Limiting Behavior in Missing Sums of Sumsets

Aditya Jambhale[1], Rauan Kaldybayev[2], Steven J. Miller[3], and Chris Yao[4]

[1] Faculty of Mathematics, University of Cambridge
[2] Department of Mathematics, Williams College
Current address: Department of Mathematics, UC Davis
[3] Department of Mathematics, Williams College
[4] Department of Mathematics, Yale University
Current address: Department of Mathematics, UC Berkeley

Abstract. We study $|A+A|$ as a random variable, where $A \subseteq \{0, \dots, N\}$ is a random subset such that each $0 \le n \le N$ is included with probability $0 < p < 1$, and where $A+A$ is the set of sums $a+b$ for a, b in A. Lazarev, Miller, and O'Bryant studied the distribution of $2N+1-|A+A|$, the number of summands not represented in $A+A$ when $p = 1/2$. A recent paper by Chu, King, Luntzlara, Martinez, Miller, Shao, Sun, and Xu generalizes this to all $p \in (0,1)$, calculating the first and second moments of the number of missing summands and establishing exponential upper and lower bounds on the probability of missing exactly n summands, mostly working in the limit of large N. We provide exponential bounds on the probability of missing at least n summands, find another expression for the second moment of the number of missing summands, extract its leading-order behavior in the limit of small p, and show that the variance grows asymptotically slower than the mean, proving that for small p, the number of missing summands is very likely to be near its expected value.

Keywords: Sumsets; More sums than differences sets

Table of Contents

1 Introduction

Fix a real number $0 < p < 1$ and an integer $N \geq 0$, and let A be a random subset of $\{0, \ldots, N\}$ such that each n between 0 and N is included in A independently with probability p. We consider the sumset

$$A + A \;\coloneqq\; \{a + b : a, b \in A\} \subseteq \{0, \ldots, 2N\}\,. \tag{1.1}$$

There is an extensive literature on "more sums than differences" (MSTD) sets, defined as those sets A whose sumset cardinalities $|A + A|$ are greater than difference set cardinalities $|A - A|$, where $A - A$ is the set of elements $a - b$ with $a, b \in A$.

MSTD sets are unusual because addition is commutative while subtraction is anticommutative, and one would expect $A-A$ to usually have more elements than $A+A$; see for example [1,2,3,4,5,6,8,10,11,13,15,16,17,18,19,20,21,22,23,24,25,26].

While there were known constructions of infinite families of MSTD sets, these examples had density zero as $N \to \infty$. It was surprising when Martin and O'Bryant [14] proved that positive fraction of all sets $A \subseteq \{1, \ldots, n\}$ are MSTD. Martin and O'Bryant were also interested in the distribution of $|A + A|$ as a random variable and calculated some fundamental results, such as the expectation value of $|A + A|$ in the case $p = 1/2$. Lazarev, Miller, and O'Bryant [12] proved further results, such as exponential decay of the probability of missing many summands, and gave a rigorous proof to the observation that sumsets show a noticeable bias towards missing an even number of summands, for $p = 1/2$. The 2020 paper of [3] generalized [12]'s proofs to the case of arbitrary p. We cover some of these results while also proving certain new ones. In particular, we carefully study the second moment $\mathbb{E}\left[Y^2\right]$ and use it to show that the distribution of missing summands is sharply peaked around the mean for large N and small p.

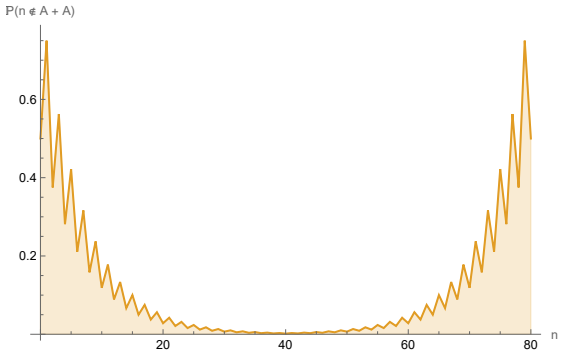
We note the following facts about the distribution of $A + A$.

1. The set $A + A$ is "almost full" in the middle. While numbers near N are almost certainly included in $A + A$, numbers close to 0 (the *left fringe*) or $2N$ (the *right fringe*) have a significant chance of being left out [27]. See Figure 1.
2. The set $A + A$ has "symmetry" around N in the sense that $|A + A|$ and $|2N - (A + A)|$ are identically distributed.
3. If $j - i > N$, the inclusions of i and j in $A + A$ are independent, but for general i and j they are not.

We continue to investigate the number of elements missing from $A + A$. We define the random variables Y, Z, W to count missing summands in the left fringe, right fringe, and the whole of $A + A$ respectively. Let Y be the number of integers at most N that are missing from $A + A$,

$$\begin{aligned} Y \;&\coloneqq\; |\,\{0 \leq n \leq N : n \notin A + A\}\,| \\ &=\; N + 1 - |(A + A) \cap \{0, \ldots, N\}\,|, \end{aligned} \tag{1.2}$$

Fig. 1. Probabilities of non-inclusion of n into $A + A$ for $0 \leq n \leq 2N$ and $p = 1/2$, $N = 40$.



let Z be the number of integers from $N+1$ to $2N$ that are missing from $A + A$,

$$\begin{aligned} Z &:= |\{N+1 \leq n \leq 2N : n \notin A + A\}| \\ &= N - |(A + A) \cap \{N+1, \ldots, 2N\}|, \end{aligned} \tag{1.3}$$

and W the number of integers up to $2N$ that are missing from $A + A$,

$$\begin{aligned} W &:= |\{0 \leq n \leq 2N : n \notin A + A\}| \\ &= 2N + 1 - |A + A| = Y + Z. \end{aligned} \tag{1.4}$$

Define X_n as the indicator variable for the *non*-inclusion of n in $A + A$:

$$X_n := [n \notin A + A] = \begin{cases} 1 & n \notin A + A \\ 0 & n \in A + A. \end{cases} \tag{1.5}$$

Then,

$$Y = \sum_{n=0}^{N} X_n, \quad Z = \sum_{n=N+1}^{2N} X_n, \quad W = \sum_{n=0}^{2N} X_n. \tag{1.6}$$

Note Y and Z have largely the same probability distributions due to the symmetry about N, except that Y ranges from 0 to $N+1$ while Z from 0 to N. We make use of this symmetry to simplify calculations, proving results about Y and using Theorem 1 to convert to similar statements about W.

As in [3] and [14], we have for $0 \leq n \leq N$,

$$\mathbb{P}(n \in A + A) = \begin{cases} 1 - (1 - p^2)^{\frac{n+1}{2}} & n \text{ odd} \\ 1 - (1 - p)(1 - p^2)^{n/2} & n \text{ even.} \end{cases} \tag{1.7}$$

We can use symmetry to write an analogous formula for $N < n \leq 2N$ as

$$\mathbb{P}(n \in A + A) = \begin{cases} 1 - (1 - p^2)^{\frac{(2N-n)+1}{2}} & n \text{ odd} \\ 1 - (1 - p)(1 - p^2)^{(2N-n)/2} & n \text{ even.} \end{cases} \tag{1.8}$$

Recall that $Y = \sum_{n=0}^{N} X_n$, so by linearity of expectation,

$$\begin{aligned}\mathbb{E}[Y] &= \sum_{n \text{ even}} (1-p)(1-p^2)^{n/2} + \sum_{n \text{ odd}} (1-p^2)^{\frac{n+1}{2}} \\ &= \left(\frac{2}{p^2} - \frac{1}{p} - 1\right) - \left(\sqrt{1-p^2}\right)^N \begin{cases} \frac{(2-p)(1-p^2)}{p^2} & N \text{ even} \\ \frac{(2-p-p^2)\sqrt{1-p^2}}{p^2} & N \text{ odd.} \end{cases}\end{aligned} \tag{1.9}$$

For the entire sumset, the expected number of missing summands is

$$\mathbb{E}[W] = \left(\frac{4}{p^2} - \frac{2}{p} - 2\right) - \left(\sqrt{1-p^2}\right)^N \begin{cases} \frac{4-2p-2p^2+p^3}{p^2} & N \text{ even} \\ \frac{(4-2p-p^2)\sqrt{1-p^2}}{p^2} & N \text{ odd.} \end{cases} \tag{1.10}$$

In §2, we study the number of missing summands in the left and right fringes. It is well known that the left and right fringes are independent when their lengths are smaller than $N/2$ [3], but larger sized fringes (of length $\geq N/2$) have not been studied extensively. While the left and right fringes are not truly independent in this case, we prove the following theorem, which intuitively says that Y and Z are "asymptotically independent".

Theorem 1. *For any $0 \leq m \leq 2N$,*

$$\left|\mathbb{P}(W = m) - \sum_{y=0}^{m} \mathbb{P}(Y = y)\,\mathbb{P}(Z = m - y)\right| \leq \frac{8}{p^2}(1-p^2)^{N/4}. \tag{2.5}$$

We say that as $N \to \infty$, W is the convolution of Y with Z.

In §3, we study the k^{th} moment of the number of missing summands $\mathbb{E}\left[Y^k\right]$ and bound the probability of missing at least n summands. We take a different approach than the authors of [27] and [3], who study $m_{n;p}(k) \coloneqq \mathbb{P}(2N + 1 - |A + A| = k)$ and $m_p(k) \coloneqq \lim_{n\to\infty} m_{n;p}(k)$, which allows us to obtain a simpler bound. For α defined in (3.3), we have the following.

Corollary 2. *For any real number $\varepsilon > 0$, (and again, for $n > 1/\alpha$),*

$$\begin{aligned}\mathbb{P}(Y \geq n) &= O\left(n\left(\sqrt{1-p^2}\right)^n\right) \\ &= O\left(\left(\sqrt{1-p^2} + \varepsilon\right)^n\right).\end{aligned} \tag{3.7}$$

We then improve on this exponential bound in §4 by using a more detailed estimate for the variance. For suitable λ_1 as defined in (4.3), we have the following.

Corollary 4. *We have*

$$\mathbb{P}(Y \geq n) = O\left((\lambda_1 + \varepsilon)^n\right) \tag{4.7}$$

for all $\varepsilon > 0$. *For* $p = 1/2$, $\lambda_1 = \varphi/2 \approx 0.81$ *where* φ *is the golden ratio. More precisely, for* $n > 1/\alpha'$,

$$\mathbb{P}\left(Y \geq n\right) \;\leq\; \left(\frac{2}{p^2} - \frac{1}{p} - 1\right) e^{-(n-1)(\alpha' - 1/n)} + \frac{2n\alpha' e^{-n\alpha'+1}}{\lambda_1}, \tag{4.8}$$

where $\alpha' \coloneqq \log\left(1/\lambda_1\right)$.

We study the behavior of the second moment $\mathbb{E}\left[Y^2\right]$ in the limit as $N \to \infty$ in §5, providing an exact expression for it. By considering this limit, we find a simpler expression of the second moment than that of [3], which finds a closed-form expression for the second moment for finite N. The authors hope that further considering the "infinite case" (i.e. chosing $A \subseteq \mathbb{N}$) may lead to interesting results in the finite case, which is of broader interest. Finally, in §6, we conclude by finding the leading order term of the second moment $\mathbb{E}\left[Y^2\right]$ in the limit of large N and determining the asymptotic behavior of $\mathrm{Var}(Y)$.

Proposition 5. *There is an error term* $\delta(p)$ *such that*

$$\lim_{N\to\infty} \mathbb{E}\left[Y^2\right] \;=\; \frac{4}{p^4} + \delta(p), \tag{6.15}$$

where $\lim_{p\to 0} \delta(p)/p^{-4} = 0$.

In §7, we conclude by considering future work and questions that arise naturally from the results presented here.

2 Independence of the Fringes

This section proves that missing summands in the left and right fringes are almost independent. Note that if we had defined the left fringe as integers at most $N/2$ missing from $A + A$ and the right fringe as integers between $3N/2$ and $2N$, we would automatically have independence, but this is not true in our case. We show that the distribution of the total number of missing summands is almost the convolution with itself of the distribution of the number of missing summands in one fringe (Theorem 1). For the rest of this paper we will focus on counting missing summands in the left fringe, which is convenient. Define random variables $\tilde{Y}$ and $\tilde{Z}$ as

$$\tilde{Y} \;\coloneqq\; \sum_{n=0}^{\lfloor N/2 \rfloor} X_n, \qquad \tilde{Z} \;\coloneqq\; \sum_{n=\lfloor 3N/2 \rfloor + 1}^{2N} X_n \tag{2.1}$$

to count the number of missing summands on the "very left" and "very right," respectively. These are exactly independent, since X_i and X_j are independent whenever $|i - j| > N$. (If $j - i > N$, then $0 \leq i < N < j \leq 2N$, and X_i depends on the inclusion of $0, \ldots, i$ into A while X_j depends on the inclusion of $j - N, \ldots, N$.) By Lemma 1 below, Y is equal to $\tilde{Y}$ with high probability and Z to $\tilde{Z}$, and therefore, Y and Z are almost independent.

Lemma 1. *The expectation values* $\mathbb{E}\left[Y-\tilde{Y}\right]$ *and* $\mathbb{E}\left[Z-\tilde{Z}\right]$ *are bounded above by* $\frac{2}{p^2}\left(1-p^2\right)^{N/4}$ *and below by* 0.

Proof. By (1.7), the probability for the non-inclusion of i in $A+A$ is at most $(1-p^2)^{(i+1)/2}$. Therefore,

$$\mathbb{E}\left[Y-\tilde{Y}\right] \;\leq\; \sum_{i=\lfloor N/2\rfloor+1}^{N}\left(\sqrt{1-p^2}\right)^{i+1} \;<\; \frac{2}{p^2}\left(\sqrt{1-p^2}\right)^{N/2}, \qquad (2.2)$$

and a similar calculation works for $Z-\tilde{Z}$. The expectation values are nonnegative because each is a sum of probabilities $\mathbb{E}\left[X_i\right]$.

Corollary 1. *The probabilities of disagreement* $\mathbb{P}\left(Y\neq\tilde{Y}\right)$ *and* $\mathbb{P}\left(Z\neq\tilde{Z}\right)$ *are both bounded above by* $\frac{2}{p^2}\left(1-p^2\right)^{N/4}$.

Proof. $Y-\tilde{Y}$ and $Z-\tilde{Z}$ can only take nonnegative integer values, and Markov's inequality gives us the desired result.

2.1 Convolution of Left and Right Fringes

Recall that the total number of missing summands W is the sum of the number of missing summands Y on the left and Z on the right. Since the latter two are largely independent, the distribution of W is close to the convolution of Y with Z. Theorem 1 is similar to Theorems 6.4 and 6.9 of [3].

Lemma 2. *If* S,T *are random variables that take values in some finite set* A*, and if* x *is a possible value they can take, then*

$$\left|\mathbb{P}\left(S=x\right)-\mathbb{P}\left(T=x\right)\right| \;\leq\; \mathbb{P}\left(S\neq T\right). \qquad (2.3)$$

Proof. Consider the random variable (S,T), which takes on values in the Cartesian product $A\times A$. Then $\mathbb{P}\left(S\neq T\right)$ is the sum of probabilities $\mathbb{P}\left(S=y,T=z\right)$ over all "off-diagonal" pairs $y\neq z$, while

$$\begin{aligned}\left|\mathbb{P}\left(S=x\right)-\mathbb{P}\left(T=x\right)\right| &= \left|\sum_{y\in A}\mathbb{P}\left(S=x,T=y\right)-\sum_{y\in A}\mathbb{P}\left(S=y,T=x\right)\right| \\ &= \left|\sum_{y\neq x}\mathbb{P}\left(S=x,T=y\right)-\sum_{y\neq x}\mathbb{P}\left(S=y,T=x\right)\right| \\ &\leq \sum_{y\neq x}\mathbb{P}\left(S=x,T=y\right)+\sum_{y\neq x}\mathbb{P}\left(S=y,T=x\right)\end{aligned} \qquad (2.4)$$

is at most the sum over the column $\{x\}\times A$ and the row $A\times\{x\}$ excepting the diagonal point (x,x). Clearly, this is not greater than the sum over all off-diagonal elements.

Theorem 1. *For any* $0 \leq m \leq 2N$,

$$\left| \mathbb{P}(W = m) - \sum_{y=0}^{m} \mathbb{P}(Y = y)\, \mathbb{P}(Z = m - y) \right| \;\leq\; \frac{8}{p^2}(1-p^2)^{N/4}. \tag{2.5}$$

We say that as $N \to \infty$, W *is the convolution of* Y *with* Z.

Proof. Define $\tilde{W} \coloneqq \tilde{Y} + \tilde{Z}$. Since $\tilde{Y}$ and $\tilde{Z}$ are independent,

$$\mathbb{P}\left(\tilde{W} = m\right) \;=\; \sum_{y=0}^{m} \mathbb{P}\left(\tilde{Y} = y\right) \mathbb{P}\left(\tilde{Z} = m - y\right). \tag{2.6}$$

To translate this equality involving $\tilde{Y}, \tilde{Z}, \tilde{W}$ into an inequality involving Y, Z, W, we use Lemmas 1 and 2. For the left-hand side,

$$\left|\mathbb{P}(W = m) - \mathbb{P}\left(\tilde{W} = m\right)\right| \;\leq\; \mathbb{P}\left(W \neq \tilde{W}\right) \;\leq\; \mathbb{E}\left[W - \tilde{W}\right] \;\leq\; \frac{4}{p^2}(1-p^2)^{N/4}, \tag{2.7}$$

where we have used that $W - \tilde{W}$ only takes on nonnegative integer values and applied the linearity of expectation to find $\mathbb{E}\left[W - \tilde{W}\right]$ as $\mathbb{E}\left[Y - \tilde{Y}\right] + \mathbb{E}\left[Z - \tilde{Z}\right]$. For the right-hand side, we note that

$$\begin{aligned}
&\left|\mathbb{P}\left(\tilde{Y} = y\right)\mathbb{P}\left(\tilde{Z} = m - y\right) - \mathbb{P}(Y = y)\, \mathbb{P}(Z = m - y)\right| \\
&\qquad \leq \left|\mathbb{P}\left(\tilde{Y} = y\right) - \mathbb{P}(Y = y)\right| \mathbb{P}\left(\tilde{Z} = m - y\right) \\
&\qquad\quad + \left|\mathbb{P}\left(\tilde{Z} = m - y\right) - \mathbb{P}(Z = m - y)\right| \mathbb{P}(Y = y) \\
&\qquad \leq \frac{2}{p^2}\left(1 - p^2\right)^{N/4} \left(\mathbb{P}\left(\tilde{Z} = m - y\right) + \mathbb{P}(Y = y)\right),
\end{aligned} \tag{2.8}$$

and therefore

$$\begin{aligned}
&\left|\mathbb{P}\left(\tilde{Y} = y\right)\mathbb{P}\left(\tilde{Z} = m - y\right) - \mathbb{P}(Y = y)\, \mathbb{P}(Z = m - y)\right| \\
&\qquad \leq \frac{2}{p^2}\left(1 - p^2\right)^{N/4} \left(\sum_{y=0}^{m} \mathbb{P}\left(\tilde{Z} = m - y\right) + \sum_{y=0}^{m} \mathbb{P}(Y = y)\right) \\
&\qquad \leq \frac{4}{p^2}\left(1 - p^2\right)^{N/4}.
\end{aligned} \tag{2.9}$$

Now, (2.6), (2.7), and (2.9), together with the triangle inequality, imply the desired result.

3 Exponential Bounds on Missing Many Summands

This section presents analogs of [12]'s equations (4.6) and (4.14) for arbitrary p. Our derivations start with different intuitions and follow a different approach, but interestingly, we arrive at largely the same bounds.

3.1 A bound on the k^{th} moment of Y

From (1.7), the probability of non-inclusion of n into $A+A$ is at most $(1-p^2)^{n+1}$. The probability of multiple numbers being non-included is less than or equal to the probability of each individual non-inclusion. Therefore, for integers $0 \leq n_1, \ldots, n_k \leq N$,

$$\mathbb{P}\left(n_1, \ldots, n_k \notin A+A\right) \;\leq\; \left(\sqrt{1-p^2}\right)^{1+\max\{n_1,\ldots,n_k\}}. \tag{3.1}$$

The number of tuples $(n_1, \ldots, n_k)$ with $\max\{n_1, \ldots, n_k\} \leq n$ is $(n+1)^k$. The expectation value of Y^k can then be bounded as

$$\begin{aligned}
\mathbb{E}\left[Y^k\right] \;&\leq\; \sum_{n_1=0}^{N} \cdots \sum_{n_k=0}^{N} \left(\sqrt{1-p^2}\right)^{1+\max\{n_1,\ldots,n_k\}} \\
&<\; \sum_{n=0}^{\infty} \left((n+1)^k - n^k\right) \left(\sqrt{1-p^2}\right)^{n+1} \\
&\leq\; k \sum_{n=1}^{\infty} n^{k-1} \left(\sqrt{1-p^2}\right)^{n} \;<\; \frac{2k!}{\alpha^k},
\end{aligned} \tag{3.2}$$

where

$$\alpha \;\coloneqq\; \log \frac{1}{\sqrt{1-p^2}} \;=\; \left|\log \sqrt{1-p^2}\right|. \tag{3.3}$$

The derivation assumed $k \geq 1$, but in fact (3.2) is also valid for $k = 0$ because $\mathbb{E}\left[Y^0\right] = 1$. Equation (3.2) is a rather crude bound, but it is tight enough for the application of Chernoff's inequality. For $p = 1/2$, $\sqrt{1-p^2} \approx 0.87$ and $\alpha \approx 0.14$. Corollary 3 gives a slightly better bound on the k^{th} moment, one with an "α" of $-\log(\varphi/2) \approx 0.21$.

3.2 Applying the Chernoff Bound

Whenever $|t| < \alpha$, the moment generating function $M(t)$ is bounded by

$$\begin{aligned}
M(t) \;&=\; \mathbb{E}\left[e^{tY}\right] \;=\; \sum_{k=0}^{\infty} \frac{\mathbb{E}\left[Y^k\right] t^k}{k!} \;\leq\; \sum_{k=0}^{\infty} \frac{\frac{2k!}{\alpha^k} t^k}{k!} \\
&=\; 2 \sum_{k=0}^{\infty} \left(\frac{t}{\alpha}\right)^k \;=\; \frac{2}{1-t/\alpha}.
\end{aligned} \tag{3.4}$$

By the Chernoff bound,

$$\mathbb{P}\left(Y \geq n\right) \;\leq\; \inf_{t>0} \left\{M(t) e^{-tn}\right\} \;=\; \inf_{t>0} \left\{\frac{2e^{-tn}}{1-t/\alpha}\right\}. \tag{3.5}$$

For $n > 1/\alpha$, the infimum $e^{-\alpha n+1}n$ is attained at $t = \alpha - 1/n$. For $n \leq 1/\alpha$, the infimum 1 is at $t = 0$ and the bound is trivial. Thus, for $n > 1/\alpha$,

$$\mathbb{P}(Y \geq n) \;\leq\; 2\,\alpha n\, e^{-\alpha n+1} \;=\; O(n\, e^{-\alpha n}). \tag{3.6}$$

Recall that $\alpha = -\log\sqrt{1-p^2}$.

Corollary 2. *For any real number $\varepsilon > 0$, (and again, for $n > 1/\alpha$),*

$$\begin{aligned}\mathbb{P}(Y \geq n) \;&=\; O\left(n\left(\sqrt{1-p^2}\right)^n\right)\\ &=\; O\left(\left(\sqrt{1-p^2}+\varepsilon\right)^n\right).\end{aligned} \tag{3.7}$$

For $p = 1/2$, $\sqrt{1-p^2} \approx 0.87$, $\alpha \approx 0.14$, and $1/\alpha \approx 6.95$, and the bound starts being valid at $n = 7$. Corollary 4 gives a slightly better bound, $O\left((0.81+\varepsilon)^n\right)$, which corresponds to an "α" of 0.21. We note $\mathbb{P}(Y \geq m)$ cannot be bounded tighter than exponential. If $0, \ldots, n/2$ are missing from A, then $0, \ldots, n$ are missing from $A + A$. Therefore, for even n,

$$\mathbb{P}(Y \geq n) \;\geq\; \mathbb{P}(0, \ldots, n \notin A + A) \;\geq\; \mathbb{P}(0, \ldots, n/2 \notin A) \;=\; (1-p)^{n/2}. \tag{3.8}$$

Corollary 4 and (3.8) together establish an approximate decay rate for $\mathbb{P}(Y \geq n)$. Bounded above and below by two exponential functions, $\mathbb{P}(Y \geq n)$ must itself be "approximately exponential." Figure 2 gives the result of Monte Carlo simulation (1×10^6 trial runs) with $p = 1/2$ and $N = 200$, together with theoretical upper and lower bounds given by (3.6) and Corollary 4, respectively. The outcome of simulations is close to the lower bound and somewhat far from the upper bound.

By Theorem 1, (3.6) and (3.8) about the probabilities of missing many summands from the left-fringe range $0, \ldots, N$ translate into similar statements about missing many summands from the range $0, \ldots, 2N$ of the entire sumset $A + A \subseteq \{0, \ldots, 2N\}$.

4 Probability of Missing Two Summands

This section provides a simplified expression for Proposition 3.5 from [3], an exact formula for the probability of non-inclusion of two given numbers into $A+A$. The derivation of this simplified formula uses similar ideas as in the graph theoretic framework used in [3] and [12], but modified slightly. As such, we have opted to relegate most proofs to Appendix A.

The probability $\mathbb{P}(m, n \notin A + A)$ exhibits exponential decay in both m and n at a rate of about $\varphi/2 \approx 0.81$ for $p = 1/2$ (Corollary 4), although the exact rate of decay depends on the ratio $l = \left\lceil \frac{n+1}{m-n} \right\rceil$. The probability also depends on the parities of m, n, l. The numbers a_k are introduced in Definition 3, and is the same a_k as in Lemma 3.1 of [3]. They start with $a_1 = 1$ and decay exponentially.

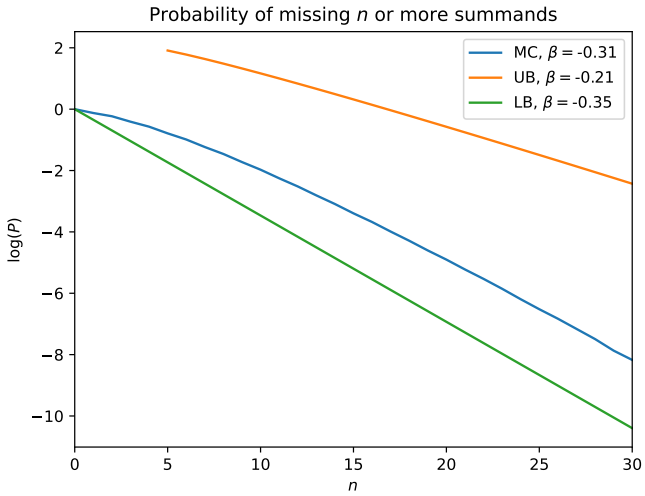


Fig. 2. Probabilities of missing more than n summands on the left fringe for $p = 1/2$ and $N = 200$. Monte Carlo simulation (MC) with 1×10^6 trial runs, theoretical upper bound (UB) from Corollary 4, and theoretical lower bound (LB) from (3.8) are shown. Here, β is the slope of $\log(\mathbb{P}(Y \geq n))$ as n increases, equal to $\log\sqrt{1-p}$ for LB and $\log \lambda_1$ for UB (see eq. 4.3). For MC, β is estimated numerically by fitting a least-squares line, which entails not only random error but also systematic error because the original curve seems to be concave.

Lemma 3. *We have $a_1 = 1$, $a_2 = 1 - p^2$, and for $3 \leq k \leq N$, a_k is given by the recurrence*

$$a_k \;=\; (1-p)a_{k-1} + p(1-p)a_{k-2}. \tag{4.1}$$

We now reformulate Prop 3.5 of [3].

Proposition 1. *The probability of non-inclusion of two nonnegative integers $n < m \leq N$ into $A + A$ is*

$$\mathbb{P}(m, n \notin A + A) \;=\; a_{2l+2}^{\lfloor d_1/2 \rfloor} a_{2l}^{\lfloor d_2/2 \rfloor} \begin{cases} 1 & s = (1,1,0) \text{ or } (1,1,1) \\ (1-p)a_l & s = (1,0,1) \text{ or } (0,1,0) \\ (1-p)a_{l-1} & s = (1,0,0) \text{ or } (0,1,1) \\ (1-p)^2 a_l a_{l-1} & s = (0,0,0) \text{ or } (0,0,1), \end{cases}$$

where $l = \left\lceil \frac{n+1}{m-n} \right\rceil$ is the "degree of twistedness" as in (A.13)*, d_1 and d_2 count the number of integers in $n+1, \ldots, m$ greater than or equal to and less than the threshold $l(m-n)$, respectively,*

$$d_1 \;=\; (m+1) - l(m-n), \quad d_2 \;=\; l(m-n) - (n+1), \tag{4.2}$$

and $s \coloneqq (m, n, l) \mod 2$ encodes the parities of m, n, l.

Define

$$\lambda_1 \coloneqq \frac{1-p+\sqrt{(1-p)(1+3p)}}{2}, \quad \lambda_2 \coloneqq \frac{1-p-\sqrt{(1-p)(1+3p)}}{2}. \tag{4.3}$$

One can check that a_k is given by

$$a_k = \frac{1-\lambda_2}{\lambda_1-\lambda_2}\lambda_1^k + \frac{-(1-\lambda_1)}{\lambda_1-\lambda_2}\lambda_2^k. \tag{4.4}$$

In particular, since $\lambda_2 < \lambda_1$,

$$\lambda_1^k < a_k \leq \lambda_1^{k-1}. \tag{4.5}$$

Proposition 1 now gives us the following lemma.

Lemma 4. *For $l \geq 2$, $(1-p)a_{l-1} \leq \sqrt{a_{2l}}$. Moreover, since $a_k \leq \lambda_1^{k-1}$, we have $\mathbb{P}(m,n \notin A+A) \leq a_{2l+2}^{d_1/2} a_{2l}^{d_2/2}$ and $\mathbb{P}(m,n \notin A+A) \leq \lambda_1^{1+\frac{m+n}{2}}$.*

Corollary 3. *The k^{th} moment of the number of missing summands on the left fringe is bounded by*

$$\mathbb{E}\left[Y^k\right] \leq \mathbb{E}[Y] + \frac{2k!}{\lambda_1|\log\lambda_1|} \leq \left(\frac{2}{p^2}-\frac{1}{p}-1\right) + \frac{2k!}{\lambda_1|\log\lambda_1|}. \tag{4.6}$$

Corollary 4. *We have*

$$\mathbb{P}(Y \geq n) = O\left((\lambda_1+\varepsilon)^n\right) \tag{4.7}$$

for all $\varepsilon > 0$. For $p = 1/2$, $\lambda_1 = \varphi/2 \approx 0.81$ where φ is the golden ratio. More precisely, for $n > 1/\alpha'$,

$$\mathbb{P}(Y \geq n) \leq \left(\frac{2}{p^2}-\frac{1}{p}-1\right) e^{-(n-1)(\alpha'-1/n)} + \frac{2n\alpha' e^{-n\alpha'+1}}{\lambda_1}, \tag{4.8}$$

where $\alpha' \coloneqq \log(1/\lambda_1)$.

Proof. By Corollary 3, the moment generating function is bounded by

$$M(t) \leq \left(\frac{2}{p^2}-\frac{1}{p}-1\right) e^t + \frac{2/\lambda_1}{1-t/\alpha'}. \tag{4.9}$$

By Chernoff's inequality, $\mathbb{P}(Y \geq n)$ is less than or equal to $M(t)e^{-nt}$ for every $t > 0$ where $M(t)$ is defined. In particular, we may take $t = \alpha' - 1/n$.

5 The Second Moment

There is little hope that $\mathbb{P}(m, n \notin A + A)$, as given in Proposition 1, can be summed to a closed-form expression. To simplify, we take the limit $N \to \infty$. For small p, many summands will be missing from $A + A$, so we expect $\mathbb{E}\left[Y^2\right]$ to blow up to infinity as p gets small. Since $\mathbb{E}[Y] = 2/p^2 - 1/p - 1$ in the limit $N \to \infty$, we hypothesize that $\mathbb{E}\left[Y^2\right]$ can be likewise expressed as a Laurent series in p. We find an exact (but not closed-form) expression for $\lim_{N\to\infty} \mathbb{E}\left[Y^2\right]$ and show that the leading term in its asymptotic expansion near $p = 0$ is $4p^{-4}$.

Define

$$S \coloneqq \lim_{N\to\infty} \sum_{m=0}^{N} \sum_{n=0}^{m-1} \mathbb{P}(m, n \notin A + A), \tag{5.1}$$

where $\mathbb{P}(m, n \notin A + A)$ is given by Proposition 1, so that

$$\lim_{N\to\infty} \mathbb{E}\left[Y^2\right] = \lim_{N\to\infty} \mathbb{E}[Y] + 2S = \left(\frac{2}{p^2} - \frac{1}{p} - 1\right) + 2S. \tag{5.2}$$

The difficulty in summing $\mathbb{P}(m, n \notin A + A)$ is that it depends on l, the degree of twistedness defined in (A.13), but other than that, $\mathbb{P}(m, n \notin A + A)$ is pretty much a geometric series. Define

$$U_l \coloneqq a^l_{2l}/a^{l-1}_{2l+2}, \quad V_l \coloneqq a^l_{2l+2}/a^{l+1}_{2l}, \tag{5.3}$$

so that for $n < m \leq N$,

$$\mathbb{P}(m, n \notin A + A) = U_l^{\frac{m+1}{2}} V_l^{\frac{n+1}{2}} \begin{cases} 1 & s = (1,1,0) \text{ or } (1,1,1) \\ (1-p)a_l & s = (1,0,1) \text{ or } (0,1,0) \\ (1-p)a_{l-1} & s = (1,0,0) \text{ or } (0,1,1) \\ (1-p)^2 a_l a_{l-1} & s = (0,0,0) \text{ or } (0,0,1). \end{cases}$$

We break up the plane $\mathbb{Z}^2_{\geq 0}$ into "wedges" of fixed l. For nonnegative integers m and l', define

$$g_{m,l'} \coloneqq \left\lfloor \frac{(m+1)(l'-1)}{l'} \right\rfloor, \tag{5.4}$$

so that $l \geq l'$ (recall that $l \coloneqq \left\lceil \frac{n+1}{m-n} \right\rceil$) if and only if $n \geq g_{m,l'}$. For each m and l', the collection of n's such that l is equal to l' is precisely $g_{m,l'}, \ldots, g_{m,l'+1} - 1$. Therefore,

$$S = \lim_{N\to\infty} \sum_{l'=1}^{\infty} \sum_{m=0}^{\infty} \sum_{n=g_{m,l'}}^{g_{m,l'+1}-1} \mathbb{P}(m, n \notin A + A). \tag{5.5}$$

We may define

$$\begin{aligned} S_l^{11} &\coloneqq \sum_{m \text{ odd}} \sum_{n \text{ odd}} U_l^{\frac{m+1}{2}} V_l^{\frac{n+1}{2}}, \\ S_l^{00} &\coloneqq \left((1-p)^2 a_l a_{l-1}\right) \sum_{m \text{ even}} \sum_{n \text{ even}} U_l^{\frac{m+1}{2}} V_l^{\frac{n+1}{2}}, \\ S_l^{10} &\coloneqq \left(\begin{cases} (1-p)a_l & l \text{ odd} \\ (1-p)a_{l-1} & l \text{ even} \end{cases} \right) \sum_{m \text{ odd}} \sum_{n \text{ even}} U_l^{\frac{m+1}{2}} V_l^{\frac{n+1}{2}} \\ S_l^{01} &\coloneqq \left(\begin{cases} (1-p)a_{l-1} & l \text{ odd} \\ (1-p)a_l & l \text{ even} \end{cases} \right) \sum_{m \text{ even}} \sum_{n \text{ odd}} U_l^{\frac{m+1}{2}} V_l^{\frac{n+1}{2}}, \end{aligned} \tag{5.6}$$

so that

$$S \;=\; \sum_{l=1}^{\infty} \left(S_l^{11} + S_l^{00} + S_l^{10} + S_l^{01} \right). \tag{5.7}$$

(A small abuse of notation: instead of summing over a dummy variable we sum over l) Each one of the sums in (5.6) is almost of the form $\sum_{i=0}^{\infty} \sum_{j=0}^{i-1} \alpha^i \beta^j$. For example,

$$\begin{aligned} S_l^{11} \;=\; \sum_{m \text{ odd}} \sum_{n \text{ odd}} U_l^{\frac{m+1}{2}} V_l^{\frac{n+1}{2}} \;&=\; \sum_{b=0}^{\infty} U_l^{b+1} \sum_{a=g_{bl}}^{g_{b,l+1}-1} V_l^{a+1} \\ &=\; \frac{U_l V_l}{1-V_l} \left(\sum_{b=0}^{\infty} U_l^b V^{g_{bl}} - \sum_{b=0}^{\infty} U_l^b V_l^{g_{b,l+1}} \right), \end{aligned} \tag{5.8}$$

where we used the substitution $m = 2b+1$ and $n = 2a+1$, and also the fact that $\left\lceil \frac{(2a+1)+1}{(2b+1)-(2a+1)} \right\rceil = \left\lceil \frac{a+1}{b-a} \right\rceil$. The exponent $g_{b,l+1}$ grows linearly with b, up to occasional corrections having to do with the floor function. Lemma 5, which is proven below, allows us to evaluate such "floor-geometric sums". The result is that

$$S_l^{11} \;=\; \sum_{l=1}^{\infty} \frac{a_{2l}}{(1-a_{2l+2})(1-a_{2l})}. \tag{5.9}$$

The other sums can be likewise evaluated, leading to

$$S \;=\; \sum_{l=1}^{\infty} \frac{a_{2l} + (1-p)a_{l-1} + (1-p)a_l a_{2l} + (1-p)^2 a_l a_{l-1}}{(1-a_{2l+2})(1-a_{2l})} - \left(\frac{2}{p^2} - \frac{1}{p} - 1 \right). \tag{5.10}$$

From (5.2), we deduce the following.

Proposition 2. *We have*

$$\lim_{N\to\infty} \mathbb{E}\left[Y^2\right] = -\left(\frac{2}{p^2}-\frac{1}{p}-1\right)+ \\ +2\sum_{l=1}^{\infty}\frac{a_{2l}+(1-p)a_{l-1}+(1-p)a_la_{2l}+(1-p)^2a_la_{l-1}}{(1-a_{2l+2})(1-a_{2l})}. \tag{5.11}$$

This is an exact expectation value of the square of the number of missing summands in the left fringe as $N\to\infty$. The summands in (5.11) decay exponentially, since $a_k \le \lambda_1^{k-1}$. Equation (5.11) reduces to [12]'s Theorem 1.5 for $p = 1/2$ and also works for general p. We achieved significant simplification over [12] Theorem 1.5, in the sense that breaking the plane into "wedges" and summing over these wedges instead of coordinate pairs converted a double infinite sum into a single infinite sum and removed floor functions and parity dependence.

Figure 3 compares the result of numerically evaluating (5.11) and of Monte Carlo simulations with $M = 1\times 10^5$ runs for some values of p and for $N = 400$, as well as the $4p^{-4}$ approximation which will be discussed in the next section. Expected errors were calculated as the square root of random error squared plus systematic error squared, where random error due to the finite size of the Monte Carlo simulation was simplistically taken to be $\Delta\mathbb{E}\left[Y^2\right] = 2\mathbb{E}\left[Y^2\right]/\sqrt{M}$, and systematic error due to the finite N used in the simulation was estimated as

$$\mathbb{E}\left[Y^2\right]_\infty - \mathbb{E}\left[Y^2\right]_N = \sum_{\max\{m,n\}\ge N+1}\mathbb{P}\left(m,n\notin A+A\right) \\ \le \sum_{n=N+1}^{\infty}\left((n+1)^2-n^2\right)\left(\sqrt{1-p^2}\right)^{n+1}. \tag{5.12}$$

The log-log plot is almost linear with a slope of -4, and the approximation $\mathbb{E}\left[Y^2\right]\approx 4/p^4-2/p^2+1/p+1$ (6.14) appears very accurate at small p. The fact that discrepancies between Monte Carlo and (5.11) shrink together with expected errors serves as independent evidence that the complicated algebra leading up to (5.11) was probably correct.

Lemma 5. *For numbers α,β with $|\alpha|,|\beta|<1$ and integers $0\le k<l$,*

$$\sum_{n=0}^{\infty}\alpha^n\beta^{\left\lfloor\frac{(l-1)n+k}{l}\right\rfloor} = \frac{1}{1-\alpha\beta}\left(1+\frac{\alpha^{k+1}\beta^k(1-\beta)}{1-\alpha^l\beta^{l-1}}\right). \tag{5.13}$$

Proof. As n increases, $(l-1)n+k$ modulo l goes as $k,k-1,\ldots,0$, then jumps to $l-1$ and settles into a cyclic mode $l-1,l-2,\ldots,0,l-1,l-2,\ldots,0$. As n goes to $n+1$, the quantity $\left\lfloor\frac{(l-1)n+k}{l}\right\rfloor$ increases by 1 if $(l-1)n+k$ modulo l is nonzero and stays the same if $(l-1)n+k$ modulo l is zero. Motivated by this, we make the observation that for $0\le n\le k$,

$$\left\lfloor\frac{(l-1)n+k}{l}\right\rfloor = n+\left\lfloor\frac{k-n}{l}\right\rfloor = n, \tag{5.14}$$

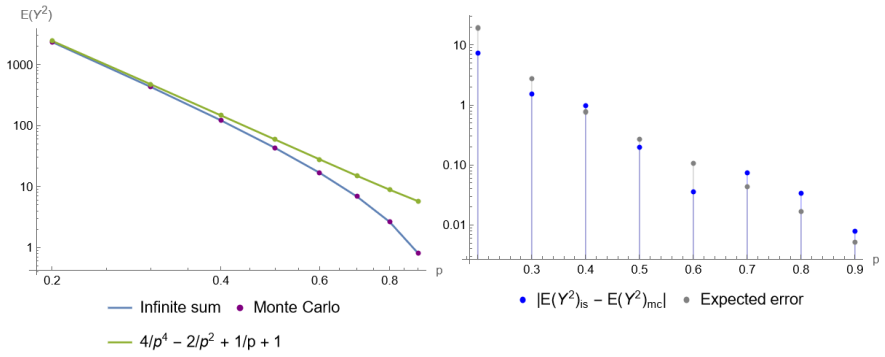


Fig. 3. Second moment $\mathbb{E}\left[Y^2\right]$ of the number of missing summands on the left fringe: theoretical prediction (5.11), Monte Carlo values, and the $4p^{-4}$ approximation (6.14) (left); discrepancies between Monte Carlo values $\mathbb{E}\left[Y^2\right]_{\text{mc}}$ and the infinite sum $\mathbb{E}\left[Y^2\right]_{\text{is}}$ from (5.11), together with what we expect the discrepancies to be based on simulation size and N (right).

and that if we write n as $ls + d + k$ for some integers s, d with $1 \leq d \leq l$, then

$$\left\lfloor \frac{(l-1)n+k}{l} \right\rfloor = \left\lfloor (l-1)s + k + \frac{(l-1)d}{l} \right\rfloor = (l-1)s + k + d - 1. \quad (5.15)$$

If we split the sum in question into the regions $[0, k]$ and $[k+1, \infty)$ and apply the two equations above, the sum becomes a collection of geometric series each of which is easy to evaluate:

$$\begin{aligned} \sum_{n=0}^{\infty} \alpha^n \beta^{\left\lfloor \frac{(l-1)n+k}{l} \right\rfloor} &= \sum_{n=0}^{k} \alpha^n \beta^n + \sum_{s=0}^{\infty} \sum_{d=1}^{l} \alpha^{ls+d+k} \beta^{(l-1)s+d+k-1} \\ &= \sum_{n=0}^{k} (\alpha\beta)^n + \alpha^k \beta^{k-1} \left(\sum_{s=0}^{\infty} \left(\alpha^l \beta^{l-1}\right)^s \right) \left(\sum_{d=1}^{l} (\alpha\beta)^d \right). \end{aligned} \quad (5.16)$$

6 Concentration of Y and the Asymptotics of the Second Moment

The first moment $\mathbb{E}[Y]$ in the limit of large N is $2p^{-2}$ to leading order in p. Therefore, we might expect the second moment $\mathbb{E}\left[Y^2\right]$ in this limit to grow as $(2p^{-2})^2 = 4p^{-4}$. We prove that that is indeed the case.

Moreover, we show that the variance $\text{Var}(Y)$ is asymptotically strictly less than p^{-4} and that therefore for small p, the number of missing summands Y in the left fringe is concentrated around the mean $2/p^2 - 1/p - 1$. By Theorem 1, this translates into saying that the total number of missing summands is also concentrated.

6.1 $\mathbb{E}\left[\boldsymbol{Y^2}\right]$ to Leading Order

Recall that (5.11) provides an exact formula for $\lim_{N\to\infty}\mathbb{E}\left[Y^2\right]$ in terms of an infinite series whose value is hard to compute. Since we expect this infinite series to behave as p^{-4}, for $0<p<1$ and L a positive integer, let us define $f(p,L)$ to be p^4 times its L^{th} partial sum,

$$f(p,L) \;\coloneqq\; \sum_{l=1}^{L} \frac{p^4\left(a_{2l}+(1-p)a_{l-1}+(1-p)a_la_{2l}+(1-p)^2a_la_{l-1}\right)}{(1-a_{2l+2})(1-a_{2l})}, \quad (6.1)$$

where the a_k's are to be understood as depending on this new value of p as in Lemma 3 or (4.4), so that we might compute $\lim_{p\to 0}\mathbb{E}\left[Y^2\right]/p^{-4}$ as twice the limit of $f(p,L)$ as L goes to infinity and p to zero. The limit $L\to\infty$ is to be taken first and $p\to 0$ second. The other order of limits, when p is first taken to zero and then L to infinity, is much easier to evaluate. We evaluate this second order of limits and prove that since $f(p,L)$ is sufficiently convergent, the limits may be exchanged.

Proposition 3. *We have $f(p,L)$ converges pointwise in p to $\sum_{l=1}^{L}\frac{4}{4l^2-1}$.*

Proof. From (4.3), one can compute that $\lambda_1 = 1-p^2+O(\lambda^3)$, $\lambda_2 = O(p)$, $C_1 = 1+p^2+O(\lambda^3)$, $C_2 = O(p)$. Since $a_{2l} = C_1\lambda_1^{2l}+C_2\lambda_2^{2l}$,

$$\lim_{p\to 0}\frac{1-a_{2l}}{p^2} \;=\; 2l-1. \quad (6.2)$$

As p goes to zero, each summand in (6.1) converges to $\frac{4}{4l^2-1}$. Since there are finitely many summands, the desired result follows.

Lemma 6. *Let μ be a real number between 0 and 1, and let R be a positive real number. For x a real number between 0 and R,*

$$1-\mu^x \;\geq\; \frac{1-\mu^R}{R}x. \quad (6.3)$$

Proof. $1-\mu^x$ is a function with a strictly negative second derivative whose plot intersects the line $\frac{1-\mu^R}{R}x$ at the two points $x=0$ and $x=R$.

Proposition 4. *We have $f(p,L)$ is uniformly Cauchy in L.*

Proof. For any tolerance $\varepsilon>0$, which we may assume to be less than 1, let $\varepsilon' \coloneqq \varepsilon/64$, and let

$$K \;\coloneqq\; \left\lceil \frac{9|\log\varepsilon'|^2}{\varepsilon'} \right\rceil. \quad (6.4)$$

For integers a,b with $K\leq a<b$, the difference $f(p,b)-f(p,a)$ may be bounded as

$$f(p,b)-f(p,a) \;<\; \sum_{l=a+1}^{\infty}\frac{4p^4\lambda_1^{l-2}}{(1-\lambda_1^{2l+1})(1-\lambda_1^{2l-1})}, \quad (6.5)$$

where we have used (4.5), $a_k \leq \lambda_1^{k-1}$. One can check that $\lambda_1 = 1 - p^2 + O(p^3)$. The denominator in (6.5) is approximately $(2l+1)(2l-1)p^4$ for small l and approximately constant for large l. Define

$$r \;\coloneqq\; \left\lceil \frac{|\log \varepsilon'|}{|\log \lambda_1|} \right\rceil + 2 \tag{6.6}$$

to quantify the boundary between the "small l" and "large l" regions, so that $\lambda^{l-2} \leq \varepsilon'$. For $l \geq r$, the numerator is small and the denominator is 1 up to an ε'-sized correction. Since $\lambda_1 \approx 1 - p^2$, the value of r depends on p as $O(1/p^2)$, reflecting the fact that a_k takes longer to converge to zero if p is small. The large-l portion of the sum in (6.5) can be bounded as

$$\begin{aligned} \sum_{l=r}^{\infty} \frac{4p^4 \lambda_1^{l-2}}{(1-\lambda_1^{2l+1})(1-\lambda_1^{2l-1})} \;&<\; \sum_{l=r}^{\infty} \frac{4p^4 \lambda_1^{l-2}}{(1-\varepsilon')^2} \\ &=\; \frac{8p^2}{(1-\varepsilon')^2} \frac{p^2/2}{1-\lambda_1} \lambda_1^{r-2} \\ &<\; 32\varepsilon' \;=\; \frac{\varepsilon}{2}. \end{aligned} \tag{6.7}$$

We upper-bound the sum in (6.5) for all $0 < p < 1$ by considering the large-p and small-p regimes, where "largeness" of p is defined in reference to a and ε'. When $r \leq a+1$, which is the large-p regime, the entire sum bounding $f(p,b) - f(p,a)$ in (6.5) is itself bounded by the geometric series from (6.7), so we're done. Let us consider the small p regime when $r > a+1$ (and also $a \geq K$ by assumption). From the definition of r, and from the fact that $|\log \lambda_1| \geq 1 - \lambda_1 \geq p^2/2$ we have the inequalities

$$\begin{aligned} p^2/2 \;&\leq\; |\log \lambda_1| \;\leq\; \frac{|\log \varepsilon'|}{r-3} \;\leq\; \frac{|\log \varepsilon'|}{K-1}, \\ 2r-1 \;&\leq\; \frac{2|\log \varepsilon'|}{|\log \lambda_1|} + 5 \;\leq\; \frac{3|\log \varepsilon'|}{|\log \lambda_1|} \;\leq\; \frac{6|\log \varepsilon'|}{p^2}, \end{aligned} \tag{6.8}$$

where we also use that $K \geq 6$. By Lemma 6 we have that for $0 \leq x \leq 2r-1$,

$$\frac{1-\lambda_1^x}{p^2} \;\geq\; \frac{1-\lambda_1^{2r-1}}{p^2(2r-1)} x \;>\; \frac{1-\varepsilon'}{6|\log \varepsilon'|} x \;\geq\; \frac{x}{12|\log \varepsilon'|}, \tag{6.9}$$

and therefore the small-l region of the sum in (6.5) may be bounded as

$$\begin{aligned} \sum_{l=a+1}^{r-1} \frac{4p^4 \lambda_1^{l-2}}{(1-\lambda_1^{2l+1})(1-\lambda_1^{2l-1})} \;&<\; \sum_{l=a+1}^{r-1} \frac{4(12|\log \varepsilon'|)^2 \lambda_1^{l-2}}{(2l+1)(2l-1)} \\ &<\; 576|\log \varepsilon'|^2 \sum_{l=a+1}^{\infty} \frac{1}{4l^2-1} \\ &=\; \frac{576|\log \varepsilon'|^2}{2a+1} \;<\; \frac{288|\log \varepsilon'|^2}{K} \;\leq\; \frac{\varepsilon}{2}. \end{aligned} \tag{6.10}$$

Combining (6.7) and (6.10), for the small-p case we obtain the bound

$$\sum_{l=a+1}^{\infty} \frac{4p^4\lambda_1^{l-2}}{(1-\lambda_1^{2l+1})(1-\lambda_1^{2l-1})} \;<\; \frac{\varepsilon}{2}+\frac{\varepsilon}{2} \;=\; \varepsilon \tag{6.11}$$

as desired. Since the threshold K does not depend on p, $f(p,L)$ is uniformly Cauchy in L.

Propositions 3 and 4 allow us to do an exchange of limits:

$$\lim_{p\to 0}\sum_{l=1}^{\infty} \frac{p^4\left(a_{2l}+(1-p)a_{l-1}+(1-p)a_l a_{2l}+(1-p)^2 a_l a_{l-1}\right)}{(1-a_{2l+2})(1-a_{2l})} \;=$$

$$= \lim_{p\to 0}\lim_{L\to\infty} f(p,L) \;=\; \lim_{L\to\infty}\lim_{p\to 0} f(p,L) \;=\; \sum_{l=1}^{\infty}\frac{4}{4l^2-1} \;=\; 2. \tag{6.12}$$

Therefore, the infinite sum from (5.11) is, to leading order, given by

$$\sum_{l=1}^{\infty} \frac{a_{2l}+(1-p)a_{l-1}+(1-p)a_l a_{2l}+(1-p)^2 a_l a_{l-1}}{(1-a_{2l+2})(1-a_{2l})} \;=\; \frac{2}{p^4}+\ldots, \tag{6.13}$$

where the "$\cdots$" represents an error term $\delta(p)$ with $\lim_{p\to 0}\delta(p)/p^{-4}=0$. So, the second moment $\mathbb{E}\left[Y^2\right]$ can be roughly approximated as

$$\lim_{N\to\infty}\mathbb{E}\left[Y^2\right] \;\approx\; \frac{4}{p^4}-\frac{2}{p^2}+\frac{1}{p}+1. \tag{6.14}$$

This approximation was obtained by combining (5.11) and (6.13). While it probably does not represent the correct asymptotic expansion of $\mathbb{E}\left[Y^2\right]$ to zeroth order, it seems like a reasonable approximation. Figure 3 compares the results of (6.14) with those of (5.11) and of Monte Carlo simulations. What can be concluded from (5.11) and (6.13) the following.

Proposition 5. *There is an error term $\delta(p)$ such that*

$$\lim_{N\to\infty}\mathbb{E}\left[Y^2\right] \;=\; \frac{4}{p^4}+\delta(p), \tag{6.15}$$

where $\lim_{p\to 0}\delta(p)/p^{-4}=0$.

By Theorem 1, for the second moment of the total number of missing summands in the large-N limit we likewise have

$$\lim_{N\to\infty}\mathbb{E}\left[W^2\right] \;=\; \lim_{N\to\infty}\left(2\mathbb{E}\left[Y^2\right]+2\mathbb{E}\left[Y\right]^2\right) \;=\; \frac{16}{p^4}+\cdots. \tag{6.16}$$

The value of N for which $\mathbb{E}\left[Y^2\right]$ and $\mathbb{E}\left[W^2\right]$ approach their $N\to\infty$ limits increases as p becomes smaller. By (5.12), the value of N needed for $\mathbb{E}\left[Y^2\right]$ to get to within a tolerance of ε of its $N\to\infty$ limit can be roughly approximated as

$$N_\varepsilon \;\approx\; \frac{8|\log p|}{p^2}+\frac{2|\log(\varepsilon/8)|}{p^2}. \tag{6.17}$$

Equations (5) and (6.16) concern the double limit $\lim_{p\to 0}\lim_{N\to\infty} p^4(\dots)$, and the ordering of the limits matters. In fact, for any fixed N, $\mathbb{E}\left[Y^2\right]$ is just bounded by $(N+1)^2$ and $\mathbb{E}\left[W^2\right]$ by $(2N+1)^2$ because the two tandom variables count missing summands in $0,\dots,N$ and $0,\dots,2N$, respectivey, so the limit $\lim_{N\to\infty}\lim_{p\to 0} p^4(\dots)$ if the "…" is substituted with $\mathbb{E}\left[Y^2\right]$ or $\mathbb{E}\left[W^2\right]$ is simply zero.

6.2 Concentration of Y

As p goes to zero, the variance of Y grows slower than the mean squared. That is, if we denote by $\mathbb{E}[Y]_\infty$ the limit of $\mathbb{E}[Y]$ as N goes to infinity, and likewise for $\mathbb{E}\left[Y^2\right]$, they relate to each other in such a way that the variance is small,

$$\lim_{p\to 0}\frac{\mathbb{E}\left[Y^2\right]_\infty - \left(\mathbb{E}[Y]_\infty\right)^2}{\left(\mathbb{E}[Y]_\infty\right)^2} \;=\; \lim_{p\to 0}\left(\frac{p^4\mathbb{E}\left[Y^2\right]_\infty}{4} - 1\right) \;=\; 0, \tag{6.18}$$

where we have used that $\mathbb{E}[Y]_\infty = 2p^{-2} + o(p^{-2})$ and $\mathbb{E}[Y_2]_\infty = 4p^{-4} + o(p^{-4})$, (1.9) and (5).

This means that for smaller and smaller p, if N is taken sufficiently large (depending on p), the distribution of the number of missing summands on the left fringe Y will be sharply concentrated around the mean $2/p^2 - 1/p - 1$.

The Central Limit Theorem with Weak Dependence does not apply to $Y = \sum X_n$ because the X_n's do not represent a stationary process, but (6.18) does prove that for small p and sufficiently large N, the random variable $Y/\mathbb{E}[Y]$ approaches a delta distribution.

Figure 4 demonstrates the cumulative probability distribution of Y normalized by the mean $\mathbb{E}[Y]$. For $N = 800$ and each of several values of p, the following Monte Carlo simulation was run. A collection of 1×10^6 random sets A were generated and the sumsets $A + A$ computed, and the mean number of missing summands across these subsets was obtained, and the number of sumsets missing less than a given fraction of the mean was counted. We note that the mean in each simulation was taken to be the sample mean and not $2/p^2 - 1/p - 1$, although the two are close. As p gets smaller, the cumulative distribution function approaches a step function $\mathbb{P}(Y \le y) \approx H(y/\mathbb{E}[Y] - 1)$.

7 Future Work

We list a few natural directions for future work.

1. In §3, the bounds for $\mathbb{P}(n_1,\dots,n_k \notin A + A)$ and $\mathbb{E}\left[Y^k\right]$ are not optimal, as shown in Figure 2. Does there exist a better upper bound for $\mathbb{E}\left[Y^k\right]$, and hence a better upper bound for $\mathbb{P}(Y \ge n)$?
2. In §5, we take the limit $N\to\infty$ to obtain a closed-form expression for $\mathbb{E}\left[Y^2\right]$ in the limit. Does there exist a closed-form expression for $\mathbb{E}\left[Y^2\right]$ in general?

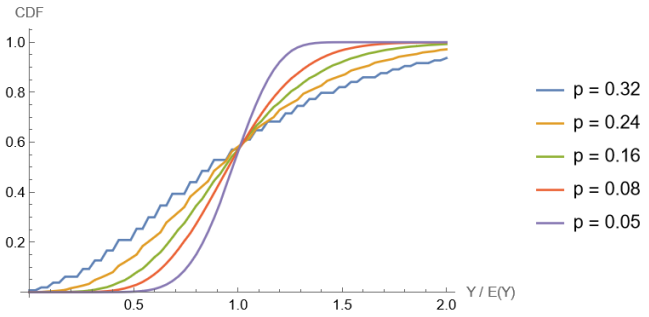


Fig. 4. The cumulative distribution function of Y, normalized by $\mathbb{E}[Y]$, for $N = 800$ and $p = 0.05, 0.08, 0.16, 0.24, 0.32$. (Monte Carlo simulation.)

3. In §6, we isolate the leading term of $\mathbb{E}\left[Y^2\right]$ in the limit $N \to \infty$. Can lower order terms in this expansion be found? More generally, can an explicit expansion in terms of $1/p$ be found?

These results only study the sumset $A+A$. The behavior of missing differences in the difference set $A-A$ in the limit as $N \to \infty$ has not been studied extensively. How can these results be modified to be applicable to difference sets?

A Appendix

This section derives Proposition 1, an exact formula for the probability of non-inclusion of two given numbers into $A + A$, equivalent to but simpler than Proposition 3.5 from [3]. The probability $\mathbb{P}(m, n \notin A + A)$ exhibits exponential decay in both m and n at a rate of about $\varphi/2 \approx 0.81$ for $p = 1/2$ (Corollary 4), although the exact rate of decay depends on the ratio $l = \left\lceil \frac{n+1}{m-n} \right\rceil$. The probability also depends on the parities of m, n, l. The numbers a_k are introduced in Definition 3, they start with $a_1 = 1$ and decay exponentially.

Proposition 1. *The probability of non-inclusion of two nonnegative integers $n < m \leq N$ into $A + A$ is*

$$\mathbb{P}(m, n \notin A + A) \;=\; a_{2l+2}^{\lfloor d_1/2 \rfloor} a_{2l}^{\lfloor d_2/2 \rfloor} \begin{cases} 1 & s = (1,1,0) \text{ or } (1,1,1) \\ (1-p)a_l & s = (1,0,1) \text{ or } (0,1,0) \\ (1-p)a_{l-1} & s = (1,0,0) \text{ or } (0,1,1) \\ (1-p)^2 a_l a_{l-1} & s = (0,0,0) \text{ or } (0,0,1), \end{cases}$$

where $l = \left\lceil \frac{n+1}{m-n} \right\rceil$ is the "degree of twistedness" as in (A.13)*, d_1 and d_2 count the number of integers in $n+1, \ldots, m$ greater than or equal to and less than the threshold $l(m-n)$, respectively,*

$$d_1 \;=\; (m+1) - l(m-n), \quad d_2 \;=\; l(m-n) - (n+1), \tag{4.2}$$

and $s \coloneqq (m, n, l) \mod 2$ encodes the parities of m, n, l.

To visualize the condition for $m, n \notin A + A$, draw the number line. For every $0 \leq x \leq m$, connect x with $m - x$ using a semicircle that goes below the number line, and for every $0 \leq x \leq n$, connect x with $n - x$ using a semicircle that goes above the number line. Then, $m, n \notin A + A$ if and only if for every drawn semicircle, at least one of the endpoints lies in A^c. An example of such a diagram, which we call snail, is given in Figure 5 for $m = 17$, $n = 13$. It is curious that the diagram splits in two disjoint spirals. In general, a diagram will split into a collection of spirals, and it is easy to calculate the lengths and counts of these spirals.

Spirals can either have two free ends, as in Figure 5, or have one free and one looped end, as in Figure 6. We define orbits to formalize the pictorial notion of spirals. The orbits associated with Figure 5 are $(15, 2, 11, 6, 7, 10, 3, 14)$ and $(17, 0, 13, 4, 9, 8, 5, 12, 1, 16)$, as well as the "reverses" $(14, 3, 10, 7, 6, 11, 2, 15)$ and $(16, 1, 12, 5, 8, 9, 4, 13, 0, 17)$. The orbits associated with Figure 6 are $(14, 3, 9, 8, 4, 13)$, $(16, 1, 11, 6, 6)$, and $(17, 0, 12, 5, 7, 10, 2, 15)$, as well as the "reverses" $(13, 4, 8, 9, 3, 14)$ and $(15, 2, 10, 7, 5, 12, 0, 17)$. The fact that $(16, 1, 11, 6, 6)$ ends with a repeated 6 is called a *loop*. Looped orbits don't have reverses, so the repeated number is always at the end and not at the start.

Fig. 5. Snail diagram for $m = 17$, $n = 13$.

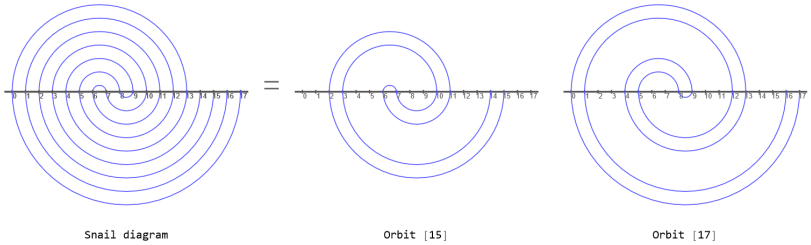
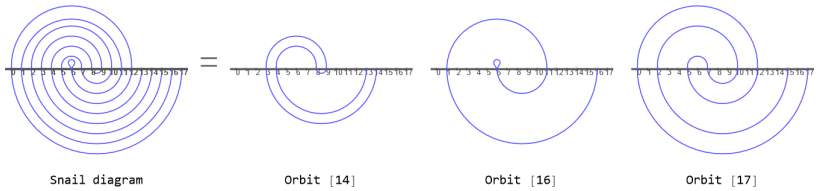


Fig. 6. Snail diagram for $m = 17$, $n = 12$.



Definition 1. *Let $n < r \leq m$ be nonnegative integers. We wish to study the numbers one can reach from r via the reflection maps $i \mapsto m-i$ and $i \mapsto n-i$ while staying in the nonnegative integers. Let $r_1 = r$, and for $t \geq 2$, let $r_t = m - r_{t-1}$ for t even and $r_t = n - r_{t-1}$ for t odd. Define the* orbit *of r as*

$$[r]_{mn} \;=\; (r_1, \ldots, r_k), \tag{A.1}$$

where k is the smallest positive integer such that r_{k+1} is either negative or equals r_{k-1}. (Such a k always exists because $r_{2p+1} = r - p(m-n)$ decreases with p.)

One can check that

$$r_t \;=\; \begin{cases} r - \frac{t-1}{2}(m-n) & t \text{ odd} \\ m - r + \frac{t-2}{2}(m-n) & t \text{ even} \end{cases} \tag{A.2}$$

for all $t \geq 1$.

Definition 2. *A tuple $(x_1, \ldots, x_k)$ of nonnegative integers is called a* chain *of length k. This chain is said to be* satisfied *if for every $1 \leq i \leq k-1$, either $x_i \notin A$ or $x_{i+1} \notin A$ (or both).*

Lemma 7 (Collusion of chains). *If chains $(r_1, \ldots, r_k)$ and $(q_1, \ldots, q_l)$ are such that $r_k = q_1$, then they are simultaneously satisfied if and only if the chain $(r_1, \ldots, r_k, q_2, \ldots, q_l)$ is satisfied.*

Proof. The combined chain has the same adjacencies as the first two chains.

Theorem 2. *Two nonnegative integers $n < m$ are simultaneously non-included in $A + A$ if and only if every one of the chains $[r]_{mn}$ for $n < r \leq m$ is satisfied.*

Proof. If some orbit $[r]_{mn} = (r_1, \ldots, r_k)$ is not satisfied, there exists some i such that r_i and r_{i+1} are both in A. Then $r_i + r_{i+1}$ is in $A + A$, and by the definition of an orbit, $r_i + r_{i+1}$ is either m or n.

Supose that $[r]_{mn}$ is satisfied for all r. Observe that m is non-included in $A+A$ if and only if every one of the chains $(0, m), (1, m-1), \ldots, (m, 0)$ is satisfied, and likewise for n. Define the set C as

$$C \coloneqq \{(0, m), (1, m-1), \ldots, (m, 0)\} \sqcup \{(0, n), (1, n-1), \ldots, (n, 0)\}, \quad \text{(A.3)}$$

so that $m, n \notin A+A$ if and only if every one of the chains in C is satisfied. We can consider C modulo the equivalence relation $\sim$, where $(x, y) \sim (z, w)$ if and only if there exists a sequence of numbers $a_0, \ldots, a_k$ with $a_0 \in \{x, y\}$, $a_k \in \{z, w\}$, and $(a_i, a_{i+1}) \in C$ for all $0 \leq i < k$. Let E be an equivalence class, and let

$$r = \max\{x : \exists y \in \mathbb{Z}_{\geq 0} : (x, y) \in E \text{ or } (y, x) \in E\} \quad \text{(A.4)}$$

be the greatest number encountered in E. Then $r > n$, because if r were less than or equal to n, $(r, n-r)$ would be in E, and $(m-(n-r), n-r)$ would be in E, but $r + (m-n) > r$.

Since $n - r$ is negative, $(r, n-r)$ or $(n-r, r)$ cannot be in E, and it has to be that $(r, m-r)$ and $(m-r, r)$ are in E. One can verify that if the orbit of r is $[r]_{mn} = (r_1, \ldots, r_k)$, then

$$\{(r_1, r_2), (r_2, r_3), \ldots, (r_{k-1}, r_k)\} \cup \{(r_2, r_1), (r_3, r_2), \ldots, (r_k, r_{k-1})\} \quad \text{(A.5)}$$

is a set containing $(r, m-r)$ and closed under the discussed equivalence relation. Therefore, E is equal to this set. By Lemma 7, all chains in E are satisfied if and only if $[r]_{mn}$ is satisfied, which is true by assumption. Since C is equal to the disjoint union of its equivalence classes, and every chain in every equivalence class is satisfied, m and n are non-included in $A + A$.

A.1 Loopless orbits

Lemma 8. *If x and $n < m$ are integers, and if $x \equiv n/2 \pmod{m-n}$, then $m-x$ and $n-x$ are also equivalent to $n/2$; if $x \equiv m/2 \pmod{m-n}$, then $m-x$ and $n-x$ are also equivalent to $m/2$.*

Proof. For the first part, $m - n/2 = (m-n) + n/2 \equiv n/2$ and $n - n/2 = n/2$. For the second part, $m - m/2 = m/2$ and $n - m/2 = -(m-n) + m/2 \equiv m/2$.

Throughout the rest of this subsection, we let $n < r \leq m$ be nonnegative integers and $[r]_{mn} = (r_1, \ldots, r_k)$ the orbit of r.

Lemma 9. *If r is not equivalent to $m/2$ or $n/2$ modulo $m-n$, then $r_1, \ldots, r_k$ are all distinct. (We say that the orbit is* loopless*.)*

Proof. By (A.2), the odd entries of r are strictly decreasing and the even entries are strictly increasing, so r_s cannot equal to r_t when $s \neq t$ have the same parity. To rule out the other case, suppose $t - s = 2d + 1$ for some nonnegative integer d. If s is odd and t even, $r_s = m - r_{s+1}$ and $r_t = m - r_{t-1}$, and if s is even and t odd, $r_s = n - r_{s+1}$ and $r_t = n - r_{t-1}$; in either case, equality $r_s = r_t$ implies $r_{s+1} = r_{t-1}$. Applying this result inductively d times, we find that $r_u = r_{u+1}$, where $u = s + d$. Therefore, either $r_u = n/2$ or $r_u = m/2$. By Lemma 8 and by induction, this would imply that r is equivalent to either $m/2$ or $n/2$ modulo $m - n$, which is not the case.

Lemma 10. *If r is not equivalent to $m/2$ or $n/2$ modulo $m - n$, the length of its orbit is*

$$k \;=\; 2\left\lceil \frac{r+1}{m-n} \right\rceil. \tag{A.6}$$

Proof. By Lemma 9, the r_t are all distinct, so by Definition 1, k is simply the smallest positive integer such that r_{k+1} is negative. By (A.2), the even entries r_{2p+2} are all positive, so it has to be that $k + 1$ is odd. Thus,

$$r_{k+1} \;=\; r - \frac{k}{2}(m-n) \;\leq\; -1, \tag{A.7}$$

which is equivalent to saying that $\frac{k}{2} \geq \frac{r+1}{m-n}$. By definition of the ceiling function, the smallest k that satisfies this is $2\left\lceil \frac{r+1}{m-n} \right\rceil$.

Corollary 5. *The endpoint r_k satisfies $k \;=\; 2\left\lceil \frac{r_k+1}{m-n} \right\rceil$.*

Proof. The orbit of r_k is $[r_k]_{mn} = (r_k, \ldots, r_1)$, the reverse of $[r]_{mn}$. It has the same length, so $k = 2\left\lceil \frac{r_k+1}{m-n} \right\rceil$.

A.2 Looped orbits

Lemma 11. *If r is equivalent to $m/2$ or $n/2$ modulo $m - n$, the length of its orbit is*

$$k \;=\; \left\lceil \frac{r+1}{m-n} \right\rceil + 1. \tag{A.8}$$

Proof. Suppose r is equivalent to $m/2$. Write $r = m/2 + j(m - n)$ for some integer j. Note that j is the unique integer satisfying $n < m/2 + j(m - n) \leq m$. In particular, j is the smallest integer satisfying $n + 1 \leq m/2 + j(m - n)$, so we may write

$$j \;=\; \left\lceil \frac{n+1-m/2}{m-n} \right\rceil \;=\; \left\lceil \frac{m/2+1}{m-n} \right\rceil - 1. \tag{A.9}$$

The orbit of r includes j repetitions of $x \mapsto m - x \mapsto x - (m - n)$ followed by one final m-reflection $m/2 \mapsto m - m/2$. Since there are $2j + 1$ reflections done, the number of points k is $2j + 2$. Then

$$\left\lceil \frac{r+1}{m-n} \right\rceil \;=\; j + \left\lceil \frac{m/2+1}{m-n} \right\rceil \;=\; 2j+1 \;=\; k-1, \tag{A.10}$$

which is what we wanted to show. Now suppose r is equivalent to $n/2$. Write $r = n/2 + j(m-n)$ for some integer j. Note again that j is the unique integer satisfying $n < n/2 + j(m-n) \leq m$. In particular, j is the smallest integer satisfying $n+1 \leq n/2 + j(m-n)$, so we may write

$$j \;=\; \left\lceil \frac{n/2+1}{m-n} \right\rceil. \tag{A.11}$$

The orbit of r includes j repetitions of $x \mapsto m-x \mapsto x-(m-n)$. Since there are $2j$ reflections done, the number of points k is $2j+1$. Then

$$\left\lceil \frac{r+1}{m-n} \right\rceil \;=\; j + \left\lceil \frac{n/2+1}{m-n} \right\rceil \;=\; 2j \;=\; k-1, \tag{A.12}$$

which is what we wanted to show.

A.3 Orbit counts

Throughout this subsection, $n < m$ are nonnegative integers and the "degree of twistedness"

$$l \;\coloneqq\; \left\lceil \frac{n+1}{m-n} \right\rceil \tag{A.13}$$

is a useful number that encodes how many twists the snail diagram for m, n has. The calculational significance of l is that for $n+1 \leq x \leq l(m-n)-1$,

$$l \;\leq\; \left\lceil \frac{n+2}{m-n} \right\rceil \;\leq\; \left\lceil \frac{x+1}{m-n} \right\rceil \;\leq\; \left\lceil \frac{(l(m-n)-1)+1}{m-n} \right\rceil \;=\; l, \tag{A.14}$$

and for $l(m-n) \leq x \leq m$,

$$l+1 \;=\; \left\lceil \frac{l(m-n)+1}{m-n} \right\rceil \;\leq\; \left\lceil \frac{x+1}{m-n} \right\rceil \;\leq\; \left\lceil \frac{m+1}{m-n} \right\rceil \;=\; l+1, \tag{A.15}$$

so that for $n+1 \leq x \leq m$,

$$\left\lceil \frac{x+1}{m-n} \right\rceil \;=\; \begin{cases} l & x < l(m-n) \\ l+1 & x \geq l(m-n). \end{cases} \tag{A.16}$$

Let a_1 be the number of loopless orbits of length $2(l+1)$ up to reversal (e.g., $(r_1, \ldots, r_k)$ is declared equivalent to $(r_k, \ldots, r_1)$), and a_2 the number of loopless orbits of length $2l$ up to reversal. Then, the number of loopless orbits of length $2(l+1)$ is $2a_1$, and those of length $2l$ is $2a_2$. By Lemma 10, for the loopless orbits of length $2(l+1)$, both endpoints have to be in $l(m-n), \ldots, m+1$, and for the loopless orbits of length $2l$, both endpoints have to be in $n+1, \ldots, l(m-n)-1$. Let c_1 be the number of integers in $l(m-n), \ldots, m+1$ that do not constitute the endpoint of a loopless orbit, and let c_2 be the number of integers in $n+1, \ldots, l(m-n)-1$ that

do not constitute the endpoint of a loopless orbit. Denote $d_1 \coloneqq (m+1) - l(m-n)$ and $d_2 \coloneqq l(m-n) - (n+1)$. Then,

$$\begin{aligned} d_1 &= 2a_1 + c_1, \\ d_2 &= 2a_2 + c_2. \end{aligned} \tag{A.17}$$

By Lemmas 10 and 11, the points in $l(m-n), \ldots, m$ that do not constitute the endpoint of a loopless orbit constitute the endpoint of a looped orbit of length $l+2$, and the points in $n+1, \ldots, l(m-n)-1$ that do not constitute the endpoint of a loopless orbit constitute the endpoint of a looped orbit of length $l+1$. Therefore, c_1 is the number of looped orbits of length $l+2$ and c_2 is the number of loopless orbits of length $l+1$.

Proposition 6. *Depending on the parities of m, n, l, the counts of different types of orbits are as follows, and there are no other orbits except the ones listed.*

m	n	l	c_1	c_2	$2a_1$	$2a_2$
1	1	1, 0	0	0	d_1	d_2
0	0	1, 0	1	1	$d_1 - 1$	$d_2 - 1$
1	0	1	1	0	$d_1 - 1$	d_2
1	0	0	0	1	d_1	$d_2 - 1$
1	0	1	0	1	d_1	$d_2 - 1$
1	0	0	1	0	$d_1 - 1$	d_2

Proof. Case 1. (Neither m nor n is even.) By Lemma 10, all orbits are loopless, so $c_1 = c_2 = 0$.

Case 2. (Both m and n are even.) The integers $n+1, \ldots, m$ include every number modulo $m-n$ exactly once. Let q_1 be the unique integer in $n+1, \ldots, m$ equivalent to $m/2$ modulo $m-n$, and q_2 equivalent to $n/2$. Since $m/2 \not\equiv n/2 \pmod{m-n}$, $q_1 \neq q_2$. By Lemma 11, q_1 and q_2 constitute the endpoints of looped orbits, and by Lemma 10, the orbits that don't end at q_1 or q_2 are all loopless. Therefore, $c_1 + c_2 = 2$. Since d_1 is odd and $2a_1$ is even, c_1 is odd. The only possibility is $c_1 = c_2 = 1$.

Cases 3-6. (One of m and n is even.) If m is even, one orbit has a loop at $m/2$ and the rest are loopless, and if n is even, one orbit has a loop at $n/2$ and the rest are loopless; so $c_1 + c_2 = 1$. When d_1 is odd, since $2a_1$ is even, it has to be that $c_1 = 1$ and $c_2 = 0$. When d_2 is odd, since $2a_2$ is even, it has to be that $c_1 = 0$ and $c_2 = 1$.

A.4 Probabilities

Definition 3. *For $k \geq 1$, let a_k be the probability that the chain $(1, \ldots, k)$ is satisfied.*

Recalling the definition of a chain, we get the following equivalent definition of a_k. If a string of zeros and ones of length k is selected at random such that the probability of a 1 occurring is p, then a_k is the probability that no two consecutive entries are 1.

Lemma 3. *We have $a_1 = 1$, $a_2 = 1 - p^2$, and for $3 \leq k \leq N$, a_k is given by the recurrence*

$$a_k \;=\; (1-p)a_{k-1} + p(1-p)a_{k-2}. \tag{4.1}$$

Proof. The chain (1) is satisfied trivially. The chain $(1, 2)$ is not satisfied if and only if 1 and 2 are both in A, which happens with probability p^2. For $3 \leq k \leq N$, we note that $(1, \ldots, k)$ is satisfied if and only if $(1, \ldots, k-1)$ and $(k-1, k)$ are satisfied. With probability $1-p$, k is non-included in A. In that case, $(k-1, k)$ is satisfied with probability 1 and the probability of satisfaction of $(1, \ldots, k-1)$ remains a_{k-1}. Therefore, the conditional probability of the satisfaction of $(1, \ldots, k)$ given that $k \notin A$ is a_{k-1}. With probability p, k is included in A. In that case, $(k-1, k)$ is satisfied if and only if $k-1$ is non-included in A. Therefore, $(1, \ldots, k)$ is satisfied if and only if $(1, \ldots, k-1)$ is satisfied and $k-1 \notin A$, which happens if and only if $(1, \ldots, k-2)$ is satified and $k-1 \notin A$. These are independent events that occur with probabilities a_{k-2} and $1-p$, respectively. Therefore, the conditional probability of the satisfaction of $(1, \ldots, k)$ given that $k \in A$ is $(1-p)a_{k-2}$. Summing over the two possible cases $k \notin A$, $k \in A$, we obtain the desired recurrence. The assumption $k \leq N$ is needed because we used $\mathbb{P}(k \in A) = p$.

Lemma 12. *The probability of satisfaction of a loopless orbit $(r_1, \ldots, r_k)$ is a_k.*

Proof. Since $r_1, \ldots, r_k$ are distinct, the map ϕ that sends $i \in [1, k]$ to r_i and $i \in [k+1, N]$ to i is a bijection from $[1, N]$ to itself. The orbit $(r_1, \ldots, r_k)$ is satisfied if for every i, at least one of r_i and r_{i+1} is not included in A, which is if and only if at least one of i and $i+1$ is not included in $\phi^{-1}(A)$. Since ϕ^{-1} is a bijection, $\phi^{-1}(A)$ has the same probability distribution as A.

Lemma 13. *The probability of satisfaction of a looped orbit $(r_1, \ldots, r_{k-1}, r_k = r_{k-1})$ is $(1-p)a_{k-2}$.*

Proof. The chain $(r_1, \ldots, r_{k-1}, r_k)$ is satisfied if and only if $(r_1, \ldots, r_{k-1})$ and (r_{k-1}, r_k) are both satisfied, which is if and only if $r_{k-1} \notin A$ and $(r_1, \ldots, r_{k-1})$ is satisfied, which is if and only if $r_{k-1} \notin A$ and $(r_1, \ldots, r_{k-2})$ is satisfied. The two events are independent and occur with probabilities $1-p$ and a_{k-2}, respectively.

Finally, we can prove Proposition 1.

Proposition 1. *The probability of non-inclusion of two nonnegative integers $n < m \leq N$ into $A + A$ is*

$$\mathbb{P}(m, n \notin A + A) \;=\; a_{2l+2}^{\lfloor d_1/2 \rfloor} a_{2l}^{\lfloor d_2/2 \rfloor} \begin{cases} 1 & s = (1,1,0) \text{ or } (1,1,1) \\ (1-p)a_l & s = (1,0,1) \text{ or } (0,1,0) \\ (1-p)a_{l-1} & s = (1,0,0) \text{ or } (0,1,1) \\ (1-p)^2 a_l a_{l-1} & s = (0,0,0) \text{ or } (0,0,1), \end{cases}$$

where $l = \left\lceil \frac{n+1}{m-n} \right\rceil$ *is the "degree of twistedness" as in* (A.13)*,* d_1 *and* d_2 *count the number of integers in* $n+1, \dots, m$ *greater than or equal to and less than the threshold* $l(m-n)$*, respectively,*

$$d_1 \;=\; (m+1) - l(m-n), \quad d_2 \;=\; l(m-n) - (n+1), \tag{4.2}$$

and $s \coloneqq (m, n, l) \mod 2$ *encodes the parities of* m, n, l*.*

Proof. If $[r]_{mn} = (r_1, \dots, r_k)$ and $[q]_{mn} = (q_1, \dots, q_l)$ are two orbits, they are either equal (e.g., $k = l$ and $r_i = q_i$ for all i), inverses of each other (e.g., $k = l$ and $r_i = q_{k+1-i}$ for all i), or disjoint (e.g., $r_i \neq q_j$ for all i, j). Since disjoint orbits depend on the inclusion of different numbers into A, their satisfactions are independent random events. Orbits that are inverses of each other, $(r_1, \dots, r_k)$ and $(r_k, \dots, r_1)$, are satisfied in all the same circumstances. Theorem 2 proves that m and n are non-included in $A + A$ if and only if all orbits are satisfied, and Proposition 6 counts the different kinds of orbits. The probability that m and n are non-included in $A + A$ is the product of the probabilities of satisfaction of the different disjoint orbits, which are given by Lemmas 12 and 13.

Lemma 4. *For* $l \geq 2$*,* $(1-p)a_{l-1} \leq \sqrt{a_{2l}}$*. Moreover, since* $a_k \leq \lambda_1^{k-1}$*, we have* $\mathbb{P}(m, n \notin A + A) \leq a_{2l+2}^{d_1/2} a_{2l}^{d_2/2}$ *and* $\mathbb{P}(m, n \notin A + A) \leq \lambda_1^{1+\frac{m+n}{2}}$*.*

Proof. By Lemma 13, $(1-p)a_{l-1}$ is the probability that $(1, \dots, l-1, l-1)$ is satisfied, which is also equal to the probability that $(l+1, l+1, \dots, 2l)$ is satisfied. Therefore, $(1-p)^2 a_{l-1}^2$ is the probability that $(1, \dots, l-1, l-1, l+1, l+1, \dots, 2l)$ is satisfied, which happens if and only if $(1, \dots, l-1)$, $(l-1, l-1, l+1, l+1)$, and $(l+1, 2l)$ are simultaneously satisfied. By Lemma 12, a_{2l} is the probability that $(1, \dots, 2l)$ is satisfied, which happens if and only if $(1, \dots, l-1)$, $(l-1, l, l+1)$, and $(l+1, \dots, 2l)$ are simultaneously satisfied. If $(l-1, l-1, l+1, l+1)$ is satisfied, then $l-1$ and $l+1$ are non-included in A, which implies that $(l-1, l, l+1)$ is satisfied. This proves the first inequality. The last two inequalities follow.

Acknowledgements

This work was completed during the 2023 SMALL REU program at Williams College. It was supported in part by NSF Grants DMS1561945 and DMS1659037, Williams College, and Churchill College, Cambridge.

References

1. M. Asada, S. Manski, S. J. Miller, and H. Suh, *Fringe pairs in generalized MSTD sets*, International Journal of Number Theory **13** (2017), no. 10, 2653–2675.
2. A. Bower, R. Evans, V. Luo and S. J. Miller, *Coordinate sum and difference sets of d-dimensional modular hyperbolas*, Integers **13** (2013), #A31.

3. H. V. Chu, D. King, N. Luntzlara, T. Martinez, S. J. Miller, L. Shao, C. Sun, and V. Xu, *Generalizing the distribution of missing sums in sumsets*, Journal of Number Theory **239** (2022), 402-444
4. H. Chu, N. Luntzlara, S. J. Miller and L. Shao, *Generalizations of a Curious Family of MSTD Sets Hidden By Interior Blocks*, Integers **20A** (2020), #A5.
5. H. Chu, N. McNew, S. J. Miller, V. Xu and S. Zhang, *When Sets Can and Cannot Have MSTD Subsets*, Journal of Integer Sequences **21** (2018), Article 18.8.2.
6. T. Do, A. Kulkarni, S.J. Miller, D. Moon, and J. Wellens, *Sums and Differences of Correlated Random Sets*, Journal of Number Theory **147** (2015), 44–68.
7. S. Harvey-Arnold, S. J. Miller and F. Peng, *Distribution of missing differences in diffsets*, In: Nathanson, M.B. (eds) Combinatorial and Additive Number Theory IV. CANT 2020. Springer Proceedings in Mathematics & Statistics, vol 347. Springer, Cham.
8. P. V. Hegarty, *Some explicit constructions of sets with more sums than differences*, Acta Arithmetica **130** (2007), no. 1, 61–77.
9. P. V. Hegarty and S. J. Miller, *When almost all sets are difference dominated*, Random Structures and Algorithms **35** (2009), no. 1, 118–136.
10. A. Hemmady, A. Lott and S. J. Miller, *When almost all sets are difference dominated in $\mathbb{Z}/n\mathbb{Z}$*, Integers **17** (2017), #A54.
11. G. Iyer, O. Lazarev, S. J. Miller and L. Zhang, *Generalized more sums than differences sets,* Journal of Number Theory **132** (2012), no. 5, 1054–1073.
12. O. Lazarev, S. J. Miller, K. O'Bryant, *Distribution of Missing Sums in Sumsets*, Experimental Mathematics **22** (2013), no. 2, 132–156.
13. J. Marica, *On a conjecture of Conway*, Canadian Mathematical Bulletin **12** (1969), 233–234.
14. G. Martin and K. O'Bryant, *Many sets have more sums than differences*, in Additive Combinatorics, CRM Proc. Lecture Notes, vol. 43, Amer. Math. Soc., Providence, RI, 2007, pp. 287–305.
15. S. J. Miller, B. Orosz and D. Scheinerman, *Explicit constructions of infinite families of MSTD sets*, Journal of Number Theory **130** (2010) 1221–1233.
16. S. J. Miller and D. Scheinerman, *Explicit constructions of infinite families of mstd sets,* In: Chudnovsky, D., Chudnovsky, G. (eds.) Additive Number Theory: Festschrift in Honor of the Sixtieth Birthday of Melvyn B. Nathanson, pp. 229-248. Springer, New York (2010)
17. S. J. Miller, S. Pegado and L. Robinson, *Explicit Constructions of Large Families of Generalized More Sums Than Differences Sets*, Integers **12** (2012), #A30.
18. S. J. Miler and K. Vissuet, *Most Subsets are Balanced in Finite Groups*, Combinatorial and Additive Number Theory, CANT 2011 and 2012 (Melvyn B. Nathanson, editor), Springer Proceedings in Mathematics & Statistics (2014), 147–157.
19. M. B. Nathanson, *Problems in additive number theory, 1*, Additive combinatorics, 263–270, CRM Proc. Lecture Notes **43**, Amer. Math. Soc., Providence, RI, 2007.

20. M. B. Nathanson, *Sets with more sums than differences*, Integers **7** (2007), #A5.
21. D. Penman and M. Wells, *On sets with more restricted sums than differences*, Integers **13** (2013), #A57.
22. I. Z. Ruzsa, *On the cardinality of $A + A$ and $A - A$*, Combinatorics year (Keszthely, 1976), vol. 18, Coll. Math. Soc. J. Bolyai, North-Holland-Bolyai Tàrsulat, 1978, 933–938.
23. I. Z. Ruzsa, *Sets of sums and differences*. In: Séminaire de Théorie des Nombres de Paris 1982-1983, pp. 267–273. Birkhäuser, Boston (1984).
24. I. Z. Ruzsa, *On the number of sums and differences*, Acta Mathematica Hungarica **59** (1992), 439–447.
25. W. G. Spohn, *On Conway's conjecture for integer sets,* Canadian Mathematical Bulletin **14** (1971), 461-462.
26. Y. Zhao, *Constructing MSTD sets using bidirectional ballot sequences*, Journal of Number Theory **130** (2010), no. 5, 1212–1220.
27. Y. Zhao, *Sets characterized by missing sums and differences*, Journal of Number Theory **131** (2011), no. 11, 2107–2134.