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 $\{0, \ldots, n\}$ 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 $\rho_{s,d}^n$ of subsets of $\{0, \ldots, n\}$ that are missing exactly $s$ sums in $\{0, \ldots, 2n\}$ and exactly $2d$ differences in $\{-n, \ldots, n\}$ 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 $\rho_{s,d}^n$ 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 $\rho_{s,d}^n$. We define a geometric characteristic of polytopes called local point symmetry, and show that $\rho_{s,d}^n$ 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

1. Introduction 2
2. Sums and Differences of Edge Elements 5
3. Middle Sums and Differences 10
4. Proof of Theorem 1.13 18
5. Proof of Theorem 1.14 20
6. Future Directions 22
Appendix A. Number of Pairs of Strictly Antipodal Vertices 24
References 25

Date: January 24, 2015.

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, and Jonas Meyer for supplying the proof of the volume inequality (6.2). We would also like to thank our referee, whose detailed comments greatly improved our exposition at several points throughout this paper, as well as gave us additional interesting questions to consider for future work.

© 2015. This manuscript version is made available under the Elsevier user license http://www.elsevier.com/open-access/userlicense/1.0/
1. Introduction

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

$$A + A = \{a_1 + a_2 : a_1, a_2 \in A\},$$
$$A - A = \{a_1 - a_2 : a_1, a_2 \in A\}.$$ (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. Let $[a, b]$ denote the set $\{x \in \mathbb{Z} : a \leq x \leq b\}$. 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 $\rho_n$ of subsets of $[0, n]$ 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 [Heg] then extended their work and showed that for any $s, d \in \mathbb{N}_0$, the proportion $\rho_{n, d}^s$ of subsets $A \subset [0, n]$ satisfying

$$|\lfloor 0, 2n \rfloor \setminus (A + A)| = s, \quad |\lfloor -n, n \rfloor \setminus (A - A)| = 2d$$ (1.2)

also remains bounded below by a positive constant in the limit. Later, in 2010, Zhao [Z] showed that both $\rho_n$ and $\rho_{n, d}^s$ converge as $n \to \infty$, with $\rho_n$ 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 $D > 0$.

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 $\rho_{n, d}^s$ of subsets $A \subset L(nP)$ such that

$$|(L(nP) + L(nP)) \setminus (A + A)| = s, \quad |(L(nP) - L(nP)) \setminus (A - A)| = 2d,$$ (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.

1See [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 review some terminology from combinatorial geometry. See [Zi] for a more detailed development. Since $P$ is the fixed polytope of our analysis, we use $Q$ to denote an arbitrary polytope in the following definitions.

**Definition 1.1.** A hyperplane in $\mathbb{R}^D$ is a set $\{x \in \mathbb{R}^D : a \cdot x = z\}$ for some normal vector $a \in \mathbb{R}^D$ and scalar $z \in \mathbb{R}$. Each hyperplane determines two closed halfspaces: $\{x \in \mathbb{R}^D : a \cdot x \leq z\}$ and $\{x \in \mathbb{R}^D : a \cdot x \geq z\}$.

**Definition 1.2.** A convex polytope in $\mathbb{R}^D$ is the bounded intersection of finitely many closed halfspaces in $\mathbb{R}^D$, or equivalently, the convex hull of finitely many points in $\mathbb{R}^D$.

**Definition 1.3.** Given a convex polytope $Q$, a hyperplane $H$ supports $Q$, or is a supporting hyperplane of $Q$, if $Q \cap H \neq \emptyset$ and $Q$ is contained in one of the closed halfspaces of $H$.

**Definition 1.4.** Given a convex polytope $Q$, a face of $Q$ is a set $F = Q \cap H$ for any supporting hyperplane $H$ of $Q$. We say $F$ is a $k$-face in particular if its affine hull $\text{aff}(F)$ has dimension $k$.

**Definition 1.5.** A 0-face is called a vertex. A 1-face is called an edge. A $(D - 1)$-face is called a facet.

It is clear that each facet has a unique supporting hyperplane.

**Definition 1.6.** Let $\mathcal{H}(Q) = \{H_1, \ldots, H_m\}$ denote the unique collection of hyperplanes that support the facets of a convex polytope $Q$. Let $S(Q) = \{S_1, \ldots, S_m\}$ denote the corresponding collection of closed halfspaces.

**Definition 1.7.** Given a vertex $v$ of $Q$, let $\mathcal{H}(Q, v)$ denote the set of hyperplanes in $\mathcal{H}(Q)$ that contain $v$, and let $S(Q, v)$ denote the corresponding set of closed halfspaces.

**Definition 1.8.** Given a vertex $v$ of a convex polytope $Q$, the supporting cone $C(v)$ is the set

$$\bigcap_{S_i \in S(Q, v)} S_i.$$  \hspace{1cm} (1.4)

**Definition 1.9.** Vertices $u$ and $v$ of a convex polytope $Q$ are strictly antipodal if there exist parallel supporting hyperplanes $H_1$ and $H_2$ of $P$ such that $H_1 \cap Q = \{u\}$ and $H_2 \cap Q = \{v\}$.

We now introduce the concept of local point symmetry.

**Definition 1.10.** A convex polytope $Q$ 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 $\{u, v\}$,

$$C(u) - u = v - C(v).$$  \hspace{1cm} (1.5)

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

**Example 1.11.** Any point symmetric polytope is locally point symmetric.

**Example 1.12.** Consider the hexagon $ABCDEF$ in Figure [7] 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.

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 1.13. 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 1.13 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 $k \in L(nP) - L(nP)$ for each of which there exists a unique pair of elements $p, q \in L(nP)$ that satisfies $k = p - q$. 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 1.14. 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 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 $S_n := \{(x,y) : x, y \in \{0, \ldots, n\}\}$. We see that $A + A$ lives in the square $S_n + S_n = \{(x,y) : x, y \in \{0, \ldots, 2n\}\}$ and $A - A$ lives in the square $S_n - S_n = \{(x,y) : x, y \in \{-n, \ldots, n\}\}$, 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 subset 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 subset $A + A$.

Thus, Theorems 1.13 and 1.14 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 5 and conjecture that the proportion of such subsets approaches 0 if $L(P)$ is not balanced. At the very least, Theorem 1.13 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

**Corollary 1.15.** 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 $n$,

$$\#\{A \subset L(nP) : A \text{ is sum-dominant}\} > c \cdot 2^{|L(nP)|},$$

$$\#\{A \subset L(nP) : A \text{ is difference-dominant}\} > c \cdot 2^{|L(nP)|},$$

$$\#\{A \subset L(nP) : A \text{ is balanced}\} > c \cdot 2^{|L(nP)|}. \quad (1.6)$$

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 $A \subset [0, n]$, 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 $ne_1$ and $ne_2$, then we can define an injective affine transformation $T_{nE} : \mathbb{R} \rightarrow \mathbb{R}^D$ by setting

$$T_{nE}(x) = (ne_2 - ne_1)/(nb_E) \cdot x + ne_1 = (e_2 - e_1)/b_E \cdot x + ne_1$$

(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 $T_E : \mathbb{R} \rightarrow \mathbb{R}^D$ is an injective affine transformation. Then there exists an injective affine transformation $T_{E+E} : \mathbb{R} \rightarrow \mathbb{R}^D$ such that

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

(2.2)

**Proof.** We first show that

$$(A + A) \cap (E + E) = (A \cap E) + (A \cap E).$$

(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 $k$ be a point in $E + E$. By the convexity of $E$, there exists some $e \in E$ such that $2e = k$. Thus, for any pair of points $a_1, a_2 \in A$ with $a_1 + a_2 = k$, we have that $(a_1 + a_2)/2 = e$. In other words, $a_1, a_2$ and $e$ are collinear with $e$ halfway between $a_1$ and $a_2$. Let $H$ be a supporting hyperplane of $Q$ such that $H \cap Q = E$. Suppose $a_1, a_2 \notin H$. Since $e \in E \subset H$, it must be that $a_1$ and $a_2$ are in different open half-spaces formed by $H$. But, since $H$ supports $Q$, then either $a_1$ or $a_2$ is not in $Q$—a contradiction. Thus, we have that $a_1, a_2 \in H$, and therefore $a_1, a_2 \in E$. 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 $T_E(x) = M(x) + b$ for all $x \in \mathbb{R}$, where $M : \mathbb{R} \rightarrow \mathbb{R}^D$ is an injective linear transformation and $b \in \mathbb{R}^D$ is some translation vector. Define $T_{E+E} : \mathbb{R} \rightarrow \mathbb{R}^D$ such that $T_{E+E}(x) = M(x) + 2b$ for all $x \in \mathbb{R}$. Since $M$ is injective and linear, $T_{E+E}$ is injective and affine. By (2.3),

$$(A + A) \cap (E + E) = (A \cap E) + (A \cap E) = T_E(S) + T_E(S) = (M(S) + b) + (M(S) + b) = M(S + S) + 2b = T_{E+E}(S + S),$$

(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 $v_1$ and $v_2$, let $E_1$ and $E_2$ be parallel edges such that $v_1 \in E_1$ and $v_2 \in E_2$. 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

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

(2.5)

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

$$(A - A) \cap (E_2 - E_1) = (A \cap E_2) - (A \cap E_1).$$

(2.6)

That $(A \cap E_2) - (A \cap E_1) \subset (A - A) \cap (E_2 - E_1)$ is immediate, so we need only show the forward inclusion. Let $e_1 \in E_1, e_2 \in E_2$. It suffices to show that if $t \in \mathbb{R}^D$ and $e_1 + t, e_2 + t \in Q$, then $e_1 + t \in E_1$ and $e_2 + t \in E_2$.

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 $H_2 \cap Q = E_2$, which is visually clear and follows easily from the definition of local point symmetry. By the definition of a face, there certainly exists a supporting hyperplane $H_1 = \{ x : a \cdot x = z \}$ of $Q$ such that $H_1 \cap Q = E_1$. Since $H_1$ contains vertex $v_1$, we have without loss of generality that $C(v_1)$ is contained in the halfspace $S_1 = \{ x : a \cdot x \leq z \}$. It follows from the local point symmetry of $Q$ that

$$C(v_1) \subset \{ x : a \cdot x \leq z \},$$

$$C(v_1) - v_1 \subset \{ x : a \cdot (x + v_1) \leq z \},$$

$$v_2 - C(v_2) \subset \{ x : a \cdot (x + v_1) \leq z \},$$

$$C(v_2) \subset \{ x : a \cdot (x + v_1 + v_2) \leq z \}.$$  

(2.7)

Since $Q \subset C(v_2)$, we have that the hyperplane $H_2 = \{ x : a \cdot (x + v_1 + v_2) = z \}$ supports $Q$. Furthermore, we see that $H_2$ is the unique hyperplane that is parallel to $H_1$ and contains $v_2$, from which it follows that $E_2 \subset H_2 \cap Q$. Finally, it is a simple argument by symmetry to show that $E_2 = H_2 \cap Q$.

Now let $S_1$ denote the closed half-space formed by $H_1$ that contains $Q$, and $S_2$ the closed half-space formed by $H_2$ that contains $Q$. Note that if a translation vector $t \in \mathbb{R}^D$ does not lie in $H_1$ (or $H_2$), then either $e_1 + t \not\in S_1$ or $e_2 + t \not\in S_2$. Thus, if $e_1 + t, e_2 + t \in Q$, then $t \in \mathbb{R}^D$ must lie in $H_1$. Then $e_1 + t \in H_1$ and $e_2 + t \in H_2$. Since $H_1 \cap Q = E_1$ and $H_2 \cap Q = E_2$, it follows that $e_1 + t \in E_1$ and $e_2 + t \in E_2$, and thus (2.6) follows.

We now prove the lemma. We can write $T_{E_1}(x) = M(x) + b_1$ and $T_{E_2}(x) = M(x) + b_2$ for all $x \in \mathbb{R}$, where $M : \mathbb{R} \to \mathbb{R}^D$ is an injective linear transformation and $b_1, b_2 \in \mathbb{R}^D$ are translation vectors. Define $T_{E_2 - E_1} : \mathbb{R} \to \mathbb{R}^D$ such that $T_{E_2 - E_1}(x) = M(x) + (b_2 - b_1)$ for all $x \in \mathbb{R}$. Since $M$ is injective and linear, $T_{E_2 - E_1}$ is injective and affine. By (2.6),

$$(A - A) \cap (E_2 - E_1) = (A \cap E_2) - (A \cap E_1)$$

$$= T_{E_2}(S_2) - T_{E_1}(S_1)$$

$$= (M(S_2) + b_2) - (M(S_1) + b_1)$$

$$= M(S_2 - S_1) + (b_2 - b_1)$$

$$= T_{E_2 - E_1}(S_2 - S_1),$$

(2.8)

as desired.

**Definition 2.3.** Given a set $S \in \mathbb{R}^D$, a difference vector $k \in S - S$ is uniquely formed if there exists a unique pair of elements $s_1, s_2 \in S$ satisfying $s_1 - s_2 = k$. 

\[\square\]
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 3.7.

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 \( x_1, x_2, \ldots, x_m \in \mathbb{R}^D \), a conical combination of these vectors is a vector of the form \( \alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_m x_m \) where \( \alpha_i \geq 0 \) for all \( 1 \leq i \leq m \). The polyhedral cone generated by vectors \( x_1, x_2, \ldots, x_m \) is the set of all conical combinations of \( x_1, x_2, \ldots, x_m \).

**Definition 2.5.** Let \( v \) be a vertex of \( Q \), and let \( n_1, \ldots, n_t \) denote outward-pointing normal vectors of all facets of \( Q \) that contain \( v \). The normal cone \( N(v) \) of \( Q \) at \( v \) is the polyhedral cone generated by \( n_1, \ldots, n_t \).

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 \( v_1, v_2, \ldots, v_m \). The following properties of normal cones \( N(v_i) \) are easily verified:

1. For each vertex \( v_i \), the normal cone \( N(v_j) \) is the set of outward normal vectors (of arbitrary length) to all supporting hyperplanes of \( Q \) that contain \( v_i \). The interior of \( N(v_i) \) is the set of outward normal vectors of all supporting hyperplanes \( H \) with \( H \cap Q = \{v_i\} \).
2. Vertices \( v_i \) and \( v_j \) are strictly antipodal if and only if the interiors of \( N(v_i) \) and \( -N(v_j) \) have non-empty intersection.
3. For \( i \neq j \), the interiors of \( N(v_i) \) and \( N(v_j) \) are disjoint.
4. For \( i \neq j \), the intersection of \( N(v_i) \) and \( N(v_j) \) is a \( k \)-face of both cones for some \( 0 \leq k < D \).
5. Supporting hyperplanes exist in every direction; that is, \( \bigcup_{i=1}^m N(v_i) = \mathbb{R}^D \).

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 \( v \) and an edge \( E \) of \( Q \) such that, for all \( e \in E \), the difference vectors \( k = e - v \) and \( -k \) are uniquely formed.

**Proof.** The difference vectors \( k = e - v \) and \( -k \) are uniquely formed if and only if there exists a non-zero vector \( t \in \mathbb{R}^D \) such that \( e + t, v + t \in Q \). To show that such a vertex \( v \) 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 \( H_1 \cap Q = \{v\} \) and \( H_2 \cap Q \supseteq E \). This is clear because, for any translation by a vector \( t \in \mathbb{R}^D \) of \( v \) and some \( e \in E \), we must have that \( t \) is parallel to \( H_1 \) and \( H_2 \) if \( e + t \) and \( v + t \) are to remain in the closed space bounded by \( H_1 \) and \( H_2 \). But \( H_1 \cap Q = \{v\} \), and therefore it must be that \( t = 0 \) if \( v + t \in Q \). See Figure 3 for an illustration.

First note that every vertex in a polytope is strictly antipodal with at least one other vertex. This follows from facts (5) and (2), since the \( D \)-dimensional interior of \( -N(v) \) cannot be covered
just using facets (which have dimension $D - 1$) of the other (finitely many) normal cones. Then, since $Q$ is not locally point symmetric, we have by Lemma 2.6 that the number of pairs of strictly antipodal vertices is strictly greater than $m/2$. Thus there exists some vertex $v$ of $Q$ that is strictly antipodal with at least two other vertices $u_1$ and $u_2$.

Now suppose $Q$ is $D$-dimensional, with $m$ vertices. If $G_1$ and $G'_1$ denote the pair of parallel supporting hyperplanes that give the strict antipodality between $v$ and $u_1$, then let $n_1$ denote a normal vector of these hyperplanes such that $n_1 \in N(v)$. Similarly define normal vector $n_2$. Let $n_t = tn_1 + (1 - t)n_2$, and observe that $n_t \in N(v)$ for all $0 \leq t \leq 1$. On the other hand, as $t$ varies from 0 to 1, we have that $-n_t$ moves from the interior of $N(u_1)$ to the interior of $N(u_2)$. Let $i \neq 1$ be such that $N(u_i)$ is the first cone whose interior $-n_t$ enters after $N(u_1)$. Then, since the normal cones cover $\mathbb{R}^D$ by (5) and their interiors are disjoint by (3), there must exist some $t' > 0$ such that $-n_{t'}$ lies in both $N(u_1)$ and $N(u_i)$ on their common boundary. Then the supporting hyperplane $H$ of $Q$ with outward normal vector $-n_{t'}$ contains both $u_1$ and $u_i$, and thus its intersection with $Q$ must be a $k$-face for some $k > 0$. This $k$-face contains some edge $E$. In other words, we have parallel supporting hyperplanes $H_1$ and $H_2$ of $Q$, with respective outward normal vectors $n_{t'}$ and $-n_{t'}$, such that $H_1 \cap Q = \{v\}$ and $H_2 \cap Q \supseteq E$, 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 $Q$ 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 $q'_1 - q'_2 \in Q' - Q'$ is uniquely formed if and only if $T^{-1}(q'_1) - T^{-1}(q'_2) \in Q - Q$ is uniquely formed. Thus, we can prove the lemma for $Q$ by applying the argument above to $Q'$.

\[\square\]
3. MIDDLE SUMS AND DIFFERENCES

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

\[
(A + A) \cap ([0, k] \cup [2n - k, 2n]) \subset (L + L) \cup (U + U),
\]
\[
(A - A) \cap ([-n, -n + k] \cup [n - k, n]) \subset (L - U) \cup (U - L).
\]

(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 $[0, n]$. 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

\[
B_r(Q) := \{ q \in L(Q): d(q, v) \leq r \text{ for some vertex } v \text{ of } Q \},
\]
\[
M_r(Q) := L(Q) \setminus B_r(Q),
\]

(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 closed 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 $A \subset L(nP)$,

\[
(A + A) \cap B_r(nP + nP) \subset (A \cap B_r(nP)) + (A \cap B_r(nP)),
\]
\[
(A - A) \cap B_r(nP - nP) \subset (A \cap B_r(nP)) - (A \cap B_r(nP)).
\]

(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 $p^+$.

Before proving this proposition, we first prove some useful lemmas. We start 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 $k \in M_r(nP + nP)$. Then, for some constant $c > 0$ independent of $n$,

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

(3.4)
Proof. The proof is similar to that of Lemma 5 in Martin and O’Bryant [MO]. Suppose we have \( x, y \in nP \) such that \( x + y = k \). Then \( x = k - y \in k - nP \), and similarly \( y \in k - nP \). Then \( L(nP \cap (k - nP)) \) can be partitioned into distinct pairs of lattice points that add up to \( k \), and the singleton \( \{k/2\} \) if \( k/2 \) is a lattice point. The probability that \( k \) 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 \( k/2 \) is not a lattice point, there are \( |L(nP \cap (k - nP))| / 2 \) pairs total, which gives

\[
\mathbb{P}[k \not\in A + A] \leq \left( \frac{3}{4} \right)^{|L(nP \cap (k - nP))|/2 - 1}.
\]

Thus, we may take \( c = (3/4)^{-l} \) and the lemma follows. In the case where \( k/2 \) 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

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

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 polytope \( nP \cap (k - nP) \) can get quite complicated, and we must do more work.

The key idea is that when \( k \) is very close to a vertex of \( nP + nP \), the shape \( nP \cap (k - nP) \) is simply a parallelotope.

**Lemma 3.3.** If a polyhedral cone \( C \) in \( \mathbb{R}^D \) is generated by at most \( D \) edges and if \( k \) is a point in \( C \), then \( C \cap (k - C) \) is a parallelotope.

**Proof.** Suppose \( C \) is the convex hull of \( D' \) linearly independent edges. Working within the \( D' \)-dimensional affine hull of \( C \), we have that every \( D' - 1 \) of these edges defines a facet of \( C \). Thus, the facet-defining hyperplanes of \( C \cap (k - C) \) come in \( D' \) pairs of parallel hyperplanes, so the intersection is a \( D' \)-dimensional parallelotope.

So when \( k \) is near a vertex of \( nP + nP \), the intersection is a simple shape. Conversely, when \( k \) is not close to a vertex of \( nP + nP \), the intersection has a more complicated shape, but we are saved by the fact that \( nP \cap (k - nP) \) is so large that we do not need to be careful about counting its lattice points. See Figure 4 for an illustration. It will be useful to keep this figure in mind for the following discussion.

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 \( k \in M_r(nP + nP) \) such that

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

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

\[
\mathbb{P}[k \not\in A + A] < \frac{\varepsilon_C}{|L(nP + nP)|} \tag{3.8}
\]
Figure 4. A triangle $T = \triangle ABC$ with its sumset $T + T = \triangle ADE$. On the left, the sum $k$ is relatively far from the vertices of $T + T$. Thus, while the shape of the intersection $T \cap (k - T)$ is hard to control, it fortunately contains many lattice points. On the right, the sum $k$ is relatively close to a vertex of $T + T$, and hence $T \cap (k - T)$ is a parallelotope.

for all $k \in C$. We conclude that the sum of $P[k \not\in A + A]$ over all $k$ in $C$ is at most $\varepsilon_C$, because $C \subseteq L(nP + nP)$.

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

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

(3.9)

Note that the right hand side is $\Theta(\log n)$, while $|L(nP + nP)|$ is $\Theta(nD)$. Intuitively, the above definition suggests that all points $k \in I$ should lie close to the vertices of $nP + nP$, in order to make $|L(nP \cap (k - nP))|$ 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 $nP \cap (k - nP)$ will be a parallelotope for all $k \in I$, for $n$ large. We formalize this idea in the following lemma.

**Lemma 3.4.** 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 $nP + nP$. In particular, letting $t$ take on the value of every positive integer $m$, we have the following: For each positive integer $m$ there exists $k_m$ and $n_m$ such that $k_m \in I(n_m)$ but $k_m$ has distance greater than $m \log n_m$ from each vertex of $nP + nP$.

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 $k'_m = k_m/n_m$. Note that this sequence lies inside the polytope $P + P$, which is closed and bounded, so there is a convergent subsequence $k'_m$. Let $k'$ denote the limit of this subsequence.

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

Consider the convex polytope $P \cap (k' - P)$, 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
k′ − P). Since P has lattice point vertices, a d′-face of P contains Θ(n^{d′}) lattice points. (Recall that P stays fixed and the lattice shrinks.)

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

We now show that B ⊂ P ∩ (k′_{m_i} − P) for i large. The fact that k′_{m_i} → k′ as i → ∞ is sufficient for this. First, consider any hyperplane H making a nonzero angle θ with A, and suppose H is translated normally by a distance at most δ. Then the intersection H ∩ A is translated along A by a distance at most ε/2 sin θ. In particular, among all of the (finitely many) facet-defining supporting hyperplanes of k′ − P, if we denote the minimum nonzero angle made with A by θ_{min}, then whenever k′ is translated by at most δ = ε/(2 sin θ_{min}), the facets of P ∩ (k′ − P) ∩ A are translated by at most ε/2 in their normal directions. Finally, for i large, |k′_{m_i} − k′| < δ, so B ⊂ P ∩ (k′_{m_i} − P), as desired. Since B contains Θ(n^{d′}) lattice points, this directly contradicts that k_{m_i} ∈ I(n), which says that |L(P ∩ (k′_{m_i} − P))| = O(log n). Thus k′ must in fact be a vertex of P + P, so that P ∩ (k′ − P) = \{k′/2\}.

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

This means that the shape P ∩ (k′_{m_i} − P) is simply a cone intersected with its translated opposite. Suppose P ∩ (k′_{m_i} − P) is d′-dimensional. Pick d′ edges of P at k′, extend them to rays from k′, and call their convex hull P′. Then P′ ∩ (k′_{m_i} − P′) is a parallelotope—as simple a shape as we could hope for. Furthermore, that parallelotope is a subset of P ∩ (k′_{m_i} − P), so it also has O(log n) lattice points. Since each of these d′ edges has a lattice structure, each has length O(log n) as well, so the diagonal |k′ − (k′_{m_i} − k′)| of the parallelotope is at most the sum of these lengths, which is still O(log n). Thus |k′_{m_i} − k′| is indeed O(log n), completing the proof of Lemma 3.4.

**Proof of Proposition 3.4** Now we evaluate the sum in (3.6) over points k ∈ I. We sum around one vertex of nP + nP at a time. Let v be the current vertex, and let I_v be the portion of I that lies in the ball of radius t log n about v.

Since log n/n → 0 as n → ∞, for n large we have (nP + nP) ∩ B_v = C(v) ∩ B_v, where C(v) denotes the supporting cone of nP + nP at v. Henceforth, assume n is this large. Now the only relevant portion of nP + nP is a neighborhood of v; that is, when k ∈ I_v,

\[ nP ∩ (k − nP) = C(v) ∩ (k − C(v)). \] (3.10)

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

\[ \sum_{k ∈ L(C(v))} c \left( \frac{3}{4} \right) |L(C(v) ∩ (k − C(v)))|/2 \] (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 \( v \), and we can make \( r \) as large as desired).

Recall that \( C(v) \) is the convex hull of rays from \( v \) corresponding to edges of \( P \). Since \( D \) is the dimension of our space, it is convenient to write \( C(v) \) as the union of convex hulls of \( D \)-tuples of those rays.\(^2\) Since there are finitely many \( D \)-tuples, it suffices to show that the sum is bounded in each such convex hull.

Let \( R \) be one such region, the convex hull of \( D \) rays from \( v \). We wish to show that

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

converges. Since \( R \subset C(v) \),

\[
|L(R \cap (k - R))| < |L(C(v) \cap (k - C(v)))|,
\]

so it suffices to show that

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

converges. This is easier, because \( R \cap (k - R) \) is simply a paralleloptote for any \( k \in L(R) \).

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 \( v \), 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 \( R^o \). When \( k \) is in the interior, \( R \cap (k - R) \) 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 \( k \in L(R^o) \),

\[
c_1 \cdot \text{vol}(R \cap (k - R)) < |L(R \cap (k - R))|.
\]

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

\[
S'_R := \sum_{k \in L(R^o)} c \left( \frac{3}{4} \right)^{c_1 \cdot \text{vol}(R \cap (k - R))}
\]

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

\[
S'_R \leq \sum_{k \in T(L(R^o))} c \left( \frac{3}{4} \right)^{c_1 \cdot \text{vol}(T(R) \cap (k - T(R)))}/c_2
\]

Now, notice that \( T(L(R^o)) \) 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 \( L(R^o) \subset q\mathbb{N}^D \) and we may further bound the sum above by

\[
S'_R \leq \sum_{k \in q\mathbb{N}^D} c \left( \frac{3}{4} \right)^{c_1 \cdot \text{vol}(T(R) \cap (k - T(R)))}/c_2.
\]

\(^2\)For the sake of exposition, we assume that \( P \) is a \( D \)-dimensional polytope, and thus each supporting cone must have at least \( D \) edges. In the event that \( P \) is a \( D' \)-dimensional polytope for \( D' < D \), the same arguments carry over if we replace \( \mathbb{R}^D \) with the affine hull of \( P \), use \( D' \)-tuples of rays, etc.
Let \( x = (3/4)^{c_1/c_2} \). Since \( T(R) \) is equal to the first orthant, \( T(R) \cap (k - T(R)) \) is simply a rectangular cell with opposite vertices \( 0 \) and \( k \), so our sum in (3.18) is equal to
\[
S''_R := q^D \sum_{(k_1, k_2, \ldots, k_D) \in \mathbb{N}^d} x^{k_1 k_2 \cdots k_D}.
\]

To show that this sum converges, we may rewrite the sum as
\[
S''_R = q^D \sum_{m \in \mathbb{N}} \psi(m) x^m,
\]
where \( \psi(m) \) is the number of ways of writing \( m \) as the ordered product of \( D \) positive integers. However, \( \psi(m) \) is bounded by \( m^D \), so since \( x < 1 \) the sum converges as desired.

Since the upper bound converges, our original sum
\[
\sum_{k \in L(C(v))} \left( \frac{3}{4} \right)^{|L(nP \cap (k-nP))/2|
\]
also converges. It follows that by making the constant fixed fringe radius \( r \) large enough, we can force the tail sum
\[
\sum_{k \in (C(v) \setminus B_r(nP + nP))} \left( \frac{3}{4} \right)^{|L(nP \cap (k-nP))/2|
\]
to be smaller than any \( \varepsilon_{I_r} \). Since \( I_r \) lies in \( L(C(v) \setminus B_r(nP + nP)) \), the sum over \( k \in I_r \) is also smaller than \( \varepsilon_{I_r} \). Thus if we let \( \varepsilon_I \) be the sum of \( \varepsilon_{I_r} \) over all vertices \( v \) 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 \( \varepsilon_C \) and \( \varepsilon_I \) 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. \( \square \)

We now examine the presence of middle differences.

**Proposition 3.5.** 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 \( k \in L(nP) + L(nP) \) are pairwise disjoint. Thus, the probabilities that at least one point is missing from each pair are independent, so it is easy to bound the probability that \( k \) is missing in \( A + A \). The same does not hold for differences, however, when a difference \( k \in L(nP) - L(nP) \) is small enough such that \( x, x + k, x + 2k \in L(nP) \) for some \( x \in L(nP) \). Fortunately, as in [MO], the probability that such a small difference is missing is so tiny that a crude bound is sufficient.

**Lemma 3.6.** 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 \( k \in M_r(nP - nP) \) be given. Then, for some constant \( c > 0 \) independent of \( n \),
\[
\Pr[k \not\in A - A] \leq c \left( \frac{3}{4} \right)^{|L(nP \cap (nP - k))/2|}.
\]
(3.23)
Proof. Define random variables $X_j$ by setting $X_j = 1$ if $j \in A$ and $X_j = 0$ otherwise. We have $k \not\in A - A$ if and only if $X_jX_{j+k} = 0$ for all $j \in L(nP \cap (nP - k))$.

For the first case, suppose $k$ is small such that $k \in \{nP - nP\}$, and suppose $k = (k_1, k_2, \ldots, k_D)$. The possibility $k = 0$ is trivial, as $\Pr[0 \not\in A - A] = 0$, so we may assume $k \neq 0$. Without loss of generality, let $k_1$ be nonzero, and define

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

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

$$J_n := \begin{cases} 
G_n & \text{if } |G_n| > |H_n| \\
H_n & \text{if } |H_n| \geq |G_n|.
\end{cases} \quad (3.24)$$

It is possible that $J_n$ is $G_n$ or $H_n$ depending on $n$, hence the subscript notation. It is clear that $x + k \not\in J_n$ for any $x \in J_n$, and therefore the random variables $X_jX_{j+k}$ are pairwise independent across all $j \in J_n$. As $|G_n| + |H_n| = |L(nP \cap (nP - k))|$, it is further clear that

$$|J_n| \geq \frac{1}{2}|L(nP \cap (nP - k))|. \quad (3.25)$$

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

$$\Pr[X_jX_{j+k} = 0 \text{ for all } j \in L(nP \cap (nP - k))] \leq \Pr[X_jX_{j+k} = 0 \text{ for all } j \in J_n]$$

$$= \prod_{j \in J_n} \Pr[X_jX_{j+k} = 0]$$

$$\leq \left(\frac{3}{4}\right)^{|J_n| - l}$$

$$\leq \left(\frac{3}{4}\right)^{|L(nP \cap (nP - k))/2 - l}. \quad (3.26)$$

For the second case, suppose $k \not\in \{nP - nP\}$. Then there exists no $j \in L(nP)$ such that $j, j + k, j + 2k \in L(nP)$. That is, the random variables $X_jX_{j+k}$ are pairwise independent across all $j \in L(nP \cap (nP - k))$. Then

$$\Pr[X_jX_{j+k} = 0 \text{ for all } j \in L(nP \cap (nP - k))] = \prod_{j \in L(nP \cap (nP - k))} \Pr[X_jX_{j+k} = 0]$$

$$\leq \left(\frac{3}{4}\right)^{|L(nP \cap (nP - k))/2 - l}. \quad (3.27)$$

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

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

The other aspect of the difference set case that deserves discussion is the difference set analogue of Lemma 3.4—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 $k \in Q - Q$ is close to one of these uniquely

formed differences, $Q \cap (Q - k)$ 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 $P \cap (k' - P)$ is just one point, and immediately conclude that $k'$ 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 3.7.** Let $Q$ be a locally point symmetric polytope, and let $k \in Q - Q$. The following statements are equivalent:

(i) $Q \cap (Q - k)$ consists of a single point, i.e., $k$ is a uniquely formed difference in $Q - Q$.

(ii) $k$ is a vertex of the polytope $Q - Q$.

(iii) $k = u - v$ for strictly antipodal vertices $u$ and $v$ of $Q$.

**Proof.** In the proof of this lemma, we use the following fact about supporting cones:

(1) Let $A$ be a $k$-face of $Q$, and let $u$ be given in the interior of $A$ (relative to the $k$-dimensional affine space containing $A$). If $a + x$ is in the supporting cone of some vertex $a$ of $A$, then $u + \epsilon x \in Q$ for $\epsilon$ small.

To justify (1), it suffices to show that, if $x \in C(a) - a$, then $\epsilon x \in Q - u$ for sufficiently small $\epsilon$. Observe that the set of hyperplanes supporting $Q - u$ at the origin is a subset of the hyperplanes supporting $C(a) - a$ at the origin, since each hyperplane that supports $Q$ at $u$, and therefore at the $k$-face $A$, must also support $Q$ at each of the vertices of $A$. As polytopes and supporting cones are intersections of halfspaces generated by supporting hyperplanes, it follows that there exists some $r > 0$ such that $(B(0, r) \cap (C(a) - a)) \subset (B(0, r) \cap (Q - u))$, where $B(0, r)$ denotes a closed ball of radius $\epsilon$ centered at the origin. If $x \in C(a) - a$, then certainly $\epsilon x \in B(0, r) \cap (C(a) - a)$ for sufficiently small $\epsilon$, and thus $\epsilon x \in Q - u$.

We first show (i) $\implies$ (iii). Let $u$ and $v$ be the unique points in $Q$ that satisfy $k = u - v$. Suppose that $u$ lies in a $k$-face $A$ and $v$ 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 $a \in A$ and $b \in B$ that are not strictly antipodal. Then the cones $C(a) - a$ and $C(b) - b$ must both contain some nonzero vector $x$—otherwise, if they only intersected at the origin, then there would exist a hyperplane through the origin separating them, and translates of this separating hyperplane to the vertices $a$ and $b$ would witness the strict antipodality

**Figure 5.** A locally point symmetric polytope $Q$ with strictly antipodal vertices $u$ and $v$, a difference vector $k \in Q - Q$, and the translated polytope $Q - k$. The difference $k$ is close to the uniquely formed difference $v - u$, and hence the intersection polytope $Q \cap (Q - k)$ is a parallelotope.
of \(a\) and \(b\). Then \(a + \varepsilon x\) and \(b + \varepsilon x\) both lie in \(Q\) for sufficiently small \(\varepsilon\), and it follows by fact (1) above that \(u + \varepsilon x\) and \(v + \varepsilon x\) both lie in \(Q\) (again, for further sufficiently small \(\varepsilon\)). But this contradicts the fact that the difference \(k = u - v\) is 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, \(A = \{u\}\) and \(B = \{v\}\), and \(u\) and \(v\) are strictly antipodal vertices as desired.

Next, we show (iii) \(\implies\) (ii). To do so, we first show (iii) \(\implies\) (i). Let \(H_1\) and \(H_2\) be parallel supporting hyperplanes meeting \(Q\) at \(\{u\}\) and \(\{v\}\), respectively. To prove (i), it suffices to show that, for any nonzero \(t \in \mathbb{R}^D\), either \(u + t \notin Q\) or \(v + t \notin Q\). If we suppose that \(u + t \in Q\), then it is clear that \(v + t\) lies on the side of \(H_2\) opposite \(Q\), and thus cannot lie in \(Q\). Similarly, assuming \(v + t \in Q\) gives us \(u + t \notin Q\). Thus \(k\) is a uniquely formed difference. Now, to prove (ii), it suffices to show that for any \(t\), if \(k + t\) and \(k - t\) are both in \(Q - Q\), then \(t\) must be zero. If \(k + t\) and \(k - t\) are both in \(Q - Q\), then there exist four points \(a, b, a + k + t, b + k - t\) all in \(Q\). By convexity, the midpoints \((a + b)/2\) and \((a + b + 2k)/2\) are also in \(Q\). But these two points have difference \(k\), which we have shown is uniquely formed, so the two points must be \(u\) and \(v\). Now \(u\) is a midpoint of points \(a\) and \(b\), which both lie in \(Q\). Since \(u\) is a vertex of \(Q\), we must have \(a = b = u\). But then \(v\) is the midpoint of \(u + k + t\) and \(u + k - t\), which both lie in \(Q\). Since \(v\) is also a vertex of \(Q\), it follows that \(t = 0\), as desired.

Finally, we show (ii) \(\implies\) (i). Suppose there exist \(a, a + k, b, b + k\) all in \(Q\). Then \((a + k) - b\) and \((b + k) - a\) both lie in \(Q - Q\). That is, for \(t = b - a\), we have \(k + t \in Q - Q\) and \(k - t \in Q - Q\). Since \(k\) is a vertex of \(Q - Q\), it must be that \(t = 0\), and thus \(a = b\), as desired.

The rest of the proof of Proposition 3.1 carries over to the difference set case with trivial modifications. \(\square\)

4. PROOF OF THEOREM 1.13

We begin by showing that the proportion \(\rho_{n^s,d}^s\) 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 \(nv\) and an edge \(nE\) of \(nP\) such that for all \(e \in nE\), the difference vectors \(e - nv\) and \(-k\) 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

\[
\rho_{n^s,d}^s \leq \left(\frac{n + 1}{d}\right)^{n + 1 - d} \left(\frac{1}{2}\right)^{n + 1 - d} = \Theta\left(\frac{n^d}{2^n}\right),
\]

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 \(A \cap B_r(nP) = F_r\),

\[
|B_r(nP + nP) \setminus (A + A)| = s,
\]

\[
|B_r(nP - nP) \setminus (A - A)| = 2d.
\]

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 \(nv_1\) and \(nv_2\) of \(nP\), and a pair of parallel edges \(nE_1\) and \(nE_2\) such that \(nv_1 \in nE_1\) and \(nv_2 \in nE_2\). Suppose \(nE_1\) and \(nE_2\) contain \(nb_{E_1} + 1\) and \(nb_{E_2} + 1\) lattice points, respectively. As discussed

\[3\]A hyperplane \(H = \{x : h \cdot x = z\}\) separates two convex sets \(S_1\) and \(S_2\) if \(S_1 \subset \{x : h \cdot x \leq z\}\) and \(S_2 \subset \{x : h \cdot x \geq z\}\), or vice versa.
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 \( T_{nE_1}(0) = n\nu_1 \) and \( T_{nE_2}(nb_{E_2}) = n\nu_2 \). 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

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

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

Now define \( r = \max\{r^+, r^-, r'\} \), where \( r^+ \) and \( r^- \) are the constants given by Propositions 3.1 and 3.5. Let \( B'_r(nP) \) denote the set

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

\[
F_r := T_{nE_1} \circ (L_{s,d}) \cup T_{nE_2} \circ (U_{s,d}) \cup B'_r(nP).
\]

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.

**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 \( n\nu_1 \) and \( n\nu_2 \).

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

\[
A \cap nE_1 = T_{nE_1}(S_1), \quad A \cap nE_2 = T_{nE_2}(S_2),
\]
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

\[
(A + A) \cap (nE_1 + nE_1) = T_{nE_1+nE_1}(S_1 + S_1),
\]
and

\[
(A + A) \cap (nE_2 + nE_2) = T_{nE_2+nE_2}(S_2 + S_2).
\]
It is easy to show that, then,
\[(A + A) \cap T_{nE_1 + nE_1}([0, r']) = T_{nE_1 + nE_1}((S_1 + S_1) \cap [0, r']) \]
\[= T_{nE_1 + nE_1}((L_{s,d} + L_{s,d}) \cap [0, r']), \quad (4.10)\]
and similarly
\[(A + A) \cap T_{nE_2 + nE_2}([2nbE_2 - r', 2nbE_2]) = T_{nE_2 + nE_2}((U_{s,d} + U_{s,d}) \cap [2nbE_2 - r', 2nbE_2]). \quad (4.11)\]

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 \(T_{nE_2 + nE_2}([nbE_2 - r', nbE_2])\).

Similarly, by Lemma 2.2 there exists an injective affine transformation \(T_{nE_2 - nE_1} : \mathbb{R} \to \mathbb{R}^D\) such that
\[(A - A) \cap (nE_2 - nE_1) = T_{nE_2 - nE_1}(S_2 - S_1), \quad (4.12)\]
and we can show that
\[(A - A) \cap T_{nE_2 - nE_1}([nbE_2 - r', nbE_2]) = T_{nE_2 - nE_1}((U_{s,d} - L_{s,d}) \cap [nbE_2 - r', nbE_2]). \quad (4.13)\]

It follows by (4.5) that \(A - A\) is missing exactly \(2d\) differences in the regions \(T_{nE_2 - nE_1}([nbE_2 - r', nbE_2])\) and \(-T_{nE_2 - nE_1}([nbE_2 - r', nbE_2])\).

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,
\[B_r(nP + nP) \setminus (T_{nE_1 + nE_1}([0, r']) \cup T_{nE_2 + nE_2}([2nbE_2 - r', 2nbE_2])) \subset A + A, \]
\[B_r(nP - nP) \setminus (T_{nE_2 - nE_1}([nbE_2 - r', nbE_2]) \cup -T_{nE_2 - nE_1}([nbE_2 - r', nbE_2])) \subset A - A. \quad (4.14)\]

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

Let \(p^+ > 1/2\) and \(p^- > 1/2\). By Propositions 3.1 and 3.5 we have that \(M_r(nP + nP) \subset A + A\) with probability 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.

\[\square\]

5. PROOF OF THEOREM 1.14

Similarly to the proof of Theorem 1.13 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 \(A \cap B_r(nP) = F_r\),
\[B_r(nP + nP) \setminus (A + A) = s, \quad B_r(nP - nP) \setminus (A - A) \geq 2d. \quad (5.1)\]

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 1.13. Now suppose \(P\) is not locally point symmetric. Let \(nV\) 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 \(nE_1\). If \(nE_1\) and \(nE_2\) contain, respectively, \(nbE_1 + 1\) and \(nbE_2 + 1\)
SETS CHARACTERIZED BY MISSING SUMS AND DIFFERENCES IN DILATING POLYTOPES 21

![Figure 7](image)

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 $nE_2$.

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

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

Further define

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

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

Define $r = \max\{r^+, r^-, r', 3d\}$, where $r^+$ and $r^-$ are the constants given by Propositions [3,1] and [3,5] respectively. Define

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

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

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

for some sets $S_1, S_2 \subset \mathbb{Z}$ such that $S_1 \cap [0, 3d] = R_d$, $S_2 \cap [0, r'] = L_s$, 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,

\[(A + A) \cap T_{nE_2+nE_2}([0, r']) = T_{nE_2+nE_2}((L_s + L_s) \cap [0, r'])\]  \hspace{1cm} (5.8)

and

\[(A + A) \cap T_{nE_2+nE_2}([2nb_E - r', 2nb_E]) = T_{nE_2+nE_2}((U_s + U_s) \cap [2nb_E - r', 2nb_E]).\] \hspace{1cm} (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 \(T_{nE_2+nE_2}([2nb_E - r', 2nb_E])\).

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 \([0, 3d] \subset R_d + R_d\), we can show in a similar manner to the argument above that \(A + A\) is not missing any sums in the region \(T_{nE_1+nE_1}([0, 3d])\).

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

\[B_r(nP + nP) \setminus (T_{nE_1+nE_1}([0, 3d]) \cup T_{nE_2+nE_2}([0, r']) \cup T_{nE_2+nE_2}([2nb_E - r', 2nb_E]))\] \hspace{1cm} (5.10)

are present in \(A + A\). The proof concludes identically as in that of Theorem 1.13 from here. \(\square\)

6. Future Directions

There are several natural directions in which to proceed from here. One conjecture is that the proportion \(\rho_n\) 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 \(\rho_n\) 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 1.13 nor Theorem 1.14 implies that \(\rho_n\) 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 \(\overrightarrow{AB}\) and a point in edge \(\overrightarrow{CD}\) 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 $v$, there are hyperplanes that support the tetrahedron precisely at $v$ 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 1.15, we make the following conjecture:

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

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 $n$?

There is also the question of whether there exist any convex polytopes $P$ with $|L(P) + L(P)| > |L(P) - L(P)|$. If we consider volumes instead of lattice points, the question is simple. Indeed, the Brunn-Minkowski inequality states that for nonempty compact subsets $A, B$ of $\mathbb{R}^D$,

$$\text{vol}(A + B)^{1/D} \geq \text{vol}(A)^{1/D} + \text{vol}(B)^{1/D},$$

(6.1)
with equality if and only if $A$ and $B$ are dilates of each other. Thus, when $P$ is convex,
\[
\text{vol}(P - P) \geq \left(\text{vol}(P)^{1/D} + \text{vol}(-P)^{1/D}\right)^D
\]
\[
= 2^D \text{vol}(P)
\]
\[
= \text{vol}(P + P).
\]
Equality occurs if and only if $P$ is a dilate of $-P$, which is another way of saying that $P$ is point symmetric. This lends support to the following conjecture, which we leave to future work:

**Conjecture 6.2.** Let $P$ be a polytope in $\mathbb{R}^D$ with vertices in $\mathbb{Z}^D$. Then
\[
|L(P) + L(P)| \leq |L(P) - L(P)|,
\]
with equality if and only if $P$ is point symmetric.

Finally, it is interesting to examine how the limiting proportions of $\rho_n$ 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 $\rho_n$ 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,
\[
s(Q) = m - k,
\]
where $k (0 \leq k \leq \lfloor m/2 \rfloor)$ is the number of pairs of parallel sides in $Q$.

**Theorem A.3.** For a convex $D$-dimensional polytope $Q \subset \mathbb{R}^D$, $m \geq D + 1$, $D \geq 3$,
\[
s(Q) \geq \lceil m/2 \rceil.
\]
For an even $m$, the equality $s(Q) = \lceil m/2 \rceil$ holds if and only if $m \geq 2D$ and the vertices of $Q$ can be divided into $m/2$ pairs such that for each pair $\{u, v\}$,
\[
C(u) - u = v - C(v).
\]
For an odd $m$, the equality $s(Q) = \lceil m/2 \rceil$ holds if and only if $m \geq 4D - 1$ and some $(m - 3)/2$ pairwise disjoint subsets of the form $\{u, v\}$ can be chosen from the vertex set such that
\[
C(u) - u = v - C(v)
\]
for each of them, and the remaining three vertices $x, y, z$ satisfy the relation
\[
(C(x) - x) \cap (C(y) - y) = z - C(z).
\]
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 \( v_1, v_2, \ldots, v_m \) in clockwise order. We can show that for any pair of parallel sides \( E = v_i v_{i+1} \) and \( F = v_j v_{j+1} \) 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 \( v_i \) and \( v_j \) are strictly antipodal, and \( v_{i+1} \) and \( v_{j+1} \) 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*, J. Number Theory 147 (2015), 44–68

[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.

[LO] 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.

[Zi] G. M. Ziegler, *Lectures on Polytopes*, Springer (1995).