A short proof that $w(3, k) \geq (1 - o(1))k^2$

Zach Hunter

October 26, 2022

Abstract

Here we present a short proof that the two-color van der Waerden number $w(3, k)$ is bounded from below by $(1 - o(1))k^2$. Previous work has already shown that a superpolynomial lower bound holds for $w(3, k)$. However, we believe our result is still of interest due to our techniques.

1 Introduction

In this short note, we discuss the off-diagonal van der Waerden numbers $w(3, k)$, defined as follows. For integer $k \geq 3$, we define $w(3, k)$ to be the smallest $N$ such that for any blue-red coloring of $[N] := \{1, \ldots, N\}$, there either is a blue arithmetic progression of length 3, or a red arithmetic progression of length $k$.

Based off of computational data, Graham had conjectured that $w(3, k) = O(k^2)$. Indeed, it was suggested that $w(3, k) \leq (1 + o(1))k^2$ might hold.

It turns out that Graham’s conjecture is false. Indeed, in a breakthrough paper by Green, it was shown that $w(3, k)$ grows superpolynomially [5]. This was subsequently improved by the author [7], giving the current best known lower bound.

**Theorem 1** ([7, Theorem 1]). We have that

$$w(3, k) \geq \exp(c \log^2 k/ \log \log k)$$

for some absolute constant $c > 0$.

Here, we present a proof of a much weaker lower bound.

**Theorem 2.** We have that

$$w(3, k) \geq (1 - o(1))k^2.$$  

We believe Theorem 2 is still of interest, for several reasons. First, Theorem 2 gives a better lower bound than all arguments prior to the work of [5] (see Remark 1.1 for an account of past bounds). Second, we note that our methods give better bounds for small $k$ (see Remark 3.3 for details).

Lastly, our proof is very simple and is hopefully instructive. In particular, we use basic group theory to get colorings which have desirable pseudorandom properties. This method appears to be novel, and likely has further applications; for example, forthcoming work of the author will develop these ideas to improve the lower bounds of the diagonal multicolor van der Waerden numbers [8].
Remark 1.1. Past bounds (prior to the breakthrough of [5]): Brown, Landman and Robertson proved a lower bound of \( w(3, k) \gg k^{2 - 1/\log \log k} \) with the Lovász Local Lemma [2]. This was later optimized by Li and Shu to prove \( w(3, k) \gg (k/\log k)^2 \) [9].

Aaronson et al. proved \( w(3, k) \gg k^2 \) via a slightly involved combinatorial argument [1]; this result remains unpublished and attained a worse constant than Theorem 2. We note that we were unaware of this result before we wrote an earlier draft of this argument.

Guo and Warnke proved that \( w(3, k) \gg n^2 / \log n \) by analyzing a random greedy process [6], they were unaware of the result of [1].

Acknowledgements. This work was done under the supervision of Ben Green. We are thankful for his comments on the presentation of this note, especially the suggestion to use the language of direct products. We also thank Atticus Stonestrom and Matt Kwan for helpful feedback.

Parts of this note were prepared at IST Austria, we thank them for their hospitality.

2 Preliminaries

2.1 Notation

Here we collect a few pieces of notation that we will use.

For positive integer \( n \), we write \([n] := \{1, \ldots, n\}\).

For positive integer \( k \), we refer to (non-trivial) arithmetic progressions of length \( k \) as \( k \)-AP’s. We say a set of integers \( S \) is \( k \)-AP-free if it does not contain any \( k \)-AP’s as subsets.

We extend the above concept to (additive) groups \( G \). In particular, give a group \( G \), we say \( P \subset G \) is a \( k \)-AP with respect to \( G \) is there exists \( g, d \in G, d \neq 0_G \) such that \( P = \{g, g + d, \ldots, g + (k - 1)d\} \). And similarly, we say \( S \subset G \) is \( k \)-AP-free if it does not contain any \( k \)-AP’s (with respect to \( G \)) as subsets.

Lastly, for positive integer \( N \), we write \( r_3(N) \) to be the maximum cardinality of a 3-AP-free subset \( S \subset [N] \) (which is considered a subset of \( \mathbb{Z} \)).

2.2 Some basic lemmas about groups

For later use, we recall the following well-known lemma about groups.

Lemma 2.1. Let \( n, m \) be coprime integers. We have

\[ \mathbb{Z}/nm\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}. \]

To see that Lemma 2.1 is true, one may confirm that the map \( \phi : a + nm\mathbb{Z} \mapsto (a + n\mathbb{Z}, a + m\mathbb{Z}) \) is an isomorphism.

We also note the following key fact. This observation was previously utilized in a paper by Graham [4] (which studied a quantity related to \( w(3, k) \)), and also appears in the unpublished manuscript [1].
Lemma 2.2. Let $S \subseteq [n]$ be 3-AP-free (with respect to $\mathbb{Z}$). Then for $m \geq 2n - 1$, we have that $$S + m\mathbb{Z} = \{x + m\mathbb{Z} : x \in S\} \subseteq \mathbb{Z}/m\mathbb{Z}$$ is 3-AP-free with respect to $\mathbb{Z}/m\mathbb{Z}$.

Proof. Set $G = \mathbb{Z}/m\mathbb{Z}$, and let $\varphi : \mathbb{Z} \to G$ be the homomorphism $x \mapsto x + m\mathbb{Z}$. We shall prove $\varphi(S)$ is 3-AP-free with respect to $G$.

First, we note that a subset $T$ of a group contains a 3-AP if and only if there are $x, y, z \in T$ with $x \neq y$ and $x + z = 2y$ (indeed, if $P = \{g, g + d, g + 2d\} \subseteq T$ for $d \neq 0$, then one takes $x = g, y = g + d, z = g + 2d$; the converse direction is also straight-forward).

So, we suppose for sake of contradiction that such $x, y, z \in \varphi(S)$ exist. Then, taking their preimages $\overline{x}, \overline{y}, \overline{z} \in S$, we have that $\varphi(\overline{x} + \overline{z}) \equiv 2\varphi(\overline{y}) \pmod{m}$ implies $\overline{x} + \overline{z} - 2\overline{y} \in \ker(\varphi) = m\mathbb{Z}$. Since $\overline{x}, \overline{y}, \overline{z} \in S \subseteq \mathbb{Z}$, we have that $|\overline{x} + \overline{z} - 2\overline{y}| \leq 2n - 2 < m$.

Then, the above implies that $\overline{x} + \overline{z} - 2\overline{y} = 0$. Since $\varphi(\overline{y}) = x \neq y = \varphi(\overline{y})$ (and consequently, $\overline{x} \neq \overline{y}$), this should mean that $\{\overline{x}, \overline{y}, \overline{z}\} \subseteq S$ form a 3-AP, contradicting the assumption that $S$ is 3-AP-free. Thus such $x, y, z \in \varphi(S)$ cannot occur, as desired.

Remark 2.3. To use jargon from additive combinatorics, Lemma 2.2 was a basic consequence of the fact that the additive sets $[n]$ and $[n] + m\mathbb{Z}$ are “Freiman 2-isomorphic”.

3 Proof of Theorem 1

We first need the following key lemma.

Lemma 3.1. Let $H_1, H_2$ be groups, and consider their direct product

$$G = H_1 \times H_2.$$ 

Suppose we have sets $S = \{x_1, \ldots, x_m\} \subseteq H_1$ and $T_1, \ldots, T_m \subseteq H_2$ that are each 3-AP-free in their respective groups.

Then,$$ A := \bigcup_{i=1}^{m}\{(x_i, y) : y \in T_i\}$$ is 3-AP-free with respect to $G$.

Proof. Consider any $g = (g_1, g_2) \in G$ and $d = (d_1, d_2) \in G \setminus \{0_G\}$.

Suppose for sake of contradiction that $\{g, g + d, g + 2d\} \subseteq A$. Then, we must clearly have $\{g_1, g_1 + d_1, g_1 + 2d_1\} \subseteq S$.

Because $S$ is 3-AP-free with respect to $H_1$, this means that $d_1 = 0_{H_1}$ and $g_1 \in S$. 


In particular, there must be some \( i \in [m] \) such that \( g_1 = x_i \), and \( \{g, g + d, g + 2d\} \) is contained in the coset \( \{(x, y) : y \in H_2\} \).

By the assumptions that \( d \neq 0 \) and \( d_1 = 0_{H_1} \), we must have that \( d_2 \neq 0_{H_2} \). Hence, \( \{g_2, g_2 + d_2, g_2 + 2d_2\} \) is a 3-AP with respect to \( H_2 \). However, \( A \cap \{(x, h) : h \in H_2\} = \{(x, y) : y \in T_i\} \), thus \( \{g, g + d, g + 2d\} \subset A \) would imply \( \{g_2, g_2 + d_2, g_2 + 2d_2\} \subset T_i \), contradicting our assumption that \( T_i \) is 3-AP-free (with respect to \( H_2 \)). \( \square \)

Using Lemma 3.1, we will define a random set \( A \) which is always 3-AP-free with desirable properties.

**Lemma 3.2.** Let \( p \) be a prime. Suppose \( r_3([p/2]) = m \).

Then we can randomly construct a set \( A \subset [p^2 - p] \) that is 3-AP-free (with respect to \( Z \)), so that for each \( p \)-AP \( P \subset [p^2 - p] \subset Z \) we have

\[
\mathbb{P}(A \cap P = \emptyset) = (1 - m/(p - 1))^m.
\]

Consequently (by a union bound), when \((1 - m/(p - 1))^m \leq p^{-3} \), we have \( w(3, p) > p^2 - p \).

**Remark 3.3.** A well-known infinite 3-AP-free set is the set of positive numbers \( S \subset Z \) that don’t use the digit “0” in ternary (so \( S = \{1, 2, 4, 5, 7, 8, 13, \ldots\} \)). This construction was first noted by Erdős and Turán in 1936 [3], and was conjectured to give an optimal lower bound for \( r_3(N) \) until the work of Salem and Spencer [10].

Since \( [N] \cap S \) is 3-AP-free and always has cardinality at least \( N^{\log 2/\log 3} \geq N^{63/5} \), we get a simple lower bound for \( r_3(N) \). Using this with Lemma 3.2, we can see that \( w(3, p) > p^2 - p \) for all primes \( p \geq 2^{25} \).

**Proof.** We will first construct a random set \( A_0 \subset Z/(p^2 - p)Z \), and obtain \( A \) from this set.

To begin, we note that \((p - 1) \) and \( p \) are coprime, hence \( Z/(p^2 - p)Z \cong Z/pZ \times Z/(p - 1)Z \) by Proposition 2.1. We write \( H_1 \) to denote \( Z/pZ \) and \( H_2 \) to denote \( Z/(p - 1)Z \).

Since \( r_3([p/2]) = m \), there exists some \( S = \{x_1, \ldots, x_m\} \subset \lfloor [p/2] \rfloor \) which is 3-AP-free. By Lemma 2.2, we have that \( S + pZ \subset H_1 \) and \( S + (p - 1)Z \subset H_2 \) are both 3-AP-free sets in their respective groups.

Now, for each \( i \in [m] \), we pick a random element \( t_i \in H_2 \) independently and uniformly at random. We then set \( T_i = t_i + S + (p - 1)Z \subset H_2 \), which is also 3-AP-free with respect to \( H_2 \) (since this property is invariant under translation). Lastly, we take

\[
A_0 := \bigcup_{i \in [m]} \{(x_i + Z/pZ, y) : y \in T_i\}.
\]

By Lemma 3.1, we have that \( A_0 \) is 3-AP-free (with respect to \( Z/(p^2 - p)Z \)).

Next, we consider the surjective homomorphism \( \phi : Z \to Z/(p^2 - p)Z; n \mapsto n + (p^2 - p)Z \) and write \( \pi \) to denote the bijection \( \phi|_{\lfloor p^2 - p \rfloor} \). We take \( A = \pi^{-1}(A_0) \).

It remains to confirm that \( A \) has the desired properties.

Due to \( \pi \) being a bijection, and \( \phi \) a homomorphism, we see that for any \( k \), if \( P \subset [p^2 - p] \) is a \( k \)-AP (wrt \( Z \)) then \( \pi(P) \) is a \( k \)-AP (wrt \( Z/(p^2 - p)Z \)) with \( |\pi(P)| = k \). Hence, the assumption that \( A_0 \) being 3-AP-free immediately implies that is \( A \) is 3-AP-free as well.

4
We next observe that for any $p$-AP $P_0 \subset \mathbb{Z}/(p^2 - p)\mathbb{Z}$ with $|P_0| = p$, that we must have $P_0 = \{x, x + d, \ldots, x + (k - 1)d\}$ for some $d = (d_1, d_2)$ where $d_1 \neq 0_H$ (as otherwise, $P_0$ would be contained in a coset of the subgroup $\{(0, y) : y \in H_2\}$, which has size $p - 1 < |P_0|$).

Since $H_1$ is a cyclic group of prime order, we have that $\{0_{H_1}, d_1, \ldots, (p - 1)d_1\} = H_1$. So for each $i \in [m]$, $P_0$ intersects the coset $\{(x_i + p\mathbb{Z}, y) : y \in H_2\}$. Whence, by the independence of our chosen $t_1, \ldots, t_m$, we have that $P(P_0 \cap A_0 = \emptyset) = (1 - m/(p - 1))^m$. By the discussion above, this will imply the desired analogue holds for $A$, completing our proof. □

By the discussion of Remark 3.3, we get the following.

**Corollary 3.4.** We have $w(3, p) > p^2 - p$ for all sufficiently large primes $p$.

Finally, recall that for every $\epsilon > 0$, there exists $k_0$ so that when $k > k_0$ there exists a prime $p \in [(1 - \epsilon)k, k]$ (this is a consequence of the prime number theorem). Hence, applying Corollary 3.4, we get Theorem 2.

**References**

[1] J. Aaronson, C. Even-Zohar, J. Fox, S. Peluse, L. Sauermann, K. Taczala and S. Walker, *Unpublished manuscript*.

[2] T. Brown, B. M. Landman, and A. Robertson, *Bounds on Van der Waerden Numbers and Some Related Functions*, in *Journal of Combinatorial Theory, Series A* 115 (2008), p. 1304-1309.

[3] P. Erdős and P. Turán, *On Some Sequences of Integers*, in *Journal of the London Mathematical Society* 11 (1936), p. 261-264.

[4] R. Graham, *On the growth of a van der Waerden-like function*, in *INTEGERS: Electronic Journal of Combinatorial Number Theory* 6 (2006).

[5] B. J. Green, *New lower bounds for van der Waerden numbers*, in *Forum of Mathematics, Pi* (to appear).

[6] H. Guo, L. Warnke. *On the power of random greedy algorithms*, in *European Journal of Combinatorics* 105 (2022).

[7] Z. Hunter, *Improved lower bounds for van der Waerden numbers*, in *Combinatorica* (to appear).

[8] Z. Hunter, *Lower bounds for multicolor van der Waerden numbers*, (in preparation).

[9] Y. Li and J. Shu, *A lower bound for off-diagonal van der Waerden numbers*, in *Advances in Applied Mathematics* 44 (2010), p. 243-247.

[10] R. Salem and D. C. Spencer, *On Sets of Integers Which Contain No Three Terms in Arithmetical Progression*, in *Proceedings of the National Academy of Sciences of the United States of America* 28 (1942), p. 561-564.