Finding Large Sets Without Arithmetic Progressions of Length Three
By William Gasarch, James Glenn, Clyde P. Kruskal

Abstract

There has been much work on the following question: given n, how large can a subset of $\{1, \ldots, n\}$ be that has no arithmetic progressions of length 3. We call such sets *3-free*. In this paper we review the literature of how to construct large 3-free sets. We also show how such sets can be used to obtain lower bounds on $W(3, c)$ and the L-problem.

1 Introduction

The motivation for this paper begins with van der Waerden's theorem:

Def 1.1 Let $[n]$ denote the set $\{1, \ldots, n\}$.

Def 1.2 A k-AP is an arithmetic progression of length k.

Theorem 1.3 ([?, ?]) *For all k, for all c, there exists $W(k, c)$ such that for all c-colorings of $[W(k, c)]$ there exists a monochromatic k-AP.*

We are interested in lower bound on $W(k, c)$. If COL is a c-coloring with no mono k-AP's then all of the colors are (see definition below) k-free.

Def 1.4 For $k \in \mathbb{N}$, a set A is *k-free* if it does not have any arithmetic progressions of size k.

Can we use a (large) k-free set to create a c-coloring of (some) $[n]$ without any mono k-AP? Imagine that you have a k-free set $A \subseteq [n]$. Look at $c = \frac{n}{|A|}$ shifts of it: $A_1, \ldots, A_c$. Say they cover all of $[n]$. Then you can color x by the least i such that $x \in A_i$. This would show $W(k, c) \geq n$. But can we shift A with only c shifts. Not quite but close:

Theorem 1.5 *Let $A \subseteq [n]$ be a k-free set. Let $c = \frac{2n \log n}{|A|}$. There are c shifts of A that cover all of $[n]$ Hence there is a k-free c-coloring of $[n]$.*

Proof:
Let $t \in [n]$ picked at RANDOM. Let $A(t)$ be A shifted by t (circular). Let $x \in [n]$.
Prob that $x \in A(t)$ is $\frac{|A|}{n}$.
Prob that $x \notin A(t)$ is $1 - \frac{|A|}{n} \sim e^{-|A|/n}$.
Now pick L values of t (we will determine L later).
Prob that $x \notin A(t_1) \cup \cdots \cup A(t_L) = (e^{-|A|/n})^L = e^{-L|A|/n}$.

Prob there exists $x \in [n]$, $x \notin A(t_1) \cup \cdots \cup A(t_L) \le ne^{-L|A|/n}$.
We need
$ne^{-L|A|/n} < 1$.
Let $L = \frac{2n \ln n}{|A|}$. Note that

$\frac{-L|A|}{n} = -2 \ln n$

$e^{-L|A|/n} = e^{-2 \ln n} = \frac{1}{n^2}$

$ne^{-L|A|/n} = \frac{1}{n} < 1$.

▮

The above theorem can be used to get lower bounds on $W(k, c)$ once you have k-free sets. For the case of $k = 3$ we use these 3-free sets in a different way.

Def 1.6 An L-free c-coloring of $[n] \times [n]$ is a c-coloring with no monochromatic L-shapes which are isosceles.

Theorem 1.7 *Let $n \in \mathbb{N}$. Let $c = O(\frac{n \log n}{|A|})$. There is an L-free c-coloring of $[n] \times [n]$.*

Proof:

Let A be a 3-free set of $[3n]$. By Theorem 1.5 there is a 3-free c-coloring COL of $\{1, \ldots, 3n\}$ with $O(\frac{n \log n}{|A|})$ colors.

Consider the following c-coloring of $[n] \times [n]$.

$$COL'(x, y) = COL(x + 2y).$$

We show this is an L-free coloring. If there exists x, y, λ such that

$$COL'(x, y) = COL'(x + \lambda, y) = COL(x, y + \lambda)$$

then

$$COL(x + 2y) = COL(x + \lambda + 2y) = COL(x + 2y + 2\lambda y)$$

which we rewrite as

$$COL(x + 2y) = COL(x + 2y + \lambda) = COL(x + 2y + 2\lambda y)$$

Since this is an mono 3-AP, we must have $\lambda = 0$. Hence there is no mono L. ▮

Def 1.8 Let $sz\ (n)$ be the maximum size of a 3-free subset of $[n]$. ('sz' stands for Szemeredi.)

The next fact is trivial to prove; however, since we use it throughout the paper we need a shorthand way to refer to it:

Fact 1.9 *Let $x \le y \le z$. Then x, y, z is a 3-AP iff $x + z = 2y$.*

2 The Base 3 Method

Throughout this section sz(n) will be the largest 3-free set of $\{0, \ldots, n-1\}$ instead of $\{1, \ldots, n\}$.

The following method appeared in [?] but they do not take credit for it; hence we can call it folklore. Let $n \in \mathbb{N}$. Let

$A_n = \{m \mid 0 \le m \le n$ and all the digits in the base 3 representation of m are in the set $\{0, 1\}$ $\}$.

We will later show that A_n is 3-free and $|A_n| \approx 2^{\log_3 n} = n^{\log_3 2} \approx n^{0.63}$.
Example: Let $n = 92 = 1 \times 3^4 + 0 \times 3^3 + 1 \times 3^2 + 0 \times 3^1 + 2 \times 3^0$. Hence n in base 3 is 10102. We list the elements of A_{92} in several parts.

1. The elements of A_{92} that have a 1 in the fifth place are $\{10000, 10001, 10010, 10011, 10100, 10101\}$. This has the same cardinality as the set $\{0000, 0001, 0010, 0011, 0100, 0101\}$ which is A_{0102}.
2. The elements of A_{92} that have a 0 in the fifth place are the 2^4 numbers $\{0000, 0001, \ldots, 1111\}$.

Theorem 2.1 sz(n) $= \Omega(n^{\log_3(2)} \sim Omega(n^{.63})$.

Proof:
Express n in base 3. Assume this take $L+1$ digits. Note that this is $L \ge \log_3(n) + \Omega(1)$. Let A be the set of numbers of length L in base three that use only the digits 0 or 1. By taking one less digit we guarantee that $A \subseteq [n]$. We show that $|A| \ge \Omega()$ and A is 3-free.

The number of elements in A is

$$2^L \ge 2^{\log_3(n)+\Omega(1)} = 2^{\frac{\log_2 n}{\log_2 3}+\Omega(1)} = n^{(1/log_2 3)+\Omega(1)} = \Omega(n^{\log_3(2)} = \Omega(n^{.63})$$

We show that A_n is 3-free. Let $x, y, z \in A_n$ form a 3-AP. Let x, y, z in base 3 be $x = x_{k-1} \cdots x_0$, $y = y_{k-1} \cdots y_0$, and $z = z_{k-1} \cdots a_0$, By the definition of A_n, for all i, $x_i, y_i, z_i \in \{0, 1\}$. By Fact 1.9 $x + z = 2y$. Since $x_i, y_i, z_i \in \{0, 1\}$ the addition is done *without carries*. Hence we have, for all i, $x_i + z_i = 2y_i$. Since $x_i, y_i, z_i \in \{0, 1\}$ we have $x_i = y_i = z_i$, so $x = y = z$. ▮

3 3-Free Subsets of Size $n^{0.68-\epsilon}$: The Base 5 Method

According to [?], G. Szekeres conjectured that sz(n) $= \Theta(n^{\log_3 2})$. This was disproven by Salem and Spencer [?] (see below); however, in 1999 Ruzsa (Section 13 of [?]) noticed that a minor modification to the proof of the Theorem 2.1 yields the following theorem which also disproves the conjecture. His point was that this is an easy variant of Theorem 2.1 so it is surprising that it was not noticed earlier.

Theorem 3.1 *For all $\epsilon > 0$ $\mathrm{sz}(n) \geq \Omega(n^{(\log_5 3)-\epsilon}) \sim n^{0.68-\epsilon}$.*

Proof: Let $k = \lfloor \log_5 n \rfloor - 1$. We assume $k \equiv 0 \pmod 3$. Let A be the set of positive integers that, when expressed in base 5,

1. use at most k digits,
2. use only 0's, 1's, and 2's, and
3. use *exactly* $\frac{k}{3}$ 1's.

The size of A is

$$\binom{k}{k/3} \times 2^{2k/3}$$

It is known that $\binom{k}{k/3} \sim k^{k/3}$ We leave it to the reader to workout the rest of this.

We show that A is 3-free.

We show that A_n is 3-free. Let $x, y, z \in A_n$ form a 3-AP. Let x, y, z in base 5 be $x = x_{k-1} \cdots x_0$, $y = y_{k-1} \cdots y_0$, and $z = z_{k-1} \cdots a_0$, By the definition of A_n, for all i, $x_i, y_i, z_i \in \{0, 1\}$. By Fact 1.9 $x + z = 2y$. Since $x_i, y_i, z_i \in \{0, 1, 2\}$ the addition is done *without carries.* Hence we have, for all i, $x_i + z_i = 2y_i$.

We leave it to the reader to workout the rest of this.

∎

4 3-Free Subsets of Size $n^{1-\frac{1+\epsilon}{\lg \lg n}}$: The KD Method

The first disproof of Szekeres's conjecture (that $\mathrm{sz}(n) = \Theta(n^{\log_3 2})$) was due to Salem and Spencer [?].

Theorem 4.1 *For every $\epsilon > 0$ $\mathrm{sz}(n) \geq \Omega(n^{1-\frac{1+\epsilon}{\lg \lg n}})$.*

Def 4.2 Let $d, n \in \mathbb{N}$. Let $k = \lfloor \log_{2d-1} n \rfloor - 1$. Assume that d divides k. $\mathrm{KD}_{d,n}$ is the set of all $x \leq n$ such that

1. when expressed in base $2d - 1$ only uses the digits $0, \ldots, d - 1$, and
2. each digit appears the same number of times, namely k/d.

We omit the proof of the following lemma.

Lemma 4.3 *For all d, n $\mathrm{KD}_{d,n}$ is 3-free.*

Theorem 4.4 *For every $\epsilon > 0$ there exists n_0 such that, for all $n \geq n_0$,* $\mathrm{sz}(n) \geq n^{1-\frac{1+\epsilon}{\lg\lg n}}$.

Proof sketch: An easy calculation shows that, for any d, n, $\mathrm{KD}_{d,n} \subseteq [n]$. By Lemma 4.3 $\mathrm{KD}_{d,n}$ is 3-free. Clearly

$$|\mathrm{KD}_{d,n}| = \frac{k!}{[(k/d)!]^d}.$$

By picking d such that $(2d)^{d(\lg d)^2} \sim n$ one can show that $|A| \geq n^{1-\frac{1+\epsilon}{\lg\lg n}}$. ∎

5 3-Free Subsets of Size $n^{1-\frac{3.5\sqrt{2}}{\sqrt{\lg n}}}$: The Block Method

Behrend [?] and Moser [?] both proved $\mathrm{sz}(n) \geq n^{1-\frac{c}{\sqrt{\lg n}}}$, for some value of c. Behrend proved it first and with a smaller (hence better) value of c, but his proof was nonconstructive (i.e, the proof does not indicate how to actually find such a set). Moser's proof was constructive. We present Moser's proof here; Behrend's proof is presented later.

Theorem 5.1 *[?] For all n,* $\mathrm{sz}(n) \geq n^{1-\frac{3.5\sqrt{2}}{\sqrt{\lg n}}} \sim n^{1-\frac{4.2}{\sqrt{\lg n}}}$,

Proof sketch:

Let r be such that $2^{r(r+1)/2} - 1 \leq n \leq 2^{(r+1)(r+2)/2} - 1$. Note that $r \geq \sqrt{2\lg n} - 1$.

We write the numbers in $[n]$ in base 2. We think of a number as being written in r blocks of bits. The first (rightmost) block is one bit long. The second block is two bits long. The rth block is r bits long. Note that the largest possible number is $r(r+1)/2$ 1's in a row, which is $2^{r(r+1)/2} - 1 \leq n$. We call these blocks $x_1, \ldots, x_r$. Let B_i be the number represented by the ith block. The concatenation of two blocks will represent a number in the natural way.

Example: We think of $(1001110101)_2$ as $(1001 : 110 : 10 : 1)$ so $x_1 = (1)_2 = 1$, $x_2 = (10)_2 = 2$, $x_3 = (110)_2 = 6$, and $x_4 = (1001)_2 = 9$. We also think of $x_4x_3 = (1001110)_2 = 78$.

End of Example

The set A is the set of all numbers $x_rx_{r-1}\ldots x_1$ such that

1. For $1 \leq i \leq r-2$ the leftmost bit of x_i is 0. Note that when we add together two numbers in A the first $r-2$ blocks will add with no carries.

2. $\sum_{i=1}^{r-2} x_i^2 = x_rx_{r-1}$

Example: Consider the number $(1011001101100010101011010)_2$. We break this into blocks to get $(0000010 : 110011 : 01100 : 0101 : 011 : 01 : 0)_2$. Note that there are $r = 7$ blocks and the rightmost $r-2 = 5$ of them all have a 0 as the leftmost bit. The first 5 blocks, reading from the right, as base 2 numbers, are $0 = 0$, $01 = 1$, $011 = 3$, $0101 = 5$, $01100 = 12$. The leftmost two blocks merged together are $0000010110011 = 179$. Note that $0^2+1^2+3^2+5^2+12^2 = 179$.

Hence the number $(10110011011000101011010)_2$ is in A.
End of Example

We omit the proof that A is 3-free, but note that it uses Fact 1.9.

How big is A? Once you fill in the first $r-2$ blocks, the content of the remaining two blocks is determined and will (by an easy calculation) fit in the allocated $r+(r-1)$ bits. Hence we need only determine how many ways the first $r-2$ blocks can be filled in. Let $1 \le i \le r-2$. The ith block has i places in it, but the leftmost bit is 0, so we have $i-1$ places to fill, which we can do 2^{i-1} ways. Hence there are $\prod_{i=1}^{r-2} 2^{i-1} = \prod_{i=0}^{r-3} 2^i = 2^{(r-2)(r-3)/2}$.

$(r-2)(r-3) \ge (\sqrt{2\lg n}-3)(\sqrt{2\lg n}-4) = 2\lg n - 7\sqrt{2\lg n} + 12$

So

$(r-2)(r-3)/2 \ge \lg n - 3.5\sqrt{2\lg n} + 6$

So

$2^{(r-2)(r-3)/2} \ge 2^{\lg n - 3.5\sqrt{2\lg n}+6} \sim n^{1-\frac{3.5\sqrt{2}}{\sqrt{\lg n}}}$ ∎

6 3-Free Subsets of Size $n^{1-\frac{2\sqrt{2}}{\sqrt{\lg n}}}$: The Sphere Methods

In Sections 3, 4, and 5 we presented constructive methods for finding large 3-free sets of $[n]$ for large n. In this section we present the Sphere Method which is nonconstructive.

The result and proof in this section are due to Behrend [?, ?]. We will express the number in a base and put a condition on the representation so that the numbers do not form a 3-AP. It will be helpful to think of the numbers as vectors.

Let $n \in \mathbb{N}$. We want to find a large 3-free subset of $[n]$. Let d be a number to be picked later. We will work in base $2d+1$. Hence every number in $[n]$ is written with L digits from $\{0, \ldots, 2d+1\}$ where $k = \log_{2d+1} n$.

Def 6.1 Let x be expressed in base $2d+1$ as $\sum_{i=0}^{k} x_i(2d+1)^i$. Let $\vec{x} = (x_0, \ldots, x_k)$ and $|\vec{x}| = \sqrt{\sum_{i=0}^{k} x_i^2}$.

The set $A_{d,s,k}$ defined below is the set of all numbers that, when interpreted as vectors, have norm s (norm is the square of the length). These vectors are all on a sphere of radius $\sqrt{s}$.

Def 6.2 Let $d, s, k \in \mathbb{N}$.

$$A_{d,s,k} = \left\{ x : x = \sum_{i=0}^{k-1} x_i(2d+1)^i \wedge (\forall i)[0 \le x_i \le d] \wedge (|\vec{x}|^2 = s) \right\}$$

Lemma 6.3 *If $n, d, s, k \in \mathbb{N}$ then $A_{d,s,k}$ is 3-free.*

Proof: Assume, by way of contradiction, that $x, y, z \in A_{d,s,k}$ form a 3-AP. By Fact 1.9, $x + z = 2y$. Since this is no-carry addition we have $(\forall i)[x_i + z_i = 2y_i]$. Therefore $\vec{x} + \vec{z} = 2\vec{y}$, so $|\vec{x} + \vec{z}| = |2\vec{y}| = 2|\vec{y}| = 2\sqrt{s}$. Since $|\vec{x}| = |\vec{z}| = \sqrt{s}$ and $\vec{x}$ and $\vec{z}$ are not in the same direction $|\vec{x} + \vec{z}| < 2\sqrt{s}$. This is a contradiction. ∎

Lemma 6.4 *There exists s such that $|A_{d,s,k}| = \frac{d^{k-2}}{k}$.*

Proof: The set of ALL numbers in base $2d+1$ with each digits between 0 and d is $(d+1)^k$. We divide these numbers into those with norm 1, norm 2, etc until that max norm which is $k(d+1)^2$.

SO we have $(d+1)^k$ numbers split into $(k+1)(d+1)^2$ classes. Hence there exists and s such that there are approximately

$$\frac{d^k}{kd^2}$$

elements of norm s. Hence there is some s such that $|A_{d,s,k}| \geq \frac{d^{k-2}}{k}$. ∎

From the above one can pick k and hence d such that the following happens:

Theorem 6.5 $\mathrm{sz}(n) \geq \Omega(n^{1-\frac{2+\epsilon}{\sqrt{\lg n}}})$.