SPANNING SUBSETS OF A FINITE ABELIAN GROUP OF ORDER pq

Jennifer S. Eyl

A Thesis Submitted to the
University of North Carolina at Wilmington in Partial Fulfillment
Of the Requirements for the Degree of
Master of Science

Department of Mathematics and Statistics

University of North Carolina at Wilmington

2003

Approved by

Advisory Committee

Dr. Sandra C. McLaurin Dr. John Karlof

Dr. Michael A. Freeze II
Chair

Accepted by

Dean, Graduate School

This thesis has been prepared in the style and format

consistent with the journal

American Mathematical Monthly.

TABLE OF CONTENTS

ABSTRACT

Let G be a finite abelian group, and let $S \subseteq G$ be a subset of distinct nonzero elements of G. If each element $g \in G$ of the group can be written as a nonempty sum of elements from S, then we say S spans G nontrivially. Denote the maximum cardinality of a subset S which fails to span G nontrivially by $e(G)$, as studied by Griggs in [5]. Griggs noted that the value of $e(G)$ is known for all finite abelian groups G except for $G = \mathbb{Z}/pq\mathbb{Z}$ where p, q are primes such that $p + \lfloor 2\sqrt{p-2} \rfloor + 1 < q < 2p$. We determine the value of $e(G)$ for such groups.

ACKNOWLEDGMENTS

First I would like to express my gratitude to Dr. Michael Freeze for his invaluable assistance, infinite patience, and unwavering confidence in me. Dr. Freeze is an exceptional teacher whose love of mathematics is immense, and whose support and friendship means more than he'll ever know. The whole of my experience here at UNCW has been greatly influenced by him as educator, advisor, and mentor.

Additional thanks goes to my committee members for their time, guidance, and encouragement: to Dr. John Karlof for keeping me on my toes, but also for providing valuable comic relief; to Dr. Sandra McLaurin for her advice and listening ear.

I am grateful to my parents for their continuous support, encouragement, and interest in my education. My appreciation also extends to Richard Goldston, who has been my rock during the times when I felt defeated. Lastly, I must thank Jon Duggins for all his help with LaTeX.

1 INTRODUCTION

Let $S \subseteq G \setminus \{0\}$ be a set of distinct elements where G is a finite abelian group. The set S spans G nontrivially if every element of G can be obtained by a nonempty sum of elements in S. The maximum cardinality of a subset S which fails to span G nontrivially is denoted by $e(G)$ [5]. The value of $e(G)$ is known for all finite abelian groups except for the group $G = \mathbb{Z}/pq\mathbb{Z}$ where $p,\ q$ are primes such that $p + \lfloor 2\sqrt{p-2} \rfloor + 1 < q < 2p$. In the case where $|G| = n$ for n even, the value of $e(G)$ was determined by Diderrich and Mann [4], though their work does not necessarily assume G is abelian. Diderrich's work in [3] gave the lower bound $e(G) \geq \frac{n}{p} + p - 3$ for $|G| = n$ composite where p is the smallest prime dividing n. Further, where G is an abelian group of order $n = pq$ for primes $q > 2p$, Diderrich [3] proved that this lower bound is sharp, establishing $e(G) = \frac{n}{p} + p - 3$.

For abelian groups of even order $n \geq 10$, Griggs [5] proved that Diderrich's lower bound is sharp. The same value for $e(G)$ where $G = \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$, p an odd prime was established by Mann and Wou [6] in 1986.

The remaining finite abelian group whose value of $e(G)$ is not known is $G = \mathbb{Z}/pq\mathbb{Z}$ for primes p, q satisfying $p + \lfloor 2\sqrt{p-2} \rfloor + 1 < q < 2p$ [5]. This is the setting we will focus on to establish the value of $e(G)$. The technique we will employ to explore $e(\mathbb{Z}/pq\mathbb{Z})$ with these values of $p,\ q$ is that used by Diderrich [3] in 1975 in his investigation of the size of possible spanning subsets of $G = \mathbb{Z}/pq\mathbb{Z}$. Diderrich was actually finding an upper bound on the critical value $c(G)$, which is defined as the smallest positive integer c such that any subset of nonzero elements with cardinality c will span G nontrivially. He showed that $c(\mathbb{Z}/pq\mathbb{Z}) \leq p + q - 1$ for primes $5 \leq p \leq q$. We adhere to the notation introduced by Diderrich, but we will be working in the previously described setting for primes p, q. We also bring in some more recent results which were not available to Diderrich, to help us improve his

result concerning $c(G)$. This will in turn give us the value for the case of $e(G)$ in question.

2 PRELIMINARIES

We begin by discussing some of the basic definitions and theorems used in the literature (see [3], [5], [7]), which are necessary to define our problem.

Definition 1 *Given a sequence S of G, the span of S, also called the sumset of S, denoted by ΣS is the set of elements in G obtained by all possible sums of elements from S. The sumset ΣS includes the empty sum so that $\overline{0} \in \Sigma S$. The nontrivial span of S, denoted by $\Sigma^* S$ is the set of elements in G which can be written as a nonempty sum of elements of S. If the nontrivial span contains $\overline{0}$, then S must contain a nonempty zero sum subsequence.*

Example 1 *It is known that $e(\mathbb{Z}/10\mathbb{Z}) = 4$, and a set S which realizes $e(\mathbb{Z}/10\mathbb{Z}) = 4$ is $S = \{\overline{1}, \overline{2}, \overline{7}, \overline{8}\}$. Notice that the nontrivial span of S is $\{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}\} \neq \mathbb{Z}/10\mathbb{Z}$.*

Notice that the nontrivial span here does include zero, since $\overline{1} + \overline{2} + \overline{7} = \overline{2} + \overline{8} = \overline{0} \in \Sigma^* S$. Here, the span of S and the nontrivial span of S are the same, though this will not generally be the case.

Example 2 *From the cyclic group $G = \mathbb{Z}/17\mathbb{Z}$, take $S = \{\overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{16}\}$. Here, $\Sigma S = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}, \overline{10}, \overline{11}, \overline{12}, \overline{13}, \overline{14}, \overline{16}\}$, but the nontrivial span is $\Sigma^* S = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}, \overline{10}, \overline{11}, \overline{12}, \overline{13}, \overline{14}, \overline{16}\}$.*

It is the nontrivial span that we are ultimately interested in, asking whether a set $S \subseteq G$ nontrivially spans G.

Definition 2 *The critical number $c(G)$ is the smallest positive integer c such that any subset of $G \setminus \{0\}$ with cardinality c spans G nontrivially.*

Definition 3 *The invariant $e(G)$ denotes the maximum cardinality of a subset of $G \setminus \{0\}$ which fails to span G nontrivially.*

Note that since $\Sigma^* S \neq G$ in Example 2, the set S fails to span the entire group $G = \mathbb{Z}/17\mathbb{Z}$ nontrivially. Thus this set S realizes $e(\mathbb{Z}/17\mathbb{Z}) = 5$. However, if we add a nonzero element of G to the set, say $\overline{1}$, then we have the subset $S' = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{16}\}$. Now we see that the nontrivial span of S' is $\Sigma^* S' = \mathbb{Z}/17\mathbb{Z}$, making this new set S' an example of $c(\mathbb{Z}/17\mathbb{Z})$. In fact, this close relationship will hold in the general setting.

Proposition 1 *Let G be a finite abelian group with $|G| \geq 3$. Then $e(G) = c(G) - 1$.*

Proof: Let $S \subseteq G$ be a set of distinct nonzero elements with $|S| = c(G)$. Then by definition of $c(G)$, S spans G nontrivially. Further, by the minimality of $c(G)$, if we remove any element x from the subset S, then $S \setminus \{x\}$ will no longer span G nontrivially. Now we have a subset $S \setminus \{x\}$ of maximum cardinality which fails to span G nontrivially. Thus the set $S \setminus \{x\}$ realizes $e(G)$, and

$$e(G) = |S \setminus \{x\}| = |S| - 1 = c(G) - 1. \diamond$$

In addition to the sumset and the nontrivial span of a set, we also use the following variation of a sumset.

Definition 4 *Let S be a nonempty subset of an abelian group G. For $h \geq 2$,*

$$h^\wedge S = \{s_1 + s_2 + \cdots + s_h \mid s_1, \ldots, s_h \in S \text{ and } s_i \neq s_j \text{ for } i \neq j\}$$

is the set of sums of h distinct elements over S.

Example 3 *Consider the group $G = \mathbb{Z}/10\mathbb{Z}$, and take the subset $S = \{\overline{2}, \overline{4}, \overline{5}, \overline{7}, \overline{8}\}$. Then with $h = 3$, we have $3^\wedge S = \{(\overline{2}+\overline{4}+\overline{5}), (\overline{2}+\overline{4}+\overline{7}), (\overline{2}+\overline{4}+\overline{8}), \ldots, (\overline{5}+\overline{7}+\overline{8})\} = \{\overline{0}, \overline{1}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{9}\}$ as the set of sums of 3 elements from S.*

In looking at the invariants $c(G)$ and $e(G)$, we may need to alter the subsets of G to produce some necessary properties for completing the proofs. One of these is called an affine transform. An affine transform of a set $S \subseteq G$ is one in which we add or subtract a fixed nonzero element $g \in G$ from each element in the set S. For instance, the set $S - g = \{s - g \mid s \in S\}$. Notice that $|S| = |S - g|$, where $|S|$ denotes the size of S. This is one of the properties of affine transforms.

Another type of transform we will apply to subsets of the given group G is the e-transform, as defined by Nathanson [7].

Definition 5 *Let G be an abelian group, and take the pair (A, B) where $A, B \subseteq G$ are nonempty subsets of G. Let $e \in G$. The e-transform of (A, B) is the pair $(A(e), B(e))$ of subsets of G defined by*

$$A(e) = A \cup (B + e),$$
$$B(e) = B \cap (A - e).$$

Some properties of the e-transform which we utilize are the following.

Proposition 2 *Let A, B be nonempty subsets of the abelian group G. Let e be an element of G, and let $(A(e), B(e))$ be the e-transform of the pair (A, B). Then*

(i) $\quad A(e) + B(e) \subseteq A + B,$

and if A and B are finite sets, then

(ii) $\quad |A(e)| + |B(e)| = |A| + |B|,$ *and*

(iii) $\quad$ *If $e \in A$ and $0 \in B$, then $e \in A(e)$ and $0 \in B(e)$.*

Proof: Statement (i) follows directly from the definition of the e-transform.

If A and B are finite sets, since $A \subseteq A(e)$ and $B(e) \subseteq B$, then

$$|A(e)| - |A| \;\; = \;\; |A(e) \setminus A|$$

$$
\begin{aligned}
&= |e + (B \setminus B(e)| \\
&= |B \setminus B(e)| \\
&= |B| - |B(e)|,
\end{aligned}
$$

proving (ii). To demonstrate statement (iii), if $e \in A \subseteq A(e)$ and $0 \in B$, then $0 \in A - e$ and so $0 \in B \cap (A - e) = B(e)$.$\diamond$

With the help of these tools, we examine previously established technical results which we use to establish our new results concerning $e(G)$ for $G = Z_{pq}$ with p, q primes such that $p + \lfloor 2\sqrt{p-2} \rfloor + 1 < q < 2p$.

3 TECHNICAL RESULTS

The Cauchy-Davenport Theorem is important in our approach. The proof given here is from Nathanson's text [7].

Theorem 1 *(Cauchy-Davenport) Let p be a prime number, and let A and B be nonempty subsets of $\mathbb{Z}/p\mathbb{Z}$. Then*

$$|A+B| \geq \min(p, |A|+|B|-1).$$

Proof: Let $b_0 \in B$ and $B' = B - b_0$. Then $|B'| = |B|$ and $|A+B'| = |A+(B-b_0)| = |A+B|$. Note $0 \in B'$ and $\gcd(b,p) = 1$ for all $b \in B' \setminus \{0\}$. Certainly the theorem holds if $|A|+|B| > p$ or if $|A| = 1$ or $|B| = 1$, so suppose $|A|+|B| \leq p$ with $|A| \geq 2, |B| \geq 2$. Choose A, B such that $|B'| = |B|$ is minimal with respect to the assumption that $|A+B| < |A|+|B|-1$. If the theorem is false, then we will have $|A+B'| < |A|+|B'|-1$.

Since $|B| = |B'| \geq 2$, $\exists$ an element $b^* \in B'$, $b^* \neq 0$. If $a+b^* \in A$ for all $a \in A$ then $a+jb^* \in A$ for all $j = 1, 2, 3, \ldots$. Since $\gcd(b^*, p) = 1$, this implies $\mathbb{Z}/p\mathbb{Z} = \{a+jb^* \mid j = 0, 1, \ldots, p-1\} \subseteq A \subseteq \mathbb{Z}/p\mathbb{Z} \Rightarrow A = \mathbb{Z}/p\mathbb{Z}$, which is a contradiction. Therefore there exists an element $e \in A$ such that $e+b^* \notin A$. Now apply the e-transform to A and B', so $A(e)+B'(e) \subseteq A+B'$ and $|A(e)+B'(e)| \leq |A+B'| < |A|+|B'|-1 = |A(e)|+|B'(e)|-1$. Since $e \in A$ and $0 \in B'$, then $0 \in B'(e) \subseteq B'$ and $\gcd(b,p) = 1$ $\forall b \in B'(e) \setminus \{0\}$. Further, $e+b^* \notin A$ implies $b^* \notin A-e$ and $b^* \notin B' \cap (A-e) = B'(e)$. Therefore $|B'(e)| < |B'| = |B|$, contradicting the minimality of $|B|$. Thus $|A+B| = |A+B'| \geq \min(p, |A|+|B'|-1) = \min(p, |A|+|B|-1)$ for any nonempty subsets $A, B \subseteq \mathbb{Z}/p\mathbb{Z}$.$\diamond$

Example 4 *Consider the additive cyclic group $\mathbb{Z}/13\mathbb{Z}$. Let $A = \{\overline{1}, \overline{4}, \overline{5}\}$ and $B = \{\overline{3}, \overline{10}, \overline{12}\}$. By the Cauchy-Davenport Theorem,*

$|A+B| \geq \min(13, |A|+|B|-1) = \min(13, 5) = 5$. *In fact,* $A+B = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{7}, \overline{8}, \overline{11}\}$ *has cardinality* 8.

Nathanson [7] also provides a result which is an extension of the Cauchy-Davenport Theorem, proved by induction.

Theorem 2 *Let p be a prime number. Let $s \geq 2$, and let $A_1, A_2, \ldots, A_s$ be nonempty subsets of $\mathbb{Z}/p\mathbb{Z}$. Then*

$$|A_1 + A_2 + \cdots + A_s| \geq \min\{p, \sum_{i=1}^{s} |A_i| - s + 1\}.$$

Diderrich [3] states and proves another variation of the Cauchy-Davenport Theorem. His theorem is an improvement of Theorem 2, although it requires specific structural conditions on the sets A_i. A set A is in arithmetic progression with difference d if it is of the form $A = \{a,\ a+d,\ a+2d, \ldots\}$ where $d \neq 0$.

Theorem 3 *Let $G = \mathbb{Z}/p\mathbb{Z}$ be the additive group of prime order p. Let $A_1, \ldots, A_s$ be nonempty subsets of G such that each subset is an arithmetic progression with distinct nonzero differences $d_1, \ldots, d_s$ respectively. Let $|A_i| = l_i + 1$ for $1 \leq i \leq s$ and define $l = \min_{1 \leq i \leq s}\{l_i\}$. Let $A_0 \subseteq G$ be a subset of G of size $|A_0| \geq 3$ that is not in progression. Then either $\sum_0^s A_i = G$, or*

$$|\sum_{0}^{s} A_i| \ \geq \sum_{0}^{s} |A_i| - 1.$$

Further, if $s \geq 8$, then

$$|\sum_{0}^{s} A_i| \ \geq \sum_{0}^{s} |A_i| + l \sum_{1}^{\frac{s}{2}-1} i - \frac{s}{2} - 2 \geq \sum_{0}^{s} |A_i|.$$

This theorem is relied upon heavily by Diderrich in his argument, which we follow closely to obtain our results. Another theorem Diderrich [3] uses which we need is

the following.

Theorem 4 *(Mann-Olson) Let $A \subseteq G$ be a finite nonempty subset of $G \cong \mathbb{Z}/p\mathbb{Z}$, and let $h \in \mathbb{Z}^+$. Then if $h < |A|$, we have $|h^\wedge A| \geq |A|$.*

Although we do use this result from Mann and Olson, we will also apply a stronger theorem from Nathanson's text [7] which was established by Erdös and Heilbronn in 1994. This newer result helps us to improve Diderrich's result, as this theorem was not available when he did his work concerning $c(\mathbb{Z}/pq\mathbb{Z})$.

Theorem 5 *(Erdös-Heilbronn) Let $G = \mathbb{Z}/p\mathbb{Z}$ be the additive group of prime order p, and take $A \subseteq G$ to be a nonempty subset of G. Then*

$$|h^\wedge A| \geq \min\{p,\ h|A| - h^2 + 1\}.$$

Example 5 *Consider $G = \mathbb{Z}/13\mathbb{Z}$ and take $A = \{\overline{2}, \overline{5}, \overline{6}, \overline{9}, \overline{10}\}$. Then by the Erdös-Heilbronn result with $h = 3$, $|3^\wedge A| \geq \min\{13,\ 3|A| - 3^2 + 1\} = \min\{13,\ 7\} = 7$, so the set of all subsums of 3 distinct elements of A will have cardinality at least 7. In fact, it can be calculated that $3^\wedge A = \{\overline{0}, \overline{3}, \overline{4}, \overline{5}, \overline{7}, \overline{8}, \overline{11}, \overline{12}\}$, having size 8, satisfying the inequality.*

Dias da Silva and Hamidoune [2] proved a theorem concerning the critical number of $\mathbb{Z}/p\mathbb{Z}$, p a prime number, which Griggs uses in [5] to find $e(\mathbb{Z}/p\mathbb{Z})$:

Theorem 6 *(Dias da Silva-Hamidoune) Let $S \subseteq \mathbb{Z}/p\mathbb{Z}$ with cardinality c_p+1, where $c_p = \lfloor (4p-7)^{\frac{1}{2}} \rfloor$ is the critical value of $\mathbb{Z}/p\mathbb{Z}$. Then every element of $\mathbb{Z}/p\mathbb{Z}$ can be written as a sum of $\lfloor (c_p+1)/2 \rfloor$ elements of S.*

This theorem led Griggs [5] to be able to calculate $e(\mathbb{Z}/p\mathbb{Z})$ for prime $p \geq 3$, giving a slightly nicer formula for c_p:

Lemma 1 *For p a prime number, $\lfloor\sqrt{4p-7}\rfloor = \lfloor 2\sqrt{p-2}\rfloor$.*

Proof: Suppose there exists some integer n such that $\sqrt{4p-8} < n < \sqrt{4p-7}$. Since each of these is positive, we square each part, preserving the inequalities. Now we have

$$4p - 8 < n^2 < 4p - 7,$$

a contradiction for $n \in \mathbb{Z}$. Thus, there is no integer n where $\sqrt{4p-8} < n < \sqrt{4p-7}$, implying that there is some integer m such that

$$m \leq \sqrt{4p-8} < \sqrt{4p-7} < m + 1.$$

Hence, even in the case where $\sqrt{4p-8} \in \mathbb{Z}$, taking the floor function we have $\lfloor\sqrt{4p-7}\rfloor = \lfloor 2\sqrt{p-2}\rfloor$.$\diamond$

Theorem 7 *Let $p \geq 3$ be prime. Then $e(\mathbb{Z}/p\mathbb{Z}) = c_p - 1$, where $c_p = \lfloor 2\sqrt{p-2}\rfloor$.*

Proof: Given that c_p is the critical value of $\mathbb{Z}/p\mathbb{Z}$, the result follows from Proposition 1.$\diamond$

To construct a set S realizing $e(\mathbb{Z}/p\mathbb{Z})$, we borrow the technique used by Griggs to prove his Theorem 4 in [5]. He starts with an element $a \in G$, and constructs the set as $S = \{-a, -a+1, \ldots, a\}$. For the example here, we use this type of construction together with the calculated value of $e(\mathbb{Z}/p\mathbb{Z})$ to obtain an appropriate set.

Example 6 *Let $G = \mathbb{Z}/13\mathbb{Z}$. Griggs' theorem implies $c_{13} = \lfloor 2\sqrt{13-2}\rfloor = 6$ and $e(\mathbb{Z}/13\mathbb{Z}) = 6 - 1 = 5$. So consider the set $S = \{\overline{-2}, \overline{-1}, \overline{1}, \overline{2}, \overline{3}\} = \{\overline{1}, \overline{2}, \overline{3}, \overline{11}, \overline{12}\}$. Then $\Sigma S = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{10}, \overline{11}, \overline{12}\} \neq \mathbb{Z}/13\mathbb{Z}$, and S satisfies $e(\mathbb{Z}/13\mathbb{Z})$.*

We now have the tools necessary to refine Diderrich's technique for exploring the value of $e(G)$ where $G = \mathbb{Z}/pq\mathbb{Z}$. His work was in this group where primes p and q

satisfy $5 \leq p \leq q$, but since the case in which $e(\mathbb{Z}/pq\mathbb{Z})$ is unknown is even more specific, we narrow down to primes p, q such that $p + \lfloor 2\sqrt{p-2} \rfloor + 1 < q < 2p$.

4 NOTATION

In this section, we let $G = \mathbb{Z}/pq\mathbb{Z}$ with primes p, q where $p + \lfloor 2\sqrt{p-2} \rfloor + 1 < q < 2p$, and take $S \subseteq G$ a nonempty subset of distinct nonzero elements of G. The argument we follow is the one used by Diderrich to determine his upper bound of $|S| \leq p+q-1$ as the smallest cardinality required for a subset S to span G nontrivially. We first explain the notation and setup to be used for this technique.

Taking H to be the subgroup of G of order q, let $a_1, \ldots, a_s$ denote elements of S which are not in H. Then define the following sets

$$\begin{aligned} B_i &= (a_i + H) \cap S \quad 1 \leq i \leq s, \\ B_0 &= H \cap S. \end{aligned}$$

Putting $k_i = |B_i|$ for $0 \leq i \leq s$, we have $\sum_{i=0}^{s} k_i = p + q - 1$.

Diderrich arranges the notation so that

$$\begin{aligned} &k_i \geq 3, && 1 \leq i \leq t, \quad t - \text{tuples}; \\ &k_i = 1, && t < i \leq t + r, \quad r - \text{singletons}; \\ &k_i = 2, && t + r < i \leq t + r + u, \quad u - \text{doublets}. \end{aligned}$$

Notice then, that $s = t+r+u$ and $k_0 + \sum_{i=1}^{t} k_i + r + 2u = p+q-1 = |S|$. Moreover, since H is of order q we have $G/H \cong \mathbb{Z}/p\mathbb{Z}$, so $s = t + r + u \leq p - 1$.

Now let $x \in \mathbb{Z}/p\mathbb{Z}$ be an element of the quotient group G/H. Then x can be represented by $a_1, \ldots, a_s$ as

$$x = \sum_{i=1}^{s} f_i a_i$$

where f_i are integers with $0 \leq f_i \leq k_i$ and not all $f_i = 0$. For any coefficient f_i in this representation of x, if $f_i = 0$ or $f_i = k_i$, we call this f_i a collapsed coefficient.

Then the amount of collapse of x is denoted by $C_x = \sum(k_i - 1)$ where the sum extends over all the collapsed coefficients in the given representation of x. Further, if such a representation exists for each element of $\mathbb{Z}/p\mathbb{Z}$, we consider the collapse of the representation of $\mathbb{Z}/p\mathbb{Z}$, which is denoted by $C = \max_{x \in \mathbb{Z}/p\mathbb{Z}} C_x$.

Once we establish a representation of $\mathbb{Z}/p\mathbb{Z}$, this implies that we can obtain a representation of each coset of $H \cong \mathbb{Z}/q\mathbb{Z}$ in $G = \mathbb{Z}/pq\mathbb{Z}$. The next step is to show that we can obtain every element in each of the cosets of H.

Since finding such a representation by specifically writing each element of $\mathbb{Z}/p\mathbb{Z}$ as a sum of elements of S can become tedious at best for larger groups, Diderrich uses a more general approach. He constructs the following sets D and $A_i,\ 1 \leq i \leq t+r$:

$$\begin{aligned} A_i &= \{a_i, \ldots, (k_i - 1)a_i\} \text{ for } 1 \leq i \leq t; \\ A_i &= \{0, a_i\} \text{ for } t < i \leq t + r; \\ D &= \{b_0, b_0 - b_1, b_0 - b_2, \ldots, b_0 - b_{u-u_0}\} \end{aligned}$$

where u_0 is a parameter such that $0 \leq u_0 < u$, $b_j = a_{t+r+u_0+j}$ for $1 \leq j \leq u - u_0$, and

$$b_0 = \sum_{j=1}^{u-u_0} b_j.$$

The parameter u_0 is introduced here for possible use when $2 \leq k_0 \leq u < p-3$. In this setting, it may be helpful to let $u_0 = k_0 - 2$. However, even when $2 \leq k_0 \leq u < p-3$, choosing $u_0 = 0$ will often suffice, as well as when these conditions are not met. We will be using $u_0 = 0$, unless otherwise noted. Given such construction of these sets, if $D + \sum_{i=1}^{t+r} A_i = \mathbb{Z}/p\mathbb{Z}$, then this gives a representation of $\mathbb{Z}/p\mathbb{Z}$ with collapse $C \leq u_0 + 1 \leq u$. Further, if $u_0 = 0$, we have $C \leq 1$. To show that we do have a representation of $G/H \cong \mathbb{Z}/p\mathbb{Z}$, we simply need $|D + \sum_{i=1}^{t+r} A_i| \geq p$.

Lemma 2 *Choosing $u_0 = 0$, either of the following conditions is sufficient to show*

$|D + \sum_{i=1}^{t+r} A_i| \geq p$:

(i) $u + 2t + 2r \geq p$,

(ii) $p - 1 - k_0 - t + r - u \geq 0$.

Proof: Using Theorem 3 we have

$$\begin{aligned} |D + \sum_{i=1}^{t+r} A_i| &\geq |D| + \sum_{i=1}^{t+r} |A_i| - 1 \\ &= u + 1 + \sum_{i=1}^{t} (k_i - 1) + 2r - 1 \\ &= u + \sum_{i=1}^{t} k_i - t + 2r \\ &\geq u + 2t + 2r \quad \text{since } \sum_{i=1}^{t} k_i \geq 3t, \end{aligned}$$

obtaining (i).

Next, since

$$\begin{aligned} p + q - 1 &= k_0 + \sum_{i=1}^{t} k_i + r + 2u \\ &= k_0 + (u + \sum_{i=1}^{t} k_i - t + 2r) + t - r + u, \end{aligned}$$

we can write

$$u + \sum_{i=1}^{t} k_i - t + 2r = p + q - 1 - k_0 - t + r - u,$$

giving us

$$|D + \sum_{i=1}^{t+r} A_i| \geq p + q - 1 - k_0 - t + r - u.$$

Now to show $p+q-1-k_0-t+r-u \geq p$, it is sufficient to show $q-1-k_0-t+r-u \geq 0$. Then, since $q > p$, it will suffice if $p - 1 - k_0 - t + r - u \geq 0$, obtaining (ii).$\diamond$

After we have a representation of each of the cosets of H in G, we must show that we can obtain every element in each of those cosets. Recall that our representation

of $G/H \cong \mathbb{Z}/p\mathbb{Z}$ yields for each element $x \in \mathbb{Z}/p\mathbb{Z}$ the sum $x = \sum_{i=1}^{s} f_i a_i$ where $f_i \in \mathbb{Z}$ with $0 \le f_i \le k_i$ and not all $f_i = 0$. Using these coefficients f_i for $1 \le i \le s$, define the sets

$$\begin{aligned} E_i &= \{0\} \quad \text{if } f_i = 0 \\ E_i &= f_i^{\wedge} B_i \quad \text{if } 1 \le f_i \le k_i \end{aligned}$$

where $f_i^{\wedge} B_i$ denotes the set of sums of f_i distinct elements from B_i.

Also define

$$\begin{aligned} E_0 &= \{0, z_i\} + \cdots + \{0, z_{k_0}\} \\ \text{where} \quad B_0 &= \{z_1, \ldots, z_{k_0}\} \quad \text{if } k_0 \ge 1, \\ \text{and} \quad E_0 &= \{0\} \quad \text{if } k_0 = 0. \end{aligned}$$

To show $\sum_0^s E_i = x + H$, it is enough to show $|\sum_0^s E_i| \ge q$.

Lemma 3 *If* $(p+q-1) + \hat{C} - C - s \ge q$ *where* $p+q-1 = |S|$, *then* $|\sum_0^s E_i| \ge q$.

Proof: Theorem 3 gives us $|E_0| \ge k_0 + 1$ if $0 \le k_0 \le 1$, and $|E_0| \ge k_0 + k_0 - 1$, if $k_0 \ge 2$. The result is $|E_0| \ge k_0 + \hat{C}$ since $\hat{C} = \max\{1,\ k_0 - 1\}$.

In estimating $|E_i|$ for $1 \le i \le s$, clearly $|E_i| = 1$ if f_i is a collapsed coefficient, and Theorem 4 gives us $|E_i| \ge |B_i| = k_i$ if f_i is not a collapsed coefficient. Now we have$\sum_0^s |E_i| \ge \sum_0^s k_i + \hat{C} - C$ where C is the collapse, and by Theorem 2 we have

$$\begin{aligned} |\sum_0^s E_i| &\ge \sum_0^s |E_i| - s \\ &\ge \sum_0^s k_i + \hat{C} - C - s \\ &= p + q - 1 + \hat{C} - C - s. \end{aligned}$$

So if $p+q-1+\hat{C}-C-s \geq q$, then $|\sum_0^s E_i| \geq q$.$\diamond$

Now, since our construction of sets D and $A_i,\ 1 \leq i \leq t+r$ resulted in $C \leq \max\{\hat{C}, p-s\}$, then if $\max\{\hat{C}, p-s\} = \hat{C}$ we have

$$p+q-1+\hat{C}-C-s = q+[(p-s)-1]+(\hat{C}-C) \geq q,$$

and $\max\{\hat{C}, p-s\} = p-s$ yields

$$p+q-1+\hat{C}-C-s = q+[(p-s)-C]+(\hat{C}-1) \geq q.$$

Thus, $|\sum_0^s E_i| \geq q$, and $\sum_0^s E_i = x+H$.

Again, we see that Diderrich's method employs two fundamental steps: First it must be shown that each of the cosets of H is represented with small collapse. For this we need $|D+\sum_{i=1}^{t+r} A_i| \geq p$ with the appropriate constructions of the sets D and A_i, $1 \leq i \leq t+r$.

The second step is to demonstrate that every element in each of the cosets can be obtained. To establish this part, we must show $|\sum_{i=0}^s E_i| \geq q$.

To demonstrate this method with a set of $p+q-1$ elements, we consider the smallest group of order pq where p and q satisfy $p+\lfloor 2\sqrt{p-2}\rfloor+1 < q < 2p$, which is $G = \mathbb{Z}/91\mathbb{Z}$. Here, $p=7$ and $q=13$, so take the set

$$S = \{\overline{2}, \overline{5}, \overline{7}, \overline{8}, \overline{10}, \overline{13}, \overline{15}, \overline{21}, \overline{24}, \overline{34}, \overline{37}, \overline{40}, \overline{43}, \overline{46}, \overline{63}, \overline{66}, \overline{71}, \overline{72}, \overline{86}\}$$

of cardinality $|S| = p+q-1 = 19$. Using Diderrich's technique, we will show that this set $S \subseteq G$ spans $G = \mathbb{Z}/91\mathbb{Z}$ nontrivially.

Now the subgroup of G having order $q=13$ is $H \cong \mathbb{Z}/13\mathbb{Z}$, and the distribution

of elements in S as representatives of the cosets of H in G is as follows:

$$\begin{aligned}
B_0 &= H \cap S = \{\overline{7}, \overline{21}, \overline{63}\} \\
B_1 &= (\bar{1} + H) \cap S = \{\overline{8}, \overline{15}, \overline{43}, \overline{71}\} \\
B_2 &= (\bar{2} + H) \cap S = \{\overline{2}, \overline{37}, \overline{72}, \overline{86}\} \\
B_3 &= (\bar{3} + H) \cap S = \{\overline{10}, \overline{24}, \overline{66}\} \\
B_4 &= (\bar{4} + H) \cap S = \{\overline{46}\} \\
B_5 &= (\bar{5} + H) \cap S = \{\overline{5}, \overline{40}\} \\
B_6 &= (\bar{6} + H) \cap S = \{\overline{13}, \overline{34}\}
\end{aligned}$$

This gives us $k_0 = 3,\ k_1 = k_2 = 4,\ k_3 = 3,\ k_4 = 1,\ k_5 = k_6 = 2$, so $t = 3,\ r = 1$, and $u = 2$. Since $k_0 > u$, we will choose $u_0 = 0$. Note that we have $s = t + r + u = 6 \leq p - 1 = 6$, and $k_0 + \sum_{i=1}^{t} k_i + r + 2u = 3 + (4 + 4 + 3) + 1 + 2(2) = 19 = |S|$.

First, we must show that we can obtain a representative of each of the cosets of $H \cong \mathbb{Z}/13\mathbb{Z}$, which we will write as elements of the quotient group $G/H \cong \mathbb{Z}/7\mathbb{Z}$. Certainly, we have a representative of each of the cosets, since none of the sets B_i, $1 \leq i \leq 6$ are empty; however, it is important that the collapse for each element, and thus the collapse of the representation of $\mathbb{Z}/7\mathbb{Z}$ is small. In fact we will need the collapse $C \leq \max\{k_0 - 1,\ p - s\} = \max\{2, 1\} = 2$. The second step will be to show that we can obtain every element in each of the H-cosets.

For the first step, define the sets

$$\begin{aligned}
A_1 &= \{\overline{8}, 2(\overline{8}), 3(\overline{8})\} = \{\overline{2}, \overline{16}, \overline{24}\}; \\
A_2 &= \{\overline{2}, 2(\overline{2}), 3(\overline{2})\} = \{\overline{2}, \overline{4}, \overline{6}\}; \\
A_3 &= \{\overline{10}, 2(\overline{10})\} = \{\overline{10}, \overline{20}\}; \\
A_4 &= \{\overline{0}, \overline{46}\};
\end{aligned}$$

$$\text{and} \quad \text{where} \qquad b_1 = \overline{5}, \quad b_2 = \overline{13}, \text{ and } \quad b_0 = b_1 + b_2,$$

$$D = \{\overline{18}, \overline{13}, \overline{5}\}.$$

Notice that we have $u + 2t + 2r = 2 + 2(3) + 2(1) = 10 \geq 7 = p$, satisfying inequality (i). Thus by Lemma 2 we have $D + \sum_{i=1}^{4} A_i = \mathbb{Z}/7\mathbb{Z}$ with collapse $C \leq u_0 + 1 = 1$.

The second step is to establish that we can obtain every element in each of the cosets of $H \cong \mathbb{Z}/13\mathbb{Z}$. Here, we first consider the coset $\overline{1} + H$ and the corresponding sets E_i for $1 \leq i \leq 6$. If $\overline{1} = 2(\overline{8}) + 1(\overline{2}) + 1(\overline{10}) + 1(\overline{46}) + 1(\overline{5}) + 1(\overline{13})$, then define the sets

$$\begin{aligned}
E_1 &= 2^{\wedge}B_1 = \{\overline{8}, \overline{15}, \overline{23}, \overline{43}, \overline{51}, \overline{58}, \overline{71}, \overline{79}, \overline{86}\} \\
E_2 &= 1^{\wedge}B_2 = \{\overline{2}, \overline{37}, \overline{72}, \overline{86}\} \\
E_3 &= 1^{\wedge}B_3 = \{\overline{10}, \overline{24}, \overline{66}\} \\
E_4 &= 1^{\wedge}B_4 = \{\overline{46}\} \\
E_5 &= 1^{\wedge}B_5 = \{\overline{5}, \overline{40}\} \\
E_6 &= 1^{\wedge}B_6 = \{\overline{13}, \overline{34}\}
\end{aligned}$$

and since $B_0 = \{\overline{7}, \overline{21}, \overline{63}\}$, we have

$$\begin{aligned}
E_0 &= \{\overline{0}, \overline{7}\} + \{\overline{0}, \overline{21}\} + \{\overline{0}, \overline{63}\} \\
&= \{\overline{0}, \overline{7}, \overline{21}, \overline{28}, \overline{63}, \overline{70}, \overline{84}\}.
\end{aligned}$$

Notice that even though there is a collapsed coefficient on $\overline{46}$, since collapse is

defined with $k_i - 1$ we have $C_{\overline{1}} = k_4 - 1 = 1 - 1 = 0$. Theorem 2 gives us

$$|\sum_{0}^{6} E_i| \geq \sum_{0}^{6} |E_i| - 6 = 21 - 6 = 15 \geq q = 13,$$

implying that $\sum_0^6 E_i = \overline{1} + H$.

However, recalling that we have already established that our representation has collapse $C \leq 1$ where $C = \max_{x \in \mathbb{Z}/p\mathbb{Z}} C_x$, we can apply Lemma 3 to show that we can do this for all of the cosets. We need $p + q - 1 + \hat{C} - C - s \geq q$, where $\hat{C} = \max\{k_0 - 1, 1\}$. Here we have $\hat{C} = \max\{2,\ 1\} = 2$, so
$p + q - 1 + \hat{C} - C - s \geq 7 + 13 - 1 + 2 - 1 - 6 = 14 \geq q = 13$, implying that we are able to obtain all the elements in each of the subsets. Therefore, this set S with $|S| = p + q - 1 = 19$ spans $G = \mathbb{Z}/91\mathbb{Z}$ nontrivially. We note, however, that in fact only 18 distinct elements are needed to span $\mathbb{Z}/91\mathbb{Z}$ nontrivially.

Diderrich established that given $|D+\sum_{i=1}^{t+r} A_i| \geq p$ with $C \leq \max\{\hat{C}, p-s\}$, then we have $|\sum_0^s E_i| \geq q$ and hence a nontrivial span of G. His method used the estimate $|\sum_0^s E_i| \geq p+q-1+\hat{C}-C-s \geq q$, starting with a set of $p+q-1$ elements. Once we have shown that we still obtain $|D+\sum_{i=1}^{t+r} A_i| \geq p$ with a set of $p+q-2$ elements, our goal is to increase the lower bound of $|\sum_0^s E_i|$ by at least 1, which will allow for the smaller set of $p+q-2$ elements to suffice in the cases where we will not already have sufficient conditions for $p+q-2+\hat{C}-C-s \geq q$. We will then have $|\sum_0^s E_i| \geq q$ for a set of $p+q-2$ elements. For the smaller set S, we use a slight variation of Lemma 3 to give us this last inequality.

Lemma 4 *If $p+q-2+\hat{C}-C-s \geq$ where $p+q-2=|S|$, then $|\sum_0^s E_i| \geq q$.*

Proof: This result is obtained in the same manner that we used to establish Lemma 3.$\diamond$

Recall that the value of $k_0 = |B_0|$ represents the number of elements from G which are in the intersection of our set S and the maximal subgroup of G. It is the various values of k_0 with which we approach the argument for a set of $p+q-2$ elements to span $G = \mathbb{Z}/pq\mathbb{Z}$ nontrivially where $p+\lfloor 2\sqrt{p-2}\rfloor + 1 < q < 2p$.

Proposition 3 *Let $S \subseteq G$ be a subset of $p+q-2$ distinct nonzero elements with $k_0 \geq \lfloor 2\sqrt{q-2}\rfloor$. Then S spans G nontrivially.*

Proof: Notice that by Theorem 6 and Lemma 1, $\lfloor 2\sqrt{q-2}\rfloor = c_q$ is the critical number for the subgroup $H \cong \mathbb{Z}/q\mathbb{Z}$. This implies that $E_0 = H$. Now we are left with at least $p-1$ distinct nonzero elements from G distributed across the sets B_i, $1 \leq i \leq s$. If we let $B = B_1 \cup \cdots \cup B_s$, then we must show $|\Sigma B| \geq p$.

Since $(B_1 \cup \{\overline{0}\}) + \cdots + (B_s \cup \{\overline{0}\}) \subseteq \Sigma B$, then using Theorem 2 we have

$$\begin{aligned} |\Sigma B| \geq |\sum_{i=1}^{s}(B_i \cup \{\overline{0}\})| &\geq \min\{p, \sum_{i=1}^{s}|B_i \cup \{\overline{0}\}| - s + 1\} \\ &= \sum_{i=1}^{s}(k_i + 1) - s + 1 \\ &\geq (p - 1 + s) - s + 1 \\ &= p.\diamond \end{aligned}$$

To demonstrate that $p + q - 2$ elements span G nontrivially with some of the remaining possible values of k_0, we will need the following lemma.

Lemma 5 *If $k_0 \leq \lfloor 2\sqrt{q-2} \rfloor - 1$, then $|D + \sum_{i=1}^{t+r} A_i| \geq p$.*

Proof: Let $k_0 \leq \lfloor 2\sqrt{q-2} \rfloor - 1$. By Theorem 3 we have

$$\begin{aligned} |D + \sum_{i=1}^{t+r} A_i| &\geq |D| + \sum_{i=1}^{t+r}|A_i| - 1 \\ &= u + \sum_{i=1}^{t} k_i - t + 2r. \end{aligned}$$

So if $u + \sum_{i=1}^{t} k_i - t + 2r \geq p$, we are finished. Suppose to the contrary that $u + \sum_{i=1}^{t} k_i - t + 2r \leq p - 1$. Since by our constructions, $p + q - 2 = k_0 + \sum_{i=1}^{t} k_i + r + 2u$, we can solve this equation for $\sum_{i=1}^{t} k_i$, yielding

$$\begin{aligned} u + (p + q - 2 - k_0 - r - 2u) - t + 2r &\leq p - 1 \\ q - u - t + r &\leq k_0 + 1 \\ q - (u + t + r) + 2r &\leq k_0 + 1. \end{aligned}$$

With $u + t + r = s \leq p - 1$, we have

$$\begin{aligned} q - (p-1) + 2r &\leq k_0 + 1 \\ q - p + 2r &\leq k_0. \end{aligned}$$

Since $q - p \leq q - p + 2r$, and we are assuming $k_0 \leq \lfloor 2\sqrt{q-2} \rfloor - 1$, the result is

$$q - p + 1 \leq \lfloor 2\sqrt{q-2} \rfloor.$$

Here, since $q - p + 1$ is positive, squaring both sides preserves the inequality, giving us

$$\begin{aligned} (q-p)^2 + 2(q-p) + 1 &\leq 4(q-2) \\ q^2 - 2pq + p^2 + 2q - 2p + 1 &\leq 4q - 8 \\ q^2 - 2pq - 2q + p^2 - 2p + 1 &\leq 0 \\ q^2 - (2p+2)q + (p^2 - 2p + 1) &\leq 0. \end{aligned}$$

By considering this as a quadratic in terms of q, we can apply the quadratic formula to find that

$$q \leq p + 1 + 2\sqrt{p-2}.$$

Certainly we know $0 \leq 2\sqrt{p-2} - \lfloor 2\sqrt{p-2} \rfloor < 1$, and since q and $p+1$ are integers, we then have

$$q \leq p + 1 + \lfloor 2\sqrt{p-2} \rfloor,$$

which is a contradiction to the original restrictions of $p + \lfloor 2\sqrt{p-2} \rfloor + 1 < q < 2p$. Thus $k_0 < \lfloor 2\sqrt{q-2} \rfloor$ implies $u + \sum_{i=1}^{t} k_i - t + 2r \geq p$, and we have a representation

of $G/H \cong \mathbb{Z}/p\mathbb{Z}$ with collapse $C \leq 1$.$\diamond$

We now look at the next range of values for k_0.

Proposition 4 *Given a subset S with $|S| = p+q-2$, if $3 \leq k_0 < \lfloor 2\sqrt{q-2} \rfloor$, then S spans G nontrivially.*

Proof: Since $k_0 < \lfloor 2\sqrt{q-2} \rfloor$, Lemma 5 gives us a representation of $\mathbb{Z}/p\mathbb{Z}$ with collapse $C \leq 1$. Notice that since $k_0 \geq 3$, we have $\hat{C} \geq 2$. By Lemma 4 we have $p+q-2+\hat{C}-C-s \geq p+q-2+2-1-(p-1) = q$, implying that we obtain every element in each of the cosets and thus a nontrivial span of $G = \mathbb{Z}/pq\mathbb{Z}$.$\diamond$

We note the following general result.

Lemma 6 *If $t \geq \lfloor 2\sqrt{p-2} \rfloor$, then the representation of the quotient group $G/H \cong \mathbb{Z}/p\mathbb{Z}$ has collapse $C = 0$.*

Proof: Recall from Section 3 that for a cyclic group of prime order p, we have the critical number $c_p = \lfloor 2\sqrt{p-2} \rfloor$.

Let $G = \mathbb{Z}/pq\mathbb{Z}$ as previously described, and $G/H \cong \mathbb{Z}/p\mathbb{Z}$. In establishing a representation of the quotient group, we consider the cosets as elements of the additive cyclic group of order p. Suppose $t \geq \lfloor 2\sqrt{p-2} \rfloor = c_p$, the critical value of $\mathbb{Z}/p\mathbb{Z}$. We take one representative from each of the sets B_i, $1 \leq i \leq s$, so that none of the corresponding coefficients will be 0. We may still take at least one representative from each of the t cosets containing 3 or more elements without having a collapsed coefficient. Since we have at least $\lfloor 2\sqrt{p-2} \rfloor$ of these cosets, one element from each will be enough to span $\mathbb{Z}/p\mathbb{Z}$. Thus we have obtained a representation of $\mathbb{Z}/p\mathbb{Z}$ with collapse $C = 0$.$\diamond$

We have only $k_0 \leq 2$ left to consider and we examine this range of values under two different settings.

Proposition 5 *Let $|S| = p+q-2$ with $k_0 \leq 2$. If $k_i \leq 3$ for $1 \leq i \leq s$, then S spans G nontrivially.*

Proof: Since $k_0 \leq 2 < \lfloor 2\sqrt{q-2} \rfloor$, then by Lemma 5 we have a representation of $\mathbb{Z}/p\mathbb{Z}$ with collapse $C \leq 1$. We still must show $|\sum_{i=0}^{s} E_i| \geq q$ to establish that we can obtain every element in each of the H-cosets. By Lemma 4, it is enough to show $(p+q-2) + \hat{C} - C - s \geq q$. With $k_0 \leq 2$ implying that $\hat{C} = 1$, and $C \leq 1$ we have $(p+q-2) + \hat{C} - C - s \geq (p+q-2) + 1 - 1 - s$. If $s \leq p-2$, we are finished, so suppose $s = p-1$. Using this equation and our assumption that $k_i \leq 3$ for $1 \leq i \leq s$, we have

$$\begin{aligned} p+q-2 &= k_0 + \sum_{i=1}^{t} k_i + r + 2u \\ &= k_0 + 3t + r + 2u \\ &= k_0 + 2t + u + (t + r + u) \\ &= k_0 + 2t + u + (p-1). \end{aligned}$$

Simplifying and solving for k_0 results in

$$\begin{aligned} k_0 &= q - 1 - 2t - u \\ &= q - 1 - [t + (t + u + r) - r] \\ &= q - 1 - (t + p - 1 - r) \\ &= q - p - t + r. \end{aligned}$$

Recalling that $p + \lfloor 2\sqrt{p-2} \rfloor + 1 < q < 2p$, we then have

$$\begin{aligned} k_0 + t = q - p + r &> (p + \lfloor 2\sqrt{p-2} \rfloor + 1) - p + r \\ &= \lfloor 2\sqrt{p-2} \rfloor + 1 + r \\ &\geq \lfloor 2\sqrt{p-2} \rfloor + 1. \end{aligned}$$

Notice that we now have

$$\begin{aligned} t &> \lfloor 2\sqrt{p-2} \rfloor + 1 - k_0 \\ \text{so} \quad t &\geq \lfloor 2\sqrt{p-2} \rfloor + 2 - k_0, \end{aligned}$$

and since $k_0 \leq 2$, we have $t \geq \lfloor 2\sqrt{p-2} \rfloor$. Consequently, Lemma 6 implies that we have collapse $C = 0$. Now Lemma 4 is satisfied:

$$(p+q-2) + \hat{C} - C - s \geq (p+q-2) + 1 - 0 - (p-1) = q.,$$

yielding a nontrivial span of $G = \mathbb{Z}/pq\mathbb{Z}$.$\diamond$

Finally, we address the the remaining case of $k_0 \leq 2$ where $\max\{k_i\} \geq 4$ for $1 \leq i \leq s$. For this setting we introduce a slight variation in the construction of the sets A_i for $1 \leq i \leq t+r$.

Since our notation has been set up such that the cosets having 3 or more elements are the first cosets $B_i, \quad 1 \leq i \leq t$, we will also assume that the first coset B_1 is one for which $|B_1| = k_1 \geq 4$. Then define the set

$$A_1 = \{2a_1, \ldots, (k_1 - 2)a_1\},$$

while sets A_i for $2 \leq i \leq t+r$ and set D are the same as defined in Section 4. Notice that with this construction we lose two elements in $|D + \sum_{i=1}^{t+r} A_i| \geq |D| + \sum_{i=1}^{t+r} |A_i| - 1$, so we have

$$|D| + \sum_{i=1}^{t+r} |A_i| - 1 = u + \sum_{i=1}^{t} k_i - t + 2r - 2,$$

and to imply that we have a representation of $\mathbb{Z}/p\mathbb{Z}$ with $C \leq 1$, we must show that $u + \sum_{i=1}^{t} k_i - t + 2r - 2 \geq p$.

Lemma 7 *Let S be a subset of $p+q-2$ distinct nonzero elements of $G = \mathbb{Z}/pq\mathbb{Z}$ and $k_0 \leq 2$. Then we have $u + \sum_{i=1}^{t} k_i - t + 2r - 2 \geq p$.*

Proof: Recall that $p+q-2 = k_0 + \sum_{i=1}^{t} k_i + r + 2u$ implies $\sum_{i=1}^{t} k_i = p+q-2-k_0-r-2u$. Now we have

$$\begin{aligned} u + \sum_{i=1}^{t} k_i - t + 2r - 2 &= u + (p+q-2-k_0-r-2u) - t + 2r - 2 \\ &= p+q-4-k_0+r-u-t \\ &= p+q-4-k_0+r-(s-r) \\ &= p+q-4-k_0+2r-s. \end{aligned}$$

Since $s \leq p-1$, we see that

$$\begin{aligned} p+q-4-k_0+2r-s &\geq p+q-4-k_0+2r-p+1 \\ &= q-3-k_0+2r \\ &> (p+\lfloor 2\sqrt{p-2} \rfloor + 1) - 3 - k_0 + 2r \\ &= p + \lfloor 2\sqrt{p-2} \rfloor - 2 - k_0 + 2r \end{aligned}$$

for the given values of primes p, q. This gives us

$$\begin{aligned} u + \sum_{i=1}^{t} k_i - t + 2r - 2 &> p + \lfloor 2\sqrt{p-2} \rfloor - 2 - k_0 + 2r \\ &\geq p + \lfloor 2\sqrt{p-2} \rfloor - 4 + 2r \\ &\geq p + \lfloor 2\sqrt{p-2} \rfloor - 4 \\ &\geq p, \end{aligned}$$

since $\lfloor 2\sqrt{p-2} \rfloor \geq 4$ for $p \geq 7$.$\diamond$

With this result, we establish the following proposition.

Proposition 6 *Let* $|S| = p + q - 2$ *with* $k_0 \leq 2$. *If* $\max\{k_i\} \geq 4$ *for* $1 \leq i \leq s$, *then* S *spans* G *nontrivially.*

Proof: With $k_0 \leq 2$, Lemma 7 gives us $u + \sum_{i=1}^{t} k_i - t + 2r - 2 \geq p$ implying that we have a representation of $\mathbb{Z}/p\mathbb{Z}$ with $C \leq 1$. It remains to show that $|\sum_{i=0}^{s} E_i| \geq q$. By Theorem 2, we can say

$$\begin{aligned} |\sum_{i=0}^{s} E_i| &\geq \sum_{i=0}^{s} |E_i| - s \\ &= |E_0| + |E_1| + \sum_{i=2}^{s} |E_i| - s. \end{aligned}$$

Because of our new construction of the set A_1, we have $E_1 = h^{\wedge} B_1$ for $2 \leq h \leq k_1 - 2$. So by Theorem 5 we have

$$|E_1| = |h^{\wedge} B_1| \geq \min\{q,\ h(k_1) - h^2 + 1\}.$$

To find a lower bound on this inequality, we consider the minimum value of the quadratic expression $h(k_1) - h^2 + 1$ over the interval $2 \leq h \leq k_1 - 2$. Since the leading term is negative, the minimum will be either $h = 2$ or $h = k_1 - 2$. Both of these values of h result in the same value of $h(k_1) - h^2 + 1 = 2(k_1) - 3$, which for $k_1 \geq 4$ gives us $h(k_1) - h^2 + 1 = 2(k_1) - 3 \geq k_1 + 1$. Now we have

$$\begin{aligned} |\sum_{i=0}^{s} E_i| &\geq |E_0| + |E_1| + \sum_{i=2}^{s} |E_i| - s \\ &\geq |E_0| + (k_1 + 1) + \sum_{i=2}^{s} k_i - 1 - s, \end{aligned}$$

where we subtract one for a possible collapsed coefficient yielding $E_i = \{0\}$ for some $i \in \{2, \ldots, s\}$. Since we began with a set of $p + q - 2$ elements, we have

$p+q-2 = \sum_{i=0}^{s} k_i$, so

$$\begin{aligned} |\sum_{i=0}^{s} E_i| &\geq (k_0 + \hat{C}) + (k_1 + 1) + \sum_{i=2}^{s} k_i - 1 - s \\ &= p + q - 2 + \hat{C} - s \\ &\geq p + q - 2 + 1 - (p-1) \\ &= q, \end{aligned}$$

implying that we have all the elements in each of the cosets, and a nontrivial span of $G = \mathbb{Z}/pq\mathbb{Z}$.$\diamond$

We have now shown that for any value of $k_0 = |S \cap < \bar{p} > |$, a set of $p+q-2$ elements spans $G = \mathbb{Z}/pq\mathbb{Z}$ nontrivially, allowing us to establish the following.

Theorem 8 *Let $G = \mathbb{Z}/pq\mathbb{Z}$ be the finite abelian group of order pq where p and q are primes such that $p + \lfloor 2\sqrt{p-2} \rfloor + 1 < q < 2p$. Then $e(G) = p + q - 3$.*

Proof: Jerrold Griggs provided bounds for $e(G)$ for this setting in [5] in his Theorem 13:

$$p + q - 3 \leq e(G) \leq p + q - 2.$$

We consider four cases within the setting of $G = \mathbb{Z}/pq\mathbb{Z}$ for the described values of p, q. Using the notation defined in Section 4, we distinguish the four cases according to the value of k_0 which represents the size of the intersection of our set S with the subgroup of order q.

Case 1: $k_0 \geq \lfloor 2\sqrt{q-2} \rfloor$.

By Proposition 3 we see that a set $S \subseteq G$ of distinct nonzero elements with $|S| = p + q - 2$ spans G nontrivially.

Case 2: $3 \leq k_0 \leq \lfloor 2\sqrt{q-2} \rfloor$.

Proposition 4 implies that both key parts of the argument go through for a set of $p+q-2$ elements from $G \setminus \{0\}$. So such a set S in this case spans G nontrivially.

Case 3: $k_0 \leq 2$, and $k_i \leq 3$ for $1 \leq i \leq s$.

Proposition 5 proves that $p+q-2$ distinct nonzero elements is enough to obtain a nontrivial span of G.

Case 4: $k_0 \leq 2$, and $\max_{1 \leq i \leq s}\{k_i\} \geq 4$.

With the new construction of the set A_1, Proposition 6 yields a nontrivial span of G, given a set $S \subseteq G \setminus \{0\}$ of distinct elements with $|S| = p+q-2$.

Therefore by Griggs' bounds and the definition of $e(G)$, we have

$$e(G) = p+q-3.\diamond$$

6 CONCLUSION

We can now determine the value of $e(G)$ for all finite abelian groups G. However, further research is needed to determine the value of $e(G)$ where the group G is not abelian. It might also be interesting to examine the possible structures of subsets $S \subseteq G$ which realize $e(G)$ for a finite abelian group G. Griggs [5] constructs such a sequence in a specific group setting by arithmetic progression. This leads us to the question of whether such a construction will work in all settings where $e(G)$ is known.

In addition to his work concerning $e(G)$, Griggs [5] also studied the closely related invariant $w(G)$. The definition of $w(G)$ differs from that of $e(G)$ only in that a subset realizing $w(G)$ may include $\overline{0}$. While in most cases we have $w(G) = e(G) + 1$, for the case of $G = \mathbb{Z}/pq\mathbb{Z}$ as defined in Theorem 8 it remains to be shown.

Another related invariant is the strong Davenport constant $SD(G)$, introduced in 1999 by Chapman, Freeze, and Smith [1]. The strong Davenport constant gives the maximal cardinality of a sequence in G whose elements sum to zero, but no proper subsequence sums to zero. The value of $SD(\mathbb{Z}/m\mathbb{Z})$ is known for $1 \leq m \leq 24$, but $SD(G)$ is not generally known for other finite abelian groups. Currently the best known upper bound is given by $SD(G) \leq e(G) + 1$.

This bound is very good for small groups, and even sharp for some. However, as the order of G increases, so does the difference between these invariants. Further research is needed to determine the value of $SD(G)$ for larger groups G.

REFERENCES

[1] S. Chapman, M. Freeze, and W. Smith,"Minimal zero-sequences and the strong Davenport constant",*Discrete Mathematics*, V 203, 1999, 271-277.

[2] J. A. Dias da Silva and Y. O. Hamidoune, "Cyclic spaces for Grassman derivatives and additive theory", *Bull. London Math. Soc.*, V 26, 1994, 140-146.

[3] G. T. Diderrich, "An Adition Theorem for Abelian Groups of Order pq", *Journal of Number Theory*, V 7, 1975, 33-48.

[4] G. T. Diderrich and H. B. Mann, "Combinatorial problems in finite abelian groups", in *A Survey of Combinatorial Theory* (J. N. Srivastava, ed.), North-Holland, 1973, 95-100.

[5] J. R. Griggs, "Spanning subset sums for finite abelian groups", *Discrete Math.*,V 229, 2001, 89-99.

[6] H. B. Mann and Y. F. Wou, "An addition theorem for the elementary abelian group of type (p,p)", *Monatshefte für Math.*,V 102, 1986, 273-308.

[7] M. B. Nathanson, *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*, Springer-Verlag, New York, NY, 1996.

BIOGRAPHICAL SKETCH

Jennifer Susan Paceley Eyl was born in Wichita Falls, Texas, then lived in several other states before eventually making her way to North Carolina. It was in Boone, North Carolina where she obtained her B.S. in mathematics from Appalachian State University in 1996. After five years of learning and growing through international travel and people-oriented work, she returned to the world of academia. In 2001 she entered the graduate program in mathematics at the University of North Carolina at Wilmington, where she was fortunate enough to have the opportunity to work with Dr. Michael Freeze, her advisor and mentor.

Upon graduation in 2003, she hopes to work as a teacher on the college level while pursuing the continuation of her own education.