Results on $\phi_{\pm}(\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_1 k}, [0, s]) = 2$.

Kyle Beatty

August 10, 2023

1 Results

Definition 1. *$E(s)$ is the number of coefficient pairs in $\mathbb{Z}^2([0, s])$ whose sum is even*

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

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

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

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.

Lemma 2. *The functions $E(s)$ and $O(s)$ adhere to the following formulae*

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

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

Proposition 3. *Given any positive integer s, there is no $k > \left\lfloor \frac{s^2}{2} \right\rfloor$ such that $\phi_{\pm}(\mathbb{Z}_2 \times \mathbb{Z}_{2k}, [0, s]) = 2$.*

Lemma 4. *Let s be a positive integer, and let d, x, y be positive integers such that*

- *$s^2 - d^2$ is even*
- *x is odd*
- *$x + y = s$*
- *x and y are coprime*
- *$4xy = s^2 - d^2$*

and let $G = \mathbb{Z}_2 \times \mathbb{Z}_{s^2 - d^2}$. For any element $(a, b) \in G$, there exist $(\lambda_1, \lambda_2) \in \mathbb{Z}^2$ such that $\lambda_1 \cdot (0, x) + \lambda_2 \cdot (1, y) = (a, b)$ and either

- *$\lambda_1 \in [-2y + 1, 2y]$, $\lambda_2 \in [0, 2x - 1]$, and $|\lambda_1| + |\lambda_2| \leq s$; or*
- *$|\lambda_1| + |\lambda_2| \leq s - 1$.*

Therefore $\phi_{\pm}(G, [0, s]) = 2$.

Proposition 5. *Given positive integers s, k, let $G = \mathbb{Z}_2 \times \mathbb{Z}_{2k}$. Then if s is odd, the equation*

$$\phi_{\pm}(G, [0, s]) = 2$$

holds if and only if $k \in [1, \frac{s^2 - 1}{2}]$.

Proposition 6. *Given positive integers s, k, we let $G = \mathbb{Z}_2 \times \mathbb{Z}_{2k}$. Then the equation*

$$\phi_{\pm}(G, [0, s]) = 2$$

holds if $k \in [1, \frac{s^2-s}{2}]$.

Proposition 7. *Given a positive integer $s \equiv 0 \bmod 4$, take some even $k \in [\frac{s^2-s}{2}, \frac{s^2}{2}]$ and let $G = \mathbb{Z}_2 \times \mathbb{Z}_{2k}$. Then $\phi_{\pm}(G, [0, s]) = 2$.*

Proposition 8. *Given a positive integer $s \equiv 2 \bmod 4$, take some $k \in [\frac{s^2-s}{2}, \frac{s^2}{2}]$ such that $k \equiv 2 \bmod 4$ and let $G = \mathbb{Z}_2 \times \mathbb{Z}_{2k}$. Then $\phi_{\pm}(G, [0, s]) = 2$.*

Conjecture 9. *Given an even positive integer s, the only solutions k to the equation*

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

are those in the preceding propositions.

Proposition 10. *Given a positive integer s and a group $G = \mathbb{Z}_p \times \mathbb{Z}_{pk}$ for prime $p \geq 3$ such that $\phi_{\pm}(G, [0, s]) = 2$, there is some pair of the form $B = \{(1, x), (1, y)\} \subset G$ such that $[0, s]_{\pm}B = G$.*

Proposition 11. *Given a positive integer s and prime divisor p of $2s + 1$, let $x = \left\lfloor \frac{s}{p} \right\rfloor$, $y = \left\lceil \frac{s}{p} \right\rceil$, and $k = 2xy$. Then for the group $G = \mathbb{Z}_p \times \mathbb{Z}_{pk}$ and the subset $A = \{(1, x), (1, y)\} \subset G$, we have that $[0, s]_{\pm}A = G$. Therefore $\phi_{\pm}(G, [0, s]) = 2$.*

Conjecture 12. *The general conjecture on the maximal order of G for which $\phi_{\pm}(G, [0, s]) = 2$ is in Béla's notes.*

2 Proofs

Lemma 2. *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 Equation 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 Equation 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 Equation 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:

$$\begin{aligned} E(s) &= E(s-1) \\ E(s) &= (s-1)^2 + 2(s-1) + 1 \\ E(s) &= s^2. \end{aligned}$$

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

Proposition 3. *Given any positive integer s, there is no $k > \left\lfloor \frac{s^2}{2} \right\rfloor$ such that $\phi_{\pm}(\mathbb{Z}_2 \times \mathbb{Z}_{2k}, [0, s]) = 2$.*

Proof. Given a positive integer s, we let $G = \mathbb{Z}_2 \times \mathbb{Z}_{2k}$ for some $k > \left\lfloor \frac{s^2}{2} \right\rfloor$, noting that this implies $|G| > 2s^2$. Clearly a subset of the form $A = \{(0, x), (0, y)\} \subset G$ can not span G. We partition the subsets of size two into the following categories, and prove in turn that none of them can span G.

- $A = \{(0, x), (1, y)\}$ where x is even;
- $A = \{(0, x), (1, y)\}$ where x and y are odd;
- $A = \{(1, x), (1, y)\}$ for arbitrary x and y; and
- $A = \{(0, x), (1, y)\}$ where x is odd and y even.

Given any pair of the first form $A = \{(0, x), (1, y)\}$ with x even, note that $(0, 1) \notin [0, s]_{\pm}A$ — thus A does not span G.

Next, consider any pair of the second form, where x and y are both odd. For any coefficients $(\lambda_1, \lambda_2) \in \mathbb{Z}^2([0, s])$, let

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

and note that the parity of b is equal to that of $\lambda_1 + \lambda_2$. Therefore such a pair A will span no more than $E(s)$ elements of G with b even and $O(s)$ elements with b odd. Because $|G| > 2s^2$ there are more than s^2 elements of each parity, exceeding the upper bound represented by either $E(s)$ or $O(s)$, according to the parity of s. The argument for pairs of the third form $A = \{(1, x), (1, y)\}$ is the same, but with regard to the first component a of the spanned element instead of b.

We now suppose for contradiction that there is a pair of the fourth form $A = \{(0, x), (1, y)\}$ with x odd and y even such that $[0, s]_{\pm}A = G$. We will prove that the pair $B = \{(1, x), (1, y)\}$ also spans G, contradicting our above result. Because $[0, s]_{\pm}A = G$ there is a function $f : G \to \mathbb{Z}^2([0, s])$ such that, letting $(\lambda_1, \lambda_2) = f(a, b)$ for arbitrary $(a, b) \in G$, we have

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

We define an analogous function $g : G \to \mathbb{Z}^2([0, s])$ by the formula

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

We claim that with $(\lambda_1, \lambda_2) = g(a,b)$ for arbitrary $(a,b) \in G$, we have

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

We first consider $(a,b) \in G$ with b even, and let $(\lambda_1, \lambda_2) = g(a,b) = f(a,b)$. By the definition of f, we know that $\lambda_1 \cdot x + \lambda_2 \cdot y = b$. Because x is odd and y is even, this in turn implies that λ_1 is even. We therefore have

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

In the case where b is odd, we let $(\lambda_1, \lambda_2) = g(a,b) = f(a+1,b)$. By similar reasoning to the above, we know that λ_1 is odd, and therefore that

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

as was to be shown. We therefore have that $[0,s]_{\pm}B = G$, a contradiction, proving our final case. □

Lemma 4. *Let s be a positive integer, and let d, x, y be positive integers such that*

- *$s^2 - d^2$ is even*
- *x is odd*
- *$x + y = s$*
- *x and y are coprime*
- *$4xy = s^2 - d^2$*

and let $G = \mathbb{Z}_2 \times \mathbb{Z}_{s^2-d^2}$. For any element $(a,b) \in G$, there exist $(\lambda_1, \lambda_2) \in \mathbb{Z}^2$ such that $\lambda_1 \cdot (0,x) + \lambda_2 \cdot (1,y) = (a,b)$ and either

- *$\lambda_1 \in [-2y+1, 2y]$, $\lambda_2 \in [0, 2x-1]$, and $|\lambda_1| + |\lambda_2| \leq s$; or*
- *$|\lambda_1| + |\lambda_2| \leq s - 1$.*

Therefore $\phi_{\pm}(G, [0,s]) = 2$.

Proof. For an arbitrary element $(a,b) \in \mathbb{Z}_2 \times \mathbb{Z}_{s^2-d^2}$, we first show that there are coefficients $(\lambda_1, \lambda_2) \in \mathbb{Z}^2$ such that $\lambda_1 \cdot (0,x) + \lambda_2 \cdot (1,y) = (a,b)$.

The span of $(0,x)$ will form a subgroup $H \leq G$ of order $\frac{s^2-d^2}{x} = 4y$. This subgroup has $\frac{|G|}{4y} = 2x$ corresponding cosets. The element (a,b) that we wish to span must lie in one of these cosets, so we first show that each of the cosets can be reached by some multiple $\lambda_2 \cdot (1,y)$.

For each $\mu \in [0, 2x-1]$, the multiple $\mu \cdot (1,y)$ reaches a different coset of H, implying that this set of multiples reaches all $2x$ cosets of H: take two distinct $\mu_1, \mu_2 \in [0, 2x-1]$ and assume without loss of generality that $\mu_1 > \mu_2$. $\mu_1 \cdot (1,y)$ and $\mu_2 \cdot (1,y)$ belong to different cosets because $\mu_1 \cdot (1,y) - \mu_2 \cdot (1,y) = (\mu_1 - \mu_2) \cdot (1,y) \notin H$. To see this, let $\mu' = \mu_1 - \mu_2 \in [1, 2x-1]$ and suppose for contradiction that $\mu' \cdot (1,y) \in H$. This would imply that

$$\mu' \cdot (1,y) = c \cdot (0,x)$$

for some integer c. Because x and y are coprime, the only $\mu' \in [1, 2x-1]$ that could satisfy the above equation is x. But because x is odd, we know that

$$x \cdot (1,y) = (1,xy) \neq c \cdot (0,x)$$

for any c. We therefore conclude that $\mu \cdot (1, y)$ spans a different coset of H for each $\mu \in [0, 2x-1]$, and consequently that they span every coset.

We return to our element $(a, b) \in \mathbb{Z}_2 \times \mathbb{Z}_{s^2-d^2}$. It must lie in some coset of H, so by our findings above there must be some $\lambda_2 \in [0, 2x-1]$ such that $\lambda_2 \cdot (1, y)$ is in this same coset. Because each of these cosets is of size $4y$, there must be some $\lambda_1 \in [-2y+1, 2y]$ such that

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

There is no guarantee, however, that $(\lambda_1, \lambda_2) \in \mathbb{Z}^2([0, s])$. Based on the constraints above, we have only that

$$|\lambda_1| + |\lambda_2| \leq 2y + 2x - 1 = 2s - 1.$$

If $|\lambda_1| + |\lambda_2| \leq s$, then we have found coefficients in $\mathbb{Z}^2([0, s])$ that span (a, b) and are done, having proven the first case of our claim.

If, however, $|\lambda_1| + |\lambda_2| \in [s+1, 2s-1]$, we show that there exist $(\lambda_1', \lambda_2') \in \mathbb{Z}^2([0, s])$ that span the same element (a, b). We select these values as follows:

$$\lambda_1' = \begin{cases} \lambda_1 - 2y, & \lambda_1 \geq 0 \\ \lambda_1 + 2y, & \lambda_1 < 0 \end{cases} \qquad \lambda_2' = \lambda_2 - 2x.$$

This selection of variables implies that $|\lambda_1'| = 2y - |\lambda_1|$ and $|\lambda_2'| = 2x - |\lambda_2|$. Therefore

$$\begin{aligned} |\lambda_1'| + |\lambda_2'| &= 2y - |\lambda_1| + 2x - |\lambda_2| \\ |\lambda_1'| + |\lambda_2'| &= 2(x+y) - (|\lambda_1| + |\lambda_2|) \\ |\lambda_1'| + |\lambda_2'| &= 2s - (|\lambda_1| + |\lambda_2|). \end{aligned}$$

Because $|\lambda_1| + |\lambda_2| \in [s+1, 2s-1]$, this implies that

$$|\lambda_1'| + |\lambda_2'| \in [1, s-1],$$

Proving that (λ_1', λ_2') span the original element (a, b) will thus prove that the second case of our claim holds.

If $\lambda_1 \geq 0$, meaning $\lambda_1' = \lambda_1 - 2y$, then

$$\begin{aligned} \lambda_1' \cdot (0, x) + \lambda_2' \cdot (1, y) &= (\lambda_1 - 2y) \cdot (0, x) + (\lambda_2 - 2x) \cdot (1, y) \\ &= [\lambda_1 \cdot (0, x) + \lambda_2 \cdot (1, y)] - [2y \cdot (0, x) + 2x \cdot (1, y)] \\ &= (a, b) - (0, 4xy) \\ &= (a, b) - (0, s^2 - d^2) \\ &= (a, b) - (0, 0) \\ \lambda_1' \cdot (0, x) + \lambda_2' \cdot (1, y) &= (a, b). \end{aligned}$$

If $\lambda_1 < 0$, meaning $\lambda_1' = \lambda_1 + 2y$, then

$$\begin{aligned} \lambda_1' \cdot (0, x) + \lambda_2' \cdot (1, y) &= (\lambda_1 + 2y) \cdot (0, x) + (\lambda_2 - 2x) \cdot (1, y) \\ &= [\lambda_1 \cdot (0, x) + \lambda_2 \cdot (1, y)] - 2y \cdot (0, x) + 2x \cdot (1, y) \\ &= (a, b) - (0, 2xy) + (0, 2xy) \\ \lambda_1' \cdot (0, x) + \lambda_2' \cdot (1, y) &= (a, b). \end{aligned}$$

Since in either case, the new $(\lambda_1', \lambda_2') \in \mathbb{Z}^2([1, s-1])$ spans the same element (a, b), we have that our arbitrary element $(a, b) \in \mathbb{Z}_2 \times \mathbb{Z}_{s^2-d^2}$ is s-spanned by the elements $(0, x)$ and $(1, y)$, as was to be shown. □

Proposition 5. *Given positive integers s, k, let $G = \mathbb{Z}_2 \times \mathbb{Z}_{2k}$. Then if s is odd, the equation*

$$\phi_{\pm}(G, [0, s]) = 2$$

holds if and only if $k \in [1, \frac{s^2-1}{2}]$.

Proof. Park's Conjecture (proved previously) comprises the "only if" direction, so it suffices to prove the "if" direction. We let our claimed spanning pair be $A = \{(0, x), (1, y)\}$, where

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

We prove that A spans G for all such k by proving that it spans G for $k = \frac{s^2-1}{2}$, while paying attention to the subset it spans in the direct product with the entire set of integers $\mathbb{Z}_2 \times \mathbb{Z}$. Proving that A spans the subset $\mathbb{Z}_2 \times \{0, 1, \ldots, \frac{s^2-1}{2}\} \subset \mathbb{Z}_2 \times \mathbb{Z}$ will, by symmetry, prove our claim. We let $k = \frac{s^2-1}{2}$ for the following.

The group G and the numbers x, y, s satisfy the hypothesis of Proposition 4. We take an arbitrary $(a, b) \in G$ with $0 \leq b \leq k$ and the coefficients λ_1, λ_2 that span this element. We prove that the same coefficients λ_1, λ_2 will span (a, b) if we view it as an element of $\mathbb{Z}_2 \times \mathbb{Z}$.

Consider the first case, where $\lambda_1 \in [-2y + 1, 2y]$ and $\lambda_2 \in [0, 2x - 1]$. Because we have that

$$\frac{-s^2 + 1}{2} < (-2y + 1) \cdot x \leq \lambda_1 \cdot x + \lambda_2 \cdot y \leq 2y \cdot x + (2x - 1) \cdot y = 4xy - x < s^2 - 1,$$

the only other $(a, b') \in \mathbb{Z}_2 \times \mathbb{Z}$ with $b' \equiv b \bmod 2k$ that could be spanned by λ_1, λ_2 is $b' = b - 2k$, which by our assumption that $b \leq k$ yields $b' \leq -k$. Given the specific bounds on λ_1, λ_2, our above inequality shows that $b' \leq -k$ cannot be spanned, and therefore the coefficients span $(a, b) \in \mathbb{Z}_2 \times \mathbb{Z}$.

In the second case, where $|\lambda_1| + |\lambda_2| \leq s - 1$, we have that $\lambda_1 \cdot x + \lambda_2 \cdot y \geq -\frac{(s-1)(s+1)}{2} = -k$. In the case where the coefficients span $(a, -k)$, then $-\lambda_1, -\lambda_2$ will span (a, k) by symmetry. Therefore the only element $(a, b') \in \mathbb{Z}_2 \times \mathbb{Z}$ spanned such that $b' \equiv b \bmod 2k$ is $(a, b) \in \mathbb{Z}_2 \times \mathbb{Z}$ itself.

In both cases, the element $(a, b) \in G$ is spanned as an element of $\mathbb{Z}_2 \times \mathbb{Z}$. The negatives of the coefficients λ_1, λ_2 will span those elements $(a, b) \in G$ such that $k + 1 \leq b \leq 2k - 1$. We therefore have that for every $k \in [1, \frac{s^2-1}{2}]$, the equation

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

holds. □

Proposition 6. *Given positive integers s, k, we let $G = \mathbb{Z}_2 \times \mathbb{Z}_{2k}$. Then the equation*

$$\phi_{\pm}(G, [0, s]) = 2$$

holds if $k \in [1, \frac{s^2-s}{2}]$.

Proof. We already have a stronger result above when s is odd, so we confine ourselves to the case where s is even. Because $s - 1$ is odd, we can apply Proposition 5 to show that the pair $A = \{(0, x), (1, y)\}$ spans $\mathbb{Z}_2 \times \{0, 1, \ldots, \frac{s^2-2s}{2}\} \subset \mathbb{Z}_2 \times \mathbb{Z}$ where

$$x = \begin{cases} \frac{s}{2}, & s \equiv 2 \bmod 4 \\ \frac{s-2}{2}, & s \equiv 0 \bmod 4 \end{cases} \qquad y = \begin{cases} \frac{s-2}{2}, & s \equiv 2 \bmod 4 \\ \frac{s}{2}, & s \equiv 0 \bmod 4. \end{cases}$$

Now take any $(a, b) \in \mathbb{Z}_2 \times \mathbb{Z}$ with $b \in \left[\frac{s^2-2s}{2} + 1, \frac{s^2-s}{2}\right]$. If $s \equiv 2 \bmod 4$, let λ_1, λ_2 be the coefficients such that

$$\lambda_1 \cdot (0, x) + \lambda_2 \cdot (1, y) = (a, b - \frac{s}{2}) \quad \text{and} \quad |\lambda_1| + |\lambda_2| \leq s - 1,$$

which exist by the above theorem. Then the coefficients $\lambda_1 + 1, \lambda_2$ are such that

$$(\lambda_1 + 1) \cdot (0, x) + \lambda_2 \cdot (1, y) = (a, b) \quad \text{and} \quad |\lambda_1 + 1| + |\lambda_2| \leq s.$$

If $s \equiv 0 \bmod 4$, then let λ_1, λ_2 be the coefficients such that

$$\lambda_1 \cdot (0, x) + \lambda_2 \cdot (1, y) = (a - 1, b - \frac{s}{2}) \quad \text{and} \quad |\lambda_1| + |\lambda_2| \leq s - 1,$$

which exist by the above theorem. Then the coefficients $\lambda_1, \lambda_2 + 1$ are such that

$$\lambda_1 \cdot (0, x) + (\lambda_2 + 1) \cdot (1, y) = (a, b) \quad \text{and} \quad |\lambda_1| + |\lambda_2 + 1| \leq s.$$

We have shown that the pair A spans the subset $\mathbb{Z}_2 \times \{0, 1, \ldots, \frac{s^2-s}{2}\}$, proving our claim. □

Proposition 7. *Given a positive integer $s \equiv 0 \bmod 4$, take some even $k \in [\frac{s^2-s}{2}, \frac{s^2}{2}]$ and let $G = \mathbb{Z}_2 \times \mathbb{Z}_{2k}$. Then $\phi_{\pm}(G, [0, s]) = 2$.*

Proof. We prove the proposition by proving it for $G = \mathbb{Z}_2 \times \mathbb{Z}_{s^2-4}$, paying attention to the elements spanned in the corresponding group $\mathbb{Z}_2 \times \mathbb{Z}$.

Let $x = \frac{s-2}{2}$, $y = \frac{s+2}{2}$, and $d = 2$. These values satisfy the hypotheses of Proposition 4 (x and y are coprime because they are odd and differ by 2) so we apply it to yield the given results on the coefficients $(\lambda_1, \lambda_2) \in \mathbb{Z}^2([0, s])$ spanning each element. Take some $(a, b) \in G$ and let $(\lambda_1, \lambda_2) \in \mathbb{Z}^2([0, s])$ be the coefficients that span it. In the first case specified by the theorem, we have that

$$\lambda_1 \cdot x + \lambda_2 \cdot y \geq -s \cdot \frac{s-2}{2} \geq \frac{-s^2 + 2s}{2} \equiv \frac{s^2 + 2s - 8}{2} \bmod s^2 - 4.$$

In the second case, where $|\lambda_1| + |\lambda_2| \leq s - 1$, we have that

$$\lambda_1 \cdot x + \lambda_2 \cdot y \geq -(s-1) \cdot \frac{s+2}{2} \geq \frac{-s^2 - s + 2}{2} \equiv \frac{s^2 - s - 6}{2} \bmod s^2 - 4.$$

By the two inequalities above, we conclude that for any $(a, b) \in G$ with $b < \frac{s^2-s-6}{2}$ and spanning coefficients λ_1, λ_2 the equality

$$\lambda_1 \cdot x + \lambda_2 \cdot y = b$$

holds in the regular sense, not only $\bmod s^2 - 4$.

Now, let $k = \frac{s^2}{2}$ and let $H = \mathbb{Z}_2 \times \mathbb{Z}_{2k} = \mathbb{Z}_2 \times \mathbb{Z}_{s^2}$. We now prove that the elements $\mathbb{Z}_2 \times \{\frac{s^2-s-6}{2}, \ldots, \frac{s^2}{2}\} \subset H$ are also spanned by the pair $A = \{(0, x), (1, y)\}$, paying attention to the corresponding elements of $\mathbb{Z}_2 \times \mathbb{Z}$ that are spanned. We do this by dividing the remaining elements into four sequences.

We first address the sequence $(i, \frac{s^2-s-6}{2} + 2i)$ for $i \in \{0, 1, \ldots, \frac{s+4}{4}\}$. These elements are spanned by the coefficients $\lambda_1 = \frac{s+2}{2} - i$, $\lambda_2 = \frac{s-4}{2} + i$, and are also spanned in $\mathbb{Z}_2 \times \mathbb{Z}$ by the same coefficients.

Our second sequence is $(1 + i, \frac{s^2-s-6}{2} + 2i)$ for $i \in \{0, 1, \ldots, \frac{s+4}{4}\}$. These elements are spanned by the coefficient pairs $(\lambda_1, \lambda_2) = \{(0, s-3), (-1, s-2), (-i, -s+1+i)\}$ for $i \in \{0, 1, \ldots, \frac{s-4}{4}\}\}$.

Our third sequence is $(i, \frac{s^2}{2} - 2i)$ for $i \in \{0, 1, \frac{s+4}{4}\}$, which are respectively spanned by the coefficients $(\frac{s}{2} + i, \frac{s}{2} - i) \in \mathbb{Z}^2([0, s])$.

Our fourth sequence is $(1 + i, \frac{s^2}{2} - 2i)$ for $i \in \{0, 1, \ldots, \frac{s+4}{4}\}$, which are respectively spanned by the coefficients $(-1 + i, s - 1 - i) \in \mathbb{Z}^2([0, s])$.

While the rest of the coefficients span their respective elements in $\mathbb{Z}_2 \times \mathbb{Z}$ as well, for the coefficients $(-i, -s + 1 + i)$ for $i \in \{0, 1, \ldots, \frac{s+4}{4}\}$ we have

$$-i \cdot x + (-s + 1 + i) \cdot y = \frac{-s^2 - s + 2}{2} + 2i$$

which is equivalent $\bmod s^2$ to $\frac{s^2-s+2}{2} + 2i$, but is not equal to it in the integer sense. Because this is the only sequence for which this is the case, and successive elements of the same parity (first component) differ by 4, this implies that these elements are spanned in every group $\mathbb{Z}_2 \times \mathbb{Z}_{s^2-4i}$ for $i = 0, 1, \ldots, \frac{s}{4}$. This proves our claim. □

Proposition 8. *Given a positive integer $s \equiv 2 \bmod 4$, take some $k \in [\frac{s^2-s}{2}, \frac{s^2}{2}]$ such that $k \equiv 2 \bmod 4$ and let $G = \mathbb{Z}_2 \times \mathbb{Z}_{2k}$. Then $\phi_{\pm}(G, [0, s]) = 2$.*

Proof. We prove the proposition by proving it for $G = \mathbb{Z}_2 \times \mathbb{Z}_{s^2-16}$, paying attention to the elements spanned in the corresponding group $\mathbb{Z}_2 \times \mathbb{Z}$.

Let $x = \frac{s-4}{2}$, $y = \frac{s+4}{2}$, and $d = 4$. These values satisfy the hypotheses of Proposition 4 (x and y are coprime because they are 2 mod 4 and differ by 4) so we apply it to yield the given results on the coefficients $(\lambda_1, \lambda_2) \in \mathbb{Z}^2([0, s])$ spanning each element. Take some $(a, b) \in G$ and let $(\lambda_1, \lambda_2) \in \mathbb{Z}^2([0, s])$ be the coefficients that span it. In the first case specified by the theorem, we have that

$$\lambda_1 \cdot x + \lambda_2 \cdot y \geq -s \cdot \frac{s-4}{2} \geq \frac{-s^2+4s}{2} \equiv \frac{s^2+4s-32}{2} \bmod s^2 - 16.$$

In the second case, where $|\lambda_1| + |\lambda_2| \leq s - 1$, we have that

$$\lambda_1 \cdot x + \lambda_2 \cdot y \geq -(s-1) \cdot \frac{s+4}{2} \geq \frac{-s^2-3s+4}{2} \equiv \frac{s^2-3s-28}{2} \bmod s^2 - 16.$$

By the two inequalities above, we conclude that for any $(a, b) \in G$ with $b < \frac{s^2-3s-28}{2}$ and spanning coefficients λ_1, λ_2 the equality

$$\lambda_1 \cdot x + \lambda_2 \cdot y = b$$

holds in the regular sense, not only $\bmod s^2 - 16$.

Now, let $k = \frac{s^2}{2}$ and let $H = \mathbb{Z}_2 \times \mathbb{Z}_{2k} = \mathbb{Z}_2 \times \mathbb{Z}_{s^2}$. We now prove that the elements $\mathbb{Z}_2 \times \{\frac{s^2-3s-28}{2}, \ldots, \frac{s^2}{2}\} \subset H$ are also spanned by the pair $A = \{(0, x), (1, y)\}$, paying attention to the corresponding elements of $\mathbb{Z}_2 \times \mathbb{Z}$ that are spanned. We do this by dividing the remaining elements into eight sequences.

start of sequence	(λ_1, λ_2)
$\left(0, \frac{s^2-3s-28}{2}\right)$	$(\frac{s+4}{2} - i, \frac{s-10}{2} + i), \quad 0 \leq i \leq \left\lfloor \frac{3s+28}{8} \right\rfloor$
$\left(1, \frac{s^2-3s-28}{2}\right)$	$(-i, s-7+i), \quad 0 \leq i \leq 3 \qquad (-i, -s+1+i), \quad 0 \leq i \leq \left\lfloor \frac{3s-4}{8} \right\rfloor$
$\left(0, \frac{s^2}{2}\right)$	$(-2+i, s-2-i), \quad 0 \leq i \leq \left\lfloor \frac{3s+28}{8} \right\rfloor$
$\left(1, \frac{s^2}{2}\right)$	$\left(\frac{s}{2} + i, \frac{s}{2} - i\right), \quad 0 \leq i \leq \frac{s}{2} \qquad \left(-3+i, s-5-i\right), \quad 0 \leq i \leq \left\lfloor \frac{-s+20}{8} \right\rfloor$
$\left(0, \frac{s^2-s-4}{2}\right)$	$\left(\frac{s}{2} - i, \frac{s-2}{2} + i\right), \quad -\left\lfloor \frac{s+28}{8} \right\rfloor \leq i \leq \frac{s-2}{4}$
$\left(1, \frac{s^2-2s}{2}\right)$	$\left(\frac{s-2}{2} - i, \frac{s-2}{2} + i\right), \quad \frac{-s+2}{4} \leq i \leq \frac{s-2}{4}$
$\left(0, \frac{s^2-s-4}{2}\right)$	$\left(-2+i, s-3-i\right),\ 0 \leq i \leq \left\lfloor \frac{s+12}{4} \right\rfloor \quad \left(1-i, -s+2+i\right),\ 0 \leq i \leq \left\lfloor \frac{s-4}{8} \right\rfloor$
$\left(1, \frac{s^2-2s+8}{2}\right)$	$\left(-i, -s+2+i\right), 0 \leq i \leq \left\lfloor \frac{s-4}{4} \right\rfloor \quad \left(-2+i, s-4-i\right), 0 \leq i \leq \left\lfloor \frac{s+28}{8} \right\rfloor$

A lot of algebra will show that these coefficients (λ_1, λ_2) will span all remaining elements in the group. In the second, seventh, and eighth sequence there are elements that are spanned $\bmod s^2$ in G but not spanned in $\mathbb{Z}_2 \times \mathbb{Z}$. For each of these negatively spanned elements (a, b), the element $(a, b + 8)$ will also be negatively spanned in the same sequence. Thus, reducing k by 4 will leave the same element still spanned. Our claim follows. □

Proposition 10. *Given a positive integer s and a group $G = \mathbb{Z}_p \times \mathbb{Z}_{pk}$ for prime $p \geq 3$ such that $\phi_\pm(G, [0, s]) = 2$, there is some pair of the form $B = \{(1, x), (1, y)\} \subset G$ such that $[0, s]_\pm B = G$.*

Proof. Given our assumption that $\phi_\pm(G, [0, s]) = 2$, there is some pair $A = \{(a, x), (b, y)\} \subset G$ such that $[0, s]_\pm A = G$. Define the function $f_A : \mathbb{Z}^2([0, s]) \to G$ by the formula

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

Then our statement that $[0,s]_{\pm}A = G$ is equivalent to the statement that f_A is surjective. We may therefore choose some subset $T \subset \mathbb{Z}^2([0,s])$ with $|T| = |G|$ such that the restriction of f_A to the domain T, which we call $g_A : T \to G$, is bijective.

We now divide the problem into two cases depending on A.

Case I

If $a = b$, i.e. $A = \{(a,x),(a,y)\}$ for some $a \in \mathbb{Z}_p$, then the pair $B = \{(1,x),(1,y)\}$ also s-spans G. To prove this, we show that the bijectivity of $g_A : T \to G$ implies the injectivity and — because $|T| = |G|$ — the bijectivity of $g_B : T \to G$ defined analogously as

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

We suppose for contradiction that g_B is not injective, and that there exist therefore some distinct $(\lambda_1,\lambda_2),(\mu_1,\mu_2) \in T$ such that $g_B(\lambda_1,\lambda_2) = g_B(\mu_1,\mu_2)$. By assumption, $g_A(\lambda_1,\lambda_2) \neq g_A(\mu_1,\mu_2)$.

All arithmetic to follow is conducted mod$p$. By our equality in g_B, we have that

1. $\lambda_1 + \lambda_2 = \mu_1 + \mu_2$
2. $\lambda_1 \cdot x + \lambda_2 \cdot y = \mu_1 \cdot x + \mu_2 \cdot y$.

The inequality in g_A together with equality (2) implies further that

3. $\lambda_1 \cdot a + \lambda_2 \cdot a \neq \mu_1 \cdot a + \mu_2 \cdot a$.

But multiplying equation (2) by a clearly contradicts (3), so g_B must be injective.

Case II

If $a \neq b$, we assume without loss of generality that (continuing our arithmetic mod p) $x \neq y$. This is because the set $A = \{(a,x),(b,y)\}$ is an s-spanning set for G, which clearly implies that $\{(a,x),(-b,-y)\}$ is as well. Because $p \geq 3$, we have that $y \neq -y$, and we can choose whichever one is not equal to x.

As above, we define for the spanning pair $B = \{(1,x),(1,y)\}$ a spanning function $g_B : T \to G$ by the formula

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

We suppose for contradiction that g_B is not injective, and that there exist therefore some distinct $(\lambda_1,\lambda_2),(\mu_1,\mu_2) \in T$ such that $g_B(\lambda_1,\lambda_2) = g_B(\mu_1,\mu_2)$. By assumption, $g_A(\lambda_1,\lambda_2) \neq g_A(\mu_1,\mu_2)$.

By our equality in g_B, we have that

1. $\lambda_1 + \lambda_2 = \mu_1 + \mu_2$
2. $\lambda_1 \cdot x + \lambda_2 \cdot y = \mu_1 \cdot x + \mu_2 \cdot y$.

The inequality in g_A together with equality (2) implies further that

3. $\lambda_1 \cdot a + \lambda_2 \cdot b \neq \mu_1 \cdot a + \mu_2 \cdot b$.

Letting $c = a - b \neq 0$, (3) yields

$$(\lambda_1 + \lambda_2) \cdot b + \lambda_1 \cdot c \neq (\mu_1 + \mu_2) \cdot b + \mu_1 \cdot c,$$

which implies by (1) that $\lambda_1 \cdot c \neq \mu_1 \cdot c$, and therefore $\lambda_1 \neq \mu_1$.

However, letting $z = x - y \neq 0$ yields by (1) and (2) that

$$\begin{aligned}(\lambda_1 + \lambda_2) \cdot y + \lambda_1 \cdot z &= (\mu_1 + \mu_2) \cdot y + \mu_1 \cdot z \\ \lambda_1 \cdot z &= \mu_1 \cdot z \\ \lambda_1 &= \mu_1,\end{aligned}$$

contradicting our result above that $\lambda_1 \neq \mu_1$; consequently g_B is injective and therefore bijective. $\square$

Proposition 11. *Given a positive integer s and prime divisor p of $2s+1$, let $x = \left\lfloor \frac{s}{p} \right\rfloor$, $y = \left\lceil \frac{s}{p} \right\rceil$, and $k = 2xy$. Then for the group $G = \mathbb{Z}_p \times \mathbb{Z}_{pk}$ and the subset $A = \{(1,x),(1,y)\} \subset G$, we have that $[0,s]_{\pm}A = G$. Therefore $\phi_{\pm}(G,[0,s]) = 2$.*

Proof. First observe that by our definitions above we have that $|\langle(1,x)\rangle| = 2py$. There are therefore $\frac{|G|}{2py} = px$ cosets of the span of $(1,x)$. We prove by contradiction that for each coefficient $\lambda_2 \in [0, px-1]$, the product $\lambda_2 \cdot (1,y)$ is contained in a different coset.

Suppose for contradiction that there exist some μ_1, μ_2 with $0 \leq \mu_1 < \mu_2 \leq px-1$ such that $\mu_1 \cdot (1,y)$ and $\mu_2 \cdot (1,y)$ are in the same coset. Letting $\mu = \mu_2 - \mu_1 \in [1, px-1]$, this would imply that $\mu \cdot (1,y) \in \langle(1,x)\rangle$. We show that there is no $a \in \mathbb{Z}$ such that $a \cdot (1,x) = \mu \cdot (1,y)$, proving that $\mu \cdot (1,y)$ is not in the span of $(1,x)$.

Suppose that such an $a \in \mathbb{Z}$ did exist; it would then satisfy the following two properties

1. $a \equiv \mu \bmod p$
2. $ax \equiv \mu y \bmod pk$

Noting that $y = x+1$, the second equation implies that

$$\begin{aligned} \mu(x+1) &\equiv ax \bmod 2pxy \\ \mu &\equiv (a-\mu)\cdot x \bmod 2pxy \end{aligned}$$

which, because $a \equiv \mu \bmod p$, implies that μ is a multiple of px. This violates the assumption that $\mu \in [1, px-1]$, as there are no multiples of px in this range. Therefore for any distinct $\mu_1, \mu_2 \in [0, px-1]$, the elements $\mu_1 \cdot (1,y)$ and $\mu_2 \cdot (1,y)$ are in different cosets of $\langle(1,x)\rangle$, as we wished to show.

For any element $g \in G$, there then exists some $\lambda_2 \in [0, px-1]$ such that $\lambda_2 \cdot (1,y)$ and g are in the same coset of $\langle(1,x)\rangle$. Recalling that $|\langle(1,x)\rangle| = 2py$, there is then some $\lambda_1 \in [-py+1, py]$ such that $\lambda_1 \cdot (1,x) + \lambda_2 \cdot (1,y) = g$. We then have that

$$|\lambda_1| + |\lambda_2| \leq py + px - 1 = p(x+y) - 1 = 2s - 1.$$

If $|\lambda_1| + |\lambda_2| \leq s$, then we have found coefficients that span the element g and are done. If, however, we have that $|\lambda_1| + |\lambda_2| \in [s+1, 2s-1]$, we define new coefficients λ_1', λ_2' that also span g while staying within the desired bounds.

Let

$$\lambda_1' = \begin{cases} \lambda_1 - py, & \lambda_1 \geq 0 \\ \lambda_1 + py, & \lambda_1 < 0 \end{cases} \qquad \lambda_2' = \lambda_2 - px.$$

Both $\lambda_1' \equiv \lambda_1 \bmod p$ and $\lambda_2' \equiv \lambda_2 \bmod p$, so the first component of the element spanned remains unchanged. We now check the second component, first in the case where $\lambda_1 \geq 0$

$$\begin{aligned} \lambda_1' x + \lambda_2' y &= (\lambda_1 - py)\cdot x + (\lambda_2 - px)\cdot y \\ &= \lambda_1 x + \lambda_2 y - 2pxy \\ &= \lambda_1 x + \lambda_2 y - pk \\ \lambda_1' x + \lambda_2' y &\equiv \lambda_1 x + \lambda_2 y \bmod pk. \end{aligned}$$

Therefore λ_1', λ_2' span the same element. In the case where $\lambda_1 < 0$, we have that

$$\begin{aligned} \lambda_1' x + \lambda_2' y &= (\lambda_1 + py)\cdot x + (\lambda_2 - px)\cdot y \\ &= \lambda_1 x + \lambda_2 y + pxy - pxy \\ &= \lambda_1 x + \lambda_2 y \\ \lambda_1' x + \lambda_2' y &\equiv \lambda_1 x + \lambda_2 y \bmod pk. \end{aligned}$$

Again, λ_1', λ_2' span the same element $g \in G$ as the previous coefficients λ_1, λ_2.

Finally, we check that $|\lambda_1'|+|\lambda_2'| \leq s$, proving that the element g is spanned by the elements $(1,x),(1,y)$.

$$\begin{aligned}
|\lambda_1'| + |\lambda_2'| &= py - |\lambda_1| + px - |\lambda_2| \\
|\lambda_1'| + |\lambda_2'| &= py + px - (|\lambda_1| + |\lambda_2|) \\
|\lambda_1'| + |\lambda_2'| &= 2s + 1 - (|\lambda_1| + |\lambda_2|) \\
|\lambda_1'| + |\lambda_2'| &\leq s,
\end{aligned}$$

which proves our claim. □

References

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