NUMBER OF ARITHMETIC PROGRESSIONS IN DENSE RANDOM SUBSETS OF $\mathbb{Z}/n\mathbb{Z}$

ROSS BERKOWITZ

Abstract. We examine the behavior of the number of $k$ term arithmetic progressions in a random subset of $\mathbb{Z}/n\mathbb{Z}$. If $k = 3$ and the subset is chosen uniformly at random, then we show that the resulting distribution, while obeying a central limit theorem, doesn’t obey a local limit theorem. Additionally we prove similar results in the case of larger $k$ and differing element inclusion probabilities. The methods involve examining the random variable with respect to the Walsh/Fourier basis and a lemma concerning when sums of two random variables can be “smooth”.

1. Introduction

Understanding the asymptotic behavior of sums of dependent random variables is a fundamental question in probability theory and combinatorics today. One particular random variable that has received some attention is the number of arithmetic progressions in a random subset of $\mathbb{Z}/n\mathbb{Z}$. For any subset $S \subset \mathbb{Z}/n\mathbb{Z}$ we define $k\text{AP}(S)$ to count the number of $k$-term arithmetic progressions contained entirely in the set $S$. Our underlying probability space is choosing a random set $S$ by including each element of $\mathbb{Z}/n\mathbb{Z}$ independently at random with probability $p \in (0, 1)$, where $p$ is a fixed constant not depending on $n$. The natural question which arises is how well can we understand the distribution of $k\text{AP}(S)$ as $n$ grows?

One natural statement one can prove is that if $k$ and $p$ are fixed then $k\text{AP}$ obeys a central limit theorem. That is, if we set $\mu_n = \mathbb{E}[k\text{AP}(S)]$ and $\sigma_n^2 = \text{Var}(k\text{AP})$ then for any fixed $a, b$

$$\Pr\left[ a \leq \frac{k\text{AP} - \mu_n}{\sigma_n} \leq b \right] = \frac{1}{\sqrt{2\pi}} \int_a^b \exp\left(-\frac{t^2}{2}\right) \, dt + o(1)$$

A natural subsequent guess is that the distribution of $k\text{AP}$ is “smooth” and that nearby integers are each as likely as one another. One might guess then, that a local limit theorem estimating pointwise probabilities of $k\text{AP}$ of the following form might hold for any integer $x$:

$$\Pr[X_n = x] = \frac{1}{\sigma_n \sqrt{2\pi}} \exp\left(\frac{-(x - \mu_n)^2}{2\sigma_n^2}\right) + o\left(\frac{1}{\sigma_n}\right)$$

However this guess turns out to be false.

Theorem 1. Fix $p = \frac{1}{2}$ and $k = 3$. Then for all sufficiently large $n$ prime there is some point $x$ such that

$$\left| \Pr[3\text{AP} = x] - \frac{1}{\sigma_n \sqrt{2\pi}} \exp\left(\frac{-(x - \mu_n)^2}{2\sigma_n^2}\right) \right| = \Omega\left(\frac{1}{\sigma_n}\right)$$

We first discovered this by sampling uniformly random subsets of $\mathbb{Z}/101\mathbb{Z}$ and counting the number of length 3 arithmetic progressions. This histogram of our results may be found in Figure 1. Interestingly, it should be noted that subsequently and independently a study of Cai, Chen, Heller, and Tsegaye [CCHT18] also conjectured that such a local limit theorem failed, but did not have a proof.

1Unfortunately, I wasn’t able to find a proof of this fact in the literature but dare not take credit for proving it.
Additionally, we also explore whether a local limit theorem might hold for $k \geq 4$ or other values of $p$. We do not have a complete classification of when such a limit theorem might hold, but we can show that for any $k$ fixed and $p$ sufficiently large, that $k\text{AP}$ doesn’t obey a local limit theorem.

**Theorem 2.** Assume $k \geq 3$ fixed. Then there is some $p_k < 1$ such that for all $p \in (p_k, 1)$ and $n$ sufficiently large and prime there is some number $x \in \mathbb{N}$ such that

$$\left| \Pr[k\text{AP} = x] - \frac{1}{\sigma_n \sqrt{2\pi}} \exp \left( -\frac{(x - \mu_n)^2}{2\sigma_n^2} \right) \right| = \Omega \left( \frac{1}{\sigma_n} \right)$$

1.1. **Related Work.** A lot of attention has been given to understanding the large deviation probability of $k\text{AP}$, particularly in the sparse set regime where $p \to 0$. For example, Kohayakawa, Łuczak, and Rödl showed that there is a constant $C$ such that if $S$ is chosen uniformly from all sets containing $[C \sqrt{n}]$, then with high probability $k\text{AP}(S) \geq 1$. Recently, Warnke [War17], Bhat­tacharya, Ganguly, Shao, and Zhao [BGSZ16], and Harel, Mousset, and Samotij [HMS19] found precise upper tail bounds for $k\text{AP}$ in the sparse regime, while Janson and Warnke [JW16] proved lower tail bounds.

Additionally in recent work, Barhoumi-Andréani, Koch and Liu [BAKL19] proved a bivariate central limit theorem for $(k\text{AP}, \ell\text{AP})$, understanding the joint distribution of the number of length $k$ and $\ell$ arithmetic progressions in sparse random sets.

1.2. **Outline of our methods and the paper.** Our methods for proving Theorems 2 and 1 involve analyzing the structure of $k\text{AP}$ as a low degree polynomial using the $p$-biased fourier basis for functions $f : [2]^n \to \mathbb{R}$. This analysis shows that $k\text{AP}$ is very heavily concentrated on degree 1 terms. Using this information it is possible to express $k\text{AP}$ as the sum of two random variables.

---

These theorems and related work provide a deeper understanding of the distribution of arithmetic progressions in random sets, which is crucial for various applications in combinatorics and theoretical computer science.
X and Y, where X is the degree 1 part of X, while Y is the rest of the polynomial representation of \(k\text{AP}\). X will only take values on a very sparse set of integers, and so we prove Lemma 2 which says that if \(X + Y\) is distributed according to a discrete Gaussian, and X is distributed on a very sparse set of integers, then Y must have large variance. However, we can compute the variance of Y to be small.

Section 2 defines our random variable and the tools we will be using throughout the paper. Section 3 is our analysis of kAP using the p-biased basis. In section 4 we prove Lemma 2 while in sections 5 and 6 we use this lemma to prove theorems 2 and 4 respectively.

2. Definitions and Preliminaries

2.1. Arithmetic Progressions in \(\mathbb{Z}/n\mathbb{Z}\). We define an arithmetic progression of length k to be a k-tuple of integers \((a_1, a_2, a_3, \ldots, a_k)\) such that for some integer \(1 \leq t \leq \frac{n-1}{2}\) and all \(1 \leq i \leq k-1\) we have \(a_{i+1} = a_i + t\). The main object of study will be the \(k\)-AP counting function.

**Definition 1.** Fix any natural number \(k \geq 3\) and \(n \in \mathbb{N}\). For any \(S \subset \mathbb{Z}/n\mathbb{Z}\) let \(k\text{AP}(S)\) be the number of length \(k\) arithmetic progressions contained in \(S\). Identifying \(S\) with the indicator vector \(x \in \{0,1\}^n\) this is

\[
k\text{AP}(S) := k\text{AP}(x) := \sum_{a \in [n]} \prod_{i=0}^{k-1} x_{a + i\ell}
\]

This definition counts every set which could form an arithmetic progression at least once. If \(n\) is prime it counts each arithmetic progression exactly once, and there are \(\binom{n}{2}\) \(k\) term arithmetic progressions. It should be noted that in the case where \(n\) is composite this definition will count some sets as multiple arithmetic progressions (e.g. if \(n = 6\) then \(\{0,3\}\) will be counted by both the sequence \((0,3,0)\) and \((3,0,3)\)). To avoid this mild difficulty we will assume throughout that \(n\) is prime.

Our main lemma will be applicable when a random variable has a discrete support with large gap sizes. To capture that we use the following notation for the distance between an element and a set in \(\mathbb{R}\).

**Definition 2.** For an element \(x \in \mathbb{R}\) and \(L \subset \mathbb{R}\) we will use \(d(x,L)\) to denote the distance from \(x\) to \(L\) that is \(d(x,L) := \inf(|x-\ell|, \ell \in L)\).

To reduce notational clutter we will use \(N_{\mu,\sigma}(x)\) as a shorthand for the approximate pointwise probabilities of the discrete Gaussian of mean \(\mu\) and standard deviation \(\sigma\). That is

\[
N_{\mu,\sigma}(x) := \frac{1}{\sigma\sqrt{2\pi}} \exp\left(-\frac{(x-\mu)^2}{2\sigma^2}\right)
\]

2.2. Our probability space and the p-biased Fourier basis. In this paper we analyze the behavior of \(k\text{AP}\) on a random subset of \([n]\) where each \(i \in [n]\) is included independently with probability \(p\). Throughout \(p\) will be treated as a fixed constant \(p \in (0,1)\) not depending on \(n\). For simplicity, we also assume that \(n\) is prime to ensure that there are always \(\binom{n}{2}\) \(k\) term arithmetic progressions in \(\mathbb{Z}/n\mathbb{Z}\). \(k\text{AP}\) is a degree \(k\) polynomial in the indicator variables \(x_i\), which take the value 1 if \(i\) is in the chosen set, and 0 otherwise. In this sense \(k\text{AP}\) is a function from \(\{0,1\}^n \to \mathbb{R}\), and our probability space is \(\{0,1\}^n\) with each vector \(x \in \{0,1\}^n\) having probability \(p^{|x|}(1-p)^{n-|x|}\), where \(|x|\) is the Hamming weight of \(x\). Throughout we will write expectations implicitly with respect to this probability space. That is for any \(f : \{0,1\}^n \to \mathbb{R}\) we write

\[
\mathbb{E}[f] := \mathbb{E}[f(x)] := \sum_{x \in \{0,1\}^n} p^{|x|}(1-p)^{n-|x|} f(x)
\]
To make our computations easier we use a rescaled version of these variables with mean 0 and variance 1, sometimes called the $p$-biased Fourier basis.

**Definition 3 (Fourier Basis).**

$$
\chi_i := \chi_i(x_i) = \frac{x_i - p}{\sqrt{p(1-p)}} = \begin{cases} 
-\sqrt{\frac{p}{1-p}} & \text{if } x_i = 0 \\
\sqrt{\frac{1-p}{p}} & \text{if } x_i = 1 
\end{cases}
$$

For $S \subset [n]$ set $\chi_S = \prod_{i \in S} \chi_i$. For $S = \emptyset$ we have $\chi_\emptyset \equiv 1$. Additionally, the Fourier transform $\hat{f} : 2^{[n]} \to \mathbb{R}$ is the function valued on subsets of $[n]$ defined by

$$
\hat{f}(S) := \mathbb{E}[\chi_S f]
$$

Some useful definitions and theorems about these random variables which we will need are presented below. For a more thorough treatment and proofs, see [O’D14]. The following theorems tell us that the random variables $\chi_S$ form an orthonormal basis of the functions from $\{0,1\}^n \to \mathbb{R}$.

**Theorem 3.** *(Parseval’s/ Plancherel’s Theorem)* Let $S, T \subset [n]$ distinct subsets and $f : \{0,1\}^n \to \mathbb{R}$ the following hold

$$
\mathbb{E}[\chi_S^2] = 1
$$

$$
\mathbb{E}[\chi_S \chi_T] = 0
$$

As a consequence we also have

$$
||f||_2^2 := \mathbb{E}[f^2] = \sum_{S \subset \binom{[n]}{2}} \hat{f}(S)^2
$$

Finally, we note that this is also a formula for the variance of $f$, should it’s inputs be $p$-biased Bernoulli random variables.

$$
Var(f) = \mathbb{E}[f^2] - \mathbb{E}[f]^2 = \mathbb{E}[f^2] - \hat{f}(\emptyset)^2 = \sum_{S \neq \emptyset} \hat{f}(S)^2
$$

Additionally, it will be useful to break up our random variables into pieces based on their degree as a polynomial in the Fourier basis.

**Definition 4.** For any $S \subset [n]$ the degree of the monomial $\chi_S$ is $|S|$. For an arbitrary function $f$, we say that it has degree equal the degree of the largest monomial in its Fourier expansion. That is $\deg(f) = \max S(f(S) \neq 0) |S|$. Additionally we define the degree $k$ or degree at least/most $k$ parts of $f$ by

$$
f^=k := \sum_{|S|=k} \hat{f}(S) \chi_S
$$

$$
f^{>k} := \sum_{|S|>k} \hat{f}(S) \chi_S
$$

Similarly it will be helpful to refer to just the 2-norm of $f^=k$ and we sill use the notation

$$
W^k[f] := ||f^=k||_2 = \sum_{|S|=k} \hat{f}(S) \chi_S
$$

$$
W^[>k] := ||f^{<k}||_2 = \sum_{|S|>k} \hat{f}(S) \chi_S
$$
3. Properties of the \( k \)-AP counting function

Fix an integer \( 3 \leq k < n - 1 \), and let \( k\AP := k\AP_n \) denote the random variable counting the number of length \( k \) arithmetic progressions in the randomly chosen set \( S \subset [n] \), where each element of \([n]\) is included in \( S \) independently with probability \( p \). More formally, let \( x_i \) be the indicator random variable for inclusion of the element \( i \) in the random set \( S \subset \mathbb{Z}_n \), and assume that \( n \) is prime. Then we recall our definition

\[
k\AP := k\AP(x) := \sum_{a \in [n]} \prod_{i=0}^{k-1} x_{a+i\ell}
\]

First, we compute the Fourier transform of \( k\AP \) by substituting \( x_i = \sqrt{p(1-p)} \chi_i + p \).

\[
k\AP(x) = \sum_{a \in [n]} \prod_{i=0}^{k-1} x_{a+i\ell} = \sum_{a \in [n]} \prod_{i=0}^{k-1} \left( \sqrt{p(1-p)} \chi_{a+i\ell}(x) + p \right)
\]

\[
= \sum_{a \in [n]} \sum_{0 < \ell < \frac{n}{2}} p^{k-|S|/2} (1-p)^{|S|/2} \chi_S(x)
\]

\[
= \sum_{S \subset [n]} a_S p^{k-|S|/2} (1-p)^{|S|/2} \chi_S(x)
\]

where \( a_S \) is the number of \( k \)-AP’s containing all of the elements of \( S \). We will need bounds on the following quantity for integers \( 1 \leq s \leq k \)

\[
Q_s := \sum_{|S|=s} k\AP(S)^2 = p^{2n-s}(1-p)^s \sum_{|S|=s} a_S^2
\]

which will bound the contribution of the weight \( s \) Fourier coefficients of the \( k\AP \) random variable.

3.1. 3AP special case. For the case of \( k = 3 \) (denoted 3AP), we note that every element of \( \mathbb{Z}/n\mathbb{Z} \) lies in exactly \( \frac{3(n-1)}{2} \) 3-term arithmetic progressions (assuming that \( n \geq 5 \)). Every doubleton \((i, j) \in \binom{n}{2}\) is in exactly 3 3-AP’s. Lastly we note that the triples \( S = \{i, j, k\} \) such that 3APS \( \neq 0 \) are exactly the 3-AP’s themselves. Combining all these notes gives the following Lemma

**Lemma 1.** The transform of 3AP is

\[
3\AP(S) = \begin{cases} 
\frac{n^3}{2} & \text{if } S = \emptyset \\
\frac{3(n-1)^3}{2} & \text{if } |S| = 1 \\
3p^2(1-p) & \text{if } |S| = 2 \\
p^{1.5}(1-p)^{1.5} & \text{if } S \text{ is a 3-AP} \\
0 & \text{else}
\end{cases}
\]

Therefore

\[
W^1[3AP] = \frac{9p^5(1-p)n(n-1)^2}{4}
\]

\[
W^2[3AP] = 9p^4(1-p)^2\binom{n}{2}
\]

\[
W^3[3AP] = p^3(1-p)^3\binom{n}{2}
\]
3.2. Estimating $k\hat{A}P$. In this section we estimate $k\hat{A}P(S)$ for general integers $k$ and any set $S \subset [n]$. For $S = \varnothing$, this is just $k\hat{A}P(S) = \mathbb{E}[k\hat{A}P] = p^k\binom{k}{2}$. For singleton sets $S = \{i\}$ symmetry and double counting reveal that every element $i \in [n]$ appears in exactly $\frac{k(n-1)}{2} := a_{\{i\}}$ $k-AP$'s. Plugging into equation 1 yields

$$W^1(k\hat{A}P) = \sum_i k\hat{A}P(i)^2 = np^{2k-1}(1-p)\left(\frac{k(n-1)}{2}\right)^2 = p^{2k-1}(1-p)\frac{k^2}{4}n^3 + O(n^2)$$

For $|S| \geq 2$ and $k \geq 4$, calculating $k\hat{A}P(S)$ and $W^2(k\hat{A}P)$ can require a bit more effort. Thankfully, for our purposes it will be enough to give some relatively simple upper bounds. To do this we upper bound $a_S$, the number of $k-AP$'s containing all the elements of $S$. Picking any two elements of $S$ and specify the locations they will take in the progression (e.g. saying the first and fourth numbers of the AP are 5 and 17) determines a unique $k-AP$. Additionally, reflecting these positions across $(k+1)/2$ defines the same $k-AP$ listed in reverse order. Together these observations show that $a_S \leq \binom{k}{2}$ for any $2 \leq |S| \leq k - 1$. Additionally we have for free that $|S| \geq k$ then $a_S$ is 1 if $S$ is a $k-AP$ and 0 otherwise.

We can also bound the number of $S$ such that $k\hat{A}P(S)$ is nonzero by noting that there are exactly $\binom{\binom{n}{2}}{k}$ $k-AP$'s, each one containing exactly $\binom{k}{2}$ subsets of size $s$. Therefore we know that $k\hat{A}P$ is supported on at most $\binom{\binom{n}{2}}{k}$ sets of size $s$. Combining these estimates gives us the following bounds

$$|k\hat{A}P(S)| = a_S p^{k-|S|/2}(1-p)^{|S|/2} \leq \binom{k}{2} p^{k-|S|/2}(1-p)^{|S|/2}$$

$$W^s(k\hat{A}P) = \sum_{|S|=s} k\hat{A}P(S)^2 = p^{2k-s}(1-p)^s \sum_{|S|=s} a_S^2 \leq p^{2k-s}(1-p)^s \binom{k}{s} \binom{n}{2} \binom{k}{2}^2$$

$$\leq \frac{p^{2k-s}(1-p)^s k^{s+4} n^2}{8s!}$$

so we can conclude that

$$W^{>1}(k\hat{A}P) = \sum_{|S|>1} k\hat{A}P(S)^2 \leq \sum_{s=1}^k p^{2k-s}(1-p)^s \binom{k}{s} n^2 k^4 \leq \gamma n^2$$

(2) 

Where $\gamma := \gamma_p := \max_{s=2}^k p^{2k-s}(1-p)^s \binom{k}{s} k^4$ Finally, applying Theorem 3 yields

$$Var(k\hat{A}P) = \sum_{s \geq 1} W^s(k\hat{A}P) = p^{2k-1}(1-p)\frac{k^2}{4}n^3 + O(n^2)$$

4. Main Lemma

Lemma 2. Assume that $X,Y,Z$ are integer valued variables such that $X = Y + Z$. Fix some $0 < \epsilon, \delta < 1$ Additionally assume that for some fixed set $L \subset \mathbb{Z}$ we have

(1) $\Pr(Y \in L) > 1 - \epsilon$

(2) Let $L_T := \{x \in \mathbb{Z} \text{ s.t. } d(x, L) \leq T\}$. Then for any $x \in L_T$ there is a unique $y_x \in \mathbb{Z}$ such that $|x - y_x| \leq T$ and $\Pr[Y = y_x] \neq 0$. Note it follows that $y_x \in L$.

(3) For any integers $x_1, x_2 \in L_T$, if $|x_1 - x_2| \leq 2T$ then $\Pr[X = x] \geq (1 - \delta) \Pr[X = x_2]$.

Then we have that $\mathbb{E}[Z^2] \geq T(T+1)(1-\delta)(1-\epsilon)$

This lemma is our main engine for proving that a random variable $X$ is not smoothly distributed as a discrete Gaussian. The idea is that if $Y$ takes values only in a subset of the integers with large gap sizes, as per conditions 1 and 2, but $X + Y$ is ”smoothly” distributed as per condition 3,
then the variance of $Z$ has to comparable to that of a uniform distribution on $T$ elements. In the applications that follow, we will know $\text{Var}(Z)$ to be small ahead of time, and so be able to show that condition 3 does not hold.

Proof. Let $B$ denote the event that $X \in L_T$ and define the auxiliary random variable $\bar{X} := d(X, L)$. If $x \in L_T$ then it follows from condition 2 that $Z \geq \bar{X}$. Therefore we have $\mathbb{E}[Z^2 | B] \geq \mathbb{E}[X^2 | B]$, and so will work on computing the latter conditional expectation. By definition we have

$$\Pr(B) = \sum_{y \in L} \sum_{t = -T}^{T} \Pr[X = y + i]$$

Next we use condition 3 to compute that for any $y \in L$ and $|t| \leq T$ we have

$$\Pr[X = y + t] = \frac{1}{2T+1} \sum_{i = -T}^{T} \Pr[X = y + t] \Pr[X = y + i] \geq \frac{1 - \delta}{2T+1} \sum_{i = -T}^{T} \Pr[X = y + i]$$

Therefore it follows that

$$\sum_{y \in L} \sum_{t = -T}^{T} \Pr[X = y + t] t^2 \geq \sum_{y \in L} \sum_{t = -T}^{T} t^2 \frac{1 - \delta}{2T+1} \sum_{i = -T}^{T} \Pr[X = y + i]$$

$$= \sum_{i = -T}^{T} \frac{t^2(1 - \delta)}{2T+1} \sum_{y \in L} \sum_{t = -T}^{T} \Pr[X = y + i]$$

$$= \frac{T(T+1)(1 - \delta)}{3} \Pr(B)$$

And so we have computed the conditional expectation

$$\mathbb{E}[\bar{X}^2 \mid B] = \frac{\sum_{x \in B} \bar{X}^2 \Pr[X = x]}{\Pr(B)} \geq \frac{\sum_{y \in L} \sum_{t = -T}^{T} \Pr[X = y + t] t^2}{\Pr(B)} \geq \frac{T(T+1)(1 - \delta)}{3}$$

Further, we note that $\mathbb{E}[Z^2 \mid X \notin B, Y \in L] \geq T^2 \geq T(T+1)(1 - \delta)/3$ and so it follows that

$$\mathbb{E}[Z^2] \geq \Pr(X \in L_T) \mathbb{E}[\bar{X}^2 \mid X \in L_T] + \Pr[X \notin L_T, Y \in L] \mathbb{E}[Z^2 \mid X \notin L_T, Y \in L]$$

$$+ \Pr[X \notin L_T, Y \notin L] \mathbb{E}[Z^2 \mid X \notin L_T, Y \notin L]$$

$$\geq (1 - \Pr[X \notin L_T, Y \notin L]) \frac{T(T+1)(1 - \delta)}{3} \geq (1 - \epsilon) \frac{T(T+1)(1 - \delta)}{3}$$

\[ \square \]

5. kAP doesn’t obey a local limit theorem

In this section we prove that for any fixed $k$ if the element inclusion probability $p$ is larger than some fixed constant, then kAP is not distributed according to a discrete Gaussian supported on the integers.

Theorem 2 Assume $k \geq 3$ fixed. Let $\mu_n := \mathbb{E}[k\text{AP}]$ and $\sigma_n := \text{Var}(k\text{AP})$. Then there is some constant $p_k < 1$ depending only on $k$ such that for all $p \in (p_k, 1)$ and all $n$ prime and sufficiently large there is some point $a \in \mathbb{N}$ such that

$$|\Pr(k\text{AP} = a) - N_{\mu_n, \sigma_n}(x)| = \Omega(1/\sigma_n)$$
Proof. To apply Lemma 2 to kAP for we define our random variables to be $X = kAP$, $Y = \lfloor kAP = 1 \rfloor$ and $Z = X - Y$. We note that if we define $\ell = \sum_{i=1}^{n} x_i$ then
\[
\sum_{i=1}^{n} x_i = \sum_{i=1}^{n} \left( \frac{x_i - p}{\sqrt{p(1-p)}} \right) = n \sqrt{\frac{p}{1-p}} + \frac{\ell}{\sqrt{p(1-p)}}
\]
Therefore we see that
\[
kAP = 1 = \frac{k(n-1)}{2} p^{-\frac{1}{2}} (1-p)^{\frac{1}{2}} \sum_{i=1}^{n} x_i = \frac{kn(n-1)p^k}{2} + \frac{k(n-1)p^{k-1}}{2} \ell
\]
takes values in a lattice with gaps of size $\frac{k(n-1)p^{k-1}}{2}$. So it follows that the gaps between values in the support of $Y$ are at least $\frac{k(n-1)p^{k-1}}{2} - 1$. Additionally, by a Chernoff Bound⁴, we know that there is some fixed constant $C$ depending only on $p$ such that for all $n$ $\text{Pr}[\ell - pn] \geq C \sqrt{n} < .99$. So we can take $L$ to be
\[
L := \left\{ \frac{kn(n-1)p^k}{2} + \frac{k(n-1)p^{k-1}}{2} m \text{ s.t. } m \in \mathbb{Z}, |m - pn| < C \sqrt{n} \right\}
\]
Additionally, if we let $Z' = kAP \geq 2$ then $|Z - Z'| \leq 1$ and we can use Cauchy-Schwarz and equation 2 find that
\[
\text{Var}(Z) \leq \text{E}[Z^2] = \text{E}\left[(Z' + |Z - Z'|)^2\right] \leq \text{E}[Z'2] + 2\sqrt{\text{E}[Z'^2]} + 1 \leq k\gamma n^2 + O(n)
\]
So now we can apply Lemma 2. Fix $\delta = \frac{1}{2}$. As noted above we may take $T = \frac{k(n-1)p^{k-1}}{4} - 1$ and $\epsilon = .01$. By Lemma 2 if condition 3 of the lemma were to hold, then it would follow that $\text{Var}(Z) \geq \frac{.99 \gamma^2 n^2 }{ 2 T^2}$ and so
\[
k\gamma n^2 + O(n) \geq \frac{.99 \gamma^2 n^2 p^{2k-2}}{96} + O(n)
\]
But by definition of $\gamma$ for some integer $2 \leq s \leq k$ we have
\[
\gamma = k^4 \left( \frac{k}{s} \right) p^{-s} (1-p)^{k-s} \leq k^4 2^k p^{k+2} (1-p)^2
\]
Therefore if the above inequality holds for $n$ sufficiently large, we must have that
\[
k^5 2^k p^{k+2} (1-p)^2 \geq \frac{.99 \gamma^2 p^{2k-2}}{96}
\]
and so
\[
(1-p)^2 \geq \frac{.99 p^{k-4}}{k^5 \cdot 96 \cdot 2^k}
\]
There exists some constant $p_k < 1$ such that for all $p_k < p < 1$ the above inequality must be false. Therefore condition 3 of Lemma 1 must not hold, and so there are points $x, y \in \mathbb{N}$ such that $|x - \mu|, |y - \mu| = O(n^{1.5}) = O(\sigma)$ and $|x - y| \leq 2T = O(n)$ but $\text{Pr}[kAP = x] \geq 2 \text{Pr}[kAP = y]$. However we can compute directly that $N_{\mu_n, \sigma_n}(x), N_{\mu_n, \sigma_n}(y) = O(\sigma_n^{-1})$ and
\[
|N_{\mu_n, \sigma_n}(x) - N_{\mu_n, \sigma_n}(y)| = \frac{1}{\sigma_n \sqrt{2\pi}} \left[ \exp \left( -\frac{(x - \mu_n)^2}{2\sigma_n^2} \right) - \exp \left( -\frac{(y - \mu_n)^2}{2\sigma_n^2} \right) \right] = O \left( \frac{1}{\sqrt{n}\sigma_n} \right)
\]
But therefore it must be the case that for at least one of $x$ or $y$ we have $\text{Pr}[kAP = x] - N_{\mu_n, \sigma_n}(x) \geq \frac{1}{2} N_{\mu_n, \sigma_n}(x) - o(n^{-1/2}\sigma_n^{-1})$, finishing the proof. \(\square\)

³for example see Corollary A.1.14 in [AS08]
6. **The special case $k = 3$ and $p = \frac{1}{2}$**

In general for a fixed $k$, we do not attempt to obtain the best relationship between the probability $p$ and the lack of a local limit theorem for $k\text{AP}$. However, the particular case of a uniformly random subset of $\mathbb{Z}/n\mathbb{Z}$ and a three term arithmetic progression is of particular interest. The argument in the previous section doesn’t yield any result in the $k = 3$ $p = \frac{1}{2}$ case, and so we take a slightly more detailed approach to applying Lemma 2. Instead of using $k\text{AP} = 1$ as our random variable with large integral gaps for Lemma 4 we note that

$$3\text{AP}^2 = \frac{3}{8} \sum_{|S|=2} \chi_S = \frac{3}{8} \left( \frac{\sum_{i=1}^{n} \chi_i)^2}{2} - n \right)$$

So we may combine the degree 1 and 2 terms of $3\text{AP}$ into a single function of $\ell := \sum_{i=1}^{n} \chi_i$. In particular if we define $f$ to be the function

$$f(x) = \frac{3}{8} (x^2 - n) + \frac{3(n-1)}{16} x + \frac{\binom{n}{2}}{8}$$

then we have that $3\text{AP} = f(\ell) + 3\text{AP}^3$.

With an eye to applying Lemma 2 let $Y = f(\ell)$ and $Z = 3\text{AP}^3$.

To apply Lemma 4 we replace $Y$ with $Y' := [Y]$ (the nearest integer to $Y$) and $Z$ with $Z' := X - [Y]$ to make sure are random variables are integer valued. Since this doesn’t change any of the values taken by $Y$ or $Z$ by more than 1, it will not change the granularity of $Y$ or the variance of $Z$ by an appreciable amount. Specifically, we see that $|Z - Z'| < 1$ and subsequently

$$\mathbb{E}[Z'^2] = \mathbb{E}[Z^2] + 2Z(Z - Z') + (Z - Z')^2 \leq \mathbb{E}[Z^2] + 2\sqrt{\mathbb{E}[Z^2]} + 1 = \left(\frac{\binom{n}{2}}{64}\right) + O(n)$$

To determine the parameter $T$, how far apart the support of $Y'$ is separated set $L := \{[f(x)] \mid x \leq \sqrt{2\log(200)}\sqrt{n}\}$. By a Chernoff Bound we have that $\Pr([Y] \notin L) < \frac{1}{100}$. We note that $f$ is monotone increasing for $|x| \leq \frac{n-1}{4}$, and so the elements of $L$ all have distance at least

$$[f(\ell + 2)] - [f(\ell)] \geq \frac{3(n-1)}{8} + 6\ell + 4 - 2$$

from one another. Therefore in applying Lemma 2 we may take $T = \frac{3(n-1)}{16}(1 + O(n^{-1/2}))$. However, we know that $\text{Var}(Z') = \frac{\binom{n}{2}}{64} + O(n)$ and so if assumption 3 holds for some $\delta$ it must satisfy

$$\frac{\binom{n}{2}}{64} + O(n) \geq (1 - \epsilon)(1 - \delta)\frac{T(T + 1)}{3} = .99(1 - \epsilon) \frac{3}{256} n^2(1 + o(1))$$

Looking at the leading $n^2$ term, we see that for $n$ sufficiently large

$$\delta \geq \left(\frac{.99 \frac{3}{256} - 1}{128}\right) \geq .003$$

Therefore if we take $\delta = .002$ then condition 3 of Lemma 2 must not hold. Let $\mu_n = \mathbb{E}[3\text{AP}] = \frac{\binom{n}{2}}{8}$ and $\sigma_n^2 := \text{Var}(3\text{AP}) = \frac{9n^3}{256} + O(n^2)$. Then there are points $x, y \in \mathbb{N}$ such that

- $|x - \mu| \leq f(\sqrt{2n\log(200)}) = O(\sigma_n)$
- $|x - y| \leq n$
- $\Pr[3\text{AP} = x] \geq .998 \Pr[3\text{AP} = y]$, and therefore $|\Pr[3\text{AP} = x] - \Pr[3\text{AP} = y]| \geq .002 \Pr[3\text{AP} = y]$
However we see that $N_{\mu_n, \sigma_n}(x), N_{\mu_n, \sigma_n}(y) = \Omega(\frac{1}{\sigma_n})$ and additionally that $|N_{\mu_n, \sigma_n}(x) - N_{\mu_n, \sigma_n}(y)| = o(\frac{1}{\sigma_n})$. Therefore for at least one of $x$ or $y$ we must have that $|\Pr[3AP = x] - N_{\mu_n, \sigma_n}(x)| \geq \frac{0.01 + o(1)}{\sigma_n}$.

We state our conclusion as our theorem

**Theorem 1.** For any $n$ there is some point $x$ such that $|\Pr[3AP = x] - N_{\mu_n, \sigma_n}(x)| = \Omega(1/\sigma)$.

7. Conclusion

We conclude by pointing out some of the major questions we still have about this phenomenon. Firstly, we note that there is a large gap between the theorems we proved, and a total explanation of the behavior exhibited in Figure 1. An ideal theorem could perhaps prove that the distribution of $kAP$ tends in some sense to the lumpy sum of two Gaussians seemingly exhibited in the figure. Failing that, at least one could hope to understand how wildly the distribution oscillates in the following sense

**Question 1.** For what constant (if any) $C$ does it hold that for any $n$ there exists integers $x, y$ such that $|x - \mu|, |y - \mu| < \sigma/100$ which satisfy $\Pr[kAP = x] \Pr[kAP = y] \geq C$.

Our theorem as proved shows that we can take $C \geq 1.03$, however visual inspection of the data provided suggest that $C$ could be taken to be significantly larger. It is also possible that $C$ is not bounded, which would be an interesting outcome as well.

Additionally it is as of now for what values of $p$ does $kAP$ obey a local limit theorem. Thus we ask the question

**Question 2.** Let $k \geq 3$ be fixed. Is there a constant $p \in (0, 1)$ such that if $S$ is chosen by including each element of $\mathbb{Z}/n\mathbb{Z}$ with probability $p$ then

$$\Pr[kAP(S) = x] = N_{\mu_n, \sigma_n}(x) + o(1/\sigma_n).$$

**References**

[AS08] Noga Alon and Joel H. Spencer. *The probabilistic method*. Wiley-Interscience Series in Discrete Mathematics and Optimization. John Wiley & Sons, Inc., Hoboken, NJ, third edition, 2008. With an appendix on the life and work of Paul Erdős.

[BAKL19] Yacine Barhoumi-Andréani, Christoph Koch, and Hong Liu. Bivariate fluctuations for the number of arithmetic progressions in random sets, 2019.

[BGSZ16] Bhaswar B. Bhattacharya, Shirshendu Ganguly, Xuancheng Shao, and Yufei Zhao. Upper tails for arithmetic progressions in a random set, 2016.

[CCHT18] Bryce Cai, Annie Chen, Ben Heller, and Eyob Tsegay. Limit Theorems for Descents in Permutations and Arithmetic Progressions in $\mathbb{Z}/p\mathbb{Z}$. *arXiv e-prints*, page arXiv:1810.02425, Oct 2018.

[HMS19] Matan Harel, Frank Mousset, and Wojciech Samotij. Upper tails via high moments and entropic stability. *arXiv e-prints*, page arXiv:1904.08212, Apr 2019.

[JW16] Svante Janson and Lutz Warnke. The lower tail: Poisson approximation revisited. *Random Structures Algorithms*, 48(2):219–246, 2016.

[O'D14] Ryan O'Donnell. *Analysis of boolean functions*. Cambridge University Press, 2014.

[War17] Lutz Warnke. Upper tails for arithmetic progressions in random subsets. *Israel J. Math.*, 221(1):317–365, 2017.