Additive triples in groups of odd prime order

Sophie Huczynska Jonathan Jedwab Laura Johnson

7 May 2024

Abstract

Let p be an odd prime. For nontrivial proper subsets A, B of $\mathbb{Z}_p$ of cardinality s, t, respectively, we count the number $r(A, B, B)$ of *additive triples*, namely elements of the form $(a, b, a + b)$ in $A \times B \times B$. For given s, t, what is the spectrum of possible values for $r(A, B, B)$? In the special case $A = B$, the additive triple is called a *Schur triple*. Various authors have given bounds on the number $r(A, A, A)$ of Schur triples, and shown that the lower and upper bound can each be attained by a set A that is an interval of s consecutive elements of $\mathbb{Z}_p$. However, there are values of p, s for which not every value between the lower and upper bounds is attainable. We consider here the general case where A, B can be distinct. We use Pollard's generalization of the Cauchy-Davenport Theorem to derive bounds on the number $r(A, B, B)$ of additive triples. In contrast to the case $A = B$, we show that every value of $r(A, B, B)$ from the lower bound to the upper bound is attainable: each such value can be attained when B is an interval of t consecutive elements of $\mathbb{Z}_p$.

1 Introduction

Let G be an additive group. A *Schur triple* in a subset A of G is a triple of the form $(a, b, a+b) \in A^3$; Schur triples were originally considered only in the case $G = \mathbb{Z}$ [13]. Let $r(A)$ be the number of Schur triples in A. Several authors have studied the behaviour of $r(A)$ as A ranges over some or all subsets of a group G, and the nature of the subsets A attaining a particular value of $r(A)$.

A *sum-free set* A is one for which $r(A) = 0$, and has received much attention. The Cameron-Erdős Conjecture [2] concerns the number of sum-free sets in $\{1, 2, \dots, n\} \subset \mathbb{Z}$; this was resolved independently by Green [7] and Sapozhenko [14]. Lev and Schoen [10] studied the number of sum-free sets when G is a group of prime order. Erdős [6] asked what is the largest size of a sum-free set in an abelian group; this question was considered by Green and Ruzsa [8].

A popular problem is to determine the minimum and maximum value of $r(A)$ over all subsets A of fixed cardinality in a specified group G. The case $G = \mathbb{Z}_p$ for a prime p is of particular interest, in part because of its relation to sumset results such as the Cauchy-Davenport Theorem [3, 5]. We use the set notation $a + B := \{a + b : b \in B\}$ and $A + B := \{a + B : a \in A\}$.

Theorem 1.1 (Cauchy-Davenport Theorem [3, 5]). *Let p be prime and let A, B be non-empty subsets of $\mathbb{Z}_p$. Then $|A + B| \geq \min(p, |A| + |B| - 1)$.*

S. Huczynska and L. Johnson are with School of Mathematics and Statistics, University of St Andrews, Mathematical Institute, North Haugh, St Andrews KY16 9SS, Scotland. Email: `sh70@st-andrews.ac.uk`, `lj68@st-andrews.ac.uk`

J. Jedwab is with Department of Mathematics, Simon Fraser University, 8888 University Drive, Burnaby BC V5A 1S6, Canada. Email: `jed@sfu.ca`

S. Huczynska was funded by EPSRC grant EP/X021157/1. J. Jedwab is supported by NSERC.

The special case $A = B$ of Theorem 1.1 counts the number of distinct values that the sum $a + b$ can take as a, b range over A, without taking account of how many times the sum is attained nor whether it lies in the subset A.

The following generalization of the Cauchy-Davenport Theorem provides more infomation which is relevant to counting occurrences of each sum. The special case $j = 1$ reduces to the Cauchy-Davenport Theorem.

Theorem 1.2 (Pollard [11]). *Let p be prime and let A, B be subsets of $\mathbb{Z}_p$ of cardinality s, t, respectively. For $i \geq 1$, let S_i be the set of elements of $\mathbb{Z}_p$ expressible in at least i ways in the form $a + b$ for $a \in A$ and $b \in B$. Then*

$$\sum_{i=1}^{j} |S_i| \geq j \min(p,\, s + t - j) \quad \textit{for } 1 \leq j \leq \min(s, t).$$

Theorem 1.2 was a crucial tool in the proof of [9, Theorem 3.6], which used linear programming to determine the minimum and maximum value of $r(A)$ when A is a subset of fixed cardinality in $\mathbb{Z}_p$. The following theorem summarizes results from [9].

Theorem 1.3 (Huczynska, Mullen, Yucas [9]). *Let p be an odd prime and let $1 \leq s \leq p - 1$. Let*

$$f_s = \begin{cases} 0 & \textit{for } s \leq \frac{p+1}{3}, \\ \left\lfloor \frac{(3s-p)^2}{4} \right\rfloor & \textit{for } \frac{p+2}{3} \leq s, \end{cases}$$

$$g_s = \begin{cases} \left\lceil \frac{3s^2}{4} \right\rceil & \textit{for } s \leq \frac{2p+1}{3}, \\ s(2s - p) + (p - s)^2 & \textit{for } \frac{2p+2}{3} \leq s. \end{cases}$$

Then

(i) As A ranges over all subsets of $\mathbb{Z}_p$ of cardinality s, we have

$$f_s \leq r(A) \leq g_s.$$

(ii) The values f_s and g_s for $r(A)$ can each be attained by a set A that is an interval of s consecutive elements of $\mathbb{Z}_p$.

(iii) For certain p and s, there is at least one value in the interval $(f_s,\, g_s)$ which is not attainable as $r(A)$ for a subset A of $\mathbb{Z}_p$ of cardinality s.

The actual spectrum of possible values of $r(A)$ in the setting of Theorem 1.3 was conjectured but not resolved in [9]. For $p > 11$, not all attainable values of $r(A)$ (found by computer search) were explained by constructions in [9].

Samotij and Sudakov [12] obtained similar results to Theorem 1.3 for various abelian groups, including elementary abelian groups and $\mathbb{Z}_p$, using a different proof to that of [9]. They also showed that a subset of the group $\mathbb{Z}_p$ achieving the minimum value f_s (when this is nonzero) must be an arithmetic progression. Bajnok [1] proposed to generalize from counting Schur triples to counting $(s + 1)$-tuples, and suggested the case $G = \mathbb{Z}_p$ as a first step. This case was addressed by Chervak, Pikhurko and Staden [4], who showed that extremal configurations exist with all sets consisting of intervals.

In this paper we consider a different generalization of Schur triples. Let A, B be subsets of a group G of cardinality s, t, respectively, and let $r(A, B, B)$ be the number of *additive triples* in G, namely elements of the form $(a, b, a+b) \in A \times B \times B$. (Note that $r(A, A, A)$ is identical to $r(A)$ as used above.) For given s, t, what is the spectrum of possible values of $r(A, B, B)$? This generalization of Schur triples is not only natural, it is also closer to the setting of the Cauchy-Davenport Theorem than is the special case $A = B$. We shall always take $G = \mathbb{Z}_p$, where p is an odd prime.

Our main result is Theorem 1.4, which determines the smallest and largest value of $r(A, B, B)$ as a function of s, t, and shows that (in contrast to the special case $A = B$) every intermediate value can be attained by $r(A, B, B)$.

Theorem 1.4 (Main Theorem). *Let p be an odd prime and let $1 \leq s, t \leq p-1$. Let*

$$f(s,t) = \begin{cases} 0 & \textit{for } 2t \leq p - s + 1, \\ \left\lfloor \frac{(s+2t-p)^2}{4} \right\rfloor & \textit{for } p - s + 2 \leq 2t \leq p + s - 2, \\ s(2t - p) & \textit{for } p + s - 1 \leq 2t, \end{cases} \tag{1}$$

$$g(s,t) = \begin{cases} t^2 & \textit{for } 2t \leq s, \\ \left\lceil \frac{s(4t-s)}{4} \right\rceil & \textit{for } s + 1 \leq 2t \leq 2p - s - 1, \\ s(2t - p) + (p-t)^2 & \textit{for } 2p - s \leq 2t. \end{cases} \tag{2}$$

The set of values taken by $r(A, B, B)$ as A, B range over all subsets of $\mathbb{Z}_p$ of cardinality s, t, respectively, is the closed integer interval $[f(s,t),\, g(s,t)]$.

In Section 3 we shall show (for an odd prime p) that $f(s,t) \leq r(A, B, B) \leq g(s,t)$ for all subsets A, B of $\mathbb{Z}_p$ of cardinality s, t, respectively. In Section 4 we shall show (for an odd although not necessarily prime p) that for each integer $r \in [f(s,t),\, g(s,t)]$ and for $B = \{0, 1, \dots, t-1\}$, there is a subset A of $\mathbb{Z}_p$ of cardinality s for which $r(A, B, B) = r$. Combining these results proves Theorem 1.4.

It is interesting to note that, while the relaxation from Schur triples to additive triples yields a spectrum of values of $r(A, B, B)$ which no longer has any "missing values" between the minimum and maximum, the actual values of the minimum and maximum for $r(A, B, B)$ with $|A| = |B| = s$ are precisely the same as the minimum and maximum of $r(A, A, A)$ with $|A| = s$. Indeed, we see from (1) that

$$\begin{aligned} f(s,s) &= \begin{cases} 0 & \text{for } s \leq \frac{p+1}{3}, \\ \left\lfloor \frac{(3s-p)^2}{4} \right\rfloor & \text{for } \frac{p+2}{3} \leq s \leq p-2, \\ s(2s-p) & \text{for } s = p-1 \end{cases} \\ &= f_s \end{aligned}$$

by combining the domain $s = p-1$ with the domain $\frac{p+2}{3} \leq s \leq p-2$. We also see from (2) that

$$\begin{aligned} g(s,s) &= \begin{cases} \left\lceil \frac{3s^2}{4} \right\rceil & \text{for } s \leq \frac{2p-1}{3}, \\ s(2s-p) + (p-s)^2 & \text{for } \frac{2p}{3} \leq s \end{cases} \\ &= g_s \end{aligned}$$

by transferring the cases where $s = \frac{2p}{3}$ or $s = \frac{2p+1}{3}$ is an integer from the domain $\frac{2p}{3} \leq s$ to the domain $s \leq \frac{2p-1}{3}$.

2 Preliminary results

In this section we obtain some preliminary results for additive triples in a group G (not necessarily $\mathbb{Z}_p$). We firstly derive two expressions for $r(A, B, B)$.

Proposition 2.1. *Let G be a group and let A, B be subsets of G.*

(i) *We have*

$$r(A, B, B) = \sum_{a \in A} \big|(a + B) \cap B\big|.$$

(ii) *For each $i \geq 1$, let S_i be the set of elements of G expressible in at least i ways in the form $a + b$ for $a \in A$ and $b \in B$. Then*

$$r(A, B, B) = \sum_{i \geq 1} |S_i \cap B|.$$

Proof.

(i) By definition,

$$\begin{aligned} r(A, B, B) &= \big|\{(a, b, a + b) : a \in A,\ b \in B,\ a + b \in B\}\big| \\ &= \sum_{a \in A} \big|\{b : b \in B,\ a + b \in B\}\big| \\ &= \sum_{a \in A} \big|(a + B) \cap B\big|. \end{aligned}$$

(ii) Fix $c \in B$ and consider the set $X(c)$ of triples of the form $(a, b, a+b) \in A \times B \times B$ for which $a + b = c$. We prove the required equality by showing that the triples of $X(c)$ contribute equally to the left hand side and the right hand side. The contribution to the left hand side is $|X(c)|$. The contribution to $|S_i \cap B|$ is 1 for each i satisfying $1 \leq i \leq |X(c)|$ and is 0 for each $i > |X(c)|$, giving a total contribution to the right hand side of $|X(c)|$.

□

Write $\overline{A}$ for the complement of a subset A in a group G. We now give a relationship between $r(A, B, B)$ and $r(\overline{A}, \overline{B}, \overline{B})$.

Theorem 2.2. *Let A, B be subsets of a group G. Then*

$$r(A, B, B) + r(\overline{A}, \overline{B}, \overline{B}) = |A| \cdot |B| - |A| \cdot |\overline{B}| + |\overline{B}|^2.$$

Proof. We calculate

$$\begin{aligned} &r(A, B, B) + r(\overline{A}, \overline{B}, \overline{B}) \\ &\quad = \Big(r(A, B, B) + r(A, B, \overline{B})\Big) - \Big(r(A, B, \overline{B}) + r(A, \overline{B}, \overline{B})\Big) + \Big(r(A, \overline{B}, \overline{B}) + r(\overline{A}, \overline{B}, \overline{B})\Big) \\ &\quad = |A| \cdot |B| - |A| \cdot |\overline{B}| + |\overline{B}|^2 \end{aligned}$$

by definition of $r(A, B, B)$.

□

3 Establishing the lower and upper bounds

In this section we prove Theorem 3.1 below, which establishes a lower and upper bound on the value of $r(A,B,B)$ for all subsets A and B.

Theorem 3.1. *Let p be an odd prime, let $1 \le s,t \le p-1$, and let A,B be subsets of $\mathbb{Z}_p$ of cardinality s,t, respectively. Let $f(s,t)$ and $g(s,t)$ be the functions defined in* (1) *and* (2)*. Then $f(s,t) \le r(A,B,B) \le g(s,t)$.*

Proof. We make the following claim, which will be proved subsequently:

$$r(X,Y,Y) \ge f(|X|,|Y|) \quad \text{for all subsets } X,Y \text{ of } \mathbb{Z}_p. \tag{3}$$

Given this claim, by Theorem 2.2 we have

$$\begin{aligned} r(A,B,B) &= st - s(p-t) + (p-t)^2 - r(\overline{A},\overline{B},\overline{B}) \\ &\le st - s(p-t) + (p-t)^2 - f(p-s,p-t) \end{aligned} \tag{4}$$

using the case $(X,Y) = (\overline{A},\overline{B})$ of (3). By definition of f, we have

$$f(p-s,p-t) = \begin{cases} (p-s)(p-2t) & \text{for } 2t \le s+1, \\ \left\lfloor \frac{(2p-s-2t)^2}{4} \right\rfloor & \text{for } s+2 \le 2t \le 2p-s-2, \\ 0 & \text{for } 2p-s-1 \le 2t, \end{cases}$$

and we may adjust the three ranges for $2t$ to give the equivalent form

$$f(p-s,p-t) = \begin{cases} (p-s)(p-2t) & \text{for } 2t \le s, \\ \left\lfloor \frac{(2p-s-2t)^2}{4} \right\rfloor & \text{for } s+1 \le 2t \le 2p-s-1, \\ 0 & \text{for } 2p-s \le 2t. \end{cases}$$

Substitution in (4) and straightforward calculation then gives

$$r(A,B,B) \le g(s,t),$$

which combines with the case $(X,Y) = (A,B)$ of (3) to give the required result.

It remains to prove the claim (3) by showing that $r(A,B,B) \ge f(s,t)$. Our argument is inspired by that used in the proof of [12, Theorem 1.3]. For $i \ge 1$, let S_i be the set of elements of $\mathbb{Z}_p$ expressible in at least i ways in the form $a+b$ for $a \in A$ and $b \in B$. By Proposition 2.1(ii), for $j \ge 1$ we have

$$\begin{aligned} r(A,B,B) &\ge \sum_{i=1}^{j} |S_i \cap B| \\ &\ge \sum_{i=1}^{j} \big(|S_i| - |\overline{B}|\big) \end{aligned}$$

using the set inequality $|S_i \cap B| + |\overline{B}| \ge |S_i|$. Theorem 1.2 then gives

$$r(A,B,B) \ge j\ \min(p,\ s+t-j) - j(p-t) \quad \text{for } 1 \le j \le \min(s,t). \tag{5}$$

Case 1: $2t \le p-s+1$**.** In this range, $r(A,B,B) \ge 0$ trivially.

Case 2: $p - s + 2 \leq 2t \leq p + s - 2$**.** In this range, the value $j = \left\lceil \frac{s+2t-p}{2} \right\rceil$ satisfies $1 \leq j < \min(s,t)$ and $s + t - j < p$, so substitution in (5) gives

$$\begin{aligned} r(A,B,B) &\geq j(s+t-j) - j(p-t) \\ &= j(s+2t-p-j) \\ &= \left\lfloor \frac{(s+2t-p)^2}{4} \right\rfloor. \end{aligned}$$

Case 3: $p + s - 1 \leq 2t$**.** In this range, the value $j = s$ satisfies $1 \leq j \leq \min(s,t)$ and $s+t-j < p$, so substitution in (5) gives

$$\begin{aligned} r(A,B,B) &\geq j(s+t-j) - j(p-t) \\ &= s(2t-p). \end{aligned}$$

Combining results for Cases 1, 2, and 3 proves that $r(A,B,B) \geq f(s,t)$, as required. □

4 Achieving the spectrum constructively

In this section we constructively prove Theorem 4.1 below, which shows that each integer value r in the closed interval $[f(s,t),\, g(s,t)]$ is an attainable value of $r(A,B,B)$ for some choice of subsets A and B. The construction takes p to be odd but does not require p to be prime.

Theorem 4.1. *Let p be an odd integer, let $1 \leq s,t \leq p-1$, and let $B = \{0, 1, \ldots, t-1\}$. Let $f(s,t)$ and $g(s,t)$ be the functions defined in (1) and (2), and let $r \in [f(s,t),\, g(s,t)]$. Then there is a subset A of $\mathbb{Z}_p$ of cardinality s for which $r(A,B,B) = r$.*

We shall use a visual representation of a multiset involving balls and urns. For example, Figure 1(a) represents the multiset comprising $p - 2t + 1$ elements 0, two elements each of $1, 2, \ldots, t-1$, and one element t. We firstly use Proposition 2.1(i) to transform the condition $r(A,B,B) = r$ into an equivalent statement involving the multiset in Figure 1.

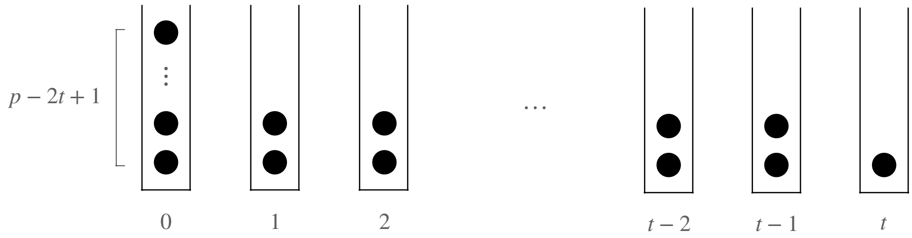
Lemma 4.2. *Let p be an odd integer, let s,t be integers satisfying $1 \leq s,t \leq p-1$, and let $B = \{0, 1, \ldots, t-1\}$. Then there is a subset A of $\mathbb{Z}_p$ of cardinality s for which $r(A,B,B) = r$ if and only if the multiset M represented in Figure 1 contains a multi-subset of cardinality s whose elements sum to r.*

Proof. Regard $\mathbb{Z}_p$ as having representatives $\big\{0, \pm 1, \pm 2, \ldots, \pm(\frac{p-1}{2})\big\}$, and let A be a subset of $\mathbb{Z}_p$. We make the following claim, which will be proved subsequently: for $a \in \{0, 1, \ldots, \frac{p-1}{2}\}$,

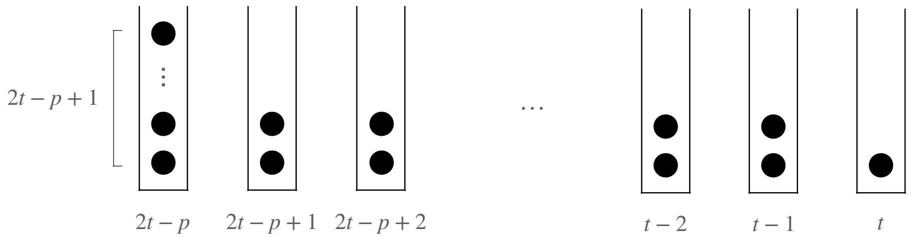
$$|(a+B) \cap B| = |(-a+B) \cap B| = \begin{cases} \max(0, t-a) & \text{for } 2t \leq p-1, \\ \max(t-a, 2t-p) & \text{for } 2t \geq p+1 \end{cases}. \tag{6}$$

Given this claim, as a ranges over $\mathbb{Z}_p = \big\{0, \pm 1, \pm 2, \ldots, \pm(\frac{p-1}{2})\big\}$, the size of the intersection $|(a+B) \cap B|$ takes each value in the multiset M (having cardinality p) exactly once. It then follows from Proposition 2.1(i) that there is a subset A of $\mathbb{Z}_p$ of cardinality s for which $r(A,B,B) = r$ if and only if M contains a multi-subset of cardinality s whose elements sum to r.

It remains to prove the claim. Let $a \in \{0, 1, \ldots, \frac{p-1}{2}\}$. It is sufficient to prove that $|(a+B) \cap B|$ takes the form stated in (6), because $|(-a+B) \cap B| = |(a+(-a+B)) \cap (a+B)| = |B \cap (a+B)|$.



(a) The case $2t \leq p - 1$



(b) The case $2t \geq p + 1$

Figure 1: The multiset M, according to whether $2t \leq p - 1$ or $2t \geq p + 1$.

Case 1: $2t \leq p - 1$. Since $a + t - 1 \leq \frac{p-1}{2} + \frac{p-1}{2} - 1 < p$, we have $a + B = \{a, a+1, \ldots, a+t-1\}$ (in which reduction modulo p is not necessary) and so

$$|(a + B) \cap B| = |\{a, a+1, \ldots, t-1\}| = \max(0, t - a),$$

as required.

Case 2: $2t \geq p + 1$. We have

$$a + B = \begin{cases} \{a, a+1, \ldots, a+t-1\} & \text{for } a + t - 1 \leq p - 1, \\ \{a, a+1, \ldots, p-1\} \cup \{0, 1, \ldots, a+t-1-p\} & \text{for } a + t - 1 \geq p, \end{cases}$$

and so

$$\begin{aligned} |(a + B) \cap B| &= \begin{cases} t - a & \text{for } a + t - 1 \leq p - 1, \\ (t - a) + (a + t - p) & \text{for } a + t - 1 \geq p \end{cases} \\ &= \max(t - a, 2t - p), \end{aligned}$$

as required.

Combining results for Cases 1 and 2 proves the claim. $\square$

The following counting result is straightforward to verify.

Lemma 4.3. *Let n, u be integers, where $1 \leq n \leq 2u - 1$. Let S be the multiset*

$$\{1, 1, 2, 2, \ldots, u-1, u-1\} \cup \{u\}.$$

Then the sum of the n smallest elements of S is $\left\lfloor \frac{(n+1)^2}{4} \right\rfloor$ and the sum of the n largest elements of S is $\left\lceil \frac{n(4u-n)}{4} \right\rceil$.

We now have the necessary ingredients to prove Theorem 4.1.

Proof of Theorem 4.1. We consider the odd integer p and the integers s, t satisfying $1 \leq s, t \leq p-1$ to be fixed. Let M be the multiset represented in Figure 1, in which we distinguish the cases $2t \leq p-1$ and $2t \geq p+1$. We make the following claim, which will be proved subsequently: the sum r_1 of the s smallest elements of M and the sum r_2 of the s largest elements of M are given in the following table.

	$2t \leq p-1$	$2t \geq p+1$
r_1	$\begin{cases} 0 & \text{for } s \leq p-2t+1, \\ \left\lfloor \frac{(s+2t-p)^2}{4} \right\rfloor & \text{for } p-2t+2 \leq s \end{cases}$	$\begin{cases} s(2t-p) & \text{for } s \leq 2t-p+1, \\ \left\lfloor \frac{(s+2t-p)^2}{4} \right\rfloor & \text{for } 2t-p+2 \leq s \end{cases}$
r_2	$\begin{cases} \left\lceil \frac{s(4t-s)}{4} \right\rceil & \text{for } s \leq 2t-1, \\ t^2 & \text{for } 2t \leq s \end{cases}$	$\begin{cases} \left\lceil \frac{s(4t-s)}{4} \right\rceil & \text{for } s \leq 2p-2t-1, \\ s(2t-p)+(p-t)^2 & \text{for } 2p-2t \leq s \end{cases}$

Given this claim, it then follows that for each integer $r \in [r_1, r_2]$ there is a multi-subset of M of cardinality s whose elements sum to r: transform the multi-subset whose elements sum to r_1 into the multi-subset whose elements sum to r_2 by repeatedly moving some ball one urn to the right until the correct number of balls is contained in urn t, then in urn $t-1$, and so on. By Lemma 4.2, for each integer $r \in [r_1, r_2]$ and for $B = \{0, 1, \ldots, t-1\}$ there is therefore a subset A of $\mathbb{Z}_p$ of cardinality s for which $r(A, B, B) = r$. The ranges for s, t in the above table can be rewritten to emphasize the value of $2t$ rather than s, and the intervals $[r_1, r_2]$ for the cases $2t \leq p-1$ and $2t \geq p+1$ then combined to give the interval $[f(s,t),\ g(s,t)]$ described in Theorem 4.1.

It remains to prove the claim.

Case 1: $2t \leq p-1$. See Figure 1(a).

The sum r_1. If $s \leq p-2t+1$ then the s smallest elements of M are each 0, so $r_1 = 0$.
Otherwise the sum of the s smallest elements of M is the sum of the first $s-(p-2t+1)$ elements of the multiset $\{1, 1, 2, 2, \ldots\ t-1, t-1\} \cup \{t\}$, which by Lemma 4.3 (with $u = t$ and $n = s-(p-2t+1)$) equals $\left\lfloor \frac{(s+2t-p)^2}{4} \right\rfloor$.

The sum r_2. If $s \leq 2t-1$ then the sum of the s largest elements of M is the sum of the s largest elements of the multiset $\{1, 1, 2, 2, \ldots\ t-1, t-1\} \cup \{t\}$, which by Lemma 4.3 (with $u = t$ and $n = s$) equals $\left\lceil \frac{s(4t-s)}{4} \right\rceil$.
Otherwise the sum of the s largest elements of M is the sum of all elements of the multiset $\{1, 1, 2, 2, \ldots, t-1, t-1\} \cup \{t\}$, which equals t^2.

Case 2: $2t \geq p+1$. See Figure 1(b).

The sum r_1. If $s \leq 2t-p+1$ then the s smallest elements of M are each $2t-p$, so $r_1 = s(2t-p)$.
Otherwise the sum of the s smallest elements of M is $s(2t-p)$ plus the sum of the first $s-(2t-p+1)$ elements of the multiset $\{1, 1, 2, 2, \ldots, p-t-1, p-t-1\} \cup \{p-t\}$, which by Lemma 4.3 (with $u = p-t$ and $n = s-(2t-p+1)$) equals $s(2t-p) + \left\lfloor \frac{(s-2t+p)^2}{4} \right\rfloor = \left\lfloor \frac{(s+2t-p)^2}{4} \right\rfloor$.

The sum r_2. If $s \leq 2p - 2t - 1$ then the sum of the s largest elements of M is the sum of the s largest elements of the multiset $\{1, 1, 2, 2, \ldots, t-1, t-1\} \cup \{t\}$, which by Lemma 4.3 (with $u = t$ and $n = s$) equals $\left\lceil \frac{s(4t-s)}{4} \right\rceil$.

Otherwise the sum of the s largest elements of M is $s(2t - p)$ plus the sum of all elements of the multiset $\{1, 1, 2, 2, \ldots, p-t-1, p-t-1\} \cup \{p - t\}$, which equals $s(2t - p) + (p - t)^2$.

Combining results for Cases 1 and 2 proves the claim. □

5 Open questions

Theorem 1.4 gives complete information about the spectrum of $r(A, B, B)$ for subsets A, B of $\mathbb{Z}_p$ of cardinality s, t, respectively, for an odd prime p.

What happens when p is not prime? For example, for $p = 9$ the interval $[f(7, 6), g(7, 6)]$ specified by (1) and (2) is $[25, 30]$, but the actual set of attainable values of $r(A, B, B)$ is the larger set $\{24\} \cup [25, 30]$. In this example, the value $r(A, B, B) = 24$ is achieved by $A = \{0, 1, 2, 4, 5, 7, 8\}$ and $B = \{0, 1, 3, 4, 6, 7\}$; the two-way implication of Lemma 4.2 tells us that this value cannot be achieved by taking B to be the interval $\{0, 1, 2, 3, 4, 5\}$.

More generally, what can be said about $r(A, B, B)$ when G is not a cyclic group?

References

[1] B. Bajnok, *Additive Combinatorics: A Menu of Research Problems*, CRC Press, Roca Baton, FL, 2018.

[2] P.J. Cameron, P. Erdős, On the number of sets of integers with various properties, in: Number Theory, Banff, AB, 1988, de Gruyter, Berlin, 1990, pp. 61–79.

[3] A.L. Cauchy, Recherches sur les nombres, *Journal de l'École Polytechnique* vol. 9 (1813), pp. 99–116.

[4] O. Chervak, O. Pikhurko and K. Staden, Minimum number of additive tuples in groups of prime order, *Electron. J. Combin.* vol. 26 (2019), no. 1, Paper No. 1.30, 15 pages.

[5] H. Davenport, On the addition of residue classes, *J. London Math. Soc.* vol. 10 (1935), pp. 30–32.

[6] P. Erdős, Extremal problems in number theory, *Proc. Sympos. Pure Math.* Vol. VIII, Amer. Math. Soc., Providence, R.I., 1965, pp. 181–189.

[7] B. Green, The Cameron–Erdős conjecture, *Bull. London Math. Soc.* vol. 36 (2004) pp. 769–778.

[8] B. Green and I. Z. Ruzsa, Sum-free sets in abelian groups, *Israel J. Math.* vol. 147 (2005), pp. 157–188.

[9] S. Huczynska, G. L. Mullen and J. L. Yucas, The extent to which subsets are additively closed, *J. Combin. Theory Ser. A* vol. 116 (2009), no.4, pp. 831–843.

[10] V. Lev, T. Schoen, Cameron–Erdős modulo a prime, *Finite Fields Appl.* vol. 8 (2002) pp. 108–119.

[11] J. M. Pollard, Addition properties of residue classes, *J. Lond. Math. Soc.* vol. 11 (1975), 147–152.

[12] W. Samotij and B. Sudakov, The number of additive triples in subsets of Abelian groups, *Math. Proc. Camb. Phil. Soc.* vol. 160 (2016), pp. 495–512.

[13] I. Schur, Uber die Kongruenz $x^m + y^m \equiv z^m \pmod{p}$, *Jber. Deutch. Mat. Verein.* vol. 25 (1916), pp. 114–117.

[14] A. A. Sapozhenko, The Cameron-Erdős conjecture (Russian), *Dokl. Akad. Nauk* vol. 393 (2003), no.6, pp. 749–752.