Monochromatic Hilbert cubes and arithmetic progressions

József Balogh*

Department of Mathematical Sciences
University of Illinois at Urbana-Champaign
IL, U.S.A.

Moscow Institute of Physics and Technology
9 Institutskiy per., Dolgoprodny, Moscow Region, 141701, Russian Federation

jobal@math.uiuc.edu

Mikhail Lavrov George Shakan Adam Zsolt Wagner

Department of Mathematical Sciences
University of Illinois at Urbana-Champaign
IL, U.S.A.

{mlavrov,shakan2,zawagne2}@illinois.edu

Submitted: Jun 7, 2018; Accepted: Mar 29, 2019; Published: May 17, 2019

Abstract

The Van der Waerden number $W(k, r)$ denotes the smallest n such that whenever $[n]$ is r–colored there exists a monochromatic arithmetic progression of length k. Similarly, the Hilbert cube number $h(k, r)$ denotes the smallest n such that whenever $[n]$ is r–colored there exists a monochromatic affine k–cube, that is, a set of the form

$$\left\{ x_0 + \sum_{b \in B} b : B \subseteq A \right\}$$

for some $|A| = k$ and $x_0 \in \mathbb{Z}$.

We show the following relation between the Hilbert cube number and the Van der Waerden number. Let $k \geqslant 3$ be an integer. Then for every $\epsilon > 0$, there is a $c > 0$ such that

$$h(k, 4) \geqslant \min\{W(\lfloor ck^2 \rfloor, 2), 2^{k^{2.5-\epsilon}}\}.$$

*Research of the first author is partially supported by NSF Grant DMS-1500121 and Arnold O. Beckman Research Award (UIUC) Campus Research Board 18132 and the Langan Scholar Fund (UIUC).

Thus we improve upon state of the art lower bounds for $h(k,4)$ conditional on $W(k,2)$ being significantly larger than 2^k. In the other direction, this shows that if the Hilbert cube number is close to its state of the art lower bounds, then $W(k,2)$ is at most doubly exponential in k.

We also show the optimal result that for any Sidon set $A \subset \mathbb{Z}$, one has

$$\left|\left\{\sum_{b\in B} b : B \subseteq A\right\}\right| = \Omega(|A|^3).$$

Mathematics Subject Classifications: 05C15, 05D10

1 Introduction

A k–term arithmetic progression (AP) in the integers is a set of the form

$$\{x_0 + dj : 0 \leqslant j \leqslant k-1\},$$

where $x_0, d \in \mathbb{Z}$. Recall the famous Van der Waerden theorem.

Theorem 1 (Van der Waerden [Wa], 1927)**.** *Let $k, r \geqslant 2$ be integers. Then there exists an n such that in any r–coloring of $[n]$, at least one color class contains a k–term AP.*

The smallest such n is said to be the *Van der Waerden number*, which we denote by $W(k,r)$. The state of the art bounds on $W(k,r)$ are as follows: Berlekamp [Be] showed for prime p we have $p \cdot 2^p \leqslant W(p+1,2)$. This result was recently generalized by Blankenship, Cummings and Taranchuk [BCT] who showed the following for p prime

$$p^{r-1}2^p \leqslant W(p+1,r). \tag{1}$$

Kozik and Shabanov [KoSh] proved the general lower bound $c \cdot r^{k-1} \leqslant W(k,r)$ for all $k \geqslant 3$, which is a slight improvement over an application of the Lovász local lemma [Sza]. The best known upper bound for $W(k,r)$ is the breakthrough result of Gowers [Go]

$$W(k,r) \leqslant 2^{2^{r^{2^{2^{k+9}}}}}.$$

This upper bound has been further improved in the case when $k = 3$ by a series of papers by Graham, Solymosi, Bourgain, Sanders and Bloom (see e.g. [Bl]) to

$$W(3,r) \leqslant 2^{cr(\ln r)^4}.$$

For $r = 2$, Graham [Gr] conjectures

$$W(k,2) < 2^{k^2}, \tag{2}$$

and offers \$1000 for a proof or disproof.

Prior to Van der Waerden's study of monochromatic APs, Hilbert studied the same problem for affine cubes.

Definition 1.1. Given a set $A \subseteq \mathbb{Z}$, its *restricted sumset* is the set

$$\Sigma^* A := \left\{ \sum_{b \in B} b : B \subseteq A \right\}.$$

An affine k–cube, or Hilbert cube, is a set of integers that has the form $x_0 + \Sigma^* A$ for some $x_0 \in \mathbb{Z}$ and $A \subset \mathbb{Z}$ with $|A| = k$.

We remark that in the literature, a Hilbert cube typically allows repeated elements in A but we do not. All of the literature we mention below, with the exception of [CFS], allows repeats. It turns out that in all cases their results can be easily transferred to our situation.

Theorem 2 (Hilbert [Hi], 1892)**.** *Let $k, r \geqslant 2$ be integers. Then there exists an n such that any r–coloring of $[n]$, at least one color class contains an affine k–cube.*

We denote the smallest such n by $h(k, r)$. Hilbert's proof yields

$$h(k, r) \leqslant r^{((3+\sqrt{5})/2)^k}. \tag{3}$$

Since every $\binom{k}{2}$–term AP is an affine k–cube, we have

$$h(k, r) \leqslant W\left(\tbinom{k}{2}, r\right). \tag{4}$$

Thus Van der Waerden's theorem implies Theorem 2 (but not the bound in (3)). Szemerédi [Sze], in his seminal paper on the density version of Van der Waerden's theorem, proved that

$$h(k, r) = O(r^{2^k}).$$

Hilbert's and Szemerédi's results are a massive improvement over combining (4) with the state of the art Van der Waerden bounds in (1). The case where $k = 2$ was asymptotically solved by Brown, Chung, Erdős and Graham [BCEG], who showed that

$$h(2, r) = (1 + o(1))r^2.$$

Their lower bound uses difference sets arising from finite projective planes, and their upper bound follows from bounds on Sidon sets. Gunderson and Rödl [GuRö] showed that for $k \geqslant 3$ we have

$$r^{(1-o(1))\left(2^k-1\right)/k} \leqslant h(k, r),$$

where $o(1) \to 0$ as $r \to \infty$. Recently Conlon, Fox and Sudakov [CFS] improved the bound of Erdős and Spencer [ErSp] by showing that there exists an absolute constant c such that

$$r^{ck^2} \leqslant h(k, r). \tag{5}$$

This is currently the best lower bound known for small values of r. Their proof heavily relies on an inverse Littlewood–Offord type theorem of Nguyen and Vu [NgVu], which we

will also use in our proof of our main result. Note that a significant improvement on (5) would improve on (1) because of (4). Unfortunately, improving the bounds on Van der Waerden numbers is a notoriously difficult problem. To circumvent this problem, in this paper we focus on improving the Conlon–Fox–Sudakov bound conditional on the fact that $W(k,2)$ is much bigger than 2^k.

Theorem 3. *Let $k \geqslant 3$ be an integer. Then for every $\epsilon > 0$, there is a $c > 0$ such that*

$$h(k,4) \geqslant \min\{W(\lfloor ck^2 \rfloor, 2), 2^{k^{2.5-\epsilon}}\}.$$

Theorem 3 asserts that either

(i) the lower bound for $W(k,2)$ in (1) is far from sharp and $h(k,4)$ is larger than (5),

(ii) the lower bound for $W(k,2)$ in (1) is nearly sharp and we can roughly reverse (4).

We remark that by Theorem 3, one can solve Graham's conjecture in (2) by providing an upper bound of $h(k,4) < 2^{k^{2.5-\epsilon}}$. Our proof of Theorem 3 can be easily adapted to provide lower bounds for $h(k,r)$ where $r > 1$ is a square of an integer. We briefly mention that Hilbert cubes have played a central role in upper bounds for van der Waerden numbers [Go, Sze], via Gower's uniformity norms and Szemerédi's cube lemma.

The idea for the proof of Theorem 3 is the following. In a random coloring of $[n]$, the probability that an affine k–cube, $x_0 + \Sigma^* A$ is monochromatic is

$$\frac{2}{2^{|\Sigma^* A|}}.$$

This probability is small when $|\Sigma^* A|$ is large. When $|\Sigma^* A|$ is small, then A should look much like an AP and we are led back to the Van der Waerden problem. Our main tools for making this argument rigorous are a paper of Nguyen and Vu [NgVu] (see Theorem 7) concerning the Littlewood–Offord theory and another paper of Szemerédi and Vu [SzVu] (see Theorem 8) on finding long APs in restricted sumsets, along with some analysis of our own (see Lemma 12) of the case when A is a large subset of a generalized AP.

To prove Theorem 3, we analyze which $A \subset \mathbb{Z}$ satisfy

$$|\Sigma^* A| = O(|A|^{2.5-\epsilon}).$$

We conclude this implies A has some additive structure, which eventually yields Theorem 3. Curiously, after this analysis we cannot rule out the case that A is a Sidon set, that is $|A+A| = \binom{|A|+1}{2}$. We use different techniques to handle this case.

Theorem 4. *There exists a $c > 0$ such that for any Sidon set $A \subset \mathbb{Z}$ one has*

$$|\Sigma^* A| \geqslant c|A|^3.$$

This result is a side product of our methods and we believe it is of independent interest. The proof is elementary, self-contained and best possible up to the constant c. To see this last point, recall the classical result that $[n]$ contains a Sidon set, say A, of size $n^{1/2}(1-o(1))$ (see e.g. [O'Br, Theorem 5]). Thus $\Sigma^* A \subset [n^{3/2}]$ and

$$|\Sigma^* A| \leqslant |A|^3(1+o(1)).$$

We briefly mention a related theorem of finding monochromatic Folkman cubes, a wide generalization of Schur's theorem that was obtained independently by Folkman, Rado and Sanders. This generalization is now commonly referred to as Folkman's theorem (see for example [GRS]). Let $F(k,r)$ be the smallest n such in that any r–coloring of $[n]$ one can find a set A of size k such that $\Sigma^* A \subseteq [n]$ and $\Sigma^* A$ is monochromatic. The state of the art bounds on $F(k,r)$ are significantly different from the best bounds on $H(k,r)$. Indeed, already for $F(k,2)$ the best upper bound due to Taylor [Ta] is tower-type, while the best lower bound is due to Balogh–Eberhard–Narayanan–Treglown–Wagner [BENTW]. They are as follows:

$$2^{2^{k-1}/k} \leqslant F(k,2) \leqslant 2^{2^{3^{2^{\cdot^{\cdot^{\cdot^{3}}}}}}},$$

where the tower on the right side has height $4k-3$.

2 Initial set-up and the random coloring

Generalized APs play a central role in our argument.

Definition 2.1. A *generalized AP (GAP) of rank* r is a set of the form

$$Q = \left\{ a + \sum_{i=1}^{r} k_i d_i : m_i < k_i \leqslant M_i \text{ for } 1 \leqslant i \leqslant r \right\}.$$

for some $a, m_1, \dots, m_r,\ M_1, \dots, M_r \in \mathbb{Z}$, and $d_1, \dots, d_r \in \mathbb{Z}$. The *volume* of Q is $(M_1 - m_1)\cdots(M_r - m_r)$. We say Q is *proper* if its volume is equal to its size. We say Q is *symmetric* if $m_i = -M_i$ for $1 \leqslant i \leqslant r$.

Proof idea. We let $N = \min\{W(\lfloor ck^2 \rfloor, 2), 2^{k^{2.5-\epsilon}/(10\log k)}\} - 1$ where $c > 0$ is a sufficiently small, fixed constant that depends on our argument. We color $[N]$ by a product coloring $\chi_1 \times \chi_2$, where

- $\chi_1 : [N] \to [2]$ avoids monochromatic APs of length $\lfloor ck^2 \rfloor$,
- $\chi_2 : [N] \to [2]$ is a uniformly random coloring.

If a Hilbert cube has many distinct elements, then the coloring χ_2 makes sure it is not monochromatic. We will show that all Hilbert cubes having very few distinct elements will contain a ck^2–term AP, in which case χ_1 ensures it is not monochromatic. □

To understand χ_2, we will need the following lemma, which appears in a short paper of Erdős and Spencer [ErSp].

Lemma 5. *Let $n, k, u \in \mathbb{N}$ be integers with $u \geqslant k(k+1)/2$. The number of sets $S \subseteq [n]$ of size k satisfying $|\Sigma^* S| \leqslant u$ is at most $(kn)^{\log u} u^{2k}$.*

The critical case for our purposes is $u = k^a$ for some $a = O(1)$ and k a fixed power of $\log n$ and so the bound in Lemma 5 is $n^{a \log k(1+o(1))}$. In this case it is easy to see that $\sim_k n^a$ proper GAPs of rank $a-1$ satisfy the hypothesis of Lemma 5. The additional $\log k$ in the exponent is not concerning for our purposes. A corollary of Lemma 5 is that a random coloring is unlikely to contain Hilbert cubes of large size.

Corollary 6. *Fix an arbitrary $a > 2$. If*

$$N \leqslant 2^{k^a/(10a \log k)} \tag{6}$$

and $\chi_2 : [N] \to \{0,1\}$ is the uniform random 2–coloring then w.h.p. (as $k \to \infty$, a fixed) χ_2 does not contain a monochromatic Hilbert cube of size at least k^a.

Proof. The probability that a Hilbert cube of size u is monochromatic under χ_2 is 2^{1-u}. By Lemma 5 the number of such cubes is $\leqslant N(kN)^{\log u} u^{2k}$, since we have at most N choices for x_0. By the union bound and (6) the probability, $p(k)$, that there is a monochromatic Hilbert cube of size at least k^a satisfies

$$p(k) \leqslant N \sum_{u \geqslant k^a} \left(k 2^{k^a/(10a \log k)}\right)^{\log u} u^{2k} 2^{1-u} \leqslant kN^2 \left(k 2^{k^a/(10a \log k)}\right)^{a \log k} k^{2ak} 2^{1-k^a} = o(1). \ \square$$

3 The AP–avoiding coloring

To analyze a Hilbert cube $x_0 + \Sigma^* A$, we ignore x_0 and focus on the structure of A. We assume that

$$|\Sigma^* A| \leqslant k^{2.5-\epsilon}, \tag{7}$$

since we Corollary 6 implies we may choose a χ_2 so that all Hilbert cubes not satisfying (7) are not monochromatic.

We proceed in several steps. First, we use a result of Nguyen and Vu [NgVu] to show that for sets satisfying (7), at least half of the set A must be contained in a GAP of small rank and volume. We consider two cases for the rank of the resulting GAP, and show that in each case $x_0 + \Sigma^* A$ is not monochromatic in $\chi_1 \times \chi_2$.

3.1 Results concerning restricted sumsets of GAPs

We first recall an inverse theorem of Nguyen and Vu.

Theorem 7 (Nguyen–Vu, special case of Theorem 2.1 in [NgVu])**.** *Let C be a constant, and let A be a k–element set with $|\Sigma^* A| \leqslant k^C$. Then there is a proper symmetric rank r GAP, Q, such that $|A \cap Q| \geqslant \frac{1}{2}k$ and $|Q| = O(k^{C-r/2})$, where the constant factor may depend on C.*

In particular, if A satisfies (7)*, then the two possible cases are*

1. $|Q| = O(k^{2-\epsilon})$ *and* Q *is a rank* 1 *GAP (an AP),*

2. $|Q| = O(k^{1.5-\epsilon})$ *and* Q *is a rank* 2 *GAP.*

To see the last point of Theorem 7, note that if Q were to have rank 3 or greater, then $|Q| = O(k^{1-\epsilon})$, which contradicts that Q contains at least half of the elements of A.

Definition 3.1. For an integer ℓ, let $\ell^* A$ denote the subset of $\Sigma^* A$ consisting of sums of exactly ℓ distinct elements

$$\ell^* A := \left\{ \sum_{b \in B} b : B \subset A,\ |B| = \ell \right\}.$$

Theorem 8 (Szemerédi–Vu, Theorem 7.1 in [SzVu])**.** *For any fixed positive integer r there are positive constants C and c depending on r such that the following holds. For any positive integers n and ℓ and any set $A \subseteq [n]$ with $\ell \leqslant \frac{1}{2}|A|$ and $\ell^r |A| \geqslant Cn$, the set $\ell^* A$ contains a proper GAP of rank r' and size at least $c\ell^{r'}|A|$, for some integer $r' \leqslant r$.*

Our standing assumption (7) is not compatible with $r' \geqslant 2$ and $\ell = \Omega(|A|)$ in Theorem 8 as long as $n = |A|^{O(1)}$. We formulate this in the following corollary.

Corollary 9. *For every positive integer r, there is a constant C' such that the following holds. Let P be an arbitrary AP with $|P| = n$, and let $A \subseteq P$ which satisfies $C'n \leqslant |A|^{r+1}$ and $|\Sigma^*(A)| = o(|A|^3)$. Then $\Sigma^* A$ contains an AP of length $\Omega_r(|A|^2)$.*

Proof. If $P = \{a + kd : 1 \leqslant k \leqslant n\}$, then apply the Freiman homomorphism $x \mapsto \frac{x-a}{d}$ maps P to $[n]$, A to a subset of $[n]$, and preserves the size of both A and $\Sigma^* A$. So we may assume that $P = [n]$ in what follows.

We take C' to be $2^r C$, where $C = C(r)$ is the corresponding constant in Theorem 8. Then we have $|A|^{r+1} \geqslant 2^r Cn$, or $(\frac{1}{2}|A|)^r |A| \geqslant Cn$. Applying Theorem 8 with $\ell = \frac{1}{2}|A|$, we conclude that $\ell^* A$ contains a proper GAP of rank r' for some $r' \leqslant r$, which has size $c(\frac{1}{2}|A|)^{r'}|A| = \frac{c}{2^{r'}}|A|^{r'+1}$. In particular, $\Sigma^* A \supset \ell^* A$ contains a GAP of size $\Omega_r(|A|^{r'+1})$. For $r' \geqslant 2$, this is incompatible with our assumption $|\Sigma^*(A)| = o(|A|^3)$ for sufficiently large $|A|$. So we may assume that $r' = 1$, and therefore $\Sigma^* A$ contains an AP of length $\Omega_r(|A|^2)$. □

The following corollary is an immediate consequence of Corollary 9 and our choice of χ_1.

Corollary 10. *Suppose a set A is of size k and contained in an AP of size $O(k^\alpha)$ for some $\alpha \geqslant 1$. Then $x_0 + \Sigma^* A$ is not monochromatic in χ_1.*

In case (1) of Theorem 7, we have that A is a subset of an AP of length $O(k^{2-\epsilon})$, and so by Corollary 10, $x_0 + \Sigma^* A$ is not monochromatic in the coloring χ_1. Thus $x_0 + \Sigma^* A$ is not monochromatic in the product coloring $\chi_1 \times \chi_2$.

3.2 Completing the proof of Theorem 3

We are now left to analyze case (2) in Theorem 7. Here at least half of the elements of A is contained in a proper, symmetric GAP, Q, of rank 2 and size $O(k^{1.5-\epsilon})$. In this case, A is basically a dense subset of a two-dimensional integer box (ignoring the technicality that while Q is proper, it may not be that $|\Sigma^* Q| = 2^{|Q|}$). In this case, the size of $\Sigma^* A$ is roughly cubic in $|A|$ as is shown by the following lemma.

Lemma 11. *There is an absolute constant C such that for $A \subseteq [m] \times [n]$, with $|A| \geqslant C\sqrt{mn}$,*

$$|\Sigma^* A| \geqslant \Omega\left(\frac{|A|^3}{(\log |A|)^4}\right).$$

This is best possible up to the logarithm, as is seen by taking $A = [m] \times [n]$. We prove Lemma 11 in the following section, but first show how it implies Theorem 3.

Since Q is proper, we may decompose it into the following six disjoint sets:

- $Q_1 = \{id_1 + jd_2 : 1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n\}$,
- $Q_2 = \{id_1 + jd_2 : 1 \leqslant i \leqslant m, -n \leqslant j \leqslant -1\}$,
- $Q_3 = \{id_1 + jd_2 : -m \leqslant i \leqslant -1, 1 \leqslant j \leqslant n\}$,
- $Q_4 = \{id_1 + jd_2 : -m \leqslant i \leqslant -1, -n \leqslant j \leqslant -1\}$,
- $Q_5 = \{id_1 : -m \leqslant i \leqslant m\}$,
- $Q_6 = \{jd_2 : -n \leqslant j \leqslant n, j \neq 0\}$.

At least one of $|A \cap Q_1|, |A \cap Q_2|, \ldots, |A \cap Q_6|$ has size at least $\frac{1}{12}|A|$. If this happens for Q_5 or Q_6, then we are in the situation of case (1) of Theorem 7, which we already handled in Corollary 10. Without loss of generality, by switching the signs of d_1 and d_2, we may assume $|A \cap Q_1| \geqslant \frac{|A|}{12}$.

Let $\phi : Q_1 \to \mathbb{Z}^2$ via $\phi(id_1 + jd_2) = (i, j)$. Since Q_1 is proper, ϕ is injective. It follows, for k sufficiently large, that we have

$$|\phi(A \cap Q_1)| = |A \cap Q_1| = \Omega(k) \geqslant C\sqrt{mn}.$$

Thus we may apply Lemma 11 to find that

$$|\Sigma^* \phi(A \cap Q_1)| = \Omega(k^{3-\epsilon}). \tag{8}$$

Combing this with (7), we have that

$$|\Sigma^*(A \cap Q_1)| = |A \cap A_1| < |\Sigma^* \phi(A \cap Q_1)|.$$

One may compare the rest of our argument to [TV, Theorem 3.40]. It follows that there is a "collision," that is there exist $1 \leqslant x_1, y_1 \leqslant km$ and $1 \leqslant x_2, y_2 \leqslant kn$, satisfying

$$x_1 d_1 + x_2 d_2 = y_1 d_1 + y_2 d_2.$$

This simplifies to

$$|d_1| \cdot |x_1 - y_1| = |d_2| \cdot |x_2 - y_2|.$$

Let

$$d := \gcd(d_1, d_2).$$

So $\frac{|d_1|}{d}$ divides $\frac{|d_2|}{d}|x_2 - y_2|$ and by Euclid's lemma $\frac{|d_1|}{d}$ divides $|x_2 - y_2|$. Thus

$$\frac{|d_1|}{d} \leqslant kn.$$

Similarly, $\frac{|d_1|}{d} \leqslant km$.

Let R be the AP with common difference d given below:

$$R = \{-m|d_1| - n|d_2|, \ldots, -d, 0, d, \ldots, m|d_1| + n|d_2|\}.$$

Then R contains every integer divisible by d between the largest and smallest element of Q, so $Q \subseteq R$. Moreover,

$$|R| \leqslant 1 + 2\frac{m|d_1| + n|d_2|}{d} \leqslant 1 + 2m \cdot kn + 2n \cdot km = O(k|Q|) = O(k^{2.5-\epsilon}).$$

By Corollary 10, $x_0 + \Sigma^*(A \cap Q_1)$ is not monochromatic in χ_1 and so neither is $x_0 + \Sigma^* A$. Thus we have handled case (2) of Theorem 7 and completed the proof of Theorem 3.

4 Restricted sumsets for dense subsets of high dimensional boxes

It remains to prove Lemma 11. We work in arbitrary dimensions, which may be of independent interest. In the following lemma, we are only interested in the case $m = 1$, but other values of m are useful as a strengthened induction hypothesis. We recall the m–fold sum is

$$mB := B + \ldots + B,$$

where there are m summands.

Lemma 12. *For all integers $d \geqslant 1$ there exists an absolute constant C_d such that the following holds.*

Suppose that $A \subseteq [N_1] \times [N_2] \times \ldots \times [N_d]$, with density $\alpha = \frac{|A|}{N_1 N_2 \cdots N_d}$ satisfies $\frac{\alpha}{(\log \alpha^{-1})^{d-i}} N_i \geqslant C_d$ for $2 \leqslant i \leqslant d$, and m is an integer. Then

$$|m\Sigma^* A| \geqslant \Omega\left(\frac{|A|^{d+1} m^d}{\log^{d^2}(\alpha^{-1})}\right).$$

Proof. We induct on d. For $d = 1$, we will show the stronger $|m\Sigma^* A| \geqslant O(|A|^2 m)$. To begin with, we have $|\Sigma^* A| \geqslant \binom{|A|+1}{2}$. Let $A = \{a_1, a_2, \ldots, a_k\}$; then an increasing sequence of $\binom{k+1}{2} + 1$ elements of $\Sigma^* A$ is given by

$$\begin{aligned} 0 &< a_1 < a_2 < \ldots < a_k \\ &< a_1 + a_k < a_2 + a_k < \ldots < a_{k-1} + a_k \\ &< a_1 + a_{k-1} + a_k < a_2 + a_{k-1} + a_k < \ldots < a_{k-2} + a_{k-1} + a_k \\ &< \ldots < \\ &< a_1 + a_2 + \ldots + a_{k-1} + a_k. \end{aligned}$$

From the estimate $|X + Y| \geqslant |X| + |Y| - 1$ we have $|mX| \geqslant m|X| - m + 1$, and therefore as long as $|A| \geqslant 2$ we have $|m\Sigma^* A| \geqslant m\binom{|A|+1}{2} - m + 1 \geqslant \frac{1}{2}|A|^2 m$.

For the induction step, assume that this lemma holds in dimension $d-1$, where $d \geqslant 2$. Partition A into *stacks*

$$A_x = \{a \in A : (a_1, \ldots, a_{d-1}) = x\}$$

indexed by $x \in [N_1] \times \cdots \times [N_{d-1}]$. The average size of a stack A_x is αN_d. Call a stack A_x *sparse* if $|A_x| \leqslant \frac{1}{2}\alpha N_d$, and *dense* otherwise. Then the total number of elements of A contained in sparse stacks is at most

$$\frac{1}{2}\alpha N_d \cdot \prod_{i=1}^{d-1} N_i = \frac{1}{2}|A|,$$

so at least $\frac{1}{2}|A|$ elements of A are in dense stacks.

The sizes of dense stacks range from $\frac{1}{2}\alpha N_d$ to N_d. For each t such that $\frac{1}{2}\alpha N_d \leqslant t \leqslant \frac{1}{2}N_d$, define

$$X_t = \{x \in [N_1] \times \cdots \times [N_{d-1}] : t < |A_x| \leqslant 2t\},$$

so that X_t indices all stacks whose sizes range from t to $2t$. By a dyadic decomposition, we can find a t so that the union of the stacks indexed by X_t is large. That is, letting $s = \lceil \log_2 \alpha^{-1} \rceil$, we can partition the indices of all the dense stacks into the disjoint union of s sets

$$\bigcup_{i=0}^{s-1} X_{2^{i-1}\alpha N_d}.$$

Since at least $\frac{1}{2}|A|$ elements of A are in dense stacks, there must be a $t = 2^{i-1}\alpha N_d$ for some i between 0 and $s-1$ such that at least $\frac{1}{2s}|A|$ elements of A are in stacks indexed by some $x \in X_t$.

For each $x \in X_t$, we choose two disjoint sets $B_x, C_x \subseteq A_x$, where $|B_x| = 2\lfloor \frac{t}{3} \rfloor$ and $|C_x| = \lfloor \frac{t}{3} \rfloor$. Since $\alpha N_d \geqslant C_d$, we have $\lfloor \frac{t}{3} \rfloor \geqslant \frac{t}{4}$, provided that we choose C_d sufficiently large. Define

$$C = \bigcup_{x \in X_t} C_x.$$

We will show that $|m\Sigma^* A|$ is large in two steps.

Let $b \in m\Sigma^* A$ be given by summing the $\lfloor \frac{t}{3} \rfloor$ smallest elements of each B_x, each with multiplicity m. Then $b + m\Sigma^* C$ is a subset of $m\Sigma^* A$. We show that not only is $|b + m\Sigma^* C|$ large, but that its projection onto the first $d-1$ coordinates is large.

In this projection, the exact elements of each C_x are irrelevant, since their first $d-1$ coordinates are just x. Being able to choose the elements of C_x, of which there are at least $\frac{t}{4}$, up to m times each is equivalent to being able to include x in a sum up to $\frac{mt}{4}$ times, and so the size of the projection is $|\frac{mt}{4}\Sigma^* X_t|$.

Since each stack A_x has size at most $2t$, and the union of all stacks indexed by X_t has size at least $\frac{|A|}{2s}$, we know that X_t itself must have size at least $\frac{|A|}{4st}$. We apply the induction hypothesis to X_t. The density of X_t in $[N_1] \times \cdots \times [N_{d-1}]$ is at least

$$\alpha' = \frac{|A|}{N_1 \cdots N_{d-1} \cdot 4st} \geqslant \frac{|A|}{N_1 \cdots N_d \cdot 4s} \geqslant \frac{\alpha}{4\lfloor \log_2(\alpha^{-1}) \rfloor},$$

which will satisfy the conditions in the induction hypothesis provided we choose C_d sufficiently large compared to C_{d-1}. Additionally, $\log(\alpha'^{-1}) = \Theta(\log \alpha^{-1})$. So we have

$$\left| \frac{mt}{4} \Sigma^* X_t \right| \geqslant \Omega\left(\frac{|X_t|^d (\frac{1}{4}mt)^{d-1}}{(\log \alpha'^{-1})^{(d-1)^2}} \right) \geqslant \Omega\left(\frac{|A|^{d-1} m^{d-1} t^{-1}}{(\log \alpha^{-1})^{(d-1)^2+d}} \right).$$

Second, for each element of $b + m\Sigma^* C$, we show that there are many elements of $m\Sigma^* A$ with the same projection onto the first $d-1$ coordinates. We can obtain such elements by replacing b with a different sum which also uses $m\lfloor \frac{t}{3} \rfloor$ elements of B_x for each x, counting multiplicity.

Let $k = \lfloor \frac{t}{3} \rfloor$, and let $B_x = \{b_{x,1}, \ldots, b_{x,2k}\}$. For a fixed x, there are at least mk^2 distinct sums of elements of B_x with total multiplicity mk. The argument here is similar to the $d = 1$ case of this lemma. Start with the smallest possible sum,

$$\sum_{i=1}^{k} m b_{x,i}.$$

For each sum with total multiplicity mk, we may increase its d^{th} coordinate by choosing the largest $i < 2k$ such that $b_{x,i}$ is included in the sum, while $b_{x,i+1}$ is included fewer than m times, and replace $b_{x,i}$ by $b_{x,i+1}$. This ends only when we reach the largest possible sum,

$$\sum_{i=k+1}^{2k} m b_{x,i}.$$

The sum of the indices on the $mb_{x,i}$, taken with multiplicity, starts at $\sum_{i=1}^{k} mi = m\binom{k+1}{2}$ and ends at $\sum_{i=k+1}^{2k} mi = mk^2 + m\binom{k+1}{2}$. In each step, since we replace some $b_{x,i}$ by $b_{x,i+1}$, the sum of indices increase by 1, so we take a total of $mk^2 \geqslant m(\frac{t}{4})^2 = \Omega(mt^2)$ steps.

Now we must aggregate this result over all $x \in X_t$. Starting at the element b as previously defined, go through the elements of X_t arbitrarily, and for each $x \in X_t$, perform the above process, taking $\Omega(mt^2)$ steps. There are a total of $|X_t| \cdot \Omega(mt^2)$ steps taken, and

each one increases the d^{th} coordinate while leaving the first $d-1$ coordinates unchanged. Altogether, for every $a \in b + m\Sigma^* C$, we obtain

$$|X_t| \cdot \Omega(mt^2) = \Omega\left(mt^2 \cdot \frac{|A|}{4st}\right) = \Omega\left(\frac{|A|mt}{\log \alpha^{-1}}\right)$$

different elements of $m\Sigma^* A$ with the same first $d-1$ coordinates as a.

Repeating this for each of the $\Omega\left(\frac{|A|^d m^{d-1} t^{-1}}{\log^{10d-10+d}|A|}\right)$ elements of $b + m\Sigma^* C$, we get

$$|m\Sigma^* A| \geqslant \Omega\left(\frac{|A|^d m^{d-1} t^{-1}}{(\log \alpha^{-1})^{(d-1)^2+d}}\right) \cdot \Omega\left(\frac{|A|mt}{\log \alpha^{-1}}\right) = \Omega\left(\frac{|A|^{d+1} m^d}{(\log \alpha^{-1})^{d^2}}\right),$$

completing the inductive step. □

In our application we will have $d = 2$. In this case, assuming that A is sufficiently large, we get the bound in a second lemma, given below. By applying a Freiman isomorphism, that bound also applies when $d > 2$ but the set A is too sparse to use Lemma 12 directly.

Lemma 13. *There is an absolute constant C such that for all $d \geqslant 2$, the following holds. Suppose that $A \subseteq [N_1] \times [N_2] \times \cdots \times [N_d]$, with $|A| \geqslant C\sqrt{N_1 N_2 \cdot \ldots \cdot N_d}$. Then*

$$|\Sigma^* A| \geqslant \Omega\left(\frac{|A|^3}{(\log |A|)^4}\right).$$

Proof. First we handle the case $d = 2$. Then this result is a direct application of Lemma 12, once we assure ourselves that it applies. Without loss of generality, assume that $N_1 \leqslant N_2$. Since $|A| \geqslant C\sqrt{N_1 N_2}$, the density $\alpha = \frac{|A|}{N_1 N_2}$ satisfies $\alpha N_2 \geqslant C\sqrt{\frac{|N_2|}{|N_1|}} \geqslant C$, so the conditions of Lemma 12 are satisfied for any C which is at least the constant C_2 from that lemma.

Taking $m = 1$, we conclude that

$$|\Sigma^* A| \geqslant \Omega\left(\frac{|A|^3}{(\log \alpha^{-1})^4}\right) = \Omega\left(\frac{|A|^3}{(\log |A|)^4}\right).$$

Next, we assume that $d > 2$ and we begin by omitting any coordinates i with $N_i = 1$, so that we may assume $N_i \geqslant 2$ for all i. Therefore if we define

$$M = \sum_{i=2}^{d} N_2 N_3 \cdot \ldots \cdot N_i,$$

we have $M \leqslant (N_2 \cdot \ldots \cdot N_i)(1 + \frac{1}{2} + \frac{1}{4} + \cdots) \leqslant 2N_2 \cdot \ldots \cdot N_i$.

We map $[N_1] \times \cdots \times [N_d]$ to $[N_1] \times [M]$ by the homomorphism $\phi\colon \mathbb{Z}^d \to \mathbb{Z}^2$ which takes

$$(x_1, x_2, \ldots, x_d) \mapsto \left(x_1, \sum_{i=2}^{d} x_i \prod_{j=2}^{i-1} N_j\right).$$

The homomorphism ϕ is injective on $[N_1] \times \cdots \times [N_d]$, so the image $\phi(A)$ has the same size as A. Therefore

$$|\phi(A)| \geqslant C\sqrt{N_1 N_2 \cdot \ldots \cdot N_d} \geqslant C\sqrt{\frac{N_1 M}{2}},$$

which is large enough for the $d = 2$ case of this lemma to apply if we choose $C = C_2\sqrt{2}$. Applying the $d = 2$ case of this lemma,

$$|\Sigma^* A| \geqslant |\Sigma^* \phi(A)| \geqslant \Omega\left(\frac{|\phi(A)|^3}{(\log|\phi(A)|)^4}\right) = \Omega\left(\frac{|A|^3}{(\log|A|)^4}\right),$$

which was what we wanted. □

Lemma 11 follows from Lemma 13 by taking $d = 2$.

5 Sidon sets

We now set out to prove Theorem 4. We prove this by starting with a small subset $X \subseteq A$, and adding elements to X slowly while ensuring that $|\Sigma^* X|$ grows quickly. In the end, $|\Sigma^* X|$ will reach $\Omega(|A|^3)$ in size before the set A is exhausted.

As long as $|\Sigma^* X|$ is relatively small, the following lemma guarantees that we can increase $|\Sigma^* X|$ by a factor of $\frac{3}{2}$ with the addition of only two new elements.

Lemma 14. *Let A be a Sidon subset of the positive integers, and let $X \subseteq A$ with $|X| \leqslant \frac{1}{2}|A|$ and $|\Sigma^* X| \leqslant \binom{\frac{1}{2}|A|}{2}$. Then we can extend X to $X' = X \cup \{a_1, a_2\}$ with $a_1, a_2 \in A \setminus X$ in such a way that $|\Sigma^* X'| \geqslant \frac{3}{2}|\Sigma^* X|$.*

Proof. Let $B = \{a_1 + a_2 : a_1, a_2 \in A \setminus X\}$. Since A is Sidon, all elements of B are distinct, so $|B| = \binom{|A\setminus X|}{2} \geqslant \binom{\frac{1}{2}|A|}{2}$. In particular, $|B| \geqslant |\Sigma^* X|$.

The total number of solutions of the equation $s_1 + b = s_2$ with $s_1, s_2 \in \Sigma^* X$ and $b \in B$ is at most $\binom{|\Sigma^* X|}{2}$: once we choose the set $\{s_1, s_2\}$, we are forced to choose the order $s_1 < s_2$, and then b, if it exists, is unique. So there exists an element $b \in B$ for which there is at most the average number

$$\frac{\binom{|\Sigma^* X|}{2}}{|B|} \leqslant \frac{|\Sigma^* X|^2}{2|B|} \leqslant \frac{|\Sigma^* X|}{2|B|} \cdot |\Sigma^* X| \leqslant \frac{1}{2}|\Sigma^* X|$$

of solutions. In other words, $|\Sigma^* X \cap (\Sigma^* X + b)| \leqslant \frac{1}{2}|\Sigma^* X|$.

Write this b as $a_1 + a_2$, and let $X' = X \cup \{a_1, a_2\}$. Then

$$|\Sigma^* X'| \geqslant |\Sigma^* X + (\Sigma^* X + b)| \geqslant |\Sigma^* X| + |\Sigma^* X + b| - |\Sigma^* X \cap (\Sigma^* X + b)| \geqslant \frac{3}{2}|\Sigma^* X|,$$

as desired. □

When $|\Sigma^* X|$ is large, the previous lemma does not apply, and we need a second iterative way to increase $|\Sigma^* X|$.

Lemma 15. *Let A be a Sidon subset of the positive integers, and let $X \subseteq A$ with $|X| \leqslant \frac{3}{4}|A|$ but $|\Sigma^* X| \geqslant \binom{\frac{1}{4}|A|}{2}$. Then we can extend X to $X' = X \cup \{a_1, a_2\}$ with $a_1, a_2 \in A \setminus X$ in such a way that $|\Sigma^* X'| \geqslant |\Sigma^* X| + \frac{1}{2}\binom{\frac{1}{4}|A|}{2}$.*

Proof. Let A' be a subset of A with $|A'| = \frac{1}{4}|A|$ and $A' \cap X = \varnothing$, and let $B = \{a_1 + a_2 : a_1, a_2 \in A'\}$. Since A is Sidon, all elements of B are distinct, so $|B| = \binom{|A'|}{2} = \binom{\frac{1}{4}|A|}{2}$; in particular, $|B| \leqslant |\Sigma^* X|$.

Let S consist of the $|B|$ largest elements of $|\Sigma^* X|$. Of the $|B|^2$ elements of $S \times B$, at most $\binom{|B|}{2}$ are ordered pairs (s, b) with $s + b \in \Sigma^* X$, because then $s + b$ would be a larger element of S, and there are $\binom{|S|}{2} = \binom{|B|}{2}$ pairs of elements of S.

So there are at least $|B|^2 - \binom{|B|}{2} > \frac{1}{2}|B|^2$ elements of $S \times B$ which are ordered pairs (s, b) with $s + b \notin \Sigma^* X$. By averaging, there is some $b \in B$ contained in at least $\frac{1}{2}|B|$ of those ordered pairs. For this choice of b, $\Sigma^* X + b$ contains at least $\frac{1}{2}|B|$ values not found in $\Sigma^* X$.

Write $b = a_1 + a_2$ for some $a_1, a_2 \in A'$, and let $X' = X \cup \{a_1, a_2\}$. Then

$$|\Sigma^* X'| \geqslant |\Sigma^* X + (\Sigma^* X + b)| \geqslant |\Sigma^* X| + \frac{1}{2}|B| \geqslant |\Sigma^* X| + \frac{1}{2}\binom{\frac{1}{4}|A|}{2},$$

as desired. □

Now we put together the details and prove Theorem 4.

Proof. Begin with $X = \varnothing$, and $|\Sigma^* X| = 1$, and repeatedly apply Lemma 14 until one of the hypotheses is violated: either $|X| \geqslant \frac{1}{2}|A|$ or $|\Sigma^* X| \geqslant \binom{\frac{1}{2}|A|}{2}$. In fact, after k iterations of Lemma 14, we will have $|\Sigma^* X| \geqslant (\frac{3}{2})^k$, so the second hypothesis will be violated when $|X|$ is only $O(\log |A|)$; for $|A|$ sufficiently large, this will happen first.

Next, apply Lemma 15 to X repeatedly, increasing $|X|$ by 2 at every step while increasing $|\Sigma^* X|$ by $\frac{1}{2}\binom{\frac{1}{4}|A|}{2} = \Omega(|A|^2)$. It will take more than $\frac{1}{8}|A|$ applications of Lemma 15 before the hypothesis that $|X| \leqslant \frac{3}{4}|A|$ is no longer satisfied. At that point, $|\Sigma^* X|$ will have size at least $\frac{1}{8}|A| \cdot \frac{1}{2}\binom{\frac{1}{4}|A|}{2} = \Omega(|A|^3)$. In particular, this means that $|\Sigma^* A| = \Omega(|A|^3)$. □

References

[BENTW] J. Balogh, S. Eberhard, B. Narayanan, A. Treglown and A. Z. Wagner. An improved lower bound for Folkman's theorem. *Bulletin of the London Mathematical Society*, 49(4): 745–747, 2017.

[Be] E. R. Berlekamp. A construction for partitions which avoid long arithmetic progressions. *Canad. Math. Bull* 11: 409–414, 1968.

[BCT] T. Blankenship, J. Cummings and V. Taranchuk. A new lower bound for van der Waerden numbers. *European Journal of Combinatorics* 69: 163–168, 2018.

[Bl] T. F. Bloom. A quantitative improvement for Roth's theorem on arithmetic progressions *Journal of the London Mathematical Society* 93.3: 643–663, 2016.

[BCEG] T. C. Brown, F. R. K. Chung, P. Erdős and R. L. Graham. Quantitative forms of a theorem of Hilbert. *J. Combin. Theory, Ser. A*, 38: 210–216, 1985.

[O'Br] K. O'Bryant. A complete annotated bibliography of work related to Sidon sequences. *The Electronic Journal of Combinatorics*, #DS11, 2004.

[CFS] D. Conlon, J. Fox and B. Sudakov. Short proofs of some extremal results. *Combinatorics, Probability and Computing*, 23.1: 8–28, 2014.

[ErSp] P. Erdős and J. Spencer. Monochromatic sumsets. *J. Combin. Theory Ser. A*, 50(1):162–163, 1989.

[Go] W. Gowers. A new proof of Szemerédi's theorem. *Geom. Funct. Anal.* 11:3 (2001), 465–588.

[Gr] R. Graham. Some of my favorite problems in Ramsey theory. *Integers: Electronic Journal of Combinatorial Number Theory* 7.2: A15, 2007.

[GRS] R. L. Graham, B. L. Rothschild and J. H. Spencer. Ramsey theory, 2nd ed. *Wiley-Interscience Series in Discrete Mathematics and Optimization*, John Wiley & Sons, Inc., New York, 1990.

[GuRö] D. S. Gunderson and V. Rödl. Extremal problems for affine cubes of integers. *Combinatorics, Probability and Computing*, 7.1: 65–79, 1998.

[Hi] D. Hilbert. Über die Irreduzibilität ganzer rationaler Funktionen mit ganzzahligen Koeffizienten. (On the irreducibility of entire rational functions with integer coefficients) *J. Reine Angew. Math.* 110 (1892), 104–129.

[KoSh] J. Kozik and D. Shabanov. Improved algorithms for colorings of simple hypergraphs and applications. *Journal of Combinatorial Theory, Series B*, 116: 312–332, 2016.

[NgVu] H. Nguyen and V. Vu. Optimal inverse Littlewood-Offord theorems. *Adv. Math.*, 226(6):5298–5319, 2011.

[Sza] Z. Szabó. An application of Lovász local lemma–A new lower bound for the van der Waerden number. *Random Structures Algorithms* 1 (1990), 343–360.

[Sze] E. Szemerédi, "On sets of integers containing no k elements in arthmetic progression," *Acta Arith.* 27 (1975), 199–245.

[SzVu] E. Szemerédi and V. Vu. Long arithmetic progressions in sumsets: thresholds and bounds. *J. Amer. Math. Soc.*, 19(1):119–169, 2006.

[Ta] A. D. Taylor. Bounds for the disjoint unions theorem. *J. Combin. Theory Ser. A* 30:, 339–344, 1981.

[TV] T. Tao, V. Vu, Additive combinatorics, Cambridge University Press Hardback, 530 pages (ISBN–13: 9780521853866; ISBN–10: 0521853869). Paperback, 512 pages.

[Wa] B. van der Waerden. Beweis einer Baudetschen Vermutung. *Nieiw. Arch. Wisk.* 15 (1927), 212–216.