SETS CHARACTERIZED BY MISSING SUMS AND DIFFERENCES IN DILATING POLYTOPES

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

ABSTRACT. A sum-dominant set is a finite set A of integers such that $|A+A| > |A-A|$. As a typical pair of elements contributes one sum and two differences, we expect sum-dominant sets to be rare in some sense. In 2006, however, Martin and O'Bryant showed that the proportion of sum-dominant subsets of $\{0,\dots,n\}$ is bounded below by a positive constant as $n \to \infty$. Hegarty then extended their work and showed that for any prescribed $s, d \in \mathbb{N}_0$, the proportion $\rho_n^{s,d}$ of subsets of $\{0,\dots,n\}$ that are missing exactly s sums in $\{0,\dots,2n\}$ and exactly $2d$ differences in $\{-n,\dots,n\}$ also remains positive in the limit.

We consider the following question: are such sets, characterized by their sums and differences, similarly ubiquitous in higher dimensional spaces? We generalize the integers in a growing interval to the lattice points in a dilating polytope. Specifically, let P be a polytope in $\mathbb{R}^D$ with vertices in $\mathbb{Z}^D$, and let $\rho_n^{s,d}$ now denote the proportion of subsets of $L(nP)$ that are missing exactly s sums in $L(nP)+L(nP)$ and exactly $2d$ differences in $L(nP)-L(nP)$. As it turns out, the geometry of P has a significant effect on the limiting behavior of $\rho_n^{s,d}$. We define a geometric characteristic of polytopes called local point symmetry, and show that $\rho_n^{s,d}$ is bounded below by a positive constant as $n \to \infty$ if and only if P is locally point symmetric. We further show that the proportion of subsets in $L(nP)$ that are missing exactly s sums and at least $2d$ differences remains positive in the limit, independent of the geometry of P. A direct corollary of these results is that if P is additionally point symmetric, the proportion of sum-dominant subsets of $L(nP)$ also remains positive in the limit.

CONTENTS

Date: June 20, 2014.

2010 *Mathematics Subject Classification.* 11P99 (primary), 11K99 (secondary).

Key words and phrases. Sum dominated sets, more sum than difference sets, convex sets.

This research was conducted as part of the 2013 SMALL REU program at Williams College and was partially supported funded by NSF grant DMS0850577 and Williams College; the third named author was also partially supported by NSF grant DMS1265673. We would like to thank our colleagues from the Williams College 2013 SMALL REU program, especially Frank Morgan, as well as Kevin O'Bryant for helpful conversations.

1. INTRODUCTION

Given a finite set $A \subset \mathbb{Z}$, we define the sumset $A + A$ and the difference set $A - A$ by

$$\begin{aligned} A + A &= \{a_1 + a_2 : a_1, a_2 \in A\}, \\ A - A &= \{a_1 - a_2 : a_1, a_2 \in A\}. \end{aligned} \tag{1.1}$$

It is natural to compare the sizes of $A + A$ and $A - A$ as we vary A over a family of sets. As addition is commutative while subtraction is not, a pair of distinct elements $a_1, a_2 \in A$ generates two differences $a_1 - a_2$ and $a_2 - a_1$ but only one sum $a_1 + a_2$. We thus expect that most of the time, the size of the difference set is greater than that of the sumset—that is, we expect most sets A to be *difference-dominant*. It is possible, however, to construct sets whose sumsets have more elements than their difference sets. Such sets are called *sum-dominant* or *More Sums Than Differences* (MSTD) sets. The first example of an MSTD set was discovered by Conway in the 1960s: $\{0, 2, 3, 4, 7, 11, 12, 14\}$. A set whose sumset has the same number of elements as its difference set is called *balanced*.

We briefly review some of the key results in the field. In 2006, Martin and O'Bryant [MO] showed that not only do MSTD sets exist, but there exist many of them in some sense. In particular, they proved that the proportion ρ_n of subsets of $\{0, 1, \dots, n\}$ that are MSTD is bounded below by a positive constant as $n \to \infty$. They show that similar results hold as well for balanced and difference-dominant sets. Hegarty [He] then extended their work and showed that for any $s, d \in \mathbb{N}_0$, the proportion $\rho_n^{s,d}$ of subsets $A \subset \{0, 1, \dots, n\}$ satisfying

$$|\{0, 1, \dots, 2n\} \setminus (A + A)| = s, \quad |\{-n, -n+1, \dots, n-1, n\} \setminus (A - A)| = 2d \tag{1.2}$$

also remains bounded below by a positive constant in the limit. Later, in 2010, Zhao [Z] showed that both ρ_n and $\rho_n^{s,d}$ converge as $n \to \infty$, with ρ_n approaching a limit $\rho \simeq 4.5 \times 10^{-4}$.

This previous work explored the behavior of sums and differences of sets in the one-dimensional lattice $\mathbb{Z}$. In particular it was observed that sum-dominant, balanced, and difference-dominant sets, as well as sets with even greater constraints on missing sums and differences, are all surprisingly ubiquitous on the line. A natural question arises: are such sets similarly common in other spaces?

In this paper, we extend the theory to sets in higher dimensional lattices, namely $\mathbb{Z}^D$ for any $D > 0$.[1] Interesting new features and complications arise in higher dimensions. Whereas on the line it is natural to consider subsets of the integers in a growing interval, in higher dimensions we can begin to consider different geometries for our overall subset region. A natural high-dimensional analogue of the interval is a convex polytope. We examine in particular the additive behavior of the lattice points in an arbitrary dilating D-dimensional convex polytope with lattice point vertices.

Let P be a convex polytope in $\mathbb{R}^D$ with vertices in $\mathbb{Z}^D$. For any set $S \subset \mathbb{R}^D$, let $L(S)$ denote the set of lattice points contained in S; that is, $L(S) = S \cap \mathbb{Z}^D$. Furthermore, let nS denote the dilation of S by a factor of n about the origin. In the spirit of Hegarty, we focus our attention to the proportion $\rho_n^{s,d}$ of subsets $A \subset L(nP)$ such that

$$|(L(nP) + L(nP)) \setminus (A + A)| = s, \quad |(L(nP) - L(nP)) \setminus (A - A)| = 2d, \tag{1.3}$$

for any prescribed $s, d \in \mathbb{N}_0$. In this paper we assume that P is fixed, and revert to the more informal description that such subsets A are missing exactly s sums and missing exactly $2d$ differences. Studying missing sums and differences rather than the number of sums and differences is the natural generalization of the 1-dimensional results, which we discuss at the end of this section and in Section 6.

[1] See [DKMMW] for another generalization to sums and differences of correlated random pairs of sets in $\mathbb{Z}$.

The geometry of P has a significant effect on the limiting behavior of $\rho_n^{s,d}$. Before we state our main results, we introduce some terminology that helps us distinguish between polytopes.

Definition 1.1. *Let P be a convex polytope. Vertices $\mathbf{u}$ and $\mathbf{v}$ of P are* strictly antipodal *if there exist parallel supporting hyperplanes, H_1 and H_2, of P such that $H_1 \cap P = \{\mathbf{u}\}$ and $H_2 \cap P = \{\mathbf{v}\}$.*

Definition 1.2. *Given a vertex $\mathbf{v}$ of P, the* supporting cone $C(\mathbf{v})$ *at $\mathbf{v}$ is the set*

$$\mathbf{v} + \bigcup_{\lambda \geq 0} \lambda(P - \mathbf{v}). \tag{1.4}$$

Equivalently, $C(\mathbf{v})$ is the convex hull of the half-lines formed by extending the edges of P at v.

Definition 1.3. *A polytope P is* point symmetric *if there exists a point $\mathbf{x}$ such that $P = \mathbf{x} - P$.*

Definition 1.4. *A convex polytope P with m vertices is* locally point symmetric *if its vertices can be partitioned into $m/2$ pairs of strictly antipodal vertices such that for each pair $\{\mathbf{u}, \mathbf{v}\}$,*

$$C(\mathbf{u}) - \mathbf{u} \;=\; \mathbf{v} - C(\mathbf{v}). \tag{1.5}$$

Note we subtract the vertex above (in $C(\mathbf{u}) - \mathbf{u}$ and $\mathbf{v} - C(\mathbf{v})$) so that the supporting cones are standardized with their apexes at the origin.

Example 1.5. *Any point symmetric polytope is locally point symmetric.*

Example 1.6. *Consider the hexagon $ABCDEF$ in Figure 1, where A and D, B and E, and C and F form pairs of strictly antipodal vertices. As $\overline{AB}$ and $\overline{DE}$, $\overline{BC}$ and $\overline{EF}$, and $\overline{CD}$ and $\overline{FA}$ form pairs of parallel edges, $ABCDEF$ is locally point symmetric.*

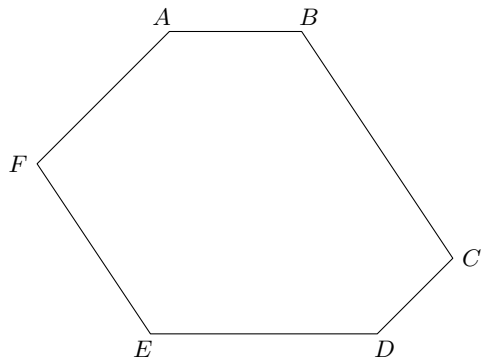

FIGURE 1. A locally point symmetric hexagon.

As it turns out, whether P has local point symmetry determines whether $\rho_n^{s,d}$ remains positive in the limit. We prove the following result.

Theorem 1.7. *Let P be a convex polytope in $\mathbb{R}^D$ with vertices in $\mathbb{Z}^D$, and let $s, d \in \mathbb{N}_0$ be given. There exists a constant $c_{s,d} > 0$ such that, for sufficiently large n, at least $c_{s,d} \cdot 2^{|L(nP)|}$ of the subsets of $L(nP)$ have exactly s missing sums and exactly $2d$ missing differences if and only if P is locally point symmetric.*

We restrict ourselves to polytopes with lattice point vertices because, as we will see, this allows us to exploit results in the one-dimensional case. The main idea behind Theorem 1.7 is that convex polytopes without local point symmetry (and these constitute the vast majority of convex polytopes) have many uniquely formed differences as they dilate by n. That is, there exist

many differences $\mathbf{k} \in L(nP) - L(nP)$ each of for which there exists a unique pair of elements $\mathbf{p}, \mathbf{q} \in L(nP)$ that satisfies $\mathbf{k} = \mathbf{p} - \mathbf{q}$. This makes it vanishingly unlikely as n grows that there is a constant number of missing differences in the region $L(nP) - L(nP)$.

On the other hand, we can weaken our condition on the number of missing differences and obtain a positive proportion in the limit, independent of the geometry of P.

Theorem 1.8. *Let P be a convex polytope in $\mathbb{R}^D$ with vertices in $\mathbb{Z}^D$, and let $s, d \in \mathbb{N}_0$ be given. There exists a constant $c_{s,d} > 0$ such that, for sufficiently large n, at least $c_{s,d} \cdot 2^{|L(nP)|}$ of the subsets of $L(nP)$ have exactly s missing sums and at least $2d$ missing differences.*

As mentioned above, studying missing sums and differences provides a more natural framework in which to consider the additive behavior of high-dimensional sets. If $D = 1$, and therefore P is an interval, then setting $2d > s$ in the theorems above implies a positive lower bound on the proportion of MSTD subsets of $L(nP)$ as $n \to \infty$; this is Hegarty's generalization [He] of the results of Martin and O'Bryant [MO]. The reason for this is that the overall set region $L(nP)$ is itself balanced, and thus having more sums than differences is equivalent to having more missing differences than missing sums. This is occasionally true in higher dimensions as well. For example, consider subsets A of the square $S_n := \{(x, y) : x, y \in \{0, \dots, n\}\}$. We see that $A + A$ lives in the square $S_n + S_n = \{(x, y) : x, y \in \{0, \dots, 2n\}\}$ and $A - A$ lives in the square $S_n - S_n = \{(x, y) : x, y \in \{-n, \dots, n\}\}$, both regions having $(2n + 1)^2$ elements.

As our polytope P varies, however, it is much more typical that the difference set region $L(nP) - L(nP)$ is larger than the sumset region $L(nP) + L(nP)$. If we now consider subsets A of the triangle $T_n := \{(x, y) \in \mathbb{Z}^2 : x \geq 0, y \geq 0, x + y \leq n\}$, then $A + A$ lives inside $T_n + T_n$, which has $2n^2 + 3n + 1$ elements, while $A - A$ lives inside $T_n - T_n$, which has $3n^2 + 3n + 1$ elements; see Figure 2. Observe that $|T_n - T_n| - |T_n + T_n| = n^2$. Since we fix the number $2d$ of missing differences independently of n, any $A \subset T_n$ that is missing exactly $2d$ differences will, for sufficiently large n, always result in a difference set $A - A$ that has more elements than is even possible in the sumset $A + A$.

Thus, Theorems 1.7 and 1.8 do not imply that the proportion of MSTD subsets of $L(nP)$ remains positive in the limit. In future study, we may begin to examine MSTD sets in higher dimensions by allowing d to depend on n—in the case of the triangle set T_n, a subset $A \subset T_n$ missing exactly s sums and exactly $2d$ differences is MSTD if and only if $d > s + n^2$. We discuss this in more detail in Section 6, and conjecture that the proportion of such subsets approaches 0 if $L(P)$ is not balanced. At the very least, Theorem 1.7 implies positive proportions of sum-dominant, balanced, and difference-dominant subsets in the limit if we add the assumption that $L(P)$ is balanced. It is simple to show that $L(P)$ is balanced if P is point symmetric. Thus, we have

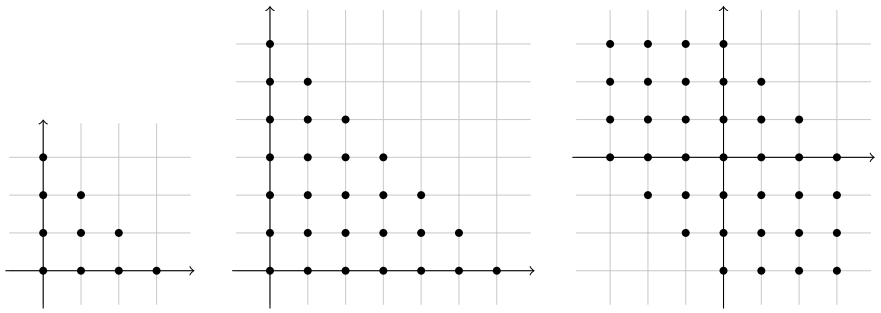

FIGURE 2. Left: T_3 with 10 elements. Middle: $T_3 + T_3$ with 28 elements. Right: $T_3 - T_3$ with 37 elements.

Corollary 1.9. *Let P be a convex, point-symmetric polytope in $\mathbb{R}^D$ with vertices in $\mathbb{Z}^D$. There exists a constant $c > 0$ such that, for sufficiently large n,*

$$\begin{aligned} \#\{A \subset L(nP) : \textit{A is sum-dominant}\} &> c \cdot 2^{|L(nP)|}, \\ \#\{A \subset L(nP) : \textit{A is difference-dominant}\} &> c \cdot 2^{|L(nP)|}, \\ \#\{A \subset L(nP) : \textit{A is balanced}\} &> c \cdot 2^{|L(nP)|}. \end{aligned} \tag{1.6}$$

2. Sums and Differences of Edge Elements

A key idea in past work on MSTD sets is the importance of fringe elements. For any set $A \subset \{0, \dots, n\}$, there are relatively few ways of forming sums near 0 and $2n$ and of forming differences near $-n$ and n. Such sums and differences are formed entirely by elements in A near 0 and n—the fringe elements. On the other hand, there are relatively many ways of forming the respective middle sums and middle differences, and thus they have high probability of being present as we let A vary. Thus, the sizes of $A + A$ and $A - A$ are predominantly affected by the elements of A in the fringe, and so it is possible to control the balance of sums and differences of A by cleverly fixing those fringe elements.

A similar idea extends to subsets of the lattice points in a polytope. In this case, the fringe elements are the points near the vertices of the polytope. In our chosen fixing of the fringe, elements along certain edges, or 1-faces, of the polytope play a particularly important role in controlling the number of missing sums and differences. To that end, we establish in this section some ancillary lemmas that highlight the behavior of sums and differences of edge elements.

Let P denote our given convex polytope in $\mathbb{R}^D$ with vertices in $\mathbb{Z}^D$. We begin with the observation that because P has lattice points as its vertices, the dilated polytope nP has at least $n + 1$ lattice points along each edge. More specifically, if an edge E of P contains $b_E + 1$ lattice points (where $b_E \geq 1$ since E contains at least its two endpoints), then its dilated form nE in nP contains $nb_E + 1$ lattice points. Furthermore, these $nb_E + 1$ lattice points are evenly spaced along the edge, and thus form their own one-dimensional lattice structure. If nE has endpoints $n\mathbf{e}_1$ and $n\mathbf{e}_2$, then we can define an injective affine transformation $T_{nE} : \mathbb{R} \to \mathbb{R}^D$ by setting

$$T_{nE}(x) \;=\; (n\mathbf{e}_2 - n\mathbf{e}_1)/(nb_E) \cdot x + n\mathbf{e}_1 \;=\; (\mathbf{e}_2 - \mathbf{e}_1)/b_E \cdot x + n\mathbf{e}_1 \tag{2.1}$$

for all $x \in \mathbb{R}$. Note T_{nE} forms a one-to-one correspondence between $[0, nb_E]$ and $L(nE)$. Thus, when constructing a set $A \subset L(nP)$, we can 'place' an arbitrarily large, one-dimensional set $S \subset [0, nb_E]$ along any edge nE by taking n to be sufficiently large and then setting $A \cap nE = T_{nE}(S)$.

Lemmas 2.1 and 2.2 essentially state that for whatever one-dimensional sets are placed along edges of nP, we can find corresponding sumsets along edges in $nP + nP$ and, sometimes, corresponding difference sets along edges in $nP - nP$.

Lemma 2.1. *Let Q be a convex polytope in $\mathbb{R}^D$ with vertices in $\mathbb{Z}^D$, let E be an edge of Q, and let $A \subset L(Q)$. Suppose $A \cap E = T_E(S)$, where $S \subset \mathbb{Z}$ and $T_E : \mathbb{R} \to \mathbb{R}^D$ is an injective affine transformation. Then there exists an injective affine transformation $T_{E+E} : \mathbb{R} \to \mathbb{R}^D$ such that*

$$(A + A) \cap (E + E) = T_{E+E}(S + S). \tag{2.2}$$

Proof. We first show that

$$(A + A) \cap (E + E) = (A \cap E) + (A \cap E). \tag{2.3}$$

As $(A \cap E) + (A \cap E) \subset (A + A) \cap (E + E)$ is immediate, we need only show the forward inclusion.

Let $\mathbf{k}$ be a point in $E + E$. By the convexity of E, there exists some $\mathbf{e} \in E$ such that $2\mathbf{e} = \mathbf{k}$. Thus, for any pair of points $\mathbf{a}_1, \mathbf{a}_2 \in A$ with $\mathbf{a}_1 + \mathbf{a}_2 = \mathbf{k}$, we have that $(\mathbf{a}_1 + \mathbf{a}_2)/2 = \mathbf{e}$. In other words, $\mathbf{a}_1$, $\mathbf{a}_2$ and $\mathbf{e}$ are collinear with $\mathbf{e}$ halfway between $\mathbf{a}_1$ and $\mathbf{a}_2$. Let H be a supporting hyperplane of Q such that $H \cap Q = E$. Suppose $\mathbf{a}_1, \mathbf{a}_2 \notin H$. Since $\mathbf{e} \in E \subset H$, it must be that $\mathbf{a}_1$ and $\mathbf{a}_2$ are in different open half-spaces formed by H. But, since H supports Q, then either $\mathbf{a}_1$ or $\mathbf{a}_2$ is not in Q—a contradiction. Thus we have that $\mathbf{a}_1, \mathbf{a}_2 \in H$, and therefore $\mathbf{a}_1, \mathbf{a}_2 \in E$. In other words, $(A + A) \cap (E + E) \subset (A \cap E) + (A \cap E)$, and (2.3) follows.

We now prove the lemma. We can write $T_E(x) = M(x) + \mathbf{b}$ for all $x \in \mathbb{R}$, where $M : \mathbb{R} \to \mathbb{R}^D$ is an injective linear transformation and $\mathbf{b} \in \mathbb{R}^D$ is some translation vector. Define $T_{2E} : \mathbb{R} \to \mathbb{R}^D$ such that $T_{2E}(x) = M(x) + 2\mathbf{b}$ for all $x \in \mathbb{R}$. Since M is injective and linear, T_{2E} is injective and affine. By (2.3),

$$\begin{aligned}(A + A) \cap 2E &= (A \cap E) + (A \cap E) \\ &= T_E(S) + T_E(S) \\ &= (M(S) + \mathbf{b}) + (M(S) + \mathbf{b}) \\ &= M(S + S) + 2\mathbf{b} \\ &= T_{2E}(S + S), \end{aligned} \tag{2.4}$$

as desired. □

Lemma 2.2. *Let Q be a locally point symmetric polytope in $\mathbb{R}^D$ with vertices in $\mathbb{Z}^D$, and let $A \subset L(Q)$. For a pair of strictly antipodal vertices $\mathbf{v}_1$ and $\mathbf{v}_2$, let E_1 and E_2 be parallel edges such that $\mathbf{v}_1 \in E_1$ and $\mathbf{v}_2 \in E_2$. Suppose $A \cap E_1 = T_{E_1}(S_1)$ and $A \cap E_2 = T_{E_2}(S_2)$, where $S_1, S_2 \subset \mathbb{Z}$ and $T_{E_1}, T_{E_2} : \mathbb{R} \to \mathbb{R}^D$ are injective affine transformations with the same associated linear transformation. Then there exists an injective affine transformation $T_{E_2 - E_1} : \mathbb{R} \to \mathbb{R}^D$ with*

$$(A - A) \cap (E_2 - E_1) = T_{E_2 - E_1}(S_2 - S_1). \tag{2.5}$$

Proof. The proof proceeds similarly to that of Lemma 2.1. We begin by showing that

$$(A - A) \cap (E_2 - E_1) = (A \cap E_2) - (A \cap E_1). \tag{2.6}$$

That $(A \cap E_2) - (A \cap E_2) \subset (A - A) \cap (E_2 - E_1)$ is immediate, so we need only show the forward inclusion. Let $\mathbf{e_1} \in E_1$, $\mathbf{e}_2 \in E_2$. It suffices to show that if $\mathbf{t} \in \mathbb{R}^D$ and $\mathbf{e}_1 + \mathbf{t}, \mathbf{e}_2 + \mathbf{t} \in Q$, then $\mathbf{e}_1 + \mathbf{t} \in E_1$ and $\mathbf{e}_2 + \mathbf{t} \in E_2$.

We first show that there exists a pair of parallel supporting hyperplanes H_1 and H_2 of Q such that $H_1 \cap Q = E_1$ and $H_2 \cap Q = E_2$. Let H_1 be a supporting hyperplane of Q such that $H_1 \cap Q = E_1$, and let H_2 be the parallel hyperplane that contains E_2. Suppose there exists some point $\mathbf{q} \in (H_2 \cap Q) \setminus E_2$. By the convexity of Q, we then have that the line segment $\overline{\mathbf{q}\mathbf{v}_2}$ is also contained in H_2. Since $\overline{\mathbf{q}\mathbf{v}_2}$ cannot be parallel to E_1, we have by the local point symmetry of Q that $\overline{\mathbf{q}\mathbf{v}_2}$ cannot be an edge of Q—otherwise, $H_1 \cap Q$ should contain another edge besides E_1 that contains $\mathbf{v}_1$ and is parallel to $\overline{\mathbf{q}\mathbf{v}_2}$. It is not hard to show then that there is some edge of Q other than E_2 that is contained in the half-space of H_2 that does not contain E_1. By the local point symmetry of Q, there must be some corresponding parallel edge of Q other than E_1 that is contained in the half-space of H_1 that does not contain E_2. As this is not the case, we have that $H_2 \cap Q = E_2$.

Now let V_1 denote the closed half-space formed by H_1 that contains Q, and V_2 the closed half-space formed by H_2 that contains Q. Note that if a translation vector $\mathbf{t} \in \mathbb{R}^D$ does not lie in H_1 (or H_2), then either $\mathbf{e}_1 + \mathbf{t} \notin V_1$ or $\mathbf{e}_2 + \mathbf{t} \notin V_2$. Thus if $\mathbf{e}_1 + \mathbf{t}, \mathbf{e}_2 + \mathbf{t} \in Q$, then $\mathbf{t} \in \mathbb{R}^D$ must lie in H_1. Then $\mathbf{e}_1 + \mathbf{t} \in H_1$ and $\mathbf{e}_2 + \mathbf{t} \in H_2$. Since $H_1 \cap Q = E_1$ and $H_2 \cap Q = E_2$, it follows that $\mathbf{e}_1 + \mathbf{t} \in E_1$ and $\mathbf{e}_2 + \mathbf{t} \in E_2$, and thus (2.6) follows.

We now prove the lemma. We can write $T_{E_1}(x) = M(x) + \mathbf{b}_1$ and $T_{E_2}(x) = M(x) + \mathbf{b}_2$ for all $x \in \mathbb{R}$, where $M : \mathbb{R} \to \mathbb{R}^D$ is an injective linear transformation and $\mathbf{b}_1, \mathbf{b}_2 \in \mathbb{R}^D$ are translation vectors. Define $T_{E_2-E_1} : \mathbb{R} \to \mathbb{R}^D$ such that $T_{E_2-E_1}(x) = M(x) + (\mathbf{b}_2 - \mathbf{b}_1)$ for all $x \in \mathbb{R}$. Since M is injective and linear, $T_{E_2-E_1}$ is injective and affine. By (2.6),

$$\begin{aligned}(A-A)\cap(E_2-E_1) &= (A\cap E_2)-(A\cap E_1)\\ &= T_{E_2}(S_2)-T_{E_1}(S_1)\\ &= (M(S_2)+\mathbf{b}_2)-(M(S_1)+\mathbf{b}_1)\\ &= M(S_2-S_1)+(\mathbf{b}_2-\mathbf{b}_1)\\ &= T_{E_2-E_1}(S_2-S_1), \qquad (2.7)\end{aligned}$$

as desired. □

Definition 2.3. *Given a set $S \in \mathbb{R}^D$, a difference vector $\mathbf{k} \in S - S$ is* uniquely formed *if there exists a unique pair of elements $\mathbf{s}_1, \mathbf{s}_2 \in S$ satisfying $\mathbf{s}_1 - \mathbf{s}_2 = \mathbf{k}$.*

The remainder of this section is devoted to proving Lemma 2.7, which asserts that there are many (at least on the order of n) uniquely formed differences in $nP - nP$ if P is not locally point symmetric. By contrast, if P is locally point symmetric, then the number of uniquely formed differences in $nP - nP$ is constant, as we will show in Lemma 3.6.

Showing Lemma 2.7 requires a brief review of geometry. In the following definitions, let Q be a convex polytope in $\mathbb{R}^D$. Further assume that Q is D-dimensional—that is, the smallest affine subspace containing Q is $\mathbb{R}^D$.

Definition 2.4. *Given vectors $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_m \in \mathbb{R}^D$, a* conical combination *of these vectors is a vector of the form $\alpha_1\mathbf{x}_1 + \alpha_2\mathbf{x}_2 + \cdots + \alpha_m\mathbf{x}_m$ where $\alpha_i \geq 0$ for all $1 \leq i \leq m$. The* polyhedral cone *generated by vectors $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_m$ is the set of all conical combinations of $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_m$.*

Definition 2.5. *Let $\mathbf{v}$ be a vertex of Q, and let $\mathbf{n}_1, \ldots, \mathbf{n}_t$ denote outward-pointing normal vectors of all facets of Q that contain $\mathbf{v}$. The* normal cone $N(\mathbf{v})$ *of Q at $\mathbf{v}$ is the polyhedral cone generated by $\mathbf{n}_1, \ldots, \mathbf{n}_t$.*

Note that normal cones have their apexes at the origin of $\mathbb{R}^d$, while supporting cones have their apexes at the vertices of the polytope.

Suppose Q has vertices $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_m$. The following properties of normal cones $N(\mathbf{v}_i)$ are easily verified:

(1) For each vertex $\mathbf{v}_i$, the normal cone $N(\mathbf{v}_i)$ is the set of outward normal vectors (of arbitrary length) to all supporting hyperplanes of Q that contain $\mathbf{v}_i$.
(2) Vertices $\mathbf{v}_i$ and $\mathbf{v}_j$ are strictly antipodal if and only if the interiors of $N(\mathbf{v}_i)$ and $-N(\mathbf{v}_j)$ have non-empty intersection.
(3) For $i \neq j$, the interiors of $N(\mathbf{v}_i)$ and $N(\mathbf{v}_j)$ are disjoint.
(4) For $i \neq j$, the intersection of $N(\mathbf{v}_i)$ and $N(\mathbf{v}_j)$ is either $\{\mathbf{0}\}$ or a facet of both cones.
(5) $\bigcup_{i=1}^{m} N(\mathbf{v}_i) = \mathbb{R}^D$.

We now introduce a useful result that follows easily from the work of Nguyên and Soltan [NS]. We provide the details in Appendix A.

Lemma 2.6. *Let Q be a D-dimensional polytope with m vertices in $\mathbb{R}^D$. Then Q is locally point symmetric if and only if Q has exactly $m/2$ pairs of strictly antipodal vertices.*

We are now ready to prove Lemma 2.7.

Lemma 2.7. *Let Q be a convex polytope in $\mathbb{R}^D$ that is not locally point symmetric. Then there is a vertex $\mathbf{v}$ and an edge E of Q such that, for all $\mathbf{e} \in E$, the difference vectors $\mathbf{k} = \mathbf{e} - \mathbf{v}$ and $-\mathbf{k}$ are uniquely formed.*

Proof. The difference vectors $\mathbf{k} = \mathbf{e} - \mathbf{v}$ and $-\mathbf{k}$ are uniquely formed if and only if there exists no non-zero vector $\mathbf{t} \in \mathbb{R}^D$ such that $\mathbf{e} + \mathbf{t}, \mathbf{v} + \mathbf{t} \in Q$. To show that such a vertex $\mathbf{v}$ and an edge E exist, it suffices to show that there exists a pair of parallel supporting hyperplanes H_1 and H_2 of Q such that $H_1 \cap Q = \{\mathbf{v}\}$ and $H_2 \cap Q = E$. This is clear because, for any translation by a vector $\mathbf{t} \in \mathbb{R}^D$ of $\mathbf{v}$ and some $\mathbf{e} \in E$, we must have that $\mathbf{t}$ is parallel to H_1 and H_2 if $\mathbf{e} + \mathbf{t}$ and $\mathbf{v} + \mathbf{t}$ are to remain in the closed space bounded by H_1 and H_2. But $H_1 \cap Q = \{\mathbf{v}\}$, and therefore it must be that $\mathbf{t} = \mathbf{0}$ if $\mathbf{v} + \mathbf{t} \in Q$. See Figure 3 for an illustration.

First assume that Q is D-dimensional, with m vertices. As Q is not locally point symmetric, and every vertex of a convex polytope is strictly antipodal with at least one other vertex, it follows by Lemma 2.6 that the number of pairs of strictly antipodal vertices is strictly greater than $m/2$. Then there exists some vertex $\mathbf{v}$ of Q that is strictly antipodal with at least two other vertices. Let $\mathbf{u}_1$ and $\mathbf{u}_2$ denote two such vertices. By property (2) above, the interiors of $N(\mathbf{v})$ and $-N(\mathbf{u}_1)$ have non-empty intersection, as do the interiors of $N(\mathbf{v})$ and $-N(\mathbf{u}_2)$. For the sake of contradiction, suppose that $N(\mathbf{v})$ is contained in $-N(\mathbf{u}_1)$. Reflection through the origin is injective, and the interiors of $N(\mathbf{u}_1)$ and $N(\mathbf{u}_2)$ are disjoint by property (3) above, so it follows that the interiors of $N(\mathbf{v})$ and $-N(\mathbf{u}_2)$ are disjoint—a contradiction. Thus, $N(\mathbf{v})$ cannot be contained in $-N(\mathbf{u}_1)$.

As the interiors of $N(\mathbf{v})$ and $-N(\mathbf{u}_1)$ still have non-empty intersection, it is not hard to show that the interior of some facet F of $-N(\mathbf{u}_1)$ has non-empty intersection with the interior of $N(\mathbf{v})$. Now note that F is also a facet of the cone $-N(\mathbf{u}')$ for some vertex $\mathbf{u}'$ that is connected to $\mathbf{u}_1$ by an edge—we let E denote this edge. Further note that F is set of (inward-pointing) normal vectors of supporting hyperplanes H of Q that satisfy $H \cap Q = E$. In other words, there exist parallel supporting hyperplanes H_1 and H_2 of Q such that $H_1 \cap Q = \{\mathbf{v}\}$ and $H_2 \cap Q = E$, as desired.

If Q is not D-dimensional—that is, the dimension of the affine hull of Q is some $D' < D$—then we can define some injective affine transformation $T : \text{aff}(Q) \to \mathbb{R}^{D'}$ from the affine hull of Q

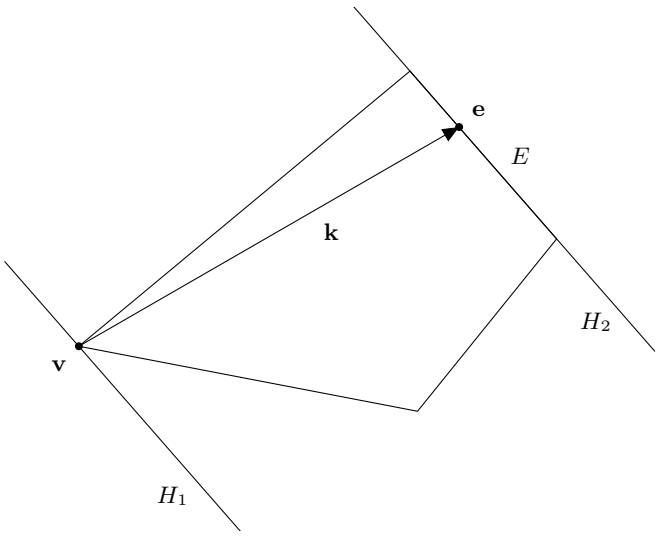

FIGURE 3. A quadrilateral Q that is not locally point symmetric. The parallel lines H_1 and H_2 support Q precisely at $\mathbf{v}$ and at E, respectively. For any non-zero translation vector $\mathbf{t}$, either $\mathbf{v} + \mathbf{t} \notin Q$ or $\mathbf{e} + \mathbf{t} \notin Q$, and the difference vector $\mathbf{k} = \mathbf{e} - \mathbf{v}$ is uniquely formed.

to $\mathbb{R}^{D'}$. As affine transformations preserve parallel lines, the image polytope $Q' = T(Q)$ is also not locally point symmetric. It is not hard to show that a difference vector $\mathbf{q}'_1 - \mathbf{q}'_2 \in Q' - Q'$ is uniquely formed if and only if $T^{-1}(\mathbf{q}'_1) - T^{-1}(\mathbf{q}'_2) \in Q - Q$ is uniquely formed. Thus, we can prove the lemma for Q by applying the argument above to Q'. □

3. Middle Sums and Differences

Let $k < n/2$, let $A \subset \{0, \dots, n\}$, and define sets $L := A \cap [0, k]$ and $U := A \cap [n-k, n]$. It is easy to see that

$$\begin{aligned} (A+A) \cap ([0,k] \cup [2n-k, 2n]) &\subset (L+L) \cup (U+U), \\ (A-A) \cap ([-n,-n+k] \cup [n-k, n]) &\subset (L-U) \cup (U-L). \end{aligned} \tag{3.1}$$

In other words, the sums and differences within radius k of the endpoints of the potential sumset and potential difference set, respectively, are formed entirely by the fringe elements within radius k of the endpoints of the base set $\{0, \dots, n\}$. Martin and O'Bryant exploit this idea in [MO] by fixing the fringe of A such that $A + A$ necessarily has more elements at its ends than does $A - A$. They then show that with high probability, all 'middle' sums and differences are present in the sumset and difference set.

The same idea extends to higher-dimensional convex polytopes. Given an arbitrary convex polytope Q and some $r > 0$, define sets

$$\begin{aligned} B_r(Q) &:= \{\mathbf{q} \in L(Q) : d(\mathbf{q}, \mathbf{v}) \le r \text{ for some vertex } \mathbf{v} \text{ of } Q\}, \\ M_r(Q) &:= L(Q) \setminus B_r(Q), \end{aligned} \tag{3.2}$$

where $d(\cdot, \cdot)$ denotes the Euclidean metric. In words, $B_r(Q)$ is the set of lattice points contained in the union of balls of radius r centered at the vertices of Q, while $M_r(Q)$ consists of all other 'middle' lattice points. It is easy to show that for any $A \subset L(nP)$,

$$\begin{aligned} (A+A) \cap B_r(nP+nP) &\subset (A \cap B_r(nP)) + (A \cap B_r(nP)), \\ (A-A) \cap B_r(nP-nP) &\subset (A \cap B_r(nP)) - (A \cap B_r(nP)). \end{aligned} \tag{3.3}$$

Thus, we can precisely control the fringe of the sumset and difference set—$(A+A) \cap B_r(nP+nP)$ and $(A-A) \cap B_r(nP-nP)$—by carefully fixing $A \cap B_r(nP)$, the fringe of A. Importantly, we choose r independently of the dilation factor n, fixing a constant number of points as n grows.

We refer to any other possible sum—that is, an element of $M_r(nP+nP)$—as a *middle sum*, and any other possible difference—that is, an element of $M_r(nP-nP)$—as a *middle difference*. If we can show that all middle sums and all middle differences are present with positive probability, then we have a positive proportion of subsets $A \subset L(nP)$ that satisfy some precise condition on the cardinalities of their sumsets and difference sets. The purpose of this section is to show that this is true if the fringe is large enough and, in the case of middle differences, if and only if P is locally point symmetric.

Proposition 3.1. *Let $0 < p^+ < 1$ be given. Then there exists some $r > 0$ such that for all sufficiently large n, the following holds: Let $F_r \subset B_r(nP)$, and let A be uniformly randomly chosen from all subsets $S \subset L(nP)$ such that $S \cap B_r(nP) = F_r$. Then $M_r(nP+nP) \subset A + A$ with probability at least p^+.*

Proof. We begin with a lemma bounding the probability that any individual middle sum is missing.

Lemma 3.2. *Let $r > 0$, and fix a fringe set $F_r \subset B_r(nP)$. Let A be chosen uniformly at random from all subsets $S \subset L(nP)$ such that $S \cap B_r(nP) = F_r$, and let $\mathbf{k} \in M_r(nP + nP)$. Then, for some constant $c > 0$ independent of n,*

$$\mathbb{P}[\mathbf{k} \notin A + A] \;\leq\; c\left(\frac{3}{4}\right)^{|L(nP\cap(\mathbf{k}-nP))|/2}. \tag{3.4}$$

Proof. The proof is similar to that of Lemma 5 in Martin and O'Bryant [MO]. Suppose we have $\mathbf{x}, \mathbf{y} \in nP$ such that $\mathbf{x} + \mathbf{y} = \mathbf{k}$. Then $\mathbf{x} = \mathbf{k} - \mathbf{y} \in \mathbf{k} - nP$, and similarly $\mathbf{y} \in \mathbf{k} - nP$. Then $L(nP \cap (\mathbf{k} - nP))$ can be partitioned into distinct pairs of lattice points that add up to $\mathbf{k}$, and the singleton $\{\mathbf{k}/2\}$ if $\mathbf{k}/2$ is a lattice point. The probability that $\mathbf{k}$ is missing in $A + A$ is then the product of the independent probabilities that in each pair, at least one point is missing. Suppose that in our fixed fringe set F_r, exactly l points are fixed as missing. Then at most l pairs contribute a probability of 1, and the remaining pairs contribute a probability of at most $3/4$. When $\mathbf{k}/2$ is not a lattice point, there are $|L(nP \cap (\mathbf{k} - nP))|/2$ pairs total, which gives

$$\mathbb{P}[\mathbf{k} \notin A + A] \;\leq\; \left(\frac{3}{4}\right)^{|L(nP\cap(\mathbf{k}-nP))|/2-l}. \tag{3.5}$$

Thus, we may take $c = (3/4)^{-l}$ and the lemma follows. In the case where $\mathbf{k}/2$ is a lattice point, a similar argument gives the same bound. □

By the union bound, the probability that at least one middle sum is missing is at most the sum of the probabilities that each individual middle sum is missing. Thus, to prove Proposition 3.1, it suffices to show

$$\sum_{\mathbf{k}\in M_r(nP+nP)} c\left(\frac{3}{4}\right)^{|L(nP\cap(\mathbf{k}-nP))|/2} \;<\; 1 - p^+ \tag{3.6}$$

for sufficiently large n and r.

In the one-dimensional case, this amounts to making a tail of a geometric series as small as desired, which is done in [MO]. Unfortunately, in D dimensions, the shape $nP \cap (\mathbf{k} - nP)$ can get quite complicated, and we must do more work. The key idea is that when $\mathbf{k}$ is close to a vertex of $nP + nP$, the shape $nP \cap (\mathbf{k} - nP)$ is a parallelotope, which is quite simple. Conversely, when $\mathbf{k}$ is not close to a vertex of $nP + nP$, we are saved by the fact that $nP \cap (\mathbf{k} - nP)$ is large, so we do not need to be careful about counting its lattice points. See Figure 4 for an illustration.

To evaluate the sum in (3.6), we partition $M_r(nP + nP)$ into two sets, a 'center' set C and an 'intermediate' set I. Fix some $\varepsilon_C > 0$. We define C as all points $\mathbf{k} \in M_r(nP + nP)$ such that

$$|L(nP \cap (\mathbf{k} - nP))| \;>\; 2\log_{3/4}\left(\frac{\varepsilon_C/c}{L(nP+nP)}\right). \tag{3.7}$$

The right hand side is constructed so that by Lemma 3.2,

$$\mathbb{P}[\mathbf{k} \notin A + A] \;<\; \frac{\varepsilon_C}{|L(nP+nP)|} \tag{3.8}$$

for all $\mathbf{k} \in C$. We conclude that the sum of $\mathbb{P}[\mathbf{k} \notin A + A]$ over all $\mathbf{k}$ in C is at most ε_C, because $C \subseteq L(nP + nP)$.

We define I to consist of the remaining points; that is, all points $\mathbf{k} \in M_r(nP + nP)$ such that

$$|L(nP \cap (\mathbf{k} - nP))| \;\leq\; 2\log_{3/4}\left(\frac{\varepsilon_C/c}{|L(nP+nP)|}\right). \tag{3.9}$$

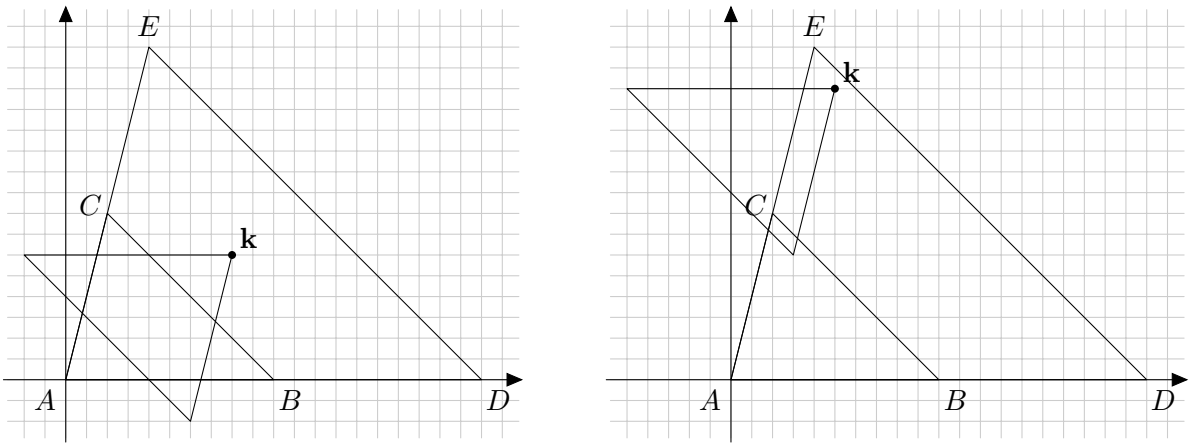

FIGURE 4. A triangle $T = \triangle ABC$ with its sumset $T + T = \triangle ADE$. On the left, the sum $\mathbf{k}$ is relatively far from the vertices of $T + T$. Thus, while the shape of the intersection $T \cap (\mathbf{k} - T)$ is hard to control, it fortunately contains many lattice points. On the right, the sum $\mathbf{k}$ is relatively close to a vertex of $T + T$, and hence $T \cap (\mathbf{k} - T)$ is a parallelotope.

Note that the right hand side is $\Theta(\log n)$, while $|L(nP + nP)|$ is $\Theta(n^D)$. Intuitively, the above definition suggests that all points $\mathbf{k} \in I$ should lie close to the vertices of $nP + nP$, in order to make $|L(nP \cap (\mathbf{k} - nP)|$ small. The set I will be located in between the fringe set F_r and the center set C. Since $\log n/n \to 0$ as $n \to \infty$, the intersection polytope $nP \cap (\mathbf{k} - nP)$ will be a parallelotope for all $\mathbf{k} \in I$, for n large. We formalize this idea in the following lemma.

Lemma 3.3. *There exists a constant $t > 0$ such that I is contained in the union of balls of radius $t \log n$ around the vertices of $nP + nP$ for all n.*

Proof. To highlight the dependence of I on n, we write $I(n)$. Assume for the sake of contradiction this lemma is false. Then for each t, there is some n such that $I(n)$ is not contained in the union of balls of radius $t \log n$ centered at the vertices of $2nP$. In particular, letting t take on the value of every positive integer m, we have the following: For each positive integer m there exists $\mathbf{k}_m$ and n_m such that $\mathbf{k}_m \in I(n_m)$ but $\mathbf{k}_m$ has distance greater than $m \log n$ from each vertex of $2nP$.

For the next step, it is useful to visualize the polytope P as fixed, and rather than dilating P by a factor of n, we shrink the underlying lattice by a factor of n.

Consider the sequence $\mathbf{k}'_m = \mathbf{k}_m/m$. Note that this sequence lies inside the polytope $P + P$, which is closed and bounded, so there is a convergent subsequence $\mathbf{k}'_{m_i}$. Let $\mathbf{k}'$ denote the limit of this subsequence.

Step 1. We claim that $\mathbf{k}'$ must be a vertex of $P + P$; that is, $P \cap (\mathbf{k}' - P)$ is just one point (the point $\mathbf{k}'/2$, a vertex of both P and $\mathbf{k}' - P$).

Consider the convex polytope $P \cap (\mathbf{k}' - P)$, and suppose that it is not just a point. Then it is a d'-dimensional polytope where $0 < d' \leq D$, and furthermore it must lie in a d'-face of P (and of $\mathbf{k}' - P$). Since P has lattice point vertices, a d'-face of P contains $\Theta(n^{d'})$ lattice points. (Recall that P stays fixed and the lattice shrinks.)

Let A be the affine d'-dimensional subspace containing $P \cap (\mathbf{k}' - P)$. Relative to A, the point $\mathbf{k}'/2$ is in the interior of $P \cap (\mathbf{k}' - P)$, with some positive distance ϵ to all its bounding faces. So let $B \subset A$ be a d'-dimensional ball centered at $\mathbf{k}'/2$ with fixed radius $\epsilon/2$, so that $B \subset P \cap (\mathbf{k}' - P)$. Then B contains $\Theta(n^{d'})$ lattice points.

We now show that $B \subset P \cap (\mathbf{k}'_{m_i} - P)$ for i large. The fact that $\mathbf{k}'_{m_i} \to \mathbf{k}'$ as $i \to \infty$ is sufficient for this. First, consider any hyperplane H making an angle θ with A, and suppose H is translated normally by a distance at most ϵ. Then the intersection $H \cap A$ is translated along A by a distance at most $\epsilon/\sin\theta$. In particular, among all bounding hyperplanes of $\mathbf{k}' - P$, there is a minimum nonzero angle $\theta_{\min}$ made with A, so that whenever $\mathbf{k}'$ is translated by at most $\delta = \epsilon/(2\sin\theta_{\min})$, the bounding faces of $P \cap (\mathbf{k}' - P) \cap A$ are translated by at most $\epsilon/2$. Finally, for i large, $|\mathbf{k}'_{m_i} - \mathbf{k}'| < \delta$, so $B \subset P \cap (\mathbf{k}'_{m_i} - P)$, as desired. Since B contains $\Theta(n^{d'})$ lattice points, this directly contradicts that $\mathbf{k}_{m_i} \in I(n)$, which says that $|L(P \cap (\mathbf{k}'_{m_i} - P))| = O(\log n)$. Thus $\mathbf{k}'$ must in fact be a vertex of $P + P$, so that $P \cap (\mathbf{k}' - P) = \{\mathbf{k}'/2\}$.

Step 2. Recall that $\mathbf{k}'/2$ is a vertex of P. For i large, $\mathbf{k}'_{m_i}$ is so close to $\mathbf{k}'$ that $P \cap (\mathbf{k}'_{m_i} - P) = C(\mathbf{k}'/2) \cap (\mathbf{k}'_{m_i} - C(\mathbf{k}'/2))$, where $C(\mathbf{k}'/2)$ denotes the supporting cone of P at $\mathbf{k}'/2$. In other words, for i large, only the local shape of P at $\mathbf{k}'/2$ matters: the only hyperplanes determining $P \cap (\mathbf{k}'_{m_i} - P)$ are those of P at $\mathbf{k}'/2$ and the corresponding hyperplanes in $\mathbf{k}'_{m_i} - P$.

This means that the shape $P \cap (\mathbf{k}'_{m_i} - P)$ is quite simple, and the number of its lattice points will be easy to analyze. Suppose $P \cap (\mathbf{k}'_{m_i} - P)$ is a d'-dimensional polytope. Pick d' edges of P at $\mathbf{k}'$, extend them to rays from $\mathbf{k}'$, and call their convex hull P'. Then $P' \cap (\mathbf{k}'_{m_i} - P')$ is a parallelotope—as simple a shape as we could hope for. Furthermore, that parallelotope is a subset of $P \cap (\mathbf{k}'_{m_i} - P)$, so it also has $O(\log n)$ lattice points. Since each of these d' edges has a lattice structure, the edges have length $O(\log n)$ as well, so the diameter of the parallelotope is $O(\log n)$. Thus $|\mathbf{k}'_{m_i} - \mathbf{k}'|$ is indeed $O(\log n)$. □

Now we evaluate the sum in (3.6) over points $\mathbf{k} \in I$. We sum around one vertex of $nP + nP$ at a time. Let $\mathbf{v}$ be the current vertex, and let $I_{\mathbf{v}}$ be the portion of I that lies in the ball of radius $t \log n$ about $\mathbf{v}$.

Since $\log n/n \to 0$ as $n \to \infty$, for n large we have $(nP + nP) \cap B_{\mathbf{v}} = C(\mathbf{v}) \cap B_{\mathbf{v}}$, where $C(\mathbf{v})$ denotes the supporting cone of $nP + nP$ at $\mathbf{v}$. Henceforth, assume n is this large. Now the only relevant portion of $nP + nP$ is a neighborhood of $\mathbf{v}$; that is, when $\mathbf{k} \in I_{\mathbf{v}}$,

$$nP \cap (\mathbf{k} - nP) \;=\; C(\mathbf{v}) \cap (\mathbf{k} - C(\mathbf{v})). \tag{3.10}$$

To show that the sum in (3.6) is small, we show that the sum

$$\sum_{\mathbf{k} \in L(C(\mathbf{v}))} c \left(\frac{3}{4}\right)^{|L(C(\mathbf{v}) \cap (\mathbf{k} - C(\mathbf{v})))|/2} \tag{3.11}$$

converges. Because the terms are positive, it suffices to bound this sum above. The reason we want to prove convergence is that our final step will be to bound (3.6) by an arbitrarily small tail of this sum (recall that we will be cutting out a constant fixed fringe region of radius r around $\mathbf{v}$, and we can make r as large as desired).

Recall that $C(\mathbf{v})$ is the convex hull of rays from $\mathbf{v}$ corresponding to edges of P. Then $C(\mathbf{v})$ is the union of convex hulls of D-tuples of those rays. Since there are finitely many D-tuples, it suffices to show that the sum is bounded in each such region.

Let R be one such region, the convex hull of D rational-slope rays from $\mathbf{v}$. We wish to show that

$$\sum_{\mathbf{k} \in L(R)} c \left(\frac{3}{4}\right)^{|L(C(\mathbf{v}) \cap (\mathbf{k} - C(\mathbf{v})))|/2} \tag{3.12}$$

converges. Since $R \subset C(\mathbf{v})$,

$$|L(R \cap (\mathbf{k} - R))| \ < \ |L(C(\mathbf{v}) \cap (\mathbf{k} - C(\mathbf{v})))|, \tag{3.13}$$

so it suffices to show that

$$S_R \ := \ \sum_{\mathbf{k} \in L(R)} c \left(\frac{3}{4}\right)^{|L(R \cap (\mathbf{k} - R))|/2} \tag{3.14}$$

converges. This is easier, because $R \cap (\mathbf{k} - R)$ is simply a parallelotope for any $\mathbf{k} \in L(R)$.

By induction on D the sum over any facet of R converges, because a facet of R is the convex hull of $D-1$ rays from $\mathbf{v}$, and the base case $D = 1$ amounts to a geometric series. Now that the boundary of R has been dealt with, it remains to sum over the lattice points in the interior of R, which we shall denote R°. When $\mathbf{k}$ is in the interior, $R \cap (\mathbf{k} - R)$ has non-zero volume. In fact, in the interior, there is a positive constant c_1 (depending on R) allowing us to bound the number of lattice points below by the volume. That is, for all $\mathbf{k} \in L(R^\circ)$,

$$c_1 |R \cap (\mathbf{k} - R)| \ < \ |L(R \cap (\mathbf{k} - R))|. \tag{3.15}$$

Using this upper bound, it suffices to show the convergence of

$$S'_R \ := \ \sum_{\mathbf{k} \in L(R^\circ)} c \left(\frac{3}{4}\right)^{c_1 |R \cap (\mathbf{k} - R)|}. \tag{3.16}$$

We can upper bound the resulting sum further. Let T be a rational affine transformation that maps R onto the first orthant. Because T increases the volumes in the exponents by at most a constant factor c_2, applying T gives us the new upper bound

$$S'_R \ \leq \ \sum_{\mathbf{k} \in T(L(R^\circ))} c \left(\frac{3}{4}\right)^{c_1 |T(R) \cap (\mathbf{k} - T(R))|/c_2}. \tag{3.17}$$

Now, notice that $T(L(R^\circ))$ is a subset of the lattice $T(\mathbb{Z}^d)$ whose points all have positive (rational) coordinates. Thus, for some rational $q > 0$, we have $L(R^\circ) \subset q\mathbb{N}^D$ and we may further bound the sum above by

$$S'_R \ \leq \ \sum_{\mathbf{k} \in q\mathbb{N}^D} c \left(\frac{3}{4}\right)^{c_1 |T(R) \cap (\mathbf{k} - T(R))|/c_2}. \tag{3.18}$$

Let $x = (3/4)^{c_1/c_2}$. Since $T(R)$ is equal to the first orthant, $T(R) \cap (\mathbf{k} - T(R))$ is simply a rectangular cell with opposite vertices 0 and $\mathbf{k}$, so our sum in (3.18) is equal to

$$S''_R \ := \ q^D \sum_{(k_1, k_2, \ldots, k_D) \in \mathbb{N}^d} x^{k_1 k_2 \cdots k_D}. \tag{3.19}$$

To show that this sum converges, we may rewrite the sum as

$$S''_R \ = \ q^D \sum_{m \in \mathbb{N}} \psi(m) x^m, \tag{3.20}$$

where $\psi(m)$ is the number of ways of writing m as the ordered product of D positive integers. However, $\psi(m)$ is clearly bounded by m^D, so since $x < 1$ the sum converges as desired.

Since the upper bound converges, our original sum

$$\sum_{\mathbf{k} \in L(C(\mathbf{v}))} \left(\frac{3}{4}\right)^{|L(nP \cap (\mathbf{k} - nP))|/2} \tag{3.21}$$

also converges. It follows that by making the constant fixed fringe radius r large enough, we can force the tail sum

$$\sum_{\mathbf{k}\in(C(\mathbf{v})\setminus B_r(nP+nP))} \left(\frac{3}{4}\right)^{|L(nP\cap(\mathbf{k}-nP))|/2} \tag{3.22}$$

to be smaller than any $\varepsilon_{I_\mathbf{v}}$. Since $I_\mathbf{v}$ lies in $L(C(\mathbf{v}) \setminus B_r(nP + nP))$, the sum over $\mathbf{k} \in I_\mathbf{v}$ is also smaller than $\varepsilon_{I_\mathbf{v}}$. Thus if we let ε_I be the sum of $\varepsilon_{I_\mathbf{v}}$ over all vertices $\mathbf{v}$ of $nP+nP$, the probability that at least one middle sum is missing is at most $\varepsilon_C + \varepsilon_I$. In particular, if we choose ε_C and ε_I so that $\varepsilon_C + \varepsilon_I < 1 - p^+$, we have at least a constant positive probability p^+ that all middle sums are present, as desired. This concludes the proof of Proposition 3.1. □

We now examine the presence of middle differences.

Proposition 3.4. *Let $0 < p^- < 1$. Suppose P is locally point symmetric. There exists some $r > 0$ such that for all sufficiently large n, the following holds: Let $F_r \subset B_r(nP)$, and let A be uniformly randomly chosen from all subsets $S \subset L(nP)$ such that $S \cap B_r(nP) = F_r$. Then $M_r(nP - nP) \subset A - A$ with probability at least p^-.*

Proof. The proof is largely identical to the proof of Proposition 3.1. We highlight the relevant differences here. In the course of the proof we state and prove two useful lemmas.

First of all, when considering sums, the pairs of points in $L(nP)$ that sum up to some $\mathbf{k} \in L(nP) + L(nP)$ are pairwise disjoint. Thus, the probabilities that at least one point is missing from each pair are independent, so it is easy to the bound the probability that $\mathbf{k}$ is missing in $A + A$. The same does not hold for differences, however, when a difference $\mathbf{k} \in L(nP) - L(nP)$ is small enough such that $\mathbf{x}, \mathbf{x}+\mathbf{k}, \mathbf{x}+2\mathbf{k} \in L(nP)$ for some $\mathbf{x} \in L(nP)$. Fortunately, as in [MO], the probability that such a small difference is missing is so tiny that a crude bound is sufficient.

Lemma 3.5. *Let $r > 0$, and fix a fringe set $F_r \subset B_r(nP)$. Let A be chosen uniformly at random from all subsets $S \subset L(nP)$ such that $S \cap B_r(nP) = F_r$, and let $\mathbf{k} \in M_r(nP - nP)$ be large. Then, for some constant $c > 0$ independent of n,*

$$\mathbb{P}[\mathbf{k} \notin A - A] \;\le\; c\left(\frac{3}{4}\right)^{|L(nP\cap(nP-\mathbf{k})|/2}. \tag{3.23}$$

Proof. Define random variables $X_\mathbf{j}$ by setting $X_\mathbf{j} = 1$ if $\mathbf{j} \in A$ and $X_\mathbf{j} = 0$ otherwise. We have $\mathbf{k} \notin A - A$ if and only if $X_\mathbf{j}X_{\mathbf{j}+\mathbf{k}} = 0$ for all $\mathbf{j} \in L(nP \cap (nP - \mathbf{k}))$.

First suppose $\mathbf{k}$ is small such that $\mathbf{k} \in \frac{1}{2}(nP - nP)$, and suppose $\mathbf{k} = (k_1, k_2, \ldots, k_D)$. Define

$$G_n \;:=\; \left\{(x_1, \ldots, x_D) \in L(nP \cap (nP - \mathbf{k})) : \left\lfloor \frac{x_1}{k_1} \right\rfloor \text{ is even}\right\}, \tag{3.24}$$

$$H_n \;:=\; \left\{(x_1, \ldots, x_D) \in L(nP \cap (nP - \mathbf{k})) : \left\lfloor \frac{x_1}{k_1} \right\rfloor \text{ is odd}\right\}, \tag{3.25}$$

$$J_n \;:=\; \begin{cases} G_n & \text{if } |G_n| > |H_n| \\ H_n & \text{if } |H_n| \ge |G_n|. \end{cases} \tag{3.26}$$

It is possible that J_n is G_n or H_n depending on n, hence the subscript notation. It is clear that $\mathbf{x} + \mathbf{k} \notin J_n$ for any $\mathbf{x} \in J_n$, and therefore the random variables $X_\mathbf{j}X_{\mathbf{j}+\mathbf{k}}$ are pairwise independent across all $\mathbf{j} \in J_n$. As $|G_n| + |H_n| = |L(nP \cap (nP - \mathbf{k}))|$, it is further clear that

$$|J_n| \;\ge\; \frac{1}{2}|L(nP \cap (nP - \mathbf{k}))|. \tag{3.27}$$

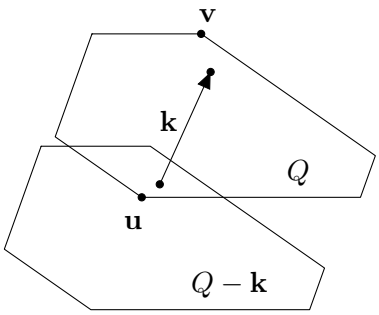

FIGURE 5. A locally point symmetric polytope Q with strictly antipodal vertices $\mathbf{u}$ and $\mathbf{v}$, a difference vector $\mathbf{k} \in Q - Q$, and the translated polytope $Q - \mathbf{k}$. The difference $\mathbf{k}$ is close to the uniquely formed difference $\mathbf{v} - \mathbf{u}$, and hence the intersection polytope $Q \cap (Q - \mathbf{k})$ is a parallelotope.

Thus, if our fixed fringe F_r is missing exactly l points, then we have that

$$\begin{aligned}\mathbb{P}[X_{\mathbf{j}}X_{\mathbf{j}+\mathbf{k}} = 0 \text{ for all } \mathbf{j} \in L(nP \cap (nP - \mathbf{k}))] &\leq \mathbb{P}[X_{\mathbf{j}}X_{\mathbf{j}+\mathbf{k}} = 0 \text{ for all } \mathbf{j} \in J_n] \\ &= \prod_{\mathbf{j}\in J_n} \mathbb{P}[X_{\mathbf{j}}X_{\mathbf{j}+\mathbf{k}} = 0] \\ &\leq \left(\frac{3}{4}\right)^{|J_n|-l} \\ &\leq \left(\frac{3}{4}\right)^{|L(nP\cap(nP-\mathbf{k})|/2-l} . \end{aligned} \tag{3.28}$$

Now suppose $\mathbf{k} \notin \frac{1}{2}(nP - nP)$. Then there exists no $\mathbf{j} \in L(nP)$ such that $\mathbf{j}, \mathbf{j} + \mathbf{k}, \mathbf{j} + 2\mathbf{k} \in L(nP)$. That is, the random variables $X_{\mathbf{j}}X_{\mathbf{j}+\mathbf{k}}$ are pairwise independent across all $\mathbf{j} \in L(nP \cap (nP - \mathbf{k}))$. Then

$$\begin{aligned}\mathbb{P}[X_{\mathbf{j}}X_{\mathbf{j}+\mathbf{k}} = 0 \text{ for all } \mathbf{j} \in L(nP \cap (nP - \mathbf{k}))] &= \prod_{\mathbf{j}\in L(nP\cap(nP-\mathbf{k}))} \mathbb{P}[X_{\mathbf{j}}X_{\mathbf{j}+\mathbf{k}} = 0] \\ &\leq \left(\frac{3}{4}\right)^{|L(nP\cap(nP-\mathbf{k}))|/2-l} . \end{aligned} \tag{3.29}$$

In both cases, we can set $c = (3/4)^{-l}$ and the lemma follows. □

We define the regions I and C in the same way as in the sumset case. In the difference set case, we analyze $nP \cap (nP - \mathbf{k})$ where in the sumset case we analyzed $nP \cap (\mathbf{k} - nP)$.

The other aspect of the difference set case that deserves discussion is the difference set analogue of Lemma 3.3—that there exists a constant $t > 0$ such that I is contained in the union of balls of radius $t \log n$ around the vertices of $nP - nP$ for all n. The reason the same proof carries through is that in any locally point symmetric polytope Q, the only uniquely formed differences are the differences between strictly antipodal vertices, and these differences are in one-to-one correspondence with the vertices of $Q - Q$. When a difference $\mathbf{k} \in Q - Q$ is close to one of these uniquely formed differences, $Q \cap (Q - \mathbf{k})$ is a parallelotope due to local point symmetry. See Figure 5 for an illustration.

To be precise, in Step 1 of the proof for the sumset case, we show that $P \cap (\mathbf{k}' - P)$ is just one point, and immediately conclude that $\mathbf{k}'$ is a vertex of $P + P$. Making the same conclusion takes some more work in the difference set case, which we do in the following lemma.

Lemma 3.6. *Let Q be a locally point symmetric polytope, and let $\mathbf{k} \in Q - Q$. The following statements are equivalent:*

(i) $Q \cap (Q - \mathbf{k})$ *consists of a single point, i.e.,* $\mathbf{k}$ *is a uniquely formed difference in* $Q - Q$.
(ii) $\mathbf{k}$ *is a vertex of the polytope* $Q - Q$.
(iii) $\mathbf{k} = \mathbf{u} - \mathbf{v}$ *for strictly antipodal vertices* $\mathbf{u}$ *and* $\mathbf{v}$ *of* Q.

Proof. In the proof of this lemma, we use the following facts about supporting cones which are not hard to prove:

(1) Vertices $\mathbf{v}_i$ and $\mathbf{v}_j$ are strictly antipodal if and only if $C(\mathbf{v}_i) - \mathbf{v}_i$ and $C(\mathbf{v}_j) - \mathbf{v}_j$ intersect only at the origin.
(2) Let A be a face of Q of dimension k (a k-face), and let $\mathbf{a}$ be given in the interior of A (relative to the k-dimensional affine space containing A). If $\mathbf{x}$ is in the supporting cone of some vertex of A, then $\mathbf{a} + \epsilon\mathbf{x} \in Q$ for ϵ small.

First, we show (i) $\implies$ (ii). Let $\mathbf{u}$ and $\mathbf{v}$ be the unique points in Q that satisfy $\mathbf{k} = \mathbf{u} - \mathbf{v}$. Suppose that $\mathbf{u}$ lies in a k-face A and $\mathbf{v}$ lies in an l-face B, where A and B are chosen so that k and l are minimal. Note that k and l may range from 0 to D.

Suppose there exist vertices $\mathbf{a} \in A$ and $\mathbf{b} \in B$ that are not strictly antipodal. Then $C(\mathbf{a}) - \mathbf{a}$ and $C(\mathbf{b}) - \mathbf{b}$ have an intersection containing some nonzero vector $\mathbf{x}$. Then for ϵ small, $\mathbf{a} + \epsilon\mathbf{x}$ and $\mathbf{b} + \epsilon\mathbf{x}$ both lie in Q, so $\mathbf{u} + \epsilon\mathbf{x}$ and $\mathbf{v} + \epsilon\mathbf{x}$ both lie in Q. Thus, the difference $\mathbf{k} = \mathbf{u} - \mathbf{v}$ is not uniquely formed.

Thus every vertex in A must be strictly antipodal to every vertex in B. Since the vertices of Q are partitioned into strictly antipodal pairs, A and B must both be 0-faces; that is, $A = \{\mathbf{u}\}$ and $B = \{\mathbf{v}\}$, and $\mathbf{u}$ and $\mathbf{v}$ are strictly antipodal vertices as desired.

Next, we show (ii) $\implies$ (iii). Let $\mathbf{u}, \mathbf{v} \in Q$ such that $\mathbf{k} = \mathbf{u} - \mathbf{v}$. Observe that a point $\mathbf{v} \in Q$ is a vertex of Q if and only if, for any non-zero translation vector $\mathbf{t}$, $\mathbf{v} + \mathbf{t} \in Q$ implies $\mathbf{v} - \mathbf{t} \notin Q$. The same statement holds for the polytope $Q - Q$. If $\mathbf{u}$ is not a vertex of Q, then we have that $\mathbf{u} + \mathbf{t}, \mathbf{u} - \mathbf{t} \in Q$ for some non-zero $\mathbf{t}$. But then this implies that $\mathbf{k} + \mathbf{t} = (\mathbf{u} + \mathbf{t}) - \mathbf{v}$ and $\mathbf{k} - \mathbf{t} = (\mathbf{u} - \mathbf{t}) - \mathbf{v}$ are both contained in $Q - Q$, which contradicts that $\mathbf{k}$ is a vertex of $Q - Q$. Applying the same argument to $\mathbf{v}$, we get that $\mathbf{u}$ and $\mathbf{v}$ must both be vertices of Q.

Now suppose $\mathbf{u}$ and $\mathbf{v}$ are not strictly antipodal vertices. We show that $\mathbf{k} + \mathbf{t}, \mathbf{k} - \mathbf{t} \in Q - Q$ for some non-zero $\mathbf{t}$, which contradicts that $\mathbf{k}$ is a vertex of $Q - Q$. Let $\mathbf{v}'$ denote the unique vertex that is strictly antipodal with $\mathbf{v}$. For some small $\epsilon > 0$, define $\mathbf{t} = \epsilon(\mathbf{v}' - \mathbf{u})$. Clearly, $\mathbf{u} + \mathbf{t} \in Q$, so $\mathbf{k} + \mathbf{t} = (\mathbf{u} + \mathbf{t}) - \mathbf{v}$ is contained in $Q - Q$. Now consider the point $\mathbf{v} + \mathbf{t}$. If $\mathbf{v} + \mathbf{t} \notin Q$, and thus the half-line formed by extending out $\mathbf{t}$ from $\mathbf{v}$ is not contained in the supporting cone $C(\mathbf{v})$, then as Q is locally point symmetric the parallel half-line formed by extending out from $\mathbf{v}'$ the vector $\mathbf{u} - \mathbf{v}'$ is not contained in $C(\mathbf{v}')$—a contradiction. Thus $\mathbf{k} - \mathbf{t} = \mathbf{u} - (\mathbf{v} + \mathbf{t})$ is contained in $Q - Q$, which also forms a contradiction. Thus, $\mathbf{u}$ and $\mathbf{v}$ must be strictly antipodal vertices.

Finally, we show (iii) $\implies$ (i). Let H_1 and H_2 be parallel supporting hyperplanes meeting Q at $\{\mathbf{u}\}$ and $\{\mathbf{v}\}$, respectively. If $\mathbf{u}' \neq \mathbf{u}$ is a point in Q, then $\mathbf{u}' - \mathbf{k}$ lies on the side of H_2 opposite Q, so it cannot lie in Q. Thus $\mathbf{k}$ is a uniquely formed difference in Q. □

The rest of the proof of Proposition 3.1 carries over to the difference set case with trivial modifications. □

4. Proof of Theorem 1.7

We begin by showing that the proportion $\rho_n^{s,d}$ of subsets $A \subset L(nP)$ missing exactly s sums and exactly $2d$ differences approaches 0 if P is not locally point symmetric. By Lemma 2.7, there exists a vertex $n\mathbf{v}$ and an edge nE of nP such that for all $\mathbf{e} \in nE$, the difference vectors $\mathbf{k} = \mathbf{e} - n\mathbf{v}$ and $-\mathbf{k}$ are uniquely formed. Recall that nE has at least $n+1$ lattice points. Then, if A is missing exactly $2d$ differences, at least $n+1-d$ of the lattice points in nE must be present. Thus, for $n > 2d-1$, we see that

$$\rho_n^{s,d} \;\leq\; \binom{n+1}{d}\left(\frac{1}{2}\right)^{n+1-d} \;=\; \Theta\left(\frac{n^d}{2^n}\right), \tag{4.1}$$

which approaches 0 as $n \to \infty$.

We now handle the main case when P is locally point symmetric. For some radius r, we aim to construct a fringe set $F_r \subset B_r(nP)$ such that, for all sets A that satisfy $A \cap B_r(nP) = F_r$,

$$B_r(nP + nP) \setminus (A + A) \;=\; s, \tag{4.2}$$

$$B_r(nP - nP) \setminus (A - A) \;=\; 2d. \tag{4.3}$$

If P is 1-dimensional (a line segment), we simply place appropriate fringe sets at its ends as in [He]. Now suppose P is m-dimensional for $m \geq 2$. We can take a pair of strictly antipodal vertices $n\mathbf{v}_1$ and $n\mathbf{v}_2$ of nP, and a pair of parallel edges nE_1 and nE_2 such that $n\mathbf{v}_1 \in nE_1$ and $n\mathbf{v}_2 \in nE_2$. Suppose nE_1 and nE_2 contain $nb_{E_1}+1$ and $nb_{E_2}+1$ lattice points, respectively. As discussed in the beginning of Section 2, there exist injective affine transformations $T_{nE_1}, T_{nE_2} : \mathbb{R} \to \mathbb{R}^D$ that form one-to-one correspondences between $[0, nb_{E_1}]$ and $L(nE_1)$, and between $[0, nb_{E_2}]$ and $L(nE_2)$, respectively. We can also specify that $T_{nE_1}(0) = n\mathbf{v}_1$ and $T_{nE_2}(nb_{E_2}) = n\mathbf{v}_2$. It is easily seen that T_{nE_1} and T_{nE_2} have the same associated linear transformation.

As shown in the proof of Theorem 8 in [He], for some $r' > 0$ and $n > 2r'$, there exist sets $L_{s,d} \subset [0, r']$ and $U_{s,d} \subset [nb_{E_2} - r', nb_{E_2}]$ such that

$$|[0, r'] \setminus (L_{s,d} + L_{s,d})| + |[2nb_{E_2} - r', 2nb_{E_2}] \setminus (U_{s,d} + U_{s,d})| \;=\; s \tag{4.4}$$

and

$$|[nb_{E_2} - r', nb_{E_2}] \setminus (U_{s,d} - L_{s,d})| \;=\; d. \tag{4.5}$$

Now define $r = \max\{r^+, r^-, r'\}$, where r^+ and r^- are the constants given by Propositions 3.1 and 3.4. Let $B'_r(nP)$ denote the set

$$B_r(nP) \setminus (T_{nE_1}([0, r']) \cup T_{nE_2}([nb_{E_2} - r', nb_{E_2}])), \tag{4.6}$$

and set

$$F_r \;:=\; T_{nE_1}(L_{s,d}) \cup T_{nE_2}(U_{s,d}) \cup B'_r(nP). \tag{4.7}$$

That is, we place $L_{s,d}$ on one end of nE_1 and $U_{s,d}$ on one end of nE_2, and fill in all other points of $B_r(nP)$. See Figure 6 for an illustration.

Now let A be uniformly randomly chosen from all subsets $S \subset L(nP)$ such that $S \cap B_r(nP) = F_r$. We see that

$$A \cap nE_1 \;=\; T_{nE_1}(S_1), \qquad A \cap nE_2 \;=\; T_{nE_2}(S_2), \tag{4.8}$$

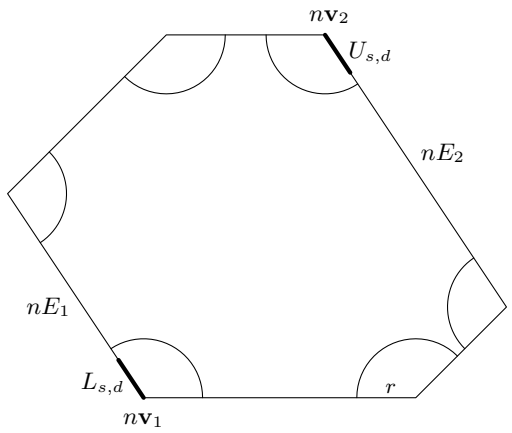

FIGURE 6. A locally point symmetric hexagon. The fringe set F_r lives within the balls of radius r centered about the vertices. The one-dimensional fringe sets $L_{s,d}$ and $U_{s,d}$ are placed on corresponding parallel edges nE_1 and nE_2 of the strictly antipodal vertices $n\mathbf{v}_1$ and $n\mathbf{v}_2$.

for some sets $S_1, S_2 \in \mathbb{Z}$ such that $S_1 \cap [0, r'] = L_{s,d}$ and $S_2 \cap [nb_{E_2} - r', nb_{E_2}] = U_{s,d}$. By Lemma 2.1, there exist injective affine transformations $T_{nE_1+nE_1}, T_{nE_2+nE_2} : \mathbb{R} \to \mathbb{R}^D$ such that

$$\begin{aligned}(A + A) \cap (nE_1 + nE_1) &= T_{nE_1+nE_1}(S_1 + S_1),\\ (A + A) \cap (nE_2 + nE_2) &= T_{nE_2+nE_2}(S_2 + S_2).\end{aligned} \tag{4.9}$$

It is easy to show that, then,

$$\begin{aligned}(A + A) \cap T_{nE_1+nE_1}([0, r']) &= T_{nE_1+nE_1}((S_1 + S_1) \cap [0, r'])\\ &= T_{nE_1+nE_1}((L_{s,d} + L_{s,d}) \cap [0, r']),\end{aligned} \tag{4.10}$$

and similarly

$$(A + A) \cap T_{nE_2+nE_2}([2nb_{E_2} - r', 2nb_{E_2}]) = T_{nE_2+nE_2}((U_{s,d} + U_{s,d}) \cap [2nb_{E_2} - r', 2nb_{E_2}]). \tag{4.11}$$

It follows from (4.4) that $A + A$ is missing a total of exactly s sums in the regions $T_{nE_1+nE_1}([0, r'])$ and $T_{nE_2+nE_2}([nb_{E_2} - r', nb_{E_2}])$.

Similarly, by Lemma 2.2, there exists an injective affine transformation $T_{nE_2-nE_1} : \mathbb{R} \to \mathbb{R}^D$ such that

$$(A - A) \cap (nE_2 - nE_1) = T_{nE_2-nE_1}(S_2 - S_1), \tag{4.12}$$

and we can show that

$$(A - A) \cap T_{nE_2-nE_1}([nb_{E_2} - r', nb_{E_2}]) = T_{nE_2-nE_1}((U_{s,d} - L_{s,d}) \cap [nb_{E_2} - r', nb_{E_2}]). \tag{4.13}$$

It follows by (4.5) that $A - A$ is missing exactly $2d$ differences in the regions $T_{nE_2-nE_1}([nb_{E_2} - r', nb_{E_2}])$ and $-T_{nE_2-nE_1}([nb_{E_2} - r', nb_{E_2}])$.

Finally, it is not hard to show that all other elements in $B_r(nP + nP)$ and $B_r(nP - nP)$ are present, that is,

$$\begin{aligned}B_r(nP + nP) \setminus (T_{nE_1+nE_1}([0, r']) \cup T_{nE_2+nE_2}([2nb_{E_2} - r', 2nb_{E_2}])) \subset A + A,\\ B_r(nP - nP) \setminus (T_{nE_2-nE_1}([nb_{E_2} - r', nb_{E_2}]) \cup -T_{nE_2-nE_1}([nb_{E_2} - r', nb_{E_2}])) \subset A - A.\end{aligned} \tag{4.14}$$

Thus, we satisfy (4.2) and (4.3).

Let $p^+ > 1/2$ and $p^- > 1/2$. By Propositions 3.1 and 3.4, we have that $M_r(nP+nP) \subset A+A$ with probabilities at least p^+, and that $M_r(nP-nP) \subset A-A$ with probability at least p^-, where p^+ and p^- are fixed independent of n. It follows that $M_r(nP+nP) \subset A+A$ and $M_r(nP-nP) \subset A-A$ with positive probability independent of n. Thus, a positive proportion of the subsets A, and thus a positive proportion of all subsets of $L(nP)$, have exactly s missing sums and exactly $2d$ missing differences. □

5. Proof of Theorem 1.8

Similarly to as in the proof of Theorem 1.7, the main task is to construct a fringe set $F_r \subset B_r(nP)$ for some radius r such that, for all sets A that satisfy $A \cap B_r(nP) = F_r$,

$$B_r(nP+nP) \setminus (A+A) \;=\; s, \qquad B_r(nP-nP) \setminus (A-A) \;\geq\; 2d. \tag{5.1}$$

Once we construct F_r, the proof concludes identically. The difference here is that because we do not assume local point symmetry in P, we are no longer guaranteed the existence of 'distant' parallel edges, and thus cannot use Lemma 2.2 to control the number of missing differences. On the other hand, we do not need to limit the number of missing differences so long as there are at least $2d$ of them. This allows us to use Lemma 2.7 to our advantage.

If P is locally point symmetric, then we simply construct F_r as in the proof of Theorem 1.7. Now suppose P is not locally point symmetric. Let $n\mathbf{v}$ and nE_1 denote, respectively, the vertex and edge returned by Lemma 2.7 when it is applied to nP, and let nE_2 denote some other edge of nP that is distinct from nE. If nE_1 and nE_2 contain, respectively, $nb_{E_1}+1$ and $nb_{E_2}+1$ lattice points, then let $T_{nE_1}, T_{nE_2} : \mathbb{R} \to \mathbb{R}^D$ denote the injective affine transformations that form one-to-one correspondences between $[0, nb_{E_1}]$ and $L(nE_1)$, and between $[0, nb_{E_2}]$ and $L(nE_2)$, respectively.

As shown in the proof of Theorem 8 in [He], for some $r' > 0$ and $n > 2r'$, there exist sets $L_s \subset [0, r']$ and $U_s \subset [nb_{E_2} - r', nb_{E_2}]$ such that

$$|[0,r'] \setminus (L_{s,0} + L_{s,0})| + |[2nb_{E_2} - r', 2nb_{E_2}] \setminus (U_{s,0} + U_{s,0})| \;=\; s. \tag{5.2}$$

Further define

$$R_d \;:=\; [0, d-1] \cup [2d, 3d-1], \tag{5.3}$$

and observe that $[0, 3d-1] \subset R_d + R_d$.

Define $r = \max\{r^+, r^-, r', 3d-1\}$, where r^+ and r^- are the constants given by Propositions 3.1 and 3.4, respectively. Define

$$B'_r(nP) \;:=\; B_r(nP) \setminus (T_{nE_1}([0,3d-1]) \cup T_{nE_2}([0,r']) \cup T_{nE_2}([nb_{E_2} - r', nb_{E_2}])), \tag{5.4}$$

and set

$$F_r \;:=\; T_{nE_1}(R_d) \cup T_{nE_2}(L_s) \cup T_{nE_2}(U_s) \cup B'_r(nP). \tag{5.5}$$

That is, we place R_d on one end of nE_1, L_s on one end of nE_2, and U_s on the other end of nE_2, and fill in all other points of $B_r(nP)$. See Figure 7 for an illustration.

Now let A be uniformly randomly chosen from all subsets $S \subset L(nP)$ satisfying $S \cap B_r(nP) = F_r$. We see that

$$A \cap nE_1 \;=\; T_{nE_1}(S_1), \qquad A \cap nE_2 \;=\; T_{nE_2}(S_2) \tag{5.6}$$

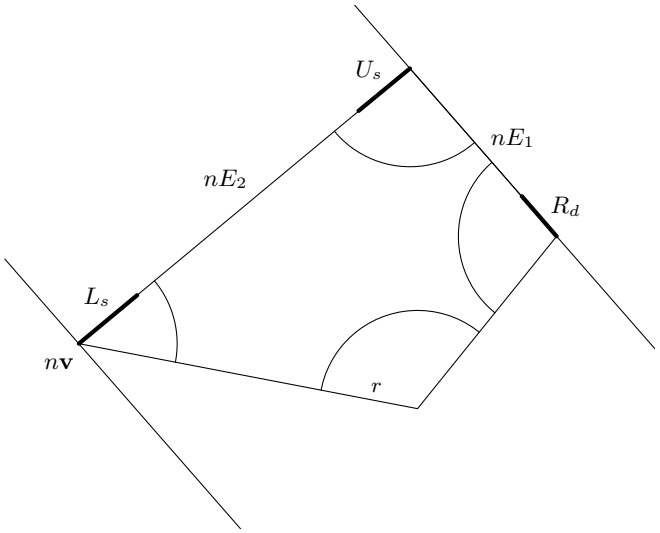

FIGURE 7. A quadrilateral that is not locally point symmetric. Again, the fringe set F_r lives within the balls of radius r centered about the vertices. The one-dimensional fringe set R_d is placed on edge nE_1, and sets L_s and U_s are placed on opposite ends of edge nE_2.

for some sets $S_1, S_2 \in \mathbb{Z}$ such that $S_1 \cap [0, 3d-1] = R_d$, $S_2 \cap [0, r'] = L_s$, and $S_2 \cap [nb_{E_2} - r', nb_{E_2}] = U_s$. By Lemma 2.1, there exists an injective affine transformation $T_{nE_2+nE_2} : \mathbb{R} \to \mathbb{R}^D$ such that

$$(A + A) \cap (nE_2 + nE_2) \;=\; T_{nE_2+nE_2}(S_2 + S_2). \tag{5.7}$$

It is easy to show that, then,

$$(A + A) \cap T_{nE_2+nE_2}([0, r']) \;=\; T_{nE_2+nE_2}((L_s + L_s) \cap [0, r']) \tag{5.8}$$

and

$$(A + A) \cap T_{nE_2+nE_2}([2nb_{E_2} - r', 2nb_{E_2}]) \;=\; T_{nE_2+nE_2}((U_s + U_s) \cap [2nb_{E_2} - r', 2nb_{E_2}]). \tag{5.9}$$

It follows from (5.2) that $A + A$ is missing a total of exactly s sums in the regions $T_{nE_2+nE_2}([0, r'])$ and $T_{nE_2+nE_2}([2nb_{E_2} - r', 2nb_{E_2}])$.

As A is missing d lattice points along the edge nE_1, it follows from Lemma 2.7 that $A - A$ is missing at least $2d$ differences. Let $T_{nE_1+nE_1} : \mathbb{R} \to \mathbb{R}^D$ be the injective affine transformation returned by Lemma 2.1 when applied to edge nE_1; because $[0, 3d-1] \subset R_d + R_d$, we can show in a similar manner to the argument above that $A + A$ is not missing any sums in the region $T_{nE_1+nE_1}([0, 3d-1])$.

Finally, it is not hard to show that all other elements in $B_r(nP + nP)$ are present. That is, all points in the set

$$B_r(nP + nP) \setminus (T_{nE_1+nE_1}([0, 3d-1]) \cup T_{nE_2+nE_2}([0, r']) \cup T_{nE_2+nE_2}([2nb_{E_2} - r', 2nb_{E_2}])) \tag{5.10}$$

are present in $A+A$. The proof concludes identically as in the proof of Theorem 1.7 from here. $\square$

6. Future Directions

There are several natural directions in which to proceed from here. One conjecture is that the proportion $\rho_n^{s,d}$ converges if P is locally point symmetric. Zhao [Z] proved this in the one-dimensional case, and with some work his arguments might be extended to arbitrary D-dimensional polytopes. This would likely involve modifying Zhao's notion of a semi-rich set so that it is defined in terms of the supporting cone for each vertex of the polytope.

Another problem is to consider the proportion ρ_n of MSTD subsets of $L(nP)$ for an arbitrary polytope P, which we discuss here in some detail. As mentioned in the introduction, neither Theorem 1.7 nor Theorem 1.8 implies that ρ_n is bounded below by a positive constant as $n \to \infty$. This is due to the fact that $L(nP)$ is usually not balanced, such that $L(nP) - L(nP)$ is much larger than $L(nP) + L(nP)$. In particular, the ratio $|L(nP) - L(nP)|/|L(nP) + L(nP)|$ is essentially constant as n grows, and so we have that $|L(nP) - L(nP)| - |L(nP) + L(nP)|$ grows on the order of n^D. Reformulating the problem in terms of missing sums and differences, we see that a subset $A \subset L(nP)$ must be missing $\sim n^D$ differences for it even possibly to be MSTD.

There are some factors that, upon first glance, suggest that there may be many such subsets. If P is not locally point symmetric (and therefore not balanced), then Lemma 2.7 shows that there are many uniquely formed differences in $L(nP) - L(nP)$. In other words, though the potential difference set is large in size, it is very fragile in that many of its differences are missing with high probability. For example, consider the lattice points of the tetrahedron nT in $\mathbb{R}^3$ determined by vertices $A = (-n, 0, 0)$, $B = (n, 0, 0)$, $C = (0, -n, n)$, and $D = (0, n, n)$. By bounding nT with supporting planes $z = 0$ and $z = n$, we see that any difference between a point in edge $\overline{AB}$ and a point in edge $\overline{CD}$ is uniquely formed. Similarly, we have that any difference formed by A and a point on the face $\triangle BCD$ is uniquely formed. As this holds for any difference vector formed by a vertex and a point on the opposite face, or by points on skew edges of nT, we see that the presence of the boundary points of nT have a significant impact on the size of the difference set—in this sense, the natural fringe extends to the entire boundary of nT rather than being restricted to the balls centered about the vertices.

However, even if we make the strong imposition that a subset $A \subset L(nT)$ is missing all boundary points of nT, this still would not amount to the necessary $\sim n^3$ missing differences. Each vertex forms around $\sim n^2$ uniquely formed differences with points on the opposite face, and each of the $\sim n$ points on the edges of nT forms $\sim n$ unique differences with points on the opposite skew edge. This suggests that subsets $A \subset L(nT)$ whose difference set is even within the range of the potential sumset become vanishingly rare as n grows.

The tetrahedron is, in a sense, very far from being locally point symmetric. The reason is that for each vertex $\mathbf{v}$, there are hyperplanes that support the tetrahedron precisely at $\mathbf{v}$ and the opposite face F. Consider now the following locally point symmetric hexagon H, depicted in Figure 8. We can compute that $|L(H) + L(H)| = 181$ and $|L(H) - L(H)| = 187$, and the difference in these cardinalities grows quadratically as we take dilations of H. In this case, however, the difference set is much more robust. Because H is locally point symmetric, we have no uniquely formed differences except those formed by pairs of strictly antipodal vertices. Thus, we are forced to impose even stronger conditions on missing points in a subset $A \subset L(nH)$ for it to miss the required $\sim n^2$ differences.

From these considerations in combination with Corollary 1.9, we make the following conjecture:

Conjecture 6.1. *Let P be polytope in $\mathbb{R}^D$ with vertices in $\mathbb{Z}^D$. Then the proportion ρ_n of MSTD subsets of $L(nP)$ approaches 0 as $n \to \infty$ if and only if $L(P)$ is not balanced.*

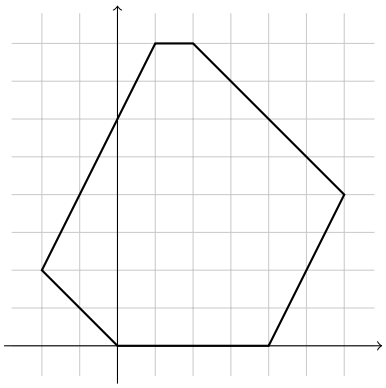

FIGURE 8. Locally point symmetric hexagon H

This raises the question of how to characterize polytopes P for which $L(P)$ is not balanced. We know that if P is point symmetric, then $L(P)$ is balanced, but does the converse hold true? Or perhaps there exists some P, locally point symmetric but not point symmetric, for which $L(P)$ is balanced. Does this imply that $L(nP)$ is also balanced for all n?

Finally, it is interesting to examine how the limiting proportions of ρ_n and $\rho_n^{s,d}$ (assuming they exist) change as we vary our polytope P. For example, if P is a rectangle in $\mathbb{R}^2$, how do they change as we vary the ratio of side lengths? What happens as we increase the number of sides? How do the limiting proportions change as we vary the dimension D? Do ρ_n and $\rho_n^{s,d}$ exhibit monotonic growth with the dilation factor n, as computations suggest when P is an interval (see [MO])? We hope to investigate these questions theoretically and numerically in a future paper.

APPENDIX A. NUMBER OF PAIRS OF STRICTLY ANTIPODAL VERTICES

We show that Lemma 2.6 follows from the work of Nguyên and Soltan [NS]. We restate Lemma 2.6 here for the reader's convenience.

Lemma A.1. *Let Q be a D-dimensional polytope with m vertices in $\mathbb{R}^D$. Then Q is locally point symmetric if and only if Q has exactly $m/2$ pairs of strictly antipodal vertices.*

Let $s(Q)$ denote the number of pairs of strictly antipodal vertices in a convex polytope Q. The following theorems come from Theorems 1 and 3 of [NS].

Theorem A.2. *For a convex polygon $Q \subset \mathbb{R}^2$ with m vertices,*

$$s(Q) \;=\; m - k, \tag{A.1}$$

where k ($0 \le k \le \lfloor m/2 \rfloor$) is the number of pairs of parallel sides in Q.

Theorem A.3. *For a convex D-dimensional polytope $Q \subset \mathbb{R}^D$, $m \ge D+1$, $D \ge 3$,*

$$s(Q) \;\ge\; \lceil m/2 \rceil. \tag{A.2}$$

For an even m, the equality $s(Q) = \lceil m/2 \rceil$ holds if and only if $m \ge 2D$ and the vertices of Q can be divided into $m/2$ pairs such that for each pair $\{\mathbf{u}, \mathbf{v}\}$,

$$C(\mathbf{u}) - \mathbf{u} \;=\; \mathbf{v} - C(\mathbf{v}). \tag{A.3}$$

For an odd m, the equality $s(Q) = \lceil m/2 \rceil$ holds if and only if $m \ge 4D-1$ and some $(m-3)/2$ pairwise disjoint subsets of the form $\{\mathbf{u}, \mathbf{v}\}$ can be chosen from the vertex set such that

$$C(\mathbf{u}) - \mathbf{u} \;=\; \mathbf{v} - C(\mathbf{v}) \tag{A.4}$$

for each of them, and the remaining three vertices $\mathbf{x}, \mathbf{y}, \mathbf{z}$ *satisfy the relation*

$$(C(\mathbf{x}) - \mathbf{x}) \cap (C(\mathbf{y}) - \mathbf{y}) \;=\; \mathbf{z} - C(\mathbf{z}). \tag{A.5}$$

Let Q be a D-dimensional polytope with m vertices in $\mathbb{R}^D$. If $D = 1$, then Q is an interval and satisfies Lemma A.1. If $D \geq 3$, then Lemma A.1 follows immediately from Theorem A.3.

It remains to show Lemma A.1 in the case $D = 2$. By Theorem A.2, it suffices to show that Q is locally point symmetric if and only if Q has exactly $m/2$ pairs of parallel sides. As showing this is easy, we sketch the idea here. The forward implication is immediate. Now suppose Q has exactly $m/2$ pairs of parallel sides, and further suppose Q has vertices $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_m$ in clockwise order. We can show that for any pair of parallel sides $E = \overline{\mathbf{v}_i\mathbf{v}_{i+1}}$ and $F = \overline{\mathbf{v}_j\mathbf{v}_{j+1}}$ of Q, there exist supporting lines L_1 and L_2 such that $L_1 \cap Q = E$ and $L_2 \cap Q = F$. From there, we can show that $\mathbf{v}_i$ and $\mathbf{v}_j$ are strictly antipodal, and $\mathbf{v}_{i+1}$ and $\mathbf{v}_{j+1}$ are strictly antipodal. That Q is locally point symmetric follows easily from there.

REFERENCES

[DKMMW] T. Do, A. Kulkarni, S. J. Miller, D. Moon, and J. Wellens, *Sums and Differences of Correlated Random Sets*, preprint 2013. http://arxiv.org/abs/1401.2588

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

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

[LMO] O. Lazarev, S. J. Miller and K. O'Bryant, *Distribution of Missing Sums in Sumsets* (2013), Experimental Mathematics **22** (2013), no. 2, 132–156.

[MO] 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, 287–305.

[NS] M. Nguyên and V. Soltan, *Lower Bounds for the Numbers of Antipodal Pairs and Strictly Antipodal Pairs of Vertices in a Convex Polytope*, Discrete & Computational Geometry **11** (1994), no. 1, 149–162.

[Z] 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 DEPARTMENT, 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

E-mail address: wilcoxjay@gmail.edu

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