Maximum Values k for $\phi_{\pm}(\mathbb{Z}_2 \times \mathbb{Z}_{2k}, [0, s]) = 2$

William Kyle Beatty

Gettysburg College
Gettysburg, PA 17325-1486 USA
E-mail: w.kyle.beatty@protonmail.com

August 18, 2021

1 Introduction

We first define the main objects of our research, then introduce Park's previous results.

Definition 1. *For a positive m and a nonnegative h, a* layer *of the m-dimensional integer lattice is defined as*

$$\mathbb{Z}^m(h) = \{(\lambda_1, \lambda_2, \ldots, \lambda_m) \in \mathbb{Z}^m : |\lambda_1| + |\lambda_2| + \ldots + |\lambda_m| = h\}.$$

For a given $s \geq 0$, we also employ an interval notation to describe subsets of the integer lattice

$$\mathbb{Z}^m([0, s]) = \{(\lambda_1, \lambda_2, \ldots, \lambda_m) \in \mathbb{Z}^m : |\lambda_1| + |\lambda_2| + \ldots + |\lambda_m| \in [0, s]\}.$$

Definition 2. *Let s be a positive integer and let $A = \{a_1, a_2, \ldots, a_m\}$. The $[0, s]$-fold signed sumset of A is defined as*

$$[0, s]_{\pm}A = \{\lambda_1 \cdot a_1 + \lambda_2 \cdot a_2 + \cdots + \lambda_m \cdot a_m : (\lambda_1, \lambda_2, \ldots, \lambda_m) \in \mathbb{Z}^m([0, s])\}.$$

Definition 3. *Let s be a positive integer, G be a group, and A a subset of G. Then A* spans *G if and only if $[0,s]_{\pm}A = G$. In this case we call A a* spanning set *of G, and denote by $\phi_{\pm}$ the size of the smallest spanning set of G for a given s:*

$$\phi_{\pm}(G,[0,s]) = \min\{|A| : [0,s]_{\pm}A = G\}.$$

Our work focuses on groups of the form $G = \mathbb{Z}_2 \times \mathbb{Z}_{2k}$ for which $\phi_{\pm}(G,[0,s]) = 2$. We include here Park's results in [2]:

Theorem 4 (Park, 2020)**.** *Given a positive integer s, let $k = \frac{s^2}{2}$ when s is even and $k = \frac{s^2-1}{2}$ when s is odd. Then $\phi_{\pm}(\mathbb{Z}_2 \times \mathbb{Z}_{2k},[0,s]) = 2$, where the spanning set of $\mathbb{Z}_2 \times \mathbb{Z}_{2k}$ is $\{(0,1),(1,s-1)\}$ when s is even and $\{(1,\frac{s-1}{2}),(1,\frac{s+1}{2})\}$ when s is odd.*

Conjecture 5 (Park, 2020)**.** *The value of k found in the theorem above is the largest possible k for which $\phi_{\pm}(\mathbb{Z}_2 \times \mathbb{Z}_{2k},[0,s]) = 2$.*

2 Main results

In this paper, we provide a proof of conjecture 5:

Theorem 6. *Given a positive integer s, the value*

$$k = \begin{cases} \frac{s^2}{2}, & s \text{ is even} \\ \frac{s^2-1}{2}, & s \text{ is odd} \end{cases}$$

is the largest k satisfying the equation

$$\phi_{\pm}(\mathbb{Z}_2 \times \mathbb{Z}_{2k},[0,s]) = 2.$$

Conjecture 7. *Let s be a positive integer. Then*

- *When s is odd, $\phi_{\pm}(\mathbb{Z}_2 \times \mathbb{Z}_{2k},[0,s]) = 2$ if and only if $k \in [1,\frac{s^2-1}{2}]$;*
- *When s is even and greater than 2, there is some $k < \frac{s^2}{2}$ such that*

$$\phi_{\pm}(\mathbb{Z}_2 \times \mathbb{Z}_{2k},[0,s]) > 2.$$

Further, we assert that when s is odd and $k \in [1, \frac{s^2-1}{2}]$, the set $\{(0,1),(1,0)\}$ spans $\mathbb{Z}_2 \times \mathbb{Z}_{2k}$ when $k < s$ (by proposition B.55 in [1]), and that the set $\{(0,x),(1,y)\}$, where

$$x = \begin{cases} \frac{s+1}{2}, & s \equiv 1 \bmod 4 \\ \frac{s-1}{2}, & s \equiv 3 \bmod 4 \end{cases} \qquad y = \begin{cases} \frac{s-1}{2}, & s \equiv 1 \bmod 4 \\ \frac{s+1}{2}, & s \equiv 3 \bmod 4, \end{cases}$$

spans $\mathbb{Z}_2 \times \mathbb{Z}_{2k}$ when $k \geq s$.

We have computationally verified the conjecture for all odd $s \leq 35$, and for all even $s \leq 20$. Values of k for each even s are included in Appendix A.

3 Methods

Given a nonnegative integer s, we define two functions $E(s)$ and $O(s)$. $E(s)$ is the number of coefficient pairs in $\mathbb{Z}^2([0,s])$ whose sum is even

$$E(s) = |\{(\lambda_1, \lambda_2) \in \mathbb{Z}^2([0,s]) \mid |\lambda_1| + |\lambda_2| \equiv 0 \bmod 2\}|$$

while $O(s)$ is the number of coefficient pairs in $\mathbb{Z}^2([0,s])$ whose sum is odd

$$O(s) = |\{(\lambda_1, \lambda_2) \in \mathbb{Z}^2([0,s]) \mid |\lambda_1| + |\lambda_2| \equiv 1 \bmod 2\}|.$$

For convenience, we call elements of the integer lattice even if the sum $|\lambda_1| + |\lambda_2|$ is even, and call them odd if the sum is odd.

We now prove a lemma concerning these two functions, which will be useful when the parity of $(\lambda_1, \lambda_2) \in \mathbb{Z}^2([0,s])$ determines some property of a group element corresponding to (λ_1, λ_2).

Lemma 8. *The functions $E(s)$ and $O(s)$ adhere to the following formulae:*

$$E(s) = \begin{cases} s^2 + 2s + 1, & s \equiv 0 \bmod 2 \\ s^2, & s \equiv 1 \bmod 2 \end{cases}$$

$$O(s) = \begin{cases} s^2, & s \equiv 0 \bmod 2 \\ s^2 + 2s + 1, & s \equiv 1 \bmod 2. \end{cases}$$

Proof. We begin with two identities derived from the table found in [1, p. 28] — one concerning the subset $\mathbb{Z}^2([0,s])$ of the integer lattice,

$$|\mathbb{Z}^2([0,s])| = 2s^2 + 2s + 1, \tag{1}$$

and a second concerning the size of an individual layer $\mathbb{Z}^2(h)$ for some $h \geq 0$,

$$|\mathbb{Z}^2(h)| = \begin{cases} 4h, & h \geq 1 \\ 1, & h = 0. \end{cases} \tag{2}$$

Because the set $\mathbb{Z}^2([0,s])$ can be partitioned into even and odd elements, the equation below follows from identity (1)

$$E(s) + O(s) = 2s^2 + 2s + 1. \tag{3}$$

Given any $h \in [0,s]$, it is clear that all the elements of the layer $\mathbb{Z}^2(h)$ will be even if h is even and odd if h is odd. With this fact and identity (2), we calculate $E(s)$ for even values of s:

$$\begin{aligned} E(s) &= |\mathbb{Z}^2(0)| + |\mathbb{Z}^2(2)| + \cdots + |\mathbb{Z}^2(s)| \\ &= 1 + 4 \cdot 2 + \cdots + 4 \cdot s \\ &= 1 + 4 \cdot (2 + 4 + \cdots + s) \\ &= 1 + 8 \cdot (1 + 2 + \cdots + \frac{s}{2}) \\ &= 1 + 8 \cdot \frac{\frac{s}{2} \cdot (\frac{s}{2} + 1)}{2} \\ &= 1 + 8 \cdot \frac{s^2 + 2s}{8} \\ E(s) &= s^2 + 2s + 1. \end{aligned}$$

By identity (3), this implies that $O(s) = s^2$ for even values of s.

We now derive the formula for $E(s)$ when s is odd. Clearly no element of the layer $\mathbb{Z}^2(s)$ will be even, so we have:

$$E(s) = E(s-1)$$
$$E(s) = (s-1)^2 + 2(s-1) + 1$$
$$E(s) = s^2.$$

By identity (3), we conclude that $O(s) = s^2 + 2s + 1$ for odd values of s. □

We now use lemma 8 to prove a fact about spanning pairs of groups $G = \mathbb{Z}_2 \times \mathbb{Z}_{2k}$ with $k > \frac{s^2}{2}$.

Proposition 9. *Let k be a positive integer such that $k > \frac{s^2}{2}$, and let $G = \mathbb{Z}_2 \times \mathbb{Z}_{2k}$. Let $A = \{(1, x), (1, y)\}$ be a subset of G. Then $[0, s]_{\pm} A \neq G$, i.e. A does not span G.*

Proof. Take any $(\lambda_1, \lambda_2) \in \mathbb{Z}^2([0, s])$, and consider the spanned element

$$(a, b) = \lambda_1 \cdot (1, x) + \lambda_2 \cdot (1, y).$$

Note that the parity of (λ_1, λ_2) corresponds to the value, and therefore the parity, of a — if $|\lambda_1| + |\lambda_2|$ is even, then $a = 0$; if it is odd, then $a = 1$.

We now show that there are either insufficient even elements of $\mathbb{Z}^2([0, s])$ to span the even $(a = 0)$ elements of G, or insufficient odd elements of $\mathbb{Z}^2([0, s])$ to span the odd $(a = 1)$ elements of G.

Recalling that $k > \frac{s^2}{2}$, calculating the size of the group yields

$$|G| = |\mathbb{Z}_2 \times \mathbb{Z}_{2k}| > 2s^2.$$

We partition G by the value of a for each element, which divides the group into two halves, each with more than s^2 elements.

By proposition 8, if s is even, there are $O(s) = s^2$ odd elements of $\mathbb{Z}^2([0, s])$. Because only odd elements (λ_1, λ_2) can span odd elements of G, this implies that A can span at most s^2 odd elements of G, which is insufficient to span G.

Again by proposition 8, if s is odd, there are $E(s) = s^2$ even elements of $\mathbb{Z}^2([0, s])$. In this case, there are insufficient even elements of $\mathbb{Z}^2([0, s])$ to span the even elements of G. Therefore, for any value of s and any $k > \frac{s^2}{2}$, the subset $A = \{(1, x), (1, y)\}$ cannot span G. □

Next, we impose a further restriction on spanning pairs of G.

Proposition 10. *Given positive s, k, and a group $G = \mathbb{Z}_2 \times \mathbb{Z}_{2k}$, let $A = \{(0, x),\ (1, y)\}$ be a subset of G. If x is even, then $[0, s]_{\pm} A \neq G$.*

Proof. We prove that if x is even, then $(0, 1) \notin [0, s]_{\pm} A$. Suppose indirectly that x is even and that $(0, 1) \in [0, s]_{\pm} A$, i.e. there exist some λ_1, λ_2 such that

$$\lambda_1 \cdot (0, x) + \lambda_2 \cdot (1, y) = (0, 1)$$

with $|\lambda_1| + |\lambda_2| \in [0, s]$. Because the first component of $(0, 1)$ is 0, the coefficient λ_2 must be even. The equation determining the second component of the sum is

$$\lambda_1 \cdot x + \lambda_2 \cdot y \equiv 1 \bmod 2k.$$

We have established that λ_2 is even, so if x is also even, then the sum on the left side of the equation must be even, while the right side must be odd, which is impossible. Therefore $(0, 1)$ cannot be in the span of A, and $[0, s]_{\pm} A \neq G$. □

A final restriction on potential spanning pairs will put the final proof of the conjecture within reach.

Proposition 11. *Let k be a positive integer such that $k > \frac{s^2}{2}$, and let $G = \mathbb{Z}_2 \times \mathbb{Z}_{2k}$. Let $A = \{(0, x), (1, y)\}$ be a subset of G. If y is odd, then $[0, s]_{\pm} A \neq G$.*

Proof. If x is even, then A does not span G by proposition 10, so we assume that both x and y are odd.

Take any $(\lambda_1, \lambda_2) \in \mathbb{Z}^2([0, s])$, and consider the spanned element

$$(a, b) = \lambda_1 \cdot (0, x) + \lambda_2 \cdot (1, y).$$

Because x and y are both odd, b is even if (λ_1, λ_2) is even, and odd if (λ_1, λ_2) is odd — the parity of the coefficients corresponds exactly with the parity of b.

We now show that there are either insufficient even elements of $\mathbb{Z}^2([0, s])$ to span the elements of G with an even second component b, or insufficient odd elements of $\mathbb{Z}^2([0, s])$ to span the elements of G whose second component is odd.

Recalling that $k > \frac{s^2}{2}$, calculating the size of the group yields

$$|G| = |\mathbb{Z}_2 \times \mathbb{Z}_{2k}| > 2s^2.$$

We partition G by the parity of each element's second component b, which divides the group into two halves, each with more than s^2 elements.

By lemma 8, if s is even, there are $O(s) = s^2$ odd elements of $\mathbb{Z}^2([0,s])$. Because of the established relationship between the parity of (λ_1, λ_2) and the spanned group element, this implies that A can span at most s^2 elements of G whose second component is odd.

Again by proposition 8, if s is odd, there are $E(s) = s^2$ even elements of $\mathbb{Z}^2([0,s])$. In this case, there are insufficient even elements of $\mathbb{Z}^2([0,s])$ to span the elements of G whose second component is even. Therefore, for any value of s and any $k > \frac{s^2}{2}$, the subset $A = \{(0,x),(1,y)\}$ cannot span G if y is odd. □

With the above restrictions on spanning pairs in place, we are ready to prove theorem 6.

Theorem 6. *Given a positive integer s, the value*

$$k = \begin{cases} \frac{s^2}{2}, & s \text{ is even} \\ \frac{s^2-1}{2}, & s \text{ is odd} \end{cases}$$

is the largest k satisfying the equation

$$\phi_{\pm}(\mathbb{Z}_2 \times \mathbb{Z}_{2k}, [0,s]) = 2.$$

Proof. Let s be a positive integer, let $k > \frac{s^2}{2}$, and let $G = \mathbb{Z}_2 \times \mathbb{Z}_{2k}$. Clearly no subset of the form $\{(0,x),(0,y)\}$ can span G, and by propositions 9, 10, and 11, we know that for G, any spanning set of two elements must have the form $A = \{(0,x),(1,y)\}$ for some odd x and even y. We show that if such a spanning set exists, then the set $A' = \{(1,x),(1,y)\}$ also spans G. By proposition 9, it is impossible for the set A' to span G, thus proving indirectly that the set A does not span G.

Let $A = \{(0,x),(1,y)\}$, with odd x and even y, be a spanning set of G. Because A spans G, there exists some function $f : G \to \mathbb{Z}^2([0,s])$ that, given some $(a,b) \in G$, returns $(\lambda_1, \lambda_2) \in \mathbb{Z}^2([0, s])$ such that

$$\lambda_1 \cdot (0, x) + \lambda_2 \cdot (1, y) = (a, b).$$

We use f to construct a similar function $g : G \to \mathbb{Z}^2([0, s])$ that, for a given $(a, b) \in G$, returns $(\lambda_1, \lambda_2) \in \mathbb{Z}^2([0, s])$ such that

$$\lambda_1 \cdot (1, x) + \lambda_2 \cdot (1, y) = (a, b),$$

proving that the set $A' = \{(1, x), (1, y)\}$ also spans G.

We begin by defining $g(a, b) = f(a, b)$ for even values of b.

Take some $(a, b) \in G$ and let $(\lambda_1, \lambda_2) = f(a, b)$, i.e.

$$\lambda_1 \cdot (0, x) + \lambda_2 \cdot (1, y) = (a, b).$$

If b is even, then because x is odd and y is even, λ_1 must be even. Consequently, we know that $\lambda_1 \cdot (1, x) = \lambda_1 \cdot (0, x)$, and therefore that

$$\begin{aligned} \lambda_1 \cdot (1, x) + \lambda_2 \cdot (1, y) &= \lambda_1 \cdot (0, x) + \lambda_2 \cdot (1, y) \\ \lambda_1 \cdot (1, x) + \lambda_2 \cdot (1, y) &= (a, b), \end{aligned}$$

so $g(a, b) = f(a, b)$ for even values of b.

Take some $(a, b) \in G$ where b is odd and let $(\lambda_1, \lambda_2) = f(a, b)$, i.e.

$$\lambda_1 \cdot (0, x) + \lambda_2 \cdot (1, y) = (a, b).$$

When b is odd, then because x is odd and y is even, λ_1 must also be odd. In this case, we define $g(a, b)$ as

$$g(0, b) = f(1, b) \quad \text{and} \quad g(1, b) = f(0, b).$$

We begin by proving that when $a = 0$, the function g satisfies the desired properties. Let $(\lambda_1, \lambda_2) = f(1, b)$ for an odd b. By the definition of f

$$\lambda_1 \cdot (0, x) + \lambda_2 \cdot (1, y) = (1, b),$$

so λ_2 must be odd. Because λ_1 and λ_2 are both odd, the sum $\lambda_1 + \lambda_2$ must be even. Therefore

$$\lambda_1 \cdot (1, x) + \lambda_2 \cdot (1, y) = (0, b),$$

and we define $g(0, b) = f(1, b)$ when b is odd.

We now prove that $g(1, b) = f(0, b)$ for odd b. Let $(\lambda_1, \lambda_2) = f(0, b)$ for some odd b. By the definition of f

$$\lambda_1 \cdot (0, x) + \lambda_2 \cdot (1, y) = (0, b),$$

so λ_2 must be even. Because λ_1 is odd and λ_2 is even, the sum $\lambda_1 + \lambda_2$ must be odd. Therefore

$$\lambda_1 \cdot (1, x) + \lambda_2 \cdot (1, y) = (1, b),$$

and we define $g(1, b) = f(0, b)$ when b is odd.

We have now proved that the function $g : G \to \mathbb{Z}^2([0, s])$ defined by the formula

$$g(a, b) = \begin{cases} f(a, b), & b \text{ is even} \\ f(1, b), & b \text{ is odd, } a = 0 \\ f(0, b), & b \text{ is odd, } a = 1 \end{cases}$$

satisfies the desired properties, meaning that the set $A' = \{(1, x), (1, y)\}$ spans G. Because proposition 9 proved this impossible, we have shown that A cannot span G, and therefore no subset of two elements can span G. □

References

[1] Béla Bajnok. *Additive Combinatorics: A Menu of Research Problems.* CRC Press, 2018.

[2] Haesoo Park. "Finding a Pair that Spans $\mathbb{Z}_2 \times \mathbb{Z}_{2k}$". In: *Research Papers in Mathematics* 22 (2020). Ed. by Béla Bajnok.

Appendices

Appendix A

For all even $s \in [4, 20]$, we include a $k < \frac{s^2}{2}$ such that $\phi_{\pm}(\mathbb{Z}_2 \times \mathbb{Z}_{2k}) > 2$. Note that these k are not necessarily the only such k for the given s.

s	k
4	7
6	16
8	29
10	47
12	67
14	92
16	127
18	161
20	199