_i(y)g_i(z, x) + \sum_{i=\ell+1}^k f_i(z)g_i(x, y). \tag{4.7}$$

Without loss of generality suppose that $j > 0$, and let

$$V = \left\{ h: X \rightarrow \mathbb{F} : \sum_{x \in X} f_i(x)h(x) = 0 \text{ for all } 1 \leq i \leq j \right\}.$$

This vector space has dimension at least $|X| - j$. Let $u \in V$ have maximal support, and set $\Sigma = \{x \in X : u(x) \neq 0\}$. Then $|\Sigma| \geq \dim V \geq |X| - j$, since otherwise there exists nonzero $r \in V$ vanishing on Σ , and the function $u + r$ would have a larger support than u . Multiply both sides of (4.7) by $u(x)$ and sum over x to reduce from a tensor to a matrix. As $u \in V$ is orthogonal to f_i for $i = 1, \dots, j$, the right side of (4.7) becomes

$$\sum_{i=j+1}^{\ell} f_i(y) \left(\sum_{x \in X} u(x)g_i(z, x) \right) + \sum_{i=\ell+1}^k f_i(z) \left(\sum_{x \in X} u(x)g_i(x, y) \right),$$

which is a function of rank at most $k - j < |X| - j$. Since the support of $F(x, y, z)$ is precisely given by a perfect matching, $\sum_{x \in X} u(x)F(x, y, z)$ will be a function with rank equal to $|\text{support}(u)| \geq |X| - j$. Thus we have a contradiction, and it follows that $\text{slice-rank}(F) = |X|$. \square

We remark that Tao's proof is inductive, and extends to higher-order tensors as well [22]. The next proof of Lemma 4.7 uses the geometric invariant theory perspective on slice rank.

Proof of Lemma 4.7. By Theorem 4.6, it suffices to prove that a diagonal is not unstable. It will be convenient to use dual bases to compute coefficients. Given bases f_a, g_b, h_c as in Definition 4.3, consider the dual bases f'_a, g'_b, h'_c ; in other words,

$$\sum_{x \in X} f_a(x)f'_a(x) = \begin{cases} 1 & \text{if } a = a', \text{ and} \\ 0 & \text{otherwise,} \end{cases}$$

and the same holds for g_b, g'_b (summing over Y) and h_c, h'_c (summing over Z). Our proof will depend on the following two observations.

First, the condition that

$$F(x, y, z) = \sum_{\substack{u_a + v_b + w_c < \\ u_{\text{avg}} + v_{\text{avg}} + w_{\text{avg}}}} r_{a,b,c} f_a(x) g_b(y) h_c(z)$$

is equivalent to the condition that

$$\sum_{x,y,z} F(x, y, z) f'_a(x) g'_b(y) h'_c(z) \neq 0 \implies u_a + v_b + w_c < u_{\text{avg}} + v_{\text{avg}} + w_{\text{avg}}, \tag{4.8}$$

since that sum is precisely the coefficient $r_{a,b,c}$.

Second, the condition (4.8) is invariant under the change of basis that replaces f'_{a_2} by $\alpha f'_{a_1} + f'_{a_2}$ as long as $u_{a_1} \geq u_{a_2}$. For if

$$\sum_{x,y,z} F(x,y,z)(\alpha f'_{a_1}(x) + f'_{a_2}(x))g'_b(y)h'_c(z) \neq 0,$$

then either $\sum_{x,y,z} F(x,y,z)f'_{a_1}(x)g'_b(y)h'_c(z) \neq 0$ or $\sum_{x,y,z} F(x,y,z)f'_{a_2}(x)g'_b(y)h'_c(z) \neq 0$, so either $u_{a_1} + v_b + w_c$ or $u_{a_2} + v_b + w_c$ is less than $u_{\text{avg}} + v_{\text{avg}} + w_{\text{avg}}$. Thus in either case $u_{a_2} + v_b + w_c$ is less than $u_{\text{avg}} + v_{\text{avg}} + w_{\text{avg}}$ as it is at most $u_{a_1} + v_b + w_c$. The same is true for the g_b and h_c .

We can now proceed to the proof. For the sake of contradiction, assume that F is a diagonal and unstable. Without loss of generality, assume that $X = Y = Z = [n]$ and that the support of F is $\{(i, i, i) : i \in [n]\}$.

View the functions $f'_a : [n] \rightarrow \mathbb{F}$ as n -dimensional vectors. Using changes of variables of the aforementioned form, we may perform Gaussian elimination until no two f'_a have their first nonzero entries in the same position. In that case, each element of $[n]$ is the position of the first nonzero entry of some f'_a , so we may index the f'_a by these positions. Do the same for the g'_b , but for the h'_c , perform Gaussian elimination so that the *last* nonzero entries have distinct positions, and index the h'_c by these positions.

Because F is diagonal,

$$\sum_{x,y,z} F(x,y,z)f'_a(x)g'_b(y)h'_c(z) = \sum_x F(x,x,x)f'_a(x)g'_b(x)h'_c(x)$$

and $F(x,x,x) \neq 0$. Now for each index $i \in [n]$, since i is the position of the first nonzero entry of f'_i and g'_i and the last nonzero entry of h'_i ,

$$f'_i(x)g'_i(x)h'_i(x) = \begin{cases} f'_i(i)g'_i(i)h'_i(i) \neq 0 & \text{if } x = i, \text{ and} \\ 0 & \text{otherwise.} \end{cases}$$

This means

$$\sum_x F(x,x,x)f'_i(x)g'_i(x)h'_i(x) = F(i,i,i)f'_i(i)g'_i(i)h'_i(i) \neq 0,$$

which implies $u_i + v_i + w_i < u_{\text{avg}} + v_{\text{avg}} + w_{\text{avg}}$. Summing over i , we have

$$\sum_{i=1}^n u_i + \sum_{i=1}^n v_i + \sum_{i=1}^n w_i < nu_{\text{avg}} + nv_{\text{avg}} + nw_{\text{avg}} = \sum_{i=1}^n u_i + \sum_{i=1}^n v_i + \sum_{i=1}^n w_i,$$

which is a contradiction, so F is not unstable. □

Lemma 4.7 has the following important consequence. If H is any abelian group and \mathbb{F} is any field, let $D_H : H \times H \times H \rightarrow \mathbb{F}$ be the tensor encoding the group structure (corresponding to multiplication in the group algebra $\mathbb{F}H$), defined by

$$D_H(x,y,z) = \begin{cases} 1 & \text{if } x + y + z = 0, \text{ and} \\ 0 & \text{if } x + y + z \neq 0. \end{cases}$$

Proposition 4.8. *If M is a tricolored sum-free set in an abelian group H , then*

$$|M| \leq \text{slice-rank}(D_H).$$

Proof. When we restrict a function $F: X \times Y \times Z \rightarrow \mathbb{F}$ to subsets X_0, Y_0, Z_0 , we can also restrict any decomposition as in (4.1), showing that

$$\text{slice-rank}(F|_{X_0 \times Y_0 \times Z_0}) \leq \text{slice-rank}(F).$$

A set $M \subseteq S \times T \times U$ on subsets $S, T, U \subseteq H$ is a tricolored sum-free set if and only if the restriction $D_H|_{S \times T \times U}$ is a diagonal; if it is, Lemma 4.7 implies that

$$|M| = \text{slice-rank}(D_H|_{S \times T \times U}) \leq \text{slice-rank}(D_H). \quad \square$$

This means we can bound the size of tricolored sum-free sets in an abelian group H by bounding the slice rank of D_H from above.

Remark 4.9. With the notion of slice rank in hand, it is natural to wonder whether upper bounds on slice rank could be applied directly to matrix multiplication to get upper bounds on its tensor rank. Indeed, since $\text{tensor-rank}(\langle n, n, n \rangle) \leq n^2 \cdot \text{slice-rank}(\langle n, n, n \rangle)$ by (4.3), upper bounds of $O(n^\delta)$ on the slice rank of $n \times n$ matrix multiplication would imply $\omega \leq 2 + \delta$. However, no nontrivial upper bounds on ω can be achieved this way: it is known that the matrix multiplication tensor is not unstable [3, Theorem 5.2], so Theorem 4.6 implies that $\text{slice-rank}(\langle n, n, n \rangle) = n^2$. (However, the topic of the slice rank of matrix multiplication itself is orthogonal to the main results of this paper.)

4.3 Upper bounds on slice rank

The following result gives us upper bounds on slice rank.

Theorem 4.10. *If F is unstable, then for any $n \geq 1$,*

$$\text{slice-rank}(F^{\otimes n}) \leq (|X|^n + |Y|^n + |Z|^n)e^{-2n \text{instability}(F)^2}.$$

We remark that in the most common case when $|X| = |Y| = |Z|$, this bound is always nontrivial for sufficiently large n . However if the sets have unequal sizes, this only improves on the trivial bound $\text{slice-rank}(F^{\otimes n}) \leq \min(|X|^n, |Y|^n, |Z|^n)$ if $\text{instability}(F)$ is sufficiently large.

Proof. It suffices to prove for all $\varepsilon < \text{instability}(F)$ that

$$\text{slice-rank}(F^{\otimes n}) \leq (|X|^n + |Y|^n + |Z|^n)e^{-2n\varepsilon^2}.$$

Given such an ε , we can choose functions f_a, g_b, h_c , weights u_a, v_b, w_c , and coefficients $r_{a,b,c}$ as in Definition 4.4 indexed by $a \in A$, $b \in B$, and $c \in C$ such that

$$F(x, y, z) = \sum_{u_a + v_b + w_c \leq R} r_{a,b,c} f_a(x) g_b(y) h_c(z)$$

with R as in (4.5). Assume without loss of generality that $u_{\min} = v_{\min} = w_{\min} = 0$, and let us define bounds $u_{\text{bd}} = u_{\text{avg}} - \varepsilon u_{\text{max}}$, and similarly for v_{bd} and w_{bd} , so that

$$R = u_{\text{avg}} + v_{\text{avg}} + w_{\text{avg}} - \varepsilon(u_{\text{max}} + v_{\text{max}} + w_{\text{max}}) = u_{\text{bd}} + v_{\text{bd}} + w_{\text{bd}}.$$

For $\mathbf{a} \in A^n$ and $\mathbf{x} \in X^n$, define $f_{\mathbf{a}}(\mathbf{x}) = \prod_{i=1}^n f_{a_i}(x_i)$ and $u_{\mathbf{a}} = u_{a_1} + \dots + u_{a_n} \in \mathbb{R}$; similarly define $g_{\mathbf{b}}(\mathbf{y})$, $v_{\mathbf{b}}$, $h_{\mathbf{c}}(\mathbf{z})$, $w_{\mathbf{c}}$, and $r_{\mathbf{a},\mathbf{b},\mathbf{c}} = \prod_{i=1}^n r_{a_i,b_i,c_i}$. Then

$$F^{\otimes n}(\mathbf{x}, \mathbf{y}, \mathbf{z}) = \sum_{(\mathbf{a},\mathbf{b},\mathbf{c})} \prod_{i=1}^n r_{a_i,b_i,c_i} f_{a_i}(x_i) g_{b_i}(y_i) h_{c_i}(z_i) = \sum_{(\mathbf{a},\mathbf{b},\mathbf{c})} r_{\mathbf{a},\mathbf{b},\mathbf{c}} f_{\mathbf{a}}(\mathbf{x}) g_{\mathbf{b}}(\mathbf{y}) h_{\mathbf{c}}(\mathbf{z}),$$

where the sum is over triples $(\mathbf{a}, \mathbf{b}, \mathbf{c})$ of tuples $\mathbf{a} \in A^n, \mathbf{b} \in B^n, \mathbf{c} \in C^n$ satisfying the condition $u_{a_i} + v_{b_i} + w_{c_i} \leq R = u_{\text{bd}} + v_{\text{bd}} + w_{\text{bd}}$ for each $i = 1, \dots, n$. This condition implies $u_{\mathbf{a}} + v_{\mathbf{b}} + w_{\mathbf{c}} \leq nR = n(u_{\text{bd}} + v_{\text{bd}} + w_{\text{bd}})$, so each such triple must satisfy at least one of the inequalities $u_{\mathbf{a}} \leq nu_{\text{bd}}, v_{\mathbf{b}} \leq nv_{\text{bd}}$, or $w_{\mathbf{c}} \leq nw_{\text{bd}}$. Therefore we can collect terms above to write

$$F^{\otimes n}(\mathbf{x}, \mathbf{y}, \mathbf{z}) = \sum_{u_{\mathbf{a}} \leq nu_{\text{bd}}} f_{\mathbf{a}}(\mathbf{x}) E_{\mathbf{a}}(\mathbf{y}, \mathbf{z}) + \sum_{v_{\mathbf{b}} \leq nv_{\text{bd}}} g_{\mathbf{b}}(\mathbf{y}) E_{\mathbf{b}}(\mathbf{x}, \mathbf{z}) + \sum_{w_{\mathbf{c}} \leq nw_{\text{bd}}} h_{\mathbf{c}}(\mathbf{z}) E_{\mathbf{c}}(\mathbf{x}, \mathbf{y}).$$

This decomposition exhibits a bound on the slice rank of $F^{\otimes n}$, so all we need to do is estimate how many terms appear in these sums. The number of tuples $\mathbf{a} \in A^n$ satisfying $u_{\mathbf{a}} \leq nu_{\text{bd}} = n(u_{\text{avg}} - \varepsilon u_{\text{max}})$ is a classical large deviation estimate: $u_{\mathbf{a}}$ is the sum of i.i.d. variables u_{a_i} taking values in $[0, u_{\text{max}}]$, and we are asking how often this deviates on one side from the mean nu_{avg} by at least $\varepsilon nu_{\text{max}}$. Even without knowing anything about the distribution of u_{a_i} , Hoeffding’s inequality [13, Theorem 1] states that this proportion is bounded by $e^{-2n\varepsilon^2}$, so the number of such tuples $\mathbf{a} \in A^n$ appearing in the first sum is at most $|A^n| e^{-2n\varepsilon^2} = |X|^n e^{-2n\varepsilon^2}$. The same bound applies to the other two sums, so we conclude that $\text{slice-rank}(F^{\otimes n}) \leq (|X|^n + |Y|^n + |Z|^n) e^{-2n\varepsilon^2}$. \square

The bound in Theorem 4.10 can be improved if we have more information about the distribution of the weights, by sharpening the large deviation estimate in the last paragraph of the proof. (If F is not symmetric between x, y , and z , it may also be helpful to use different cutoffs for the different variables.) One case is very common, so we single it out: we define the *triangle rank* $\text{triangle-rank}(F)$ to be the smallest k for which there exist functions f_a, g_b, h_c for $a, b, c \in \{0, \dots, k-1\}$ such that

$$F(x, y, z) = \sum_{a+b+c < k} r_{a,b,c} f_a(x) g_b(y) h_c(z). \tag{4.9}$$

We remark that in contrast with the definition of instability, here we do not require that the functions f_i are linearly independent or form a basis. However, it turns out we can assume this without affecting the triangle rank by the same argument as Remark 4.5(3).

We will not use the following observation directly, but it provides a representative example and was central to Ellenberg–Gijswijt’s results in [11].

Observation 4.11. *For any function $P: \mathbb{F}_p \rightarrow \mathbb{F}_p$ with p prime, the function $F(x, y, z) = P(x + y + z)$ has triangle rank at most p .*

Proof. We can represent P as a polynomial of degree less than p . Expanding $P(x+y+z)$ and collecting terms expresses $F(x,y,z) = P(x+y+z)$ as a linear combination of monomials $x^a y^b z^c$. Since $\deg P < p$, each monomial that occurs satisfies $a+b+c < p$. \square

To analyze the bounds on slice rank resulting from triangle rank, we will need to bound the proportion of tuples $\mathbf{a} \in \{0, \dots, m\}^n$ with $\sum_i a_i \leq \frac{1}{3}mn$. The bounds used in the proof of Theorem 4.10 would bound this proportion by $e^{-n/18}$, but in this case the rate function can be analyzed more carefully, leading to the following definition. For $m > 0$ and $\alpha \in (0, \frac{1}{2})$, let

$$I(m, \alpha) := \sup_{\theta < 0} \left(\alpha\theta - \log \left(\frac{1 - e^{(1+1/m)\theta}}{(m+1)(1 - e^{\theta/m})} \right) \right).$$

Proposition 4.12. *The proportion of tuples $\mathbf{a} \in \{0, \dots, m\}^n$ satisfying $\sum_i a_i \leq \alpha mn$ is at most $e^{-I(m,\alpha)n}$. Moreover, for fixed $\alpha \in (0, \frac{1}{2})$ the function $I(m, \alpha)$ is positive, is increasing in m , and converges to $\sup_{\theta < 0} (\alpha\theta - \log(\frac{e^\theta - 1}{\theta}))$ as $m \rightarrow \infty$.*

We will prove this proposition below; although the first assertion in this proposition is standard, we include the proof for completeness. Before moving to the proof of the proposition, we show that bounds on the triangle rank lead to bounds on the slice rank of tensor powers. In this case the relevant proportion will be $\alpha = \frac{1}{3}$, so for $s > 1$ let us define

$$J(s) := e^{-I(s-1, \frac{1}{3})} = \frac{1}{s} \inf_{0 < x < 1} \frac{1 - x^s}{1 - x} x^{-\frac{s-1}{3}}. \tag{4.10}$$

(The latter expression is obtained from the definition of $I(s-1, \alpha)$ by setting $x = e^{\theta/(s-1)}$.) We point out as a consequence of Proposition 4.12 that for all $s > 1$ the function $J(s)$ is decreasing, satisfies $J(s) < 1$, and (with $z = e^{-\theta/3}$)

$$\lim_{s \rightarrow \infty} J(s) = \inf_{z > 1} \frac{z - z^{-2}}{3 \log z} = 0.8414\dots \tag{4.11}$$

Proposition 4.13. *If $|X| = |Y| = |Z| = k$ and $\text{triangle-rank}(F) \leq k$, then not only is $\text{instability}(F) \geq \frac{1}{6}$, but moreover the slice rank of $F^{\otimes n}$ is at most $3(kJ(k))^n$.*

Proof. We first check the first claim. Express F as in (4.9) with the $f_a, g_b,$ and h_c linearly independent. Set $u_a = a$ for all $a = 0, 1, \dots, k-1$; if the f_a are not a basis, extend them arbitrarily to a basis and set $u_a = \frac{k-1}{2} = u_{\text{avg}}$ for all $a \geq k$ (these terms will not play any role in the decomposition). Doing the same for the other factors exhibits F as a sum as in (4.4) with $R = k-1$. Since $u_{\text{max}} = v_{\text{max}} = w_{\text{max}} = R$ and $u_{\text{avg}} = v_{\text{avg}} = w_{\text{avg}} = \frac{R}{2}$, solving for ε gives $\varepsilon = \frac{1}{6}$.

To bound the slice rank of $F^{\otimes n}$, simply follow the proof of Theorem 4.10 up until the last paragraph. The relevant estimate in this case is the number of tuples $\mathbf{a} \in \{0, \dots, k-1\}^n$ with $\sum_i a_i \leq \frac{1}{3}(k-1)n$. In place of the general bound of $k^n e^{-n/18}$ obtained there, substitute the bound of $k^n e^{-I(k-1, \frac{1}{3})n} = k^n J(k)^n$ from Proposition 4.12 to conclude that $\text{slice-rank}(F^{\otimes n}) \leq 3(kJ(k))^n$. \square

Proof of Proposition 4.12. After dividing everything by m , the first claim in the proposition states that if X_1, \dots, X_n are independent copies of a random variable X uniformly distributed on the $m + 1$ values $\{\frac{0}{m}, \frac{1}{m}, \dots, \frac{m}{m}\}$, then $\Pr(\sum_i X_i \leq \alpha n) \leq e^{-I(m, \alpha)n}$. For any $\theta < 0$, applying the order-reversing transformation $x \mapsto e^{\theta x}$ shows that $\Pr(\sum_i X_i \leq \alpha n) = \Pr(e^{\theta \sum_i X_i} \geq e^{\alpha n \theta})$. By Markov's inequality, the latter is at most $e^{-\alpha n \theta} \mathbb{E}(e^{\theta \sum_i X_i}) = (e^{-\alpha \theta} \mathbb{E}(e^{\theta X}))^n$. Setting $q = e^{\theta/m}$, we have $\mathbb{E}(e^{\theta X}) = (1 + q + \dots + q^m)/(m + 1) = \frac{1 - q^{m+1}}{1 - q} \cdot \frac{1}{m+1}$, and this concludes the proof of the first claim.

For the remaining claims, set $G(t, x) = \frac{1 - e^{t(1+x)}}{(1 + 1/x)(1 - e^{tx})}$, and set $G(0, x) = 1$ so that G is continuous at 0. By definition $I(m, \alpha)$ is the supremum over $\theta < 0$ of $\gamma(\theta, m) = \alpha \theta - \log G(\theta, \frac{1}{m})$. Note that $\gamma(0, m) = 0$; moreover, as $t \rightarrow 0$,

$$\begin{aligned} G(t, x) &= \frac{1 - e^{t(1+x)}}{(1 + 1/x)(1 - e^{tx})} \\ &= \frac{1}{1 + 1/x} \left(\frac{-t(1+x) - t^2(1+x)^2/2 + O(t^3)}{-tx - t^2x^2/2 + O(t^3)} \right) \\ &= \frac{1 + t(1+x)/2 + O(t^2)}{1 + tx/2 + O(t^2)} \\ &= 1 + t/2 + O(t^2), \end{aligned}$$

and hence $\frac{\partial \log G}{\partial t}(0, x) = \frac{\frac{\partial G}{\partial t}(0, x)}{G(0, x)} = \frac{\partial G}{\partial t}(0, x) = \frac{1}{2}$. Thus, the derivative $\frac{\partial \gamma}{\partial \theta}(0, m) = \alpha - \frac{1}{2} < 0$ is negative for all $\alpha \in (0, \frac{1}{2})$. This guarantees that there exists some $\theta < 0$ where $\gamma(\theta, m)$ is positive, proving the second claim.

Furthermore, the supremum of $\gamma(\theta, m)$ is attained at some $\theta < 0$, because $\gamma(\theta, m)$ tends to 0 as $\theta \rightarrow 0$ and $-\infty$ as $\theta \rightarrow -\infty$, while the supremum is positive. This means that to prove that $I(m, \alpha)$ is increasing in m , it suffices to prove for each fixed $\theta < 0$ that $\gamma(\theta, m)$ is increasing in m . Equivalently, we must prove that $G(t, x)$ is increasing in x when $t < 0$ and $x > 0$; we do this by proving that $\frac{\partial G}{\partial x} > 0$ in this region.

Set $h(x) = (1 - e^{tx})/x$. Note that $\frac{h(x+1)}{h(x)} = \frac{(1 - e^{t(x+1)})/(x+1)}{(1 - e^{tx})/x} = G(t, x)$. Therefore $\frac{\partial G}{\partial x} > 0$ if and only if $h'(x+1)h(x) \geq h'(x)h(x+1)$. Since $t < 0$ and $x > 0$ we have $h(x) > 0$, so this holds if and only if $\frac{h'(x+1)}{h(x+1)} > \frac{h'(x)}{h(x)}$. Hence it suffices to show that $\frac{d^2}{dx^2} \log h(x) > 0$, since then $\frac{d}{dx} \log h(x) = \frac{h'(x)}{h(x)}$ is increasing. We have that $\frac{d^2}{dx^2} \log h(x) = \frac{d}{dx} \left(-\frac{1}{x} - \frac{te^{tx}}{1 - e^{tx}} \right) = \frac{1}{x^2} - \frac{(1 - e^{tx})t^2e^{tx} - te^{tx}(-te^{tx})}{(1 - e^{tx})^2} = \frac{1}{x^2} - \frac{t^2e^{tx}}{(1 - e^{tx})^2}$, and so the proposition follows from the inequality $(1 - e^{tx})^2 > t^2x^2e^{tx}$, which we can prove as follows.

To verify this inequality, note that $n! \leq 2^{n-1}(n-1)!$ for all $n \in \mathbb{N}$ with strict inequality for all $n > 2$. Hence $\sum_{n=1}^{\infty} \frac{z^n}{n!} > \sum_{n=1}^{\infty} \frac{z^n}{2^{n-1}(n-1)!}$ for $z > 0$. Evaluating those power series shows that $e^z - 1 > ze^{z/2}$. Dividing by e^z , we obtain $1 - e^{-z} > ze^{-z/2}$. Squaring yields $(1 - e^{-z})^2 > z^2e^{-z}$; setting $z = -tx$, this becomes the desired inequality.

Finally, as $m \rightarrow \infty$ we have

$$\lim_{m \rightarrow \infty} I(m, \alpha) = \limsup_{m \rightarrow \infty} \sup_{\theta < 0} \left(\alpha \theta - \log G\left(\theta, \frac{1}{m}\right) \right).$$

Since $-\log G(\theta, x)$ is monotonically decreasing in x , $\alpha \theta - \log G(\theta, \frac{1}{m})$ is monotonically increasing in m , so the limit in m is the same as the supremum in m and hence commutes with the supremum in θ .

Thus we may switch the order of the limit and the supremum to obtain

$$\lim_{m \rightarrow \infty} I(m, \alpha) = \sup_{\theta < 0} \left(\alpha \theta - \lim_{m \rightarrow \infty} \log G \left(\theta, \frac{1}{m} \right) \right).$$

By the continuity of the logarithm and the variable change $\frac{1}{m} = x$ this equals

$$\sup_{\theta < 0} \left(\alpha \theta - \log \left(\lim_{x \rightarrow 0} \frac{h(x+1)}{h(x)} \right) \right),$$

where $h(x) = (1 - e^{\theta x})/x$. Since $\lim_{x \rightarrow 0} h(x) = -\theta$, it follows that

$$\lim_{m \rightarrow \infty} I(m, \alpha) = \sup_{\theta < 0} \alpha \theta - \log \left(\frac{e^{\theta} - 1}{\theta} \right). \quad \square$$

4.4 Tricolored sum-free sets in abelian groups of bounded exponent

In this section, we prove Theorems A and A', by way of the following sharper bound.

Theorem 4.14. *If H is an abelian group $H \cong (\mathbb{Z}/q\mathbb{Z})^n \times G$ where q is a prime power, then every tricolored sum-free set in H has cardinality at most $3 \cdot |H| \cdot J(q)^n$.*

The upper bound in Theorem 4.14 is known to be sharp up to a subexponential factor by [14, Theorem 2], conditional on a conjecture, namely [14, Conjecture 3], that was later proved independently in [18] and [19].

The proofs of these theorems depend on the following proposition.

Proposition 4.15. *If $q = p^r$ is a prime power, the triangle rank of $D_{\mathbb{Z}/q\mathbb{Z}}$ over \mathbb{F}_p is at most q .*

Proof. The triangle rank is invariant under any permutation of the sets X, Y, Z , so it suffices to bound the triangle rank of the function

$$D_{\mathbb{Z}/q\mathbb{Z}}(x, y, z + 1) = \begin{cases} 1 \in \mathbb{F}_p & \text{if } x + y + z = q - 1 \in \mathbb{Z}/q\mathbb{Z}, \text{ and} \\ 0 \in \mathbb{F}_p & \text{if } x + y + z \neq q - 1 \in \mathbb{Z}/q\mathbb{Z}. \end{cases}$$

As a consequence of Lucas' theorem, for any $0 \leq k < q$ and $m, m' \in \mathbb{N}$,

$$m \equiv m' \pmod{q} \implies \binom{m}{k} \equiv \binom{m'}{k} \pmod{p}.$$

In other words, $m \mapsto \binom{m}{k}$ descends to a well-defined function $\mathbb{Z}/q\mathbb{Z} \rightarrow \mathbb{F}_p$. We claim that

$$D_{\mathbb{Z}/q\mathbb{Z}}(x, y, z + 1) = \sum_{a+b+c=q-1} \binom{x}{a} \binom{y}{b} \binom{z}{c}.$$

Indeed, the identity $\binom{X+Y+Z}{i} = \sum_{a+b+c=i} \binom{X}{a} \binom{Y}{b} \binom{Z}{c} \in \mathbb{N}$ for $X, Y, Z \in \mathbb{N}$ descends to an identity $\binom{x+y+z}{i} = \sum_{a+b+c=i} \binom{x}{a} \binom{y}{b} \binom{z}{c} \in \mathbb{F}_p$ for $x, y, z \in \mathbb{Z}/q\mathbb{Z}$. But for any $w \in \mathbb{Z}/q\mathbb{Z}$, choosing a lift in $\{0, \dots, q-1\}$ shows that

$$\binom{w}{q-1} = \begin{cases} 1 \in \mathbb{F}_p & \text{if } w = q - 1 \in \mathbb{Z}/q\mathbb{Z}, \text{ and} \\ 0 \in \mathbb{F}_p & \text{if } w \neq q - 1 \in \mathbb{Z}/q\mathbb{Z}. \end{cases}$$

This decomposition of $D_{\mathbb{Z}/q\mathbb{Z}}(x, y, z + 1)$ shows that its triangle rank is at most q . □

Proof of Theorem 4.14. Let $q = p^r$, and consider the tensor D_H over \mathbb{F}_p . The decomposition $H \cong (\mathbb{Z}/q\mathbb{Z})^n \times G$ induces a decomposition $D_H = D_{(\mathbb{Z}/q\mathbb{Z})^n} \otimes D_G$. Proposition 4.2 thus implies

$$\text{slice-rank}(D_H) \leq \text{slice-rank}(D_{(\mathbb{Z}/q\mathbb{Z})^n}) \cdot |G|.$$

We proved in Proposition 4.15 that $\text{triangle-rank}(D_{\mathbb{Z}/q\mathbb{Z}}) \leq q$. By Proposition 4.13, this implies that $\text{slice-rank}(D_{(\mathbb{Z}/q\mathbb{Z})^n}) \leq 3(qJ(q))^n$. We conclude

$$\text{slice-rank}(D_H) \leq 3(qJ(q))^n \cdot |G| = 3 \cdot |H| \cdot J(q)^n.$$

The bound on tricolored sum-free sets in H then follows from Proposition 4.8. □

Proof of Theorem A'. If q is a prime power, Theorem 4.14 states that the size of any tricolored sum-free set in $H \cong (\mathbb{Z}/q\mathbb{Z})^n$ is at most $3 \cdot |H| \cdot J(q)^n$. To get a uniform bound we recall that $J(q)$ is decreasing by Proposition 4.12, so the worst case for this bound occurs when the prime power q is 2. Therefore if we set

$$\delta = I(1, \frac{1}{3}) = \sup_{\theta < 0} \left(\frac{\theta}{3} - \log \left(\frac{e^{2\theta} - 1}{2e^\theta - 2} \right) \right) = \log \left((2/3)2^{2/3} \right) = 0.05663 \dots,$$

then $J(q) \leq J(2) = e^{-\delta} = q^{-\frac{\delta}{\log q}}$. The size of any tricolored sum-free set in $H \cong (\mathbb{Z}/q\mathbb{Z})^n$ is thus at most

$$3 \cdot |H| \cdot J(q)^n \leq 3 \cdot |H| \cdot J(2)^n = 3q^n e^{-\delta n} = 3 \cdot |H|^{1 - \frac{\delta}{\log q}}. \quad \square$$

Proof of Theorem A. Let q_1, \dots, q_r denote all the prime powers less than or equal to m . By the Chinese remainder theorem, we can write $H \cong \prod_{i=1}^r (\mathbb{Z}/q_i\mathbb{Z})^{n_i}$. Let ℓ be the index for which n_ℓ is largest. Writing $\sum_i n_i = N$, we know that $n_\ell \geq N/r$. Since $\sum_i n_i \log q_i = \log |H|$ and $q_i \leq m$ we have $N \geq \frac{\log |H|}{\log m}$.

Next, we claim that $r < \frac{2m}{\log m}$ for all $m > 1$. By [23, (3.2) and (3.36)] we have that $r < \frac{m}{\log m} + \frac{3m}{2(\log m)^2} + \frac{1.4260m^{1/2}}{\log 2}$. This bound is at most $\frac{2m}{\log m}$ as long as $m \geq 242$. For the remaining $1 < m < 242$, one can simply check directly that the number of prime powers less than m is less than $\frac{2m}{\log m}$.

Combining these bounds on N and r shows that $n_\ell \geq \frac{N}{r} \geq \frac{\log |H|}{2m}$. By Theorem 4.14, this implies the size of any tricolored sum-free set in $H \cong (\mathbb{Z}/q_\ell\mathbb{Z})^{n_\ell} \times G$ is at most

$$3 \cdot |H| \cdot J(q_\ell)^{n_\ell} \leq 3 \cdot |H| \cdot J(q_\ell)^{\log |H| / (2m)} = 3 \cdot |H|^{1 + \log J(q_\ell) / (2m)}.$$

As in the proof of Theorem A' above, the worst case for this bound is when the prime power q_ℓ is 2; since $J(s)$ is decreasing, we can bound $\log J(q_\ell) \leq \log J(2) = -\delta$. Setting

$$\varepsilon = \delta/2 = \log \left((2/3)2^{2/3} \right) / 2 = 0.02831 \dots,$$

the bound from Theorem 4.14 then implies the size of any tricolored sum-free set in H is at most $3 \cdot |H|^{1 + \log J(q_\ell) / (2m)} \leq 3 \cdot |H|^{1 - \varepsilon/m}$. □

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, doi:10.1007/s00037-013-0060-1. 2, 3
- [2] P. Bürgisser, M. Clausen, and M. A. Shokrollahi, *Algebraic complexity theory*, Grundlehren der Mathematischen Wissenschaften **315**, Springer-Verlag, Berlin, 1997, doi:10.1007/978-3-662-03338-8. 6
- [3] P. Bürgisser and C. Ikenmeyer, *Geometric complexity theory and tensor rank*, Proceedings of the 43rd Annual ACM Symposium on Theory of Computing, 6–8 June 2011, San Jose, CA, Association for Computing Machinery, pp. 509–518, arXiv:1011.1350, doi:10.1145/1993636.1993704. 18
- [4] 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, doi:10.1109/sfcs.2005.39. 2, 3, 4, 5, 9
- [5] 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, doi:10.1109/sfcs.2003.1238217. 2, 3, 4
- [6] 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, doi:10.1137/1.9781611973105.77. 3
- [7] D. Coppersmith and S. Winograd, *Matrix multiplication via arithmetic progressions*, J. Symbolic Computation **9** (1990), 251–280, doi:10.1016/s0747-7171(08)80013-2. 2, 3
- [8] D. Coppersmith and S. Winograd, *On the asymptotic complexity of matrix multiplication*, SIAM J. Comput. **11** (1982), 472–492, doi:10.1137/0211038. 4
- [9] E. Croot, V. Lev, and P. Pach, *Progression-free sets in \mathbb{Z}_4^n are exponentially small*, Ann. of Math. (2) **185** (2017), 331–337, arXiv:1605.01506, doi:10.4007/annals.2017.185.1.7. 1, 2, 10, 11
- [10] A. M. Davie and A. J. Stothers, *Improved bound for complexity of matrix multiplication*, Proc. Roy. Soc. Edinburgh Sect. A **143** (2013), 351–369, doi:10.1017/S0308210511001648. 3
- [11] J. S. Ellenberg and D. Gijswijt, *On large subsets of \mathbb{F}_q^n with no three-term arithmetic progression*, Ann. of Math. (2) **185** (2017), 339–343, arXiv:1605.09223, doi:10.4007/annals.2017.185.1.8. 1, 2, 3, 10, 11, 19
- [12] P. Erdős and E. Szemerédi, *Combinatorial properties of systems of sets*, J. Combinatorial Theory Ser. A **24** (1978), 308–313, doi:10.1016/0097-3165(78)90060-2. 2

- [13] W. Hoeffding, *Probability inequalities for sums of bounded random variables*, J. Amer. Statist. Assoc. **58** (1963), 13–30, doi:10.1080/01621459.1963.10500830. 19
- [14] R. Kleinberg, W. F. Sawin, and D. E. Speyer, *The growth rate of tri-colored sum-free sets*, preprint, 2016, arXiv:1607.00047. 22
- [15] 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, Association for Computing Machinery, pp. 296–303, full version at arXiv:1401.7714, doi:10.1145/2608628.2608664. 3
- [16] T. Lickteig, *Typical tensorial rank*, Linear Algebra Appl. **69** (1985), 95–120, doi:10.1016/0024-3795(85)90070-9 12
- [17] D. Mumford, *Stability of projective varieties*, Enseignement Math. (2) **23** (1977), 39–110, doi:10.5169/seals-48919. 13
- [18] S. Norin, *A distribution on triples with maximum entropy marginal*, preprint, 2016, arXiv:1608.00243. 22
- [19] L. Pebody, *Proof of a conjecture of Kleinberg-Sawin-Speyer*, preprint, 2016, arXiv:1608.05740. 22
- [20] F. Petrov, *Many zero divisors in a group ring imply bounds on progression-free subsets*, preprint, 2016, arXiv:1606.03256. 3
- [21] A. Schönhage, *Partial and total matrix multiplication*, SIAM J. Comp. **10** (1981), 434–455, doi:10.1137/0210032 4
- [22] T. Tao, *A symmetric formulation of the Croot–Lev–Pach–Ellenberg–Gijswijt capset bound*, blog post, 2016, <http://terrytao.wordpress.com/2016/05/18/a>. 3, 10, 11, 12, 15, 16
- [23] J. B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. **6** (1962), 64–94, <http://projecteuclid.org/euclid.ijm/1255631807>. 2, 23
- [24] 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, doi:10.1145/2213977.2214056. 3

AUTHORS

Jonah Blasiak
 Department of Mathematics
 Drexel University
 Philadelphia, PA 19104
 jblasiak@gmail.com

Thomas Church
Department of Mathematics
Stanford University
450 Serra Mall
Stanford, CA 94305
tfchurch@stanford.edu

Henry Cohn
Microsoft Research New England
One Memorial Drive
Cambridge, MA 02142
cohn@microsoft.com

Joshua A. Grochow
University of Colorado at Boulder
Department of Computer Science
1111 Engineering Drive
Boulder, CO 80309
and
Santa Fe Institute
1399 Hyde Park Rd.
Santa Fe, NM 87501
jgrochow@santafe.edu

Eric Naslund
Mathematics Department
Princeton University
Fine Hall, Washington Road
Princeton, NJ 08544
naslund@math.princeton.edu

William F. Sawin
ETH Institute for Theoretical Studies
ETH Zürich
8092 Zürich
william.sawin@math.ethz.ch

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

Chris Umans
Computing and Mathematical Sciences
Caltech
1200 E. California Blvd.
Pasadena, CA 91125
umans@cms.caltech.edu