# SUMS AND DIFFERENCES OF CORRELATED RANDOM SETS

THAO DO, ARCHIT KULKARNI, STEVEN J. MILLER, DAVID MOON, AND JAKE WELLENS

ABSTRACT. Many questions in additive number theory (Goldbach's conjecture, Fermat's Last Theorem, the Twin Primes conjecture) can be expressed in the language of sum and difference sets. As a typical pair contributes one sum and two differences, we expect $|A-A| > |A+A|$ for finite sets $A$. However, Martin and O'Bryant showed a positive proportion of subsets of $\{0,\dots,n\}$ are sum-dominant. We generalize previous work and study sums and differences of pairs of *correlated* sets $(A,B)$ ($a \in \{0,\dots,n\}$ is in $A$ with probability $p$, and $a$ goes in $B$ with probability $\rho_1$ if $a \in A$ and probability $\rho_2$ if $a \notin A$). If $|A+B| > |(A-B)\cup(B-A)|$, we call $(A,B)$ a *sum-dominant* $(p,\rho_1,\rho_2)$*-pair*. We prove for any fixed $\vec{\rho} = (p,\rho_1,\rho_2)$ in $(0,1)^3$, $(A,B)$ is a sum-dominant $(p,\rho_1,\rho_2)$-pair with positive probability, which approaches a limit $P(\vec{\rho})$. We investigate $p$ decaying with $n$, generalizing results of Hegarty-Miller on phase transitions, and find the smallest sizes of MSTD pairs.

## CONTENTS



## 1. INTRODUCTION

Given a finite set $A \subset \mathbb{Z}$, it is natural to compare the sizes of its sumset $A+A$ and difference set $A-A$, which are defined as

$$A+A \;=\; \{a+b : a,b \in A\}, \quad A-A \;=\; \{a-b : a,b \in A\}. \tag{1.1}$$

*Date*: August 14, 2014.

2010 *Mathematics Subject Classification.* 11B13, 11P99 (primary), 05B10, 11K99, 82B26 (secondary).

*Key words and phrases.* More Sum Than Difference sets, correlated random variables, phase transition.

This research was conducted as part of the 2013 SMALL REU program at Williams College and was partially supported by NSF grant DMS0850577 and Williams College; the third named author was partially supported by NSF grants DMS0970067 and DMS1265673. We would like to thank our colleagues from SMALL for helpful discussions, Kevin O'Bryant for suggesting a variant of this problem at CANT 2013, and the referee for many valuable suggestions which improved the paper.

We have two competing influences on their respective cardinalities. For any $a \in A$, $a-a$ is always equal to $0$ while $a+a$ is different for different values of $a$. On the other hand, since addition is commutative while subtraction is not, any two different numbers $a, b \in A$ generate two differences $a-b$ and $b-a$ but only one sum $a+b$. We thus expect that most of the time the size of the difference set is at least that of the sumset; however, this is not always the case. A set whose sumset has more elements than its difference set is called *sum dominant*, or a *More Sums Than Differences* (MSTD) set. One of the earliest examples is due to Conway from the 1960's: $\{0, 2, 3, 4, 7, 11, 12, 14\}$.

We briefly review some of the key results in the field. Given a positive integer $n$ and a real number $p$ in $[0, 1]$, we choose a subset $A$ of

$$I_n \ := \ \{0, 1, \dots, n\} \tag{1.2}$$

such that each element of $I_n$ is independently chosen to $A$ with probability $p$. Let $p_{\text{MSTD}}(p, n)$ be the probability $A$ is an MSTD set, then $p_{\text{MSTD}}(1/2; n)$ is the probability that a uniformly chosen random subset of $I_n$ is an MSTD set. Martin and O'Bryant [MO] in 2002 proved that $p_{\text{MSTD}}(1/2; n)$ is greater than a positive constant for all $n \geq 14$. A similar result holds if instead each element of $I_n$ is chosen independently of the others with a fixed non-zero probability $p$, and again $p_{\text{MSTD}}(p; n) > 0$. This is somewhat contrary to our original intuition that MSTD sets should be rare, though we will see later that this percentage, while positive, is quite small. Subsequent work by Zhao [Zh2] proved that $p_{\text{MSTD}}(1/2; n)$ converges to a limit when $n \to \infty$, and Iyer, Lazarev, Miller and Zhang [ILMZ] generalized these results to comparisons of linear combinations of a set. These proofs are probabilistic and non-constructive; see [Na, MOS, MPR, Zh1] for explicit constructions of infinite families of MSTD sets. Other results include the work of Hegarty and Miller [HM] on the behavior of $p_{\text{MSTD}}(p_n; n)$ as the probability $p_n$ of including an element in $A \subset I_n$ decays with $n$, and Hegarty's [He] proof that the smallest size of an MSTD set is 8 and the example found by Conway is the smallest sum dominant set up to linear transformation.

All of the literature to date has looked at sums and differences of a set with itself. In this paper, we extend the theory to combinations of two subsets of integers (see [DKMMWW] for another generalization, specifically to subsets of $D$-dimensional polytopes). Given two finite sets of integers $A$ and $B$, define their sumset and difference set by

$$\begin{aligned} A+B &= \{a+b : a \in A, b \in B\}, \\ \pm(A-B) &= (A-B) \cup (B-A) \ = \ \{a-b, b-a : a \in A, b \in B\}. \end{aligned} \tag{1.3}$$

We investigate sums and differences of *pairs* of subsets $(A, B) \subset \{0, 1, \dots, n\}$, which are selected according to the dependent random process described below.

**Definition 1.1.** *Fix a $\vec{\rho} = (p, \rho_1, \rho_2) \in [0, 1]^3$. We call $(A, B)$ a $\vec{\rho}$-*correlated pair *if each element $k \in I_n$ is chosen into $A$ and $B$ by the following rule:*

$$\mathbb{P}(k \in A) \ = \ p; \qquad \mathbb{P}(k \in B | k \in A) \ = \ \rho_1; \qquad \mathbb{P}(k \in B | k \notin A) \ = \ \rho_2. \tag{1.4}$$

We say a correlated pair $(A, B)$ is a *More Sums Than Differences* (MSTD) or *sum dominant* pair if the size of their sumset is bigger than that of their difference set: $|A+B| > |\pm(A-B)|$. For each $n$, let $P_n(\vec{\rho})$ denote the probability a randomly chosen $\vec{\rho}-$correlated pair $(A, B)$ is an MSTD pair.

If $(\rho_1, \rho_2) = (1, 0)$ then $B = A$ and thus the problem is reduced to comparing the sizes of the sumset and the difference set of $A$ with itself; this is the $(A, A)$ case, and is the only one that has been studied extensively in literature so far. If we let $(\rho_1, \rho_2) = (0, 1)$, then $B$ contains all elements that are not in $A$ and thus $B$ is the complement of $A$; we call this the $(A, A^c)$ case. If we

let $\rho_1 = \rho_2$, then $A$ and $B$ are chosen independently. Finally, if $\vec{\rho} = (0.5, 0.5, 0.5)$ then $P_n(\vec{\rho})$ is simply the proportion of pairs of subsets of $\{0, 1, \dots, n\}$ that are MSTD. In this case, we call the MSTD correlated pair simply an MSTD pair.

In this paper, we address three questions regarding MSTD correlated pairs.

(1) For a fixed probability vector $\vec{\rho}$, does $P_n(\vec{\rho})$ converge to a positive number as $n \to \infty$?
(2) If we let $\vec{\rho}$ decay with $n$, does $P_n(\vec{\rho})$ converge to $0$ as $n \to \infty$?
(3) What are the minimal sizes of an MSTD pair and what are the minimal MSTD pairs up to linear transformation? We say $(m, n)$ is a minimal size of an MSTD pair if for any MSTD pair $(A, B)$ not having that size, then either $|A| > m$ or $|B| > n$. It can thus happen that there is more than one minimal size.

To address the first question, we exploit the probabilistic methods of Martin and O'Bryant [MO] and Zhao [Zh2]. We first construct a pair that has an MSTD *fringe*; these are the elements near the endpoints of $A$ and typically control whether or not the set is sum-dominant (see Definition 2.5 for details). Next we show that almost all MSTD correlated pairs are rich, which essentially means that we have an MSTD fringe and that a large interval of middle sums are obtained; see Definition 2.6 for details. From this we are able to answer completely the first question.

**Theorem 1.2.** *For each vector $\vec{\rho} = (p, \rho_1, \rho_2) \in [0, 1]^3$, the proportion of sum dominant $\vec{\rho}$-correlated pairs of $I_n$ converges to a limit $P(\vec{\rho})$ as $n \to \infty$. Moreover, $P(\vec{\rho}) = 0$ if $p \in \{0, 1\}$ or $\rho_1 + \rho_2 \in \{0, 2\}$, and $P(\vec{\rho})$ is strictly positive otherwise.*

From Monte-Carlo experiments, Martin and O'Bryant [MO] conjectured that the *proportion* of MSTD sets, or $P((0.5, 1, 0))$, is approximately $4.5 \times 10^{-4}$; Zhao [Zh2] has derived algorithms supporting a limit of this size. Since we expect MSTD sets to be rare, we are interested in finding the maximum value of the function $P$. The following theorem says that this search is not completely hopeless.

**Theorem 1.3.** *The function $P : [0, 1]^3 \to [0, 1]$, defined in Theorem 1.2, is continuous and thus attains its maximum at some point.*

In Section 3 we investigate $P$ and conjecture that the maximum occurs at $(0.5, 0, 1)$.

The second question for the $(A, A)$ case was first conjectured by Martin and O'Bryant [MO] and solved there by Hegarty and Miller [HM]. The question is interesting because if $(p, \rho_1, \rho_2)$ is fixed with $p > 0$ and $0 < \rho_1 + \rho_2 < 2$, then the expected sizes of $A$ and $B$ are proportional to $n$ and it is reasonable to expect a positive probability of having MSTD correlated pairs. If instead we let either $p \to 0$ or $\rho_1 + \rho_2 \to 0$ or 2, then the expected size of $A$ (if $p \to 0$) or $B$ (if $\rho_1 + \rho_2 \to 0$ or 2) is no longer proportional to $n$ and it is unclear whether or not we should have a positive probability of MSTD correlated pairs.

The case studied in [HM] is $(\rho_1, \rho_2) = (1, 0)$ and $p \to 0$ as $n \to \infty$. Before stating their main results, we fix some notation. Let $\mathscr{X}$ be a real-valued random variable depending on some integer parameter $N$, and let $f(N)$ be a real-valued function. We write $\mathscr{X} \sim f(N)$ if for any $\epsilon_1, \epsilon_2 > 0$ there exists $N_{\epsilon_1,\epsilon_2} > 0$ such that for all $N > N_{\epsilon_1,\epsilon_2}$,

$$\mathbb{P}(\mathscr{X} \notin [(1 - \epsilon_1)f(N), (1 + \epsilon_1)f(N)]) \ < \ \epsilon_2. \tag{1.5}$$

We also use standard big-Oh, small-oh and $\Theta$ notations. We write $f(x) = O(g(x))$ if there exist constants $x_0$ and $C$ such that for all $x \geq x_0$, $|f(x)| \leq Cg(x)$. If $f(x) = O(g(x))$ and $g(x) = O(f(x))$ we say $f(x) = \Theta(g(x))$. Finally, we write $f(x) = o(g(x))$ (or $g(x) \gg f(x)$) if $\lim_{x\to\infty} f(x)/g(x) = 0$. The following theorem captures the main results in [HM].

**Theorem 1.4.** *[Hegarty-Miller* [HM]*] For $p : \mathbb{N} \to (0,1)$ such that $p(N) = o(1)$ and $N^{-1} = o(p(N))$, let each $k \in I_N := \{0,\dots,N\}$ be independently chosen to be in $A$ with probability $p(N)$. The probability that $A \subset I_N$ is MSTD tends to 0.*

*Let $\mathscr{S} = |A+A|$, $\mathscr{D} = |A-A|$ and $\mathscr{S}^C = 2N+1-\mathscr{S}$, $\mathscr{D}^C = 2N+1-\mathscr{D}$ be the sizes of their complements.*

(i) *If $p = o(N^{-1/2})$, then $\mathscr{D} \sim 2\mathscr{S} \sim (Np)^2$.*

(ii) *If $p = cN^{-1/2}$ for $c \in (0,\infty)$, then for $g(x) = 2(e^{-x} - (1-x))/x$*

$$\mathscr{S} \ \sim \ g\left(\frac{c^2}{2}\right) N \qquad \text{and} \qquad \mathscr{D} \ \sim \ g(c^2)N. \tag{1.6}$$

(iii) *If $N^{-1/2} = o(p)$ then $\mathscr{S}^c \sim 2\mathscr{D}^c \sim 4/p^2$.*

This theorem identifies $N^{-1/2}$ as the *threshold function* where the phase transition happens. The ratio between sizes of the sumset and difference set behaves differently for $p$ with decay on opposite sides of this threshold. Below the threshold the ratio is almost surely $2+o(1)$ while above it is almost surely $1+o(1)$.

Building on their methods, we extend their results to our more general setting.

**Theorem 1.5.** *For fixed $\rho_1, \rho_2 \in [0,1]$, $0 < \rho_1 + \rho_2 < 2$ and a function $p : \mathbb{N} \to (0,1)$ such that $p(N) = o(1)$ and $N^{-1} = o(p(N))$, the probability that $(A,B) \subset I_N$ is an MSTD $(p(N), \rho_1, \rho_2)$-correlated pair tends to 0.*

*In particular, let $\hat{p} = p^2(2\rho_1 - \rho_1^2) + 2p(1-p)\rho_2$ where $p = p(N)$. Let $\mathscr{S} = |A+B|$ and $\mathscr{D} = |\pm(A-B)|$ and $\mathscr{S}^C = 2N+1-\mathscr{S}$, $\mathscr{D}^C = 2n-1-\mathscr{D}$ be the sizes of their complements.*

(i) *If $\hat{p} = o(N^{-1})$, then $\mathscr{D} \sim 2\mathscr{S} \sim N^2\hat{p}$.*

(ii) *If $\hat{p} = cN^{-1}$ for some $c \in (0,\infty)$. Let $g(x) = 2(e^{-x} - (1-x))/x$, then*

$$\mathscr{S} \ \sim \ g\left(\frac{c}{2}\right) N \qquad \text{and} \qquad \mathscr{D} \ \sim \ g(c)N. \tag{1.7}$$

(iii) *If $N^{-1} = o(\hat{p})$, then $\mathbb{E}(\mathscr{S}^c) \sim \mathbb{E}(2\mathscr{D}^c) \sim 4/\hat{p}$.*

Finally, we are able to answer the first part of the third question.

**Theorem 1.6.** *The minimal sizes of MSTD pairs are $(3,5)$ and $(4,4)$. Examples of MSTD pairs with such sizes are*

$$\begin{aligned} A \ &= \ \{0,1,4,6,7\}, \quad B \ = \ \{2,3,5\} \\ A \ &= \ \{0,1,4,6\}, \quad B \ = \ \{0,2,5,6\}. \end{aligned} \tag{1.8}$$

We attack these three questions in their listed order. In Sections §2 and §3 we address the first question by proving Theorem 1.2 and Theorem 1.3. We next investigate the decay of $p$ in §4 and prove the result about minimal MSTD pairs in Section §5. We conclude with a list of questions for future research.

## 2. Positive percentage of MSTD correlated pairs

In this section we generalize the arguments of [MO] and [Zh2] to the case of $(p,\rho_1,\rho_2)$-pairs $(A,B)$. Let $I_n := \{0,\dots,n\}$; we also write $[0,n]$ for this interval. Additionally, $n - A = \{n-a : a \in A\}$; we frequently enclose it in parentheses when performing unions or intersections to clearly identity the sets. We first prove an easy yet very helpful result.

**Proposition 2.1.** *If $p \in \{0,1\}$ or $\rho_1 + \rho_2 \in \{0,2\}$ then there is no $\vec{\rho}$–correlated MSTD pair in $I_n$.*

*Proof.* It is easy to see that if $p = 0$ or 1, the set $A$ is, respectively, the empty set or $I_n$. In the first case, $|A+B| = |A-B| = 0$ for any set $B$. In the latter case, if $l$ and $s$ are the largest and smallest elements of $B$ ($0 \le s \le l \le n$), then $A+B = \{s, s+1, \dots, n+l\}$ and $\pm(A-B) = \{-d, -(d-1), \dots, d-1, d\}$ where $d = \max\{n-s, l\}$. Hence $|A+B| = (n+l)-s+1 = (n-s)+l+1 \le 2d+1 = |\pm(A-B)|$. In either case, there is no MSTD correlated pair (for any $n$). Similarly, if $\rho_1+\rho_2 \in \{0,2\}$ or equivalently $(\rho_1,\rho_2) \in \{(0,0);(1,1)\}$, $B = \emptyset$ or $I_n$, and there is no MSTD pair either. □

**Therefore from now on we assume $0 < p < 1$ and $0 < \rho_1 + \rho_2 < 2$ unless stated otherwise.**

We now establish two useful lemmas which are analogous to Lemmas 7 and 11 in [MO]. Their proofs follow from Bayes's formula, and for completeness are given in Appendix A.

**Lemma 2.2.** *Let $(A,B)$ be a $(p,\rho_1,\rho_2)$-correlated pair. For any $k \in [0,2n]$, the probability $k$ does not belong to the sumset $A+B$ is*

$$\mathbb{P}(k \notin A+B) = \begin{cases} \rho_3^{\min\{\frac{k+1}{2}, \frac{2n-k+1}{2}\}} & \text{if } k \text{ is odd} \\ \rho_4\rho_3^{\min\{\frac{k}{2}, \frac{2n-k}{2}\}} & \text{if } k \text{ is even,} \end{cases} \tag{2.1}$$

*where*

$$\rho_3 = (1-\rho_1)^2p^2 + 2(1-\rho_2)p(1-p) + (1-p)^2 \quad \text{and} \quad \rho_4 = (1-\rho_1)p + (1-p). \tag{2.2}$$

**Lemma 2.3.** *Let $(A,B)$ be a $(p,\rho_1,\rho_2)$-correlated pair. For any $k \in [-n,n]$,*

$$\mathbb{P}(k \notin (A-B)\cup(B-A)) \le \begin{cases} \rho_3^{n/3} & \text{if } 1 \le k \le n/2 \\ \rho_3^{n-k} & \text{if } n/2 < k \le n, \end{cases} \tag{2.3}$$

*where $\rho_3$ is defined in Lemma 2.2.*

**Remark 2.4.** *It is easy to check that when $(\rho_1,\rho_2) = (1,0)$, $\rho_3 = 1-p^2$ and $\rho_4 = 1-p$; note this is consistent with the results in* [MO] *and* [Zh2].

We next give definitions of MSTD fringe tuples and rich MSTD pairs, analogous to Definitions 2.1 and 2.4 in [Zh2]. As we will see, these definitions characterize the behavior of almost all MSTD pairs in the limit.

**Definition 2.5** (MSTD fringe tuple)**.** *For $k < n/2$ and subsets $L, L', R, R'$ of $[0,k]$, we say $(L,L',R,R';k)$ is an* MSTD fringe tuple *if*

$$|(L+L')\cap[0,k]| + |(R+R')\cap[0,k]| > 2|((L+R')\cap[0,k]) \cup ((L'+R)\cap[0,k])|. \tag{2.4}$$

**Definition 2.6** (Rich MSTD pair)**.** *We call a pair of subsets $(A,B) \subset S$ a* rich MSTD pair with fringe tuple $(L,L',R,R';k)$ *if*

(i) $A\cap[0,k] = L$, $B\cap[0,k] = L'$,
(ii) $(n-A)\cap[0,k] = R$, $(n-B)\cap[0,k] = R'$,
(iii) $[k+1, 2n-k-1] \subseteq A+B$.

*The smallest such $k$ is called the order of this rich pair.*

Any pair $(A, B)$ satisfying (i) and (ii) is said to have *fringe profile given by* $(L, L', R, R'; k)$. These two conditions and Definition 2.5 imply that $A + B$ has more "extreme" elements than $\pm(A - B)$ (here "extreme" refers to the smallest $k$ elements and the largest $k$ elements of $I + I$ and $I - I$). If condition (iii) is also satisfied (i.e., the pair $(A, B)$ is rich) then $A + B$ has all the "non-extreme" elements of $I + I$, and thus $|A + B| > |\pm(A - B)|$. This intuition is formalized in the proof of the following lemma, and justifies our nomenclature.

**Lemma 2.7.** *A rich MSTD pair is an MSTD pair.*

*Proof.* The proof is similar to the proof of Lemma 2.5 in [Zh2]. We want $|A+B| > |\pm(A-B)|$. It suffices to show the following two inequalities:

$$|(A + B) \cap ([0, k] \cup [2n - k, 2n])| \ > \ |\pm(A - B) \cap ([-n, -n + k] \cup [n - k, n])| \tag{2.5}$$

$$|(A + B) \cap [k + 1, 2n - k - 1]| \ \geq \ |\pm(A - B) \cap [-n + k + 1, n - k - 1]|. \tag{2.6}$$

Notice (2.5) is saying that the sumset beats the difference set on the fringes, while (2.6) says that the difference set does not win in the middle, and so the inequality in (2.6) follows immediately from the richness criterion. To prove (2.5), note that

$$\begin{aligned}
(A + B) \cap [0, k] &= (L + L') \cap [0, k] \\
(A + B) \cap [2n - k, 2n] &= ((n - R) + (n - R')) \cap [2n - k, 2n] \ = \ 2n - ((R + R') \cap [0, k]) \\
(A - B) \cap [-n, -n + k] &= (L - (n - R')) \cap [-n, -n + k] \ = \ ((L + R') \cap [0, k]) - n \\
(B - A) \cap [-n, -n + k] &= (L' - (n - R)) \cap [-n, -n + k] \ = \ ((L' + R) \cap [0, k]) - n \\
(A - B) \cap [n - k, n] &= (L - (n - R')) \cap [n - k, n] \ = \ n - ((L + R') \cap [0, k]) \\
(B - A) \cap [n - k, n] &= (L' - (n - R)) \cap [n - k, n] \ = \ n - ((L' + R) \cap [0, k]).
\end{aligned} \tag{2.7}$$

Hence

$$|\pm(A - B) \cap ([-n, -n + k] \cup [n - k, n])| \ = \ 2|((L + R') \cap [0, k]) \cup ((L' + R) \cap [0, k])|, \tag{2.8}$$

while

$$|(A + B) \cap ([0, k] \cup [2n - k, 2n])| \ = \ |(L + L') \cap [0, k]| + |(R + R') \cap [0, k]|. \tag{2.9}$$

The desired inequality then follows from the definition (2.5) of an MSTD fringe tuple. □

Much like in [Zh2], we will see in the proof of Proposition 2.11 that *almost all MSTD pairs are rich*. Following [Zh2] we define a partial order on fringe tuples below, which allows us to count fringe tuples without redundancy.

**Definition 2.8** (Partial ordering of fringe tuples)**.** *We say* $(L, L', R, R'; k) > (M, M', T, T'; j)$ *if* $k > j$ *and*

$$\begin{aligned}
M \ = \ L \cap [0, j], \quad M' \ = \ L' \cap [0, j], \quad T \ = \ R \cap [0, j], \quad T' \ = \ R' \cap [0, j] \\
[j, k] \ \subseteq \ L + L', \quad [j, k] \ \subseteq \ R + R'.
\end{aligned} \tag{2.10}$$

The arguments in [Zh2] also show that minimal fringe tuples for a given rich pair $(A, B)$ are unique, and they are minimal in the partial order of all fringe tuples. This allows us to count rich MSTD pairs by their minimal fringe tuples.

Fix any $k > 0$. For $n > 2k$, let $\mathbb{P}_n[E]$ denote the probability that, out of all $(p, \rho_1, \rho_2) = \vec{\rho}$ correlated pairs of subsets $(A, B)$ of $[0, n]$, $A$ and $B$ satisfy the conditions prescribed by the event $E$.

Let $P_n(\vec{\rho})(L, L', R, R'; k)$ be the probability that the pair $(A, B) \in I_n$ is a rich MSTD $\vec{\rho}$-pair with fringe profile $(L, L', R, R'; k)$; that is $P_n(\vec{\rho})(L, L', R, R'; k)$ equals

$$\mathbb{P}_n[(A, B) \text{ has fringe profile } (L, L', R, R'; k) \text{ and } [k+1, 2n-k-1] \subseteq A+B]. \tag{2.11}$$

We write this more compactly as

$$P_n(\vec{\rho})(L, L', R, R'; k) := \mathbb{P}_n[(L, L', R, R'; k),\ [k+1, 2n-k-1] \subseteq A+B]. \tag{2.12}$$

**Lemma 2.9.** *For any fringe profile $(L, L', R, R'; k)$ and any $\vec{\rho} = (p, \rho_1, \rho_2)$, the following limit exists:*

$$P(\vec{\rho})(L, L', R, R'; k) := \lim_{n\to\infty} P_n(\vec{\rho})(L, L', R, R'; k). \tag{2.13}$$

*Proof.* Following the example in [Zh2], we break up the event $[k+1, 2n-k-1] \notin A+B$ into the disjoint events

$$[k+1, j-1] \in A+B, \quad j \notin A+B \tag{2.14}$$

for each $k < j \le 2n-k$. Thus

$$\begin{aligned}
&\mathbb{P}_n\left[(L, L', R, R'; k),\ [k+1, 2n-k-1] \subseteq A+B\right] \\
&= \mathbb{P}_n[(L, L', R, R'; k)] - \sum_{j>k}^{2n-k} \mathbb{P}_n[(L, L', R, R'; k), [k+1, j-1] \in A+B;\ j \notin A+B] \\
&= \mathbb{P}_{2k}[(L, L', R, R'; k)] - \sum_{j>k}^{2n-k} \mathbb{P}_{j+k}[(L, L', R, R'; k), [k+1, j-1] \in A+B;\ j \notin A+B],
\end{aligned} \tag{2.15}$$

where in the final line we have replaced the $n$ subscripts with smaller ones, which we can do because these events only involve at most $2k$ (resp. $j+k$) elements, and the probabilities do not change when we allow for more middle elements to belong (or not belong) to $A$ and $B$. Thus everything except the upper limit on the sum is independent of $n$. We send $n$ to infinity and find

$$\begin{aligned}
P(\vec{\rho})(L, L', R, R'; k) &:= \lim_{n\to\infty} P_n(\vec{\rho})(L, L', R, R'; k) \\
&= \mathbb{P}_{2k}[(L, L', R, R'; k)] - \sum_{j>k}^{\infty} \mathbb{P}_{j+k}[(L, L', R, R'; k), [k+1, j-1] \in A+B;\ j \notin A+B].
\end{aligned} \tag{2.16}$$

Since each term in the sum is non-negative and the total sum is bounded above by 1 (as the partial sums represent legitimate probabilities), the monotone convergence theorem says the sum converges, and thus the limiting probability exists. □

The next definition isolates our key object of study; we prove that it exists and give a formula for it in the proposition that follows.

**Definition 2.10 ($P(\vec{\rho})$).** *For $\vec{\rho} \in [0,1]^3$, set*

$$P(\vec{\rho}) := \lim_{n\to\infty} \mathbb{P}_n[(A, B) \textit{ is an MSTD } (p, \rho_1, \rho_2)\textit{-correlated pair }]. \tag{2.17}$$

**Proposition 2.11.** *The limit $P(\vec{\rho})$ exists and is given by*

$$\sum_{(L,L',R,R';k)} P(\vec{\rho})(L, L', R, R'; k), \tag{2.18}$$

*where the sum is taken over all minimal fringe tuples $(L, L', R, R'; k)$.*

*Proof.* As assumed, $0 < p < 1$ and $0 < \rho_1 + \rho_2 < 2$. Fix a positive integer $K$ and let $n$ be large enough.

Suppose $(A, B)$ is an MSTD pair of $I_n$. Let $L, L'$ be intersections of $A, B$ with $[0, K]$ and $R, R'$ be intersections of $A, B$ with $[n - K, n]$. We will prove that as $n$ grows large, the MSTD pair $(A, B)$ is a *rich* MSTD pair with probability approaching 1. Indeed, suppose $(A, B)$ is *not* a rich MSTD pair of order at most $K$. This means either $(A, B)$ is not rich, or it is rich with order greater than $K$.

In the first case, since $(L, L', R, R')$ is not an MSTD fringe, the size of difference set is not smaller than that of the sumset on the fringes. Hence there must be at least a middle difference, i.e., a difference in $[K - n, n - K]$, be missing (otherwise $(A, B)$ cannot be sum dominant). In the second case, since $(L, L', R, R', K)$ is a fringe pair, and yet $(A, B)$ is not a rich MSTD pair of order $K$, there must be a middle sum missing, i.e., there exists some number in $[K, 2n - K]$ that is not in $A + B$. Let $E$ denote this event. We use the result from Lemma 2.2 to calculate $\mathbb{P}(E)$. Note that since $p \neq 0, 1$ and $(\rho_1, \rho_2) \neq (0, 0), (1, 1)$, we have $0 < \rho_3 < 1$. We find

$$\mathbb{P}(E) \;=\; \mathbb{P}\left(\bigcup_{i=K}^{2n-K} (i \notin A + B)\right) \;\leq\; \sum_{i=K}^{2n-K} \mathbb{P}(i \notin A + B) \;\leq\; 4 \sum_{i=K/2}^{n/2} \rho_3^i \leq \frac{4}{1 - \rho_3} \rho_3^{K/2}, \quad (2.19)$$

which goes to zero as $K \to \infty$, proving the claim for missing at least one middle sum; the proof for the probability of missing at least one middle difference proceeds similarly, using Lemma 2.3.

We therefore have proved that when $n$ gets large, almost all MSTD pairs are rich MSTD with fringes. Therefore, by summing over all fringes as in (2.18), we get $P(\vec{\rho})$. Note that each term in (2.18) exists and their sum is less than 1, hence this sum converges. □

**Proposition 2.12.** *We have $P(\vec{\rho}) > 0$ for any $\vec{\rho}$ with $0 < p < 1$ and $0 < \rho_1 + \rho_2 < 2$.*

*Proof.* As the argument is similar to one in [MO], we only sketch the proof here. Unless $\rho_1 = 0$, any MSTD fringe pair $(L, R; k)$ for $(A, A)$ works as a fringe tuple $(L, L, R, R; k)$ for $(A, B)$, and occurs with fixed positive probability. One such fringe is given in [MO]: $L = \{0, 2, 3, 7, 8, 9, 10\}$ and $R = \{1, 2, 3, 6, 8, 9, 10, 11\}$. By additionally imposing that $[12, 12+j] \subset A \cap B$, for sufficiently large $j$ (which depends on $\vec{\rho}$), we can ensure that $(A, B)$ is rich with positive probability. Thus $P(\vec{\rho}) \geq P(\vec{\rho})(L, L, R, R; k) > 0$.

Now we handle the case when $\rho_1 = 0$. Since $\rho_2 > 0$, a fringe profile for $(A, A^c)$ occurs with positive probability in this case, and the same reasoning above will hold. Thus it suffices to exhibit a single MSTD fringe profile for $(A, A^c)$. One such fringe profile is $L = R = \{1, 2, 3, 5, 7, 8\}$. □

*Proof of Theorem 1.2.* The proof follows immediately from Propositions 2.1, 2.11 and 2.12. □

## 3. The probability function $P$

We now investigate the behavior of the function $P : [0, 1]^3 \to [0, 1]$, which gives the limiting probability of selecting an MSTD $\vec{\rho}$-correlated pair $(A, B)$ from $I_n$ as $n \to \infty$. We prove that $P$ is continuous, as stated in Theorem 1.3. Afterwards we compute the probability function for $n = 8$ and discuss some conjectures about the behavior of $P$.

*Proof of Theorem 1.3.* We first prove continuity away from the zeros; i.e., at points $\vec{\rho}$ such that $P(\vec{\rho}) \neq 0$. By Proposition 2.12, we know the zeros of $P$ are exactly the set

$$Z := \{(p, \rho_1, \rho_2) \in [0, 1]^3 : p \in \{0, 1\} \text{ or } (\rho_1 + \rho_2) \in \{0, 2\}\}, \quad (3.1)$$

which is a closed set in $\mathbb{R}^3$. We first show that $P$ is continuous on the open set $Z^c$, and then show that as $\vec{\rho}$ approaches any point in $Z$, the value of $P(\vec{\rho})$ approaches 0, so that $P$ is continuous on $[0,1]^3$.

We first prove that for each minimal fringe profile, $P(\vec{\rho})(L, L', R, R'; k)$ is a continuous function of $\vec{\rho}$ away from $Z$ (note that these functions are also zero on $Z$). We start with the definition:

$$\begin{aligned} P(\vec{\rho})(L, L', R, R'; k) \quad &:= \quad \mathbb{P}_{2k}[(L, L', R, R'; k)] \\ &\quad - \sum_{j>k}^{\infty} \mathbb{P}_{j+k}[(L, L', R, R'; k), [k+1, j-1] \in A + B;\, j \notin A + B]. \end{aligned} \tag{3.2}$$

The first term on the right hand side is continuous, since

$$\mathbb{P}_{2k}[(L, L', R, R'; k)] \;=\; \sum_{(A,B) \text{ has fringe profile} (L,L',R,R';k)} \mathbb{P}_{2k}[(A, B)], \tag{3.3}$$

and the probability of getting $(A, B)$ is just a polynomial in $p$, $\rho_1$ and $\rho_2$, so this sum is continuous. Similarly, each term in the second sum is continuous, as we can view each term as a sum over suitable pairs $(A, B)$ of the probability of picking the pair $(A, B)$, each of which is a polynomial.

Thus to show that the infinite sum itself is continuous, it suffices to bound the tails uniformly. We will see that this follows from

$$\mathbb{P}_{j+k}[(L, L', R, R'; k), [k+1, j-1] \in A + B;\, j \notin A + B] \;\le\; \mathbb{P}_{j+k}[j \notin A + B]. \tag{3.4}$$

The probability on the right, as computed in Lemma 2.2, is bounded above by $\rho_3^j$ where $\rho_3$ depends on $p, \rho_1, \rho_2$. For any fixed $\vec{\rho} \notin Z$, restrict to a closed ball about $\vec{\rho}$ that lies entirely inside $Z^c$. We can pick $\vec{\rho}_*$ for which $\rho_3$ attains its maximal value $q_* < 1$ on this closed ball. Thus the tails are bounded by the tails of a convergent geometric series with ratio $q_*$, so the series converges uniformly and thus $P(\vec{\rho})(L, L', R, R'; k)$ is continuous on $Z^c$.

Since

$$P(\vec{\rho}) \;=\; \sum_{(L,L',R,R';k)} P(\vec{\rho})(L, L', R, R'; k) \tag{3.5}$$

and the summands are continuous functions of $\vec{\rho}$ on $Z^c$, it suffices to show that the tail sums

$$\sum_{(L,L',R,R';k) \text{ with } k>m} P(\vec{\rho})(L, L', R, R'; k) \tag{3.6}$$

can be made uniformly small with $m$. This argument follows along the same lines as the proof of Proposition 2.14 in [Zh2]. All contributions to this tail arise from sets where $A + B$ is missing a middle sum, where in this case "middle" means not in the first or the last $m$ elements. To show that these events are unlikely we use the union bound and the fact that we have a convergent infinite geometric series, starting with some maximizer (over a closed ball in $Z^c$), $q_*$, raised to the power $m$, which goes to zero as $m \to \infty$.

Now we must show that $P(\vec{\rho})$ approaches zero as $\vec{\rho}$ approaches any point in $Z$. First we show $P(\vec{\rho})(L, L', R, R'; k) \to 0$ as the distance $\text{dist}(\vec{\rho}, Z)$ tends to 0. Note that

$$P(\vec{\rho})(L, L', R, R'; k) \;\le\; \mathbb{P}_{2k}(\vec{\rho})[(L, L', R, R'; k)]. \tag{3.7}$$

As the probability on the right is a continuous function of $\rho$ which is zero on $Z$, we have

$$\lim_{\text{dist}(\vec{\rho},Z)\to 0} P(\vec{\rho})(L, L', R, R'; k) = 0 \tag{3.8}$$

and thus the functions $P(\vec{\rho})(L, L', R, R'; k)$ are continuous on $[0,1]^3$. Observe that if $p > 0$ and $\rho_1+\rho_2 > 0$, but still $\vec{\rho} \in Z$, then the same argument involving missing middle sums and differences based on Lemmas 2.2 and 2.3 works to show that $P$ is continuous at $\vec{\rho}$. So we only need to show that $P(\vec{\rho}) \to 0$ as $p \to 0$ or $\rho_1 + \rho_2 \to 0$, which is true because of Theorem 1.5 (whose proof does not depend on Theorem 1.3; see the next section). Thus we conclude that $P(\vec{\rho})$ is continuous on $[0,1]^3$. □

The following is an immediate consequence of the continuity of $P$ and the compactness of $[0,1]^3$.

**Corollary 3.1.** *The function $P$ attains a maximum value on any compact domain. In particular, $P$ attains its maximum at some point in $[0,1]^3$. Moreover, for any $(\rho_1, \rho_2)$ fixed, $P$ as a function of $p$ attains its maximum at some point $p^*$. Similarly, for any fixed $p$, $P$ as a function of $(\rho_1, \rho_2)$ attains maximum at some point $(\rho_1^*, \rho_2^*)$.*

As $P(\vec{\rho})$ is continuous on a compact set, we can conjecture where it attains its maximal values. We start by considering the function $P_n(\vec{p})$ for $n \geq 1$, which is the probability for a $(p, \rho_1, \rho_2)$ correlated pair $(A, B)$ from $I_n$ to be an MSTD set. When $n \to \infty$ this function should converge to our function $P$. We chose $n = 8$ and numerically found all MSTD pairs of subsets $(A, B) \in I_8$. Letting $\mathcal{L}_8$ be the set of all such pairs, we found $|\mathcal{L}_8| = 96$. For each pair $(A, B)$ found, we recorded $|A|$, $|B|$ and $|A \cap B|$. Since each element of $\{0, 1, \ldots, 8\}$ is chosen independently, we can calculate

$$P_8(p, \rho_1, \rho_2) \;=\; \sum_{(A,B)\in\mathcal{L}_8} p^{|A|}(1-p)^{9-|A|}\rho_1^{|A\cap B|}(1-\rho_1)^{|A|-|A\cap B|}\rho_2^{|B|-|A\cap B|}(1-\rho_2)^{9-|A|-|B|+|A\cap B|}. \tag{3.9}$$

We plotted $P_8(\vec{\rho})$ and found its maximum appears to be at $(1/2, 0, 1)$. Numerical explorations suggest that $P(1/2, 0, 1) \approx 0.03$, which is significantly larger than $P(1/2, 1, 0) \approx 4.5 \times 10^{-4}$. These numbers, however, should be taken with a healthy degree of skepticism. These problems are computationally intense, and it is possible that the observed behavior differs for very large $n$. For a related problem with a similar numerical difficulty, see the work in [DKMMWW].

We end with some observations and conjectures. If we fix $0 < p < 1$ and $\rho_1$ not too large, we observe that $P_8$ appears to be a strictly increasing function. If we could prove this, we would then know that it would attain its maximum at $\rho_2 = 1$. On the other hand, if we fix $0 < p < 1$ and $\rho_2$ not too small, $P_8$ appears to be a strictly decreasing function, and thus would attain its maximum at $\rho_1 = 0$. Finally, if we fix $(\rho_1, \rho_2)$, in most cases it appears that the maximum of $P_8$ happens at some point $p$ close to $1/2$. In the specific case when $(\rho_1, \rho_2) = (0, 1)$, if we assume that $P_n$ is differentiable then we can easily prove that $p = 1/2$ is a critical point. Indeed, let $Q_n(p) = P_n(p, 0, 1)$. Since in this case $B = A^c$, we find $Q_n(p) = Q_n(1-p)$. Taking the derivative of both sides yields

$$Q_n'(p) \;=\; -Q'(1-p). \tag{3.10}$$

Consequently, $Q_n'(1/2) = 0$, or $p = 1/2$ is a critical point of $Q_n$, and thus of $P_n$. This suggests the following conjecture.

**Conjecture 3.2.** *The maximum of the function $P$ in $[0,1]^3$ occurs at $(1/2, 0, 1)$, and $P(\vec{\rho}) = P(1/2, 0, 1) \approx 0.03$.*

## 4. WHEN $\vec{p}$ DECAYS WITH $N$

As this section is devoted to generalizing Hegarty-Miller's [HM] work where the density depends on the length of the interval, we use $I_N := \{0, 1, \dots, N\}$ instead of $I_n$ below to be consistent with their notation. By having $\vec{p}$ decay with $N$ we expect that there will not be a positive probability of randomly choosing an MSTD correlated pair.

In Theorem 1.2, we proved that $P(\vec{\rho}) > 0$ unless $p \in \{0, 1\}$ or $\rho_1 + \rho_2 \in \{0, 2\}$. Therefore it is reasonable to consider two types of decay: either $p \to 0$ or $1$ while $\rho_1, \rho_2$ are fixed, or $(\rho_1, \rho_2)$ converges to either $(0, 0)$ or $(1, 1)$ while $p$ is fixed. In this paper we restrict ourselves to the simplest case, where we fix $(\rho_1, \rho_2)$ and let $p \to 0$. We also assume $1/N = o(p(N))$ to guarantee that $\mathbb{E}[|A|] = p(N) \cdot N$ does not tend to $0$, as otherwise $A$ is close to the empty set and the problem becomes trivial. Here we write $p(N)$ to emphasize the fact that $p$ depends on $N$. Later on, we simply write $p$ without causing confusion.

In order to prove the first and second parts of Theorem 1.5, we use the following definition, which resembles $(2.1)$ in [HM].

**Definition 4.1.** *For any $(p, \rho_1, \rho_2)$-correlated random pair $(A, B)$ of $I_N$ and any integer $k \geq 1$, let*

$$A_k \ = \ \{\{(a_1, b_1), \dots, (a_k, b_k)\} \subset A \times B : a_1 + b_1 \ = \ \cdots \ = \ a_k + b_k\}. \tag{4.1}$$

Thus $A_k$ is the set of all unordered $k$-tuples of elements in $A \times B$ having the same sum. While better notation would include $B$, we choose the simpler notation $A_k$ so that the formulas below look like the corresponding ones in [HM].

Let $X_k = |A_k|$, then if $(A, B)$ is a random pair of subsets of $I_N$, $X_k$ is a non-negative integer valued random variable. We first state a useful lemma, whose proof can be found in Appendix B.

**Lemma 4.2.** *Fix $a, b \in I_N$. The probability that the event $a \in A, b \in B$ or $a \in B, b \in A$ happens is $\hat{p} = p^2(2\rho_1 - \rho_1^2) + 2p(1-p)\rho_2$ if $a \neq b$, and $p\rho_1$ if $a = b$.*

**Proposition 4.3.** *With $\hat{p}$ defined as in Lemma 4.2, if $\hat{p} = O(N)$ then for each $k \geq 1$ we have*

$$\mathbb{E}[X_k] \ \sim \ \frac{2}{(k+1)!} \left(\frac{\hat{p}}{2}\right)^k N^{k+1}. \tag{4.2}$$

*Moreover, $X_k \sim \mathbb{E}[X_k]$ whenever $N^{-(k+1)/k} = o(\hat{p})$.*

*Proof.* As much of the proof is similar to that of Lemma 2.1 of [HM], we only give a sketch and prove the different parts. There are two types of $k$-tuples: those consisting of $2k$ distinct elements of $I_N$ (type 1 tuples) and those in which one element is repeated twice in one pair and the sum of each pair is even (type 2 tuples). Let $\xi_{1,k}(N)$ and $\xi_{2,k}(N)$ be the total numbers of $k$-tuples of those two types. As proved in [HM],

$$\xi_{1,k}(N) \ = \ \sum_{n=2k}^{2N-2k} \binom{\min\{\lfloor \frac{n}{2} \rfloor, \lfloor \frac{2N-n}{2} \rfloor\}}{k} \ \sim \ \frac{2}{2^k(k+1)!} N^{k+1} \tag{4.3}$$

and

$$\xi_{2,k}(N) \ = \ O(N^k). \tag{4.4}$$

By Lemma 4.2, the probability for each $k$-tuple of type 1 to occur is $\hat{p}^k$, and that of type 2 is $\hat{p}^{k-1}p\rho_1$. Since $X_k$ can be written as a sum of indicator variable $Y_\alpha$, one for each unordered $k$-tuple $\alpha$ of type 1 or 2, we have

$$\mathbb{E}[X_k] \ = \ \xi_{1,k}(N) \cdot \hat{p}^k + \xi_{2,k}(N) \cdot \hat{p}^{k-1} p\rho_1. \tag{4.5}$$

By the assumption $1/N = o(p)$,

$$\frac{\xi_{2,k}(N)\hat{p}^{k-1}p\rho_1}{\xi_{1,k}\hat{p}^k} \;=\; \frac{O(N^k p\rho_1)}{O(N^{k+1}\hat{p})} \;=\; \frac{1}{O(N[p(2-\rho_1)+2(1-p)\rho_2/\rho_1])} \;=\; o(1). \tag{4.6}$$

Hence

$$\mathbb{E}[X_n] \;\sim\; \xi_{1,k}(N)\cdot\hat{p}^k \;\sim\; \frac{2}{(k+1)!}\left(\frac{\hat{p}}{2}\right)^k N^{k+1}. \tag{4.7}$$

To prove the strong concentration by the mean of $X_k$ whenever $N^{-(k+1)/k} = o(\hat{p})$, we use the standard moment method as in [HM]. We first set some notation. Let

$$\Delta \;:=\; \sum_{\alpha\sim\beta}\mathbb{P}(Y_\alpha \cap Y_\beta), \tag{4.8}$$

where the sum is over pairs of $k$-tuples which have at least one number in common. The proof is completed by showing

$$\Delta \;=\; o(\mathbb{E}[X_k]^2) \;=\; o(N^{2k+2}\hat{p}^{2k}). \tag{4.9}$$

Similar to the previous part, we can prove that the main contribution to $\Delta$ comes from pairs $\{\alpha,\beta\}$ where each $k$-tuple consists of $2k$ distinct elements and has exactly one element in common. As shown in the proof of Lemma 2.1 in [HM], the number of such pairs is $O(N^{2k+1})$. For each of the $4k-1$ elements in $I_N$, the probability they are chosen to be in two $k$-tuples, each tuple containing $2k$ distinct numbers and the two tuples having exactly one common element, is $\hat{p}^{2k-2}\cdot\mathbb{P}(E)$ where $E$ denotes the event for three distinct integers $a,b,c\in I_n$ that the pairs $(a,b)$ and $(a,c)$ are each chosen in a $k$-tuple. We use the following lemma (see Appendix C for a proof).

**Lemma 4.4.** *Notation as above,* $\hat{p}^2/p \;=\; O(\mathbb{P}(E))$.

Using the assumption $1/N = o(p)$ we get

$$\frac{\Delta}{N^{2k+2}\hat{p}^{2k}} \;=\; \frac{O(N^{2k+1})\hat{p}^{2k-2}\mathbb{P}(E)}{N^{2k+2}\hat{p}^{2k}} \;=\; \frac{1}{O(Np)} = o(1), \tag{4.10}$$

or

$$\Delta \;=\; o(N^{2k+2}\hat{p}^{2k}) \;=\; o(\mathbb{E}[X_k]^2) \tag{4.11}$$

as we wish, completing the proof. □

*Proof Theorem 1.5.* We proceed similarly to the proof of Theorem 1.4 in [HM]. Although in our case we consider sums and differences of two sets instead of one, once we have the results in Proposition 4.3, the rest is the same as [HM]. As the arguments are similar, in parts (i) and (ii) below we analyze $\mathscr{S}$ first and then $\mathscr{D}$, while in part (iii) we first study $\mathscr{S}^c$ and then $\mathscr{D}^c$.

**Proof of Part (i):** In this regime $\hat{p} = o(1/N)$. Since $\rho_1,\rho_2$ are fixed, $p^2 = O(\hat{p})$ and hence $N^{-2} = o(\hat{p})$. Thus by (4.2), $\mathbb{E}[X_1]\sim\frac{1}{2}\hat{p}N^2 \gg 1$. Similarly $\mathbb{E}[X_2]\sim\frac{1}{12}N^3\hat{p}^2$ if $N^{-3/2} = o(\hat{p})$ and is $O(1)$ otherwise. Since $\hat{p} = o(1/N)$, $N^3\hat{p}^2 = o(N^2\hat{p})$. Thus in both cases $\mathbb{E}[X_2] = o(\mathbb{E}[X_1])$. Similarly, $\mathbb{E}[X_k] = o(\mathbb{E}[X_1])$ for any $k\geq 2$. In other words, as $N\to\infty$ all but a vanishing portion of pairs of elements in $(A,B)$ have distinct sums. It follows that

$$\mathscr{S} \;\sim\; \mathbb{E}[X_1] \;\sim\; \frac{1}{2}\hat{p}N^2. \tag{4.12}$$

To prove the result for $\mathscr{D}$, we define for each $k\geq 1$

$$A'_k \;:=\; \{\{(a_1,b_1),\ldots,(a_k,b_k)\}\subset A\times B\cup B\times A : a_1-b_1=\cdots=a_k-b_k\neq 0\}, \tag{4.13}$$

and proceed in a completely analogous manner to the proof of $\mathscr{S}$.

**Proof of Part (ii):** In this regime $\hat{p} = c/N$. Thus for any $k \geq 1$, $N^{-(k+1)/k} = o(N^{-1}) = o(\hat{p})$. It follows from (4.2) that

$$X_k \ \sim \ \frac{2}{(k+1)!}\left(\frac{cN^{-1}}{2}\right)^k N^{k+1} \ = \ \frac{2\cdot(c/2)^k}{(k+1)!}N. \tag{4.14}$$

Let $\mathscr{P}$ be the partition on $A_1$ from the relation

$$(a_1, b_1) \ \sim \ (a_2, b_2) \ \text{ if and only if } \ a_1 + b_1 \ = \ a_2 + b_2. \tag{4.15}$$

Let $\tau_i$ denote the number of parts of size $i$ for each $i > 0$. Then $\mathscr{S} = \sum_{i=0}^{\infty} \tau_i$. As proved in [HM],

$$\mathscr{S} \ \sim \ \sum_{k=1}^{\infty}(-1)^{k-1}X_k \ \sim \ 2\left(\sum_{k=1}^{\infty}\frac{(-1)^{k-1}\left(\frac{c}{2}\right)^k}{(k+1)!}\right)\cdot N = g(c/2)N. \tag{4.16}$$

where $g(x) = 2(e^{-x} - (1-x))/x$ as mentioned in theorem 1.5.

The proof for the difference set again proceeds similarly, using (4.13).

**Proof of Part (iii):** We use Lemmas 2.2 and 2.3. Note

$$\mathbb{E}[\mathscr{S}^c] \ = \ \sum_{i=0}^{2N}\mathbb{P}(i \notin A+B) \ \sim \ 4\sum_{i=0}^{\lfloor N/2\rfloor}\rho_3^i \ \sim \ \frac{4}{1-\rho_3}. \tag{4.17}$$

Notice that $1 - \rho_3 = \hat{p}$ since $\rho_3$ and $\hat{p}$ are the probabilities of two complementary events (alternatively, we can check it directly from their formulas). So $\mathbb{E}[\mathscr{S}^c] \sim 4/\hat{p}$. Similarly $\mathbb{E}[\mathscr{D}^c] \sim 2/\hat{p}$. □

**Remark 4.5.** *The phase transition happens when $\hat{p} = \Theta(N^{-1})$. If we let $(\rho_1, \rho_2) = (1, 0)$ then $\hat{p} = p^2$ and our result is consistent with the result in* [HM] *(see Theorem 1.4). If we let $(\rho_1, \rho_2) = (0, 1)$ then $\hat{p} = 2p(1-p) = \Theta(p)$. However, since $1/N = o(p) = o(\hat{p})$, the phase transition never happens. In this $(A, A^c)$ case, the size of the difference set is always almost surely double the size of the sumset, which somewhat supports our conjecture that MSTD pairs are most abundant in the $(A, A^c)$ case.*

## 5. Minimal MSTD pairs

In this section we prove that the minimal MSTD pair of sets has size (3,5) or (4,4).

**Lemma 5.1.** *If $A, B \subset I_n$ is an MSTD pair, then there must exist $a_1 < a_2 < a_3 \in A$ and $b_1 < b_2 < b_3 \in B$ such that $a_1 + b_3 = a_2 + b_2 = a_3 + b_1$.*

*Proof.* Assume there do not exist such $a_i, b_i$. Consider

$$\begin{aligned} I &= \{\{(a,b),(c,d)\} \subset A\times B : a+b = c+d\} \\ J &= \{\{(a,b),(c,d)\} \subset A\times B : a-b = c-d\}. \end{aligned} \tag{5.1}$$

Notice that $a + b = c + d$ if and only if $a - d = c - b$. Hence we have a bijection between $I$ and $J$. In particular, this implies $|I| = |J|$ as they are finite sets.

For each $s \in [0, 2n]$ and $d \in [-n, n]$, define

$$\begin{aligned} X_s &= \{(a,b) \in A\times B : a+b = s\} \\ Y_d &= \{(a,b) \in A\times B : a-b = d\}. \end{aligned} \tag{5.2}$$

It is easy to see that

$$\sum_s |X_s| \;=\; \sum_d |Y_d| \;=\; |A|\cdot|B| \tag{5.3}$$

and

$$|I| \;=\; \sum_{s:|X_s|\geq 2} \binom{|X_s|}{2}; \qquad |J| \;=\; \sum_{d:|Y_d|\geq 2} \binom{|Y_d|}{2}. \tag{5.4}$$

We therefore find

$$\begin{aligned} |\pm(A-B)| \;&\geq\; |A-B| \;=\; \sum_{d\in A-B} 1 \;=\; \sum_{d\in A-B} [|Y_d| - (|Y_d|-1)] \\ &\geq\; \sum_{d\in A-B} |Y_d| - \sum_{d:|Y_d|\geq 2} \binom{|Y_d|}{2} \;=\; |A|\cdot|B| - |J|. \end{aligned} \tag{5.5}$$

Note that this inequality always holds regardless of our assumption. We have a similar inequality for the difference set:

$$\begin{aligned} |A+B| \;&=\; \sum_{s\in A+B} 1 \;=\; \sum_{s\in A+B} [|X_s| - (|X_s|-1)] \\ &\geq\; \sum_{s\in A+B} |X_s| - \sum_{s:|X_s|\geq 2} \binom{|X_s|}{2} \;=\; |A|\cdot|B| - |I|. \end{aligned} \tag{5.6}$$

However, in this case the equality happens because $|X_s| - 1 = \binom{|X_s|}{2}$ as $|X_s| \leq 2$ for all $s$ by our assumption that there do not exist three pairs of the same sum. Hence $|\pm(A-B)| \geq |A||B| - |J| = |A||B| - |I| = |A+B|$, contradicting the assumption that $(A,B)$ is an MSTD pair. □

The intuition behind this lemma is that if there do not exist such $a_i, b_i$, since $a+b=c+d$ if and only if $a-d=c-b$, each *collapsed* sum generates one *collapsed* difference and thus the sumset cannot win. Incidentally, this connects our two observations in the introduction: the property that the difference of any number with itself is equal to 0 is equivalent with the commutativity of addition because $a-a=b-b(=0)$ implies $a+b=b+a$ for any $a,b\in A$. The difference set has the advantage because $0$ is a big *collapsed* difference. To see this explicitly, we write

$$\begin{aligned} |A+A| \;&=\; |A|^2 - |I| + \sum \left[ \binom{|X_s|}{2} - (|X_s|-1) \right] \;=\; M + \sum \frac{(|X_s|-1)(|X_s|-2)}{2} \\ |A-A| \;&=\; |A|^2 - |J| + \sum \left[ \binom{|Y_d|}{2} - (|Y_d|-1) \right] \;=\; M + \sum \frac{(|Y_d|-1)(|Y_d|-2)}{2}, \end{aligned} \tag{5.7}$$

where $M = |A|^2 - |I| = |A|^2 - |J|$. This implies the larger the sizes of $\{X_s\}_{s\in A+B}$ (or $\{Y_d\}_{d\in A-A}$) are, the larger the size of $A+A$ (or $A-A$) is. Hence $Y_0 = |A|$, the biggest size a $Y_d$ or $X_s$ can obtain, will give the difference set a huge advantage. This argument also somewhat supports our conjecture that $(A, A^c)$ MSTD pairs are most abundant, because $0$ is no longer a big collapsed difference.

This purely combinatorial observation can be applied to find some necessary conditions for a set, or a pair of sets to be sum-dominant in any setting (numbers, points in a plane, MSTD sets in two or higher dimension and so on). For example, an MSTD set of $I_n$ must not have only two elements because if so $|X_s| \leq 2$ and hence $|A+A| = M \leq |A-A|$. Likewise, if $A = \{a,b,c\}$ where

$0 \le a < b < c \le n$ is MSTD, then one of $X_s$ must be 3, which means $a+c = b+b = c+a = k$ for some integer $k$. This forces $A$ to be a symmetric set, and therefore not sum-dominant (see [MO]).

Going back to the proof of theorem 1.6, from Lemma 5.1 we immediately obtain the following corollary, as we saw above $A$ must have at least three elements.

**Corollary 5.2.** *There does not exist an MSTD pair $(A, B)$ of size $(2, k)$ or $(k, 2)$ for any $k \ge 2$.*

Theorem 1.6 follows directly from the above corollary and the two following propositions.

**Proposition 5.3.** *There does not exist MSTD pair $(A, B)$ of size $(3, 3)$.*

*Proof.* Our starting point is Lemma 5.1, which gives the existence of a triple in $A$ and a triple in $B$; as each of these sets has cardinality 3, we see these sets equal these special triples. Thus, if such an MSTD pair existed, we would have $A = \{a_1, a_2, a_3\}$ and $B = \{b_1, b_2, b_3\}$, with $|A + B| > |(A - B) \cup (B - A)|$, $a_1 < a_2 < a_3$ and $b_1 < b_2 < b_3$. Lemma 5.1 then implies $a_1 + b_3 = a_2 + b_2 = a_3 + b_1$, which gives $|A + B| \le 9 - 2 = 7$ because we have at least two *collapsed* sums. Without loss of generality we may assume $a_1 \le b_1$ and $a_1 = 0$.

`Case 1:` $b_1 = a_1$`:` As $b_1 = a_1$ we have $a_3 = b_3$. If $a_2 = b_2$ then $A = B$. This cannot be sum-dominant because the smallest sum-dominant set has size 8. So $a_2 \ne b_2$, and there are at least 3 positive differences $a_2, b_2, a_3$ in $(A-B)\cup(B-A)$. Since $0 \in A-B$, $|(A-B)\cup(B-A)| \ge 7 \ge |A+B|$, a contradiction.

`Case 2:` $b_1 > a_1$`:` In this case $b_1 < b_2 < b_3$ are 3 positive distinct numbers in $B - A$. Thus $|(A-B)\cup(B-A)| \ge 6$. Since $|A+B| \le 7$ we must have $(A-B)\cup(B-A)| = \{\pm b_1, \pm b_2, \pm b_3\}$. As $-b_3 < b_1 - a_3 < b_1 - a_2 < b_1$, it must happen that $b_1 - a_3 = -b_2$ and $b_1 - a_2 = -b_1$, or $a_2 = 2b_1$ and $a_3 = 2b_1 + b_2$. The difference $b_2 - a_2 = b_2 - 2b_1$ is bigger than $-b_1$ but less than $b_2$, and the only number in $\pm(A - B)$ between those two numbers is $b_1$, hence $b_2 - 2b_1 = b_1$, or $b_2 = 3b_1$. Letting $b = b_1$, we can rewrite the pair $(A, B)$ as $A = \{0, 2b, 4b\}$ and $B = \{b, 3b, 5b\}$. It is easy to check that this is not an MSTD pair. □

**Proposition 5.4.** *There does not exist an MSTD pair $(A, B)$ of size $(3, 4)$.*

The proof of this proposition is similar to that of Proposition 5.3, except there are many more cases. Details can be found in Appendix D. This completes the proof of Theorem 1.6. □

## 6. Conclusion and future work

We extended the results of [He, HM, MO, Zh2] of MSTD sets to MSTD correlated pairs. In particular, we proved that for each $\vec{\rho} = (p, \rho_1, \rho_2) \in [0, 1]^3$ the limiting probability $P(\vec{\rho})$ of picking an MSTD $\vec{\rho}$-correlated pair exists and is positive unless $p \in \{0, 1\}$ or $\rho_1 + \rho_2 \in \{0, 2\}$. Furthermore, the function $P(\vec{\rho})$ is continuous and thus attains its maximum at some point, which we conjecture is $(1/2, 0, 1)$. We characterize the phase transition when we let $\vec{\rho}$ decay with $n$. Finally, we found the minimal size of an MSTD pair $(A, B)$.

We end with some of the more interesting and important open questions.

(1) Prove or disprove Conjecture 3.2.
(2) Find an efficient algorithm to calculate values of $P(\vec{\rho})$, and investigate further the analytic properties of $P$.
(3) Prove the strong concentration of $\mathscr{S}^c$ and $\mathscr{D}^c$ in the case of slow decay (i.e., when $N^{-1/2} = o(\hat{p})$). Do similar results hold for other types of decay, namely $p \to 1$ or $(\rho_1, \rho_2) \to (0, 0), (1, 1)$?

(4) Are the examples of the MSTD pairs of size $(4,4)$ and $(3,5)$ found in Theorem 1.6 unique up to linear transformation?
(5) Generalize the results from [ILMZ] to linear combinations of correlated sets.

## APPENDIX A. PROOF OF LEMMAS 2.2 AND 2.3

*Proof of Lemma 2.2.* Let $E_{a,b}$ denote the event ($a \in A$ and $b \in B$) or ($a \in B$ and $b \in A$). For each $k \in I_n$, $k$ is not in $A+B$ if and only if for every pair $(a,b)$ in $[0,n]$ with $k = a+b$, the event $E_{a,b}$ does not happen. Let $E^c$ be short for $E^c_{a,b}$- the complement of $E_{a,b}$.

If $a \neq b$ then by Bayes' formula

$$\begin{aligned}\mathbb{P}(E^c) &= \mathbb{P}(E^c|a\in A, b\in A)\mathbb{P}(a\in A, b\in A) + \mathbb{P}(E^c|a\in A, b\notin A)\mathbb{P}(a\in A, b\notin A)\\ &\quad + \mathbb{P}(E^c|a\notin A, b\in A)\mathbb{P}(a\notin A, b\in A) + \mathbb{P}(E^c|a\notin A, b\notin A)\mathbb{P}(a\in A, b\notin A)\\ &= (1-\rho_1)^2p^2 + 2(1-\rho_2)p(1-p) + (1-p)^2 = \rho_3. \end{aligned} \tag{A.1}$$

If $a = b$, then similarly we find

$$\mathbb{P}(E^c) \;=\; \mathbb{P}(E^c|a\in A)\mathbb{P}(a\in A) + P(E^c|a\notin A)P(a\notin A) = (1-\rho_1)p + (1-p) = \rho_4. \tag{A.2}$$

Assume there are $W$ ways to write $k$ as sum of two elements $k = a_1+b_1 = \cdots = a_W + b_W$. Since no element is repeated in two different pairs (because if $a+b = a+c = k$ then $b = c$), the event each pair does not appear in $A$ is independent with each other: $E^c_{a_i,b_i}$ and $E^c_{a_j,b_j}$ are independent for all $i \neq j$. Therefore

$$\mathbb{P}(k\notin A+B) \;=\; \mathbb{P}\left(\bigcap_{i=1}^{W} E^c_{a_i,b_i}\right) \;=\; \prod_{i=1}^{W}\mathbb{P}\left(E^c_{a_i,b_i}\right). \tag{A.3}$$

It remains to count how many ways $k$ can be written as sum of two elements in $I_n$. First assume $k$ is odd. In this case $\mathbb{P}(E^c_{a_i,b_i}) = \rho_3$ for all $i$ because $k$ cannot be twice a number. If $0 \le k \le n$, there are $\frac{k+1}{2}$ ways to write $k$ as sum of two numbers:

$$k \;=\; 0+k \;=\; 1+(k-1) \;=\; \cdots \;=\; \frac{k-1}{2} + \frac{k+1}{2}. \tag{A.4}$$

If $n < k \le 2n$ there are $\frac{2n-k+1}{2}$ such ways:

$$k \;=\; n+(k-n) \;=\; (n-1)+(k-n+1) \;=\; \cdots \;=\; \frac{k+1}{2} + \frac{k-1}{2}. \tag{A.5}$$

Hence

$$\mathbb{P}(k\notin A+B) \;=\; \rho_3^{\min\{\frac{k+1}{2}, \frac{2n-k}{2}\}} \tag{A.6}$$

Now for even $k$, $\mathbb{P}(E^c_{a_i,b_i})$ is $\rho_4$ when $a_i = b_i = k/2$ and is $\rho_3$ otherwise. Similar to before, there are $\frac{k}{2}$ ways to write $k$ as sum of two *different* numbers if $0 \le k \le n$ and there are $\frac{2n-k}{2}$ such ways if $k > n$. As a consequence

$$\mathbb{P}(k\notin A+B) \;=\; \rho_4\rho_3^{\min\{\frac{k}{2}, \frac{2n-k}{2}\}}, \tag{A.7}$$

which completes the proof of lemma 2.2 □

*Proof of Lemma 2.3.* We write $k$ as differences of two elements in $I_n$: $k = k-0 = (k+1)-1 = \cdots$. If $k > n/2$, no element is repeated in two pairs, thus similar to Lemma 2.2 we have $\mathbb{P}(k \notin \pm(A-B)) = \rho_3^{n-k}$.

If $k \le n/2$, we use the same method used in Lemma 10 of [MO]. Define the set

$$J \;=\; \left\{ j : 0 < j < n-k; \quad \left\lfloor \frac{j}{k} \right\rfloor \text{ is even} \right\}. \tag{A.8}$$

In other words, $J$ contains the first $k$ integers starting at $a$, then omits the next $k$ integers, and so on. It is easy to see that $|J| \ge n/3$ and $j + k \notin J$ if $j \in J$. Therefore, if we write $k = a_i - b_i$ for $b_i \in J$, we are guaranteed that the $a_i$ and $b_i$ are all distinct. We then have the same independence as before, hence

$$\mathbb{P}(k \notin \pm(A-B)) \;\le\; \mathbb{P}(\cup_{a_i - b_i = k, b_i \in J}(a_i, b_i) \notin (A \times B) \cup (B \times A)) \;=\; \rho_3^{|J|} \le \rho_3^{n/3}. \tag{A.9}$$

□

## APPENDIX B. PROOF OF LEMMA 4.2

*Proof of Lemma 4.2.* Denote the event in the lemma by $E$. We break the analysis into two cases, depending on whether or not $a$ equals $b$.

`Case I:` $a \neq b$`:` We apply Bayes' formula to $E$. Our partition is the four disjoint events on whether or not $a$ or $b$ is in $A$.

$$\begin{aligned}
\mathbb{P}(E) &= \mathbb{P}(E|a \in A, b \in A) \cdot \mathbb{P}(a \in A, b \in A) + \mathbb{P}(E|a \in A, b \notin A) \cdot \mathbb{P}(a \in A, b \notin A) \\
&\quad + \mathbb{P}(E|a \notin A, b \in A) \cdot \mathbb{P}(a \notin A, b \in A) + \mathbb{P}(E|a \notin A, b \notin A) \cdot \mathbb{P}(a \notin A, b \notin A) \\
&= (1 - (1-\rho_1)^2) \cdot p^2 + \rho_2 \cdot p(1-p) + \rho_2 \cdot p(1-p) + 0 \\
&= p^2(2\rho_1 - \rho_1^2) + 2p(1-p)\rho_2.
\end{aligned} \tag{B.1}$$

`Case II:` $a = b$`:` We proceed similarly, and find

$$\mathbb{P}(E) \;=\; \mathbb{P}(E|a \in A) \cdot \mathbb{P}(a \in A) + \mathbb{P}(E|a \notin A) \cdot \mathbb{P}(a \notin A) \;=\; \rho_1 \cdot p. \tag{B.2}$$

□

## APPENDIX C. PROOF OF LEMMA 4.4

*Proof of Lemma 4.4.* Let $E$ be the event from the lemma, and consider the events $E_1 = (a \in A, b \in B)$ and $(a \in B, b \in A)$, and $E_2 = (a \in A, c \in B)$ and $(a \in B, c \in A)$. It immediately follows that $E = E_1 \cap E_2$. We again use Bayes' formula, with our partition the four distinct events arising from whether or not $a$ and $b$ are in $A$ and $B$. We find

$$\begin{aligned}
\mathbb{P}(E) &= \mathbb{P}(E|a \in A, a \in B) \cdot \mathbb{P}(a \in A, a \in B) + \mathbb{P}(E|a \in A, a \notin B) \cdot \mathbb{P}(a \in A, a \notin B) \\
&\quad + \mathbb{P}(E|a \notin A, a \in B) \cdot \mathbb{P}(a \notin A, a \in B) + \mathbb{P}(E|a \notin A, a \notin B) \cdot \mathbb{P}(a \notin A, a \notin B) \\
&= [p^2 + 2p(1-p)\rho_2 + (1-p)^2\rho_2^2] \cdot p\rho_1 \\
&\quad + [p^2\rho_1^2 + 2p(1-p)\rho_1\rho_2 + (1-p)^2\rho_2^2] \cdot p(1-\rho_1) + p^2 \cdot (1-p)\rho_2 + 0 \\
&= p(1-p)^2\rho_2^2 + 2p^2(1-p)\rho_1\rho_2(2-\rho_1) + p^3\rho_1(1 + \rho_1 - \rho_1^2) + p^2(1-p)\rho_2.
\end{aligned} \tag{C.1}$$

Note that we also use Bayes' formula to calculate $\mathbb{P}(E|a \in A, a \in B)$ and so on by dividing into four cases depending on whether or not each $b, c$ is in $A$ or not. Thus

$$\begin{aligned}
\hat{p}^2 &= \left[p^2\rho_1(2-\rho_1) + 2p(1-p)\rho_2\right]^2 \\
&= p^4\rho_1^2(2-\rho_1)^2 + 4p^3(1-p)\rho_1\rho_2(2-\rho_1) + 4p^2(1-p)^2\rho_2^2.
\end{aligned} \tag{C.2}$$

Since $p \to 0$ and $\rho_1, \rho_2$ are fixed, both $p\mathbb{P}(E)$ and $\hat{p}^2$ have form $Ap^2 + o(p^2)$ for some $A > 0$; hence $\hat{p}^2 = O(p\mathbb{P}(E))$ as desired. □

## APPENDIX D. PROOF OF PROPOSITION 5.4

*Proof of Proposition 5.4.* Assume $A = \{a_1, a_2, a_3\}$ and $B = \{b_1, b_2, b_3, b_4\}$ be an MSTD pair in $I_n$ where $0 \le a_1 < a_2 < a_3 \le n$ and $0 \le b_1 < b_2 < b_3 < b_4 \le n$.

**Lemma D.1.** *We have $d \in A - B$ if and only if $-d \in A - B$.*

*Proof.* By Lemma 5.1, there must exist a number $s$ such that $|X_s| = 3$, or $a_1 + b_i = a_2 + b_j = a_3 + b_k = s$ for some $1 \le k < j < i \le 4$. There are four possibilities for $(k, j, i)$, which are $(1, 2, 3), (1, 2, 4), (1, 3, 4)$ and $(2, 3, 4)$.

It is easy to see that there is no $t$ such that $|X_t| \ge 4$. If there exists another number $s' \ne s$ such that $|X_s| = |X_{s'}| = 3$, equivalently there exists $(i', j', k')$ such that $a_1 + b_{i'} = a_2 + b_{j'} = a_3 + b_{k'} = s'$. Since $s \ne s'$, $i \ne i'$, $j \ne j'$ and $k \ne k'$. The only possibility is $(k, j, i) = (1, 2, 3)$ and $(k', j', i') = (2, 3, 4)$ or vice versa. In either case,

$$a_1 + b_3 = a_2 + b_2 = a_3 + b_1 \tag{D.1}$$

$$a_1 + b_4 = a_2 + b_3 = a_3 + b_2. \tag{D.2}$$

Subtracting those two chains of equalities gives $b_4 - b_3 = b_3 - b_2 = b_2 - b_1$; let this common difference be $d$. From (D.1), $a_2 - a_1 = b_3 - b_2 = d$ and $a_3 - a_2 = b_2 - b_1 = d$, which means $(a_i)$ and $(b_i)$ are two arithmetic sequences with same distance. It is easy to check that in this case $(A, B)$ is not an MSTD pair.

This implies there exists exactly one $s \in A + B$ such that $|X_s| = 3$. From the proof of Lemma 5.1, we see that in order for $|A + B| > | \pm (A - B)|$, it must happen $|Y_d| \le 2$ for all $d \in A - B$, and $| \pm (A - B)| = |A - B|$, which means if $d \in A - B$, so is $-d$ and vice versa. □

From Lemma D.1, we see that the smallest and largest numbers in $A - B$, which are $a_1 - b_4$ and $a_3 - b_1$ respectively, must be inverses of each other. So

$$a_3 - b_1 = b_4 - a_1 \tag{D.3}$$

`Case 1:` $a_1 + b_4 \ne a_3 + b_1$ : so $(k, j, i) = (1, 2, 3)$ or $(2, 3, 4)$. It is easy to see that if $(A, B)$ is an MSTD pair, so is $(n - A, n - B)$ where $n - X = \{n - x : x \in X\}$. Therefore without loss of generality we can assume $(k, j, i) = (2, 3, 4)$, or $a_1 + b_4 = a_2 + b_3 = a_3 + b_2$. Since we can translate the set by a number, assume $b_1 = 0$ (now $a_i, b_i$ are not necessary in $I_n$). From (D.3), $a_1 = b_4 - a_3 = b_2 - a_1$, or $b_2 = 2a_1$. As $b_1 < b_2, 0 < 2a_1$, or $a_1 > 0$. We can rewrite $b_i$ by $a_i$ as follows: $b_1 = 0; b_2 = 2a_1; b_4 = a_3 - b_1 + a_1 = a_1 + a_3; b_2 = a_1 + b_4 - a_2 = 2a_1 + a_3 - a_2$. So

$$A = \{a_1, a_2, a_3\}; \quad B = \{0, 2a_1, 2a_1 + a_3 - a_2, a_3\}. \tag{D.4}$$

We can now write down all elements (might be repeated) of $A - B$ which are $\{\pm a_1, \pm a_3, a_2, a_2 - a_1 - a_3, a_2 - 2a_1, 2a_2 - 2a_1 - a_3, a_3 - 2a_1\}$. By Lemma D.1, $a_2 \in A - B \Rightarrow -a_2 \in A - B$, thus one of 4 numbers $\{a_2 - a_1 - a_3, a_2 - 2a_1, 2a_2 - 2a_1 - a_3, a_3 - 2a_1\}$ must be equal to $-a_2$.

`Case 1.1:` $a_2 - 2a_1 = -a_2$ or $a_1 = a_2$, a contradiction.
`Case 1.2:` $a_3 - 2a_1 = -a_2$, or $a_3 = 2a_1 - a_2 < a_1$, a contradiction.
`Case 1.3:` $a_2 - a_1 - a_3 = -a_2$ or $a_1 + a_3 = 2a_2$. Let $a_2 - a_1 = a_3 - a_2 = d$, then $A = \{a_1, a_1 + d, a_1 + 2d\}$ and $B = \{0, 2a_1, 2a_1 + d, 2a_1 + 2d$. We can directly check that this pair is not sum-dominant.

`Case 1.4:` $2a_2 - 2a_1 - a_3 = -a_2$, or $2a_1 + a_3 = 3a_2$. Let $a_2 - a_1 = d$, then $a_3 - a_2 = 2a_2 - 2a_1 = 2d$. Then $A = \{a_1, a_1 + d, a_1 + 3d\}$ and $B = \{0, 2a_1, 2a_1 + 2d, 2a_1 + 3d$. Again it is straightforward to check that this pair is not MSTD.

`Case 2:` $a_1 + b_4 = a_3 + b_1$: two pairs $(a_1, b_4)$ and $(a_3, b_1)$ have same sums and differences, hence $a_1 = b_1$ and $a_3 = b_4$. Without loss of generality, assume $a_1 = b_1 = 0$ (as we can translate everything by $-a_1$) and $a_2 + b_2 = a_3$. Rewrite

$$A = \{0, a_2, a_3\}, \quad B = \{0, a_3 - a_2, b_3, a_3\}. \tag{D.5}$$

$A-B$ consists of at most 9 elements $\{0, a_2, \pm a_3, a_2-a_3, 2a_2-a_3, -b_3, a_2-b_3, a_3-b_3\}$. By Lemma D.1, $-b_3 \in A - B \Rightarrow -b_3 \in A - B$. Since $0 < b_3 < a_3$, one of $\{a_2, 2a_2 - a_3, a_2 - b_3, a_3 - b_3\}$ must be equal to $b_3$.

`Case 2.1:` $a_2 = b_3$.
`Case 2.2:` $2a_2 - a_3 = b_3$.
`Case 2.3:` $a_2 - b_3 = b_3$.
`Case 2.4:` $a_3 - b_3 = b_3$.

In the first case, $|Y_0| = 3$ because $0 = a_1 - b_1 = a_2 - b_3 = a_3 - b_4$, which contradicts our observation before that $|Y_d| \le 2$ for all $d \in A - B$. In any of the other three latter cases, we reduce our sets to two variables $a_2$ and $a_3$. Continuing our argument based on Lemma D.1, we can find a relation between $a_2$ and $a_3$ and check again to see that there is no such MSTD pair. This completes the proof of Proposition 5.4. □

## REFERENCES


[DKMMWW] T. Do, A. Kulkarni, S. J. Miller, D. Moon, J. Wellens and J. Wilcox, *Sets Characterized by Missing Sums and Differences in $\mathbb{Z}^D$*, preprint 2013. http://arxiv.org/pdf/1406.2052.pdf.

[He] P. Hegarty, *Some explicit constructions of sets with more sums than differences*, Acta Arithmetica **130** (2007), no. 1, 61–77.

[HM] P. Hegarty and S. J. Miller, *When almost all sets are difference dominated*, Random Structures and Algorithms **35** (2009), no. 1, 118-136.

[ILMZ] 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.

[MO] G. Martin and K. O'Bryant, *Many sets have more sums than differences*, Additive Combinatorics, CRM Proc. Lecture Notes, vol. 43, Amer. Math. Soc., Providence, RI, 2007, pp. 287–305.

[MOS] S. J. Miller, B. Orosz, and D. Scheinerman, *Explicit constructions of infinite families of MSTD sets*, *Journal of Number Theory* **130** (2010), 1221–1233.

[MPR] S. J. Miller, S. Pegado and S. Luc Robinson, *Explicit Constructions of Large Families of Generalized More Sums Than Differences Sets* Integers **12** (2012), #A30.

[Na] M. B. Nathanson, *Sets with more sums than differences*, Integers: Electronical Journal of Combinatorical Number Theory **7** (2007), #A5.

[Zh1] Y. Zhao, *Constructing MSTD sets using bidirectional ballot sequences*, Journal of Number Theory **130** (2010), 1212–1220.

[Zh2] Y. Zhao, *Sets Characterized by Missing Sums and Differences*, Journal of Number Theory **131** (2011), 2107–2134.


*E-mail address*: thao.do@stonybrook.edu

MATHEMATICS DEPATTMENT, STONY BROOK UNIVERSITY, STONY BROOK, NY, 11794

*E-mail address*: auk@andrew.cmu.edu

DEPARTMENT OF MATHEMATICAL SCIENCES, CARNEGIE MELLON UNIVERSITY, PITTSBURGH, PA 15213

*E-mail address*: sjm1@williams.edu, Steven.Miller.MC.96@aya.yale.edu

DEPARTMENT OF MATHEMATICS AND STATISTICS, WILLIAMS COLLEGE, WILLIAMSTOWN, MA 01267

*E-mail address*: dm7@williams.edu

DEPARTMENT OF MATHEMATICS & STATISTICS, WILLIAMS COLLEGE, WILLIAMSTOWN, MA 01267

*E-mail address*: jwellens@caltech.edu

DEPARTMENT OF MATHEMATICS, CALIFORNIA INSTITUTE OF TECHNOLOGY, PASADENA, CA 91125