Journal of Number Theory 129 (2009) 1234–1245

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Minimum product set sizes in nonabelian groups of order pq

Alan Deckelbaum [*]

Department of Mathematics, Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge, MA 02139, USA

ARTICLE INFO

Article history:
Received 14 August 2007
Revised 5 February 2009
Available online 26 March 2009
Communicated by David Goss

Keywords:
Additive number theory
Cauchy–Davenport theorem
Product set
Nonabelian group

ABSTRACT

Let G be a nonabelian group of order pq, where p and q are distinct odd primes. We analyze the minimum product set cardinality $\mu_G(r,s) = \min|AB|$, where A and B range over all subsets of G of cardinalities r and s, respectively. In this paper, we completely determine $\mu_G(r,s)$ in the case where G has order $3p$ and conjecture that this result can be extended to all nonabelian groups of order pq. We also prove that for every nonabelian group of order pq there exist $1 \leqslant r, s \leqslant pq$ such that $\mu_G(r,s) > \mu_{\mathbb{Z}/pq\mathbb{Z}}(r,s)$.

1. Introduction

Let G be a group. This paper is concerned with the cardinality of the product set $AB = \{ab \mid a \in A, b \in B\}$, where A and B are finite subsets of G. In particular, given integers $1 \leqslant r, s \leqslant |G|$, we want to compute

$$\mu_G(r,s) = \min\bigl\{|AB|:\ A, B \subset G,\ |A| = r,\ |B| = s\bigr\}$$

as defined in [3]. The earliest such result is due independently to Cauchy [1] and Davenport [2], who computed $\mu_G(r,s)$ in the case that G is cyclic of prime order.

Eliahou, Kervaire, and Plagne [8] have generalized the Cauchy–Davenport theorem to compute $\mu_G(r,s)$ for all finite abelian groups G. In particular, they define a function $\kappa_G(r,s)$ that depends only on r, s, and the orders of subgroups of G, such that $\mu_G(r,s) = \kappa_G(r,s)$ for all finite abelian G. We discuss the function κ_G formally later in this paper.

[*] Fax: +1 610 649 6422.
E-mail address: deckel@mit.edu.

0022-314X/$ – see front matter © 2009 Elsevier Inc. All rights reserved.
doi:10.1016/j.jnt.2009.02.006

In [6], Eliahou and Kervaire explore the extent to which the relationship $\mu_G(r,s)=\kappa_G(r,s)$ holds for G finite but nonabelian. In many nonabelian groups, this relationship holds for all r and s. In [5], Eliahou and Kervaire mention an unpublished result that $\mu_G(r,s)$ always equals $\kappa_G(r,s)$ when G is a dihedral group. However, they prove by computer search that $\mu_G(6,9)>\kappa_G(6,9)$ when G is the nonabelian group of order 21 [6]. At the time, this was the only known group for which the relation $\mu_G(r,s)=\kappa_G(r,s)$ does not always hold.

In this paper, we study $\mu_G(r,s)$ when G is a nonabelian group of order pq, where p and q are distinct odd primes. The smallest such group, the nonabelian group of order 21, is the group mentioned in [6] for which the relation $\mu_G(r,s)=\kappa_G(r,s)$ does not always hold. We prove that for each nonabelian group of order pq there exist $1\leqslant r,s\leqslant pq$ such that $\mu_G(r,s)>\kappa_G(r,s)$, providing an infinite family of finite groups for which $\mu_G(r,s)$ does not always equal $\kappa_G(r,s)$. Furthermore, we completely determine $\mu_G(r,s)$ in the case that G is a nonabelian group of order $3p$. In this case,

$$\mu_G(r,s)=\begin{cases}\min\{f_d(r,s)\mid d\in\{1,p,3p\}\}, & \text{if } r,s>3 \text{ and } \lceil\frac{r}{3}\rceil+\lceil\frac{s}{3}\rceil<p;\\ \min\{f_d(r,s)\mid d\in\{1,3,p,3p\}\}, & \text{otherwise,}\end{cases}$$

where

$$f_d(r,s)=d\left(\left\lceil\frac{r}{d}\right\rceil+\left\lceil\frac{s}{d}\right\rceil-1\right).$$

We believe that our methods can be extended to completely determine $\mu_G(r,s)$ for all nonabelian groups G of order pq.

2. Definitions and supporting results

We begin with a formal definition of the product set of two subsets of a group.

Definition. Let G be a group, and let A and B be finite subsets of G. Then their *product set* is

$$AB=\{ab\mid a\in A,\ b\in B\}.$$

If G is abelian and written additively, we may also use the notation

$$A+B=\{a+b\mid a\in A,\ b\in B\}$$

and call it the *sumset* of A and B.

We are concerned with the minimum cardinality of the product set AB given the sizes of A and B. As mentioned in the introduction, we use the following definition from [3].

Definition. Let G be a group, and let r and s be integers with $1\leqslant r,s\leqslant|G|$. We define

$$\mu_G(r,s)=\min\bigl\{|AB|:\ A,B\subset G,\ |A|=r,\ |B|=s\bigr\}$$

and say that $A,B\subset G$ *realize* $\mu_G(r,s)$ if $|A|=r$, $|B|=s$, and $|AB|=\mu_G(r,s)$.

The function $\mu_G(r,s)$ has been extensively studied for certain groups. One of the earliest such results, the Cauchy–Davenport theorem, provides the minimum sumset size when G is cyclic of prime order. Written in terms of μ_G, the Cauchy–Davenport theorem can be stated as follows.

Theorem 1. *(Cauchy [1], Davenport [2].) Let G be the cyclic group of order p, where p is prime. Let r and s be integers with $1\leqslant r,s\leqslant p$. Then $\mu_G(r,s)=\min\{r+s-1,p\}$.*

A later result due to Vosper [10] characterizes many of the cases where $|A+B| = |A| + |B| - 1$ in cyclic groups of prime order. In our study of nonabelian groups of order pq, we will have frequent occasion to make use of Vosper's theorem, as all proper subgroups of groups of order pq are cyclic.

Theorem 2. *(Vosper [10].) Let p be a prime, and let A and B be subsets of $\mathbb{Z}/p\mathbb{Z}$. Assume that $|A| \geqslant 2$, $|B| \geqslant 2$, and $|A| + |B| < p$. Furthermore, suppose $|A+B| = |A| + |B| - 1$. Then A and B are arithmetic progressions with the same common difference.*

The function $\mu_G(r,s)$ has been studied in [3–8]. The authors of these papers introduce an arithmetic function $\kappa_G(r,s)$ that depends only on r, s, and the orders of subgroups of G. They then compare $\mu_G(r,s)$ to $\kappa_G(r,s)$ and describe several cases where these quantities are equal. We now define $\kappa_G(r,s)$ and two variants of this function, following the papers referenced above.

Definition. Let d, r, and s be positive integers. We define

$$f_d(r,s) = d\left(\left\lceil \frac{r}{d} \right\rceil + \left\lceil \frac{s}{d} \right\rceil - 1\right).$$

The functions $\kappa_G(r,s)$, $\mathcal{N}\kappa_G(r,s)$, and $\mathcal{D}\kappa_G(r,s)$ are defined as the minimum value of $f_d(r,s)$, where d ranges over certain sets of values that depend on the structure of G. (See [5] for a brief overview of these functions.)

Definition. Let G be a finite group. Let $\mathcal{D}(G)$ be the set of divisors of $|G|$, let $\mathcal{H}(G)$ be the set of orders of subgroups of G, and let $\mathcal{N}(G)$ be the set of orders of normal subgroups of G. Let r and s be integers between 1 and $|G|$, inclusive. We define

$$\kappa_G(r,s) = \min_{d \in \mathcal{H}(G)} f_d(r,s),$$
$$\mathcal{N}\kappa_G(r,s) = \min_{d \in \mathcal{N}(G)} f_d(r,s), \quad \text{and}$$
$$\mathcal{D}\kappa_G(r,s) = \min_{d \in \mathcal{D}(G)} f_d(r,s).$$

Notice that for all finite groups G and all $1 \leqslant r, s \leqslant |G|$, we have

$$\mathcal{D}\kappa_G(r,s) \leqslant \kappa_G(r,s) \leqslant \mathcal{N}\kappa_G(r,s),$$

since $\mathcal{N}(G) \subseteq \mathcal{H}(G) \subseteq \mathcal{D}(G)$.

In [8], Eliahou, Kervaire, and Plagne use the function $\kappa_G(r,s)$ to give a formula for $\mu_G(r,s)$ when G is finite abelian.

Theorem 3. *(Eliahou, Kervaire, Plagne [8].) Let G be a finite abelian group, and let $1 \leqslant r, s \leqslant |G|$. Then $\mu_G(r,s) = \kappa_G(r,s)$.*

Eliahou and Kervaire have recently shown that when G is finite nonabelian, the above result does not always hold. (See [6] for a survey of $\mu_G(r,s)$ for arbitrary finite nonabelian groups.) They have also obtained bounds on $\mu_G(r,s)$ when G is finite and solvable. We will make frequent use of these bounds in our study of nonabelian groups of order pq, as all groups of order pq are solvable.

Theorem 4. *(Eliahou, Kervaire [5].) Let G be a finite solvable group, and let $1 \leqslant r, s \leqslant |G|$. Then*

$$\mathcal{D}\kappa_G(r,s) \leqslant \mu_G(r,s) \leqslant \mathcal{N}\kappa_G(r,s).$$

While the relation $\mu_G(r,s) = \kappa_G(r,s)$ does not hold for all finite groups, under certain conditions on r and s one can show that $\mu_G(r,s) = \kappa_G(r,s)$ regardless of the structure of G. For instance, we have the following theorem.

Theorem 5. *(Eliahou, Kervaire [6].) Let G be a finite group. Let $1 \leqslant r, s \leqslant |G|$ such that $r + s = |G|$. Then $\mu_G(r,s) = \kappa_G(r,s)$.*

In this paper, we study the structure of groups of order pq in order to analyze small product sets. The main tool for this approach is the following theorem of Zemor, which restricts the subsets that we must consider when examining small product sets.

Theorem 6. *(Zemor [11].) Let G be a finite group and A a subset of G. If for every proper subgroup K of G*

$$|AK| \geqslant |A| + |K| - 1$$

and

$$|KA| \geqslant |A| + |K| - 1,$$

then for every subset B for which either $AB \neq G$ or $BA \neq G$, we have

$$|AB| \geqslant |A| + |B| - 1$$

and

$$|BA| \geqslant |A| + |B| - 1.$$

Zemor's theorem provides information about the structure of sets A and B that realize $\mu_G(r,s)$. The following theorem, due to Kemperman, gives us information about the structure of the product set AB given that $|AB|$ is small. In particular, it formalizes the notion that in order for AB to have low cardinality, each element of AB must be representable in many different ways as a product of an element of A and an element of B.

Theorem 7. *(Kemperman [9].) Let $C = AB$ be the product of two finite sets in G. If there exists an element $c \in C$ which can be written uniquely as $c = ab$ with $a \in A$ and $b \in B$, then*

$$|C| \geqslant |A| + |B| - 1.$$

We now use the above theorems to analyze $\mu_G(r,s)$ for G a nonabelian group of order pq.

3. Nonabelian groups of order *pq*

We begin with a description of nonabelian groups of order pq, where $p > q$ are distinct odd primes. Such a group exists if and only if $p \equiv 1 \pmod{q}$. There is only one nonabelian group of this order, up to isomorphism. It has the following presentation:

$$G = \langle x, y \mid x^q = y^p = 1,\ xyx^{-1} = y^n \rangle,$$

where n is a fixed integer such that $n \not\equiv 1 \pmod{p}$ and $n^q \equiv 1 \pmod{p}$. (While there might be more than one choice for n, all groups of order pq formed by this construction are isomorphic.) We notice that G is solvable, and that it contains p subgroups of order q. Let H be the subgroup of order q generated by x. All subgroups H' of order q are conjugate to H and are of the form $y^l H y^{-l}$ where $0 \leqslant l \leqslant p - 1$. Furthermore, G contains a single subgroup of order p, the normal subgroup $N = \langle y \rangle$.

Notation. For the rest of this paper, we will assume G is a nonabelian group of order pq. We will continue to use n for the integer in the definition of G such that $n \not\equiv 1 \pmod{p}$, $n^q \equiv 1 \pmod{p}$, and $xyx^{-1} = y^n$. We will let H refer to the subgroup of G generated by x, and we will let N be the subgroup generated by y.

Since all proper nontrivial subgroups of G are cyclic of prime order, we will frequently apply Theorem 2 in our analysis, and thus we will need to examine arithmetic progressions in cyclic groups of prime order. The following lemma proves that most arithmetic progressions in $\mathbb{Z}/p\mathbb{Z}$ have a unique common difference up to negation.

Lemma 8. *Let p be an odd prime, and let $S \subset \mathbb{Z}/p\mathbb{Z}$ be an arithmetic progression of length $2 \leqslant |S| \leqslant p-2$ with common difference d. Then S cannot also be an arithmetic progression of any common difference other than d and $-d$ modulo p.*

Proof. We may assume that $S = \{0, 1, 2, \dots, |S|-1\}$ by shifting the elements of S appropriately and then factoring out a common difference. We know that S is an arithmetic progression of difference d if and only if the equation $s \equiv t + d \pmod{p}$ has exactly one solution with $s \in S$ and $t \notin S$. Our goal is to show that $2 \leqslant |S| \leqslant p-2$ implies $d \equiv \pm 1$. We see that s and t also satisfy the equation $(s+1) \equiv (t+1) + d$. However, due to the uniqueness of s and t, it must be the case that either $s+1 \notin S$ or $t+1 \in S$. Similarly, we look at the equation $(s-1) \equiv (t-1) + d$ to conclude that either $s-1 \notin S$ or $t-1 \in S$.

We now have four cases. If $s+1 \notin S$ and $s-1 \notin S$, then $|S| = 1$ (as S is a set of consecutive elements of $\mathbb{Z}/p\mathbb{Z}$ and $s \in S$). If $t+1 \in S$ and $t-1 \in S$, then $|S| = p-1$ since $t \notin S$. If $s+1 \notin S$ and $t-1 \in S$, then it must be the case that s is the largest member of S (in other words, $S = \{0, 1, \dots, s\}$) and furthermore $t \equiv s+1$ (as this is the only possibility for $t \notin S$ and $t-1 \in S$). Thus, $d \equiv -1$. Similarly, if $t+1 \in S$ and $s-1 \notin S$, then $s \equiv 0$ (by the construction of S) and $t \equiv p-1$. Therefore $d \equiv 1$.

We therefore see that if $2 \leqslant |S| \leqslant p-2$, then S has a unique common difference (up to negation) in $\mathbb{Z}/p\mathbb{Z}$. □

When we analyze product sets in groups of order pq, we will need to obtain lower bounds on the sizes of particular sumsets in cyclic groups. Lemma 9 uses Theorem 6 and Lemma 8 to obtain a lower bound on a particular sumset in $\mathbb{Z}/p\mathbb{Z}$, which is stronger than the bound obtained by using the Cauchy–Davenport theorem alone.

Lemma 9. *Let p and q be odd primes. Let $A_0, A_1, \dots, A_{q-1}$, and B be subsets of $\mathbb{Z}/p\mathbb{Z}$ such that $|A_0| + |A_1| + \dots + |A_{q-1}| = u$ and $|B| = v > 1$. Assume that $u > q$, $u \not\equiv 1 \pmod{q}$, and $\lceil \frac{u}{q} \rceil + v < p$. Let $n \not\equiv 1 \pmod{p}$ be such that $n^q \equiv 1 \pmod{p}$. Then*

$$\left|(A_0 + B) \cup (A_1 + nB) \cup \left(A_2 + n^2 B\right) \cup \dots \cup \left(A_{q-1} + n^{q-1} B\right)\right| \geqslant \left\lceil \frac{u}{q} \right\rceil + v.$$

Proof. We may assume that $(A_0 + B) \cup \dots \cup (A_{q-1} + n^{q-1} B) \neq \mathbb{Z}/p\mathbb{Z}$ since $\lceil \frac{u}{q} \rceil + v < p$. Choose A_i with maximum cardinality. By the Cauchy–Davenport theorem, $|A_i + n^i B| \geqslant |A_i| + |n^i B| - 1 = |A_i| + v - 1$. If $|A_i| \geqslant \lceil \frac{u}{q} \rceil + 1$, then $|A_i + n^i B| \geqslant \lceil \frac{u}{q} \rceil + v$, and we are done. We may therefore assume that $|A_i| = \lceil \frac{u}{q} \rceil$ and that $|A_i + n^i B| = \lceil \frac{u}{q} \rceil + v - 1$. Since $|A_i| \neq 1$ (as $u > q$) and $|A_i| + v < p$, we conclude by Theorem 2 that A_i and $n^i B$ must be arithmetic progressions with the same common difference. As $n^i B$ is an arithmetic progression, so is B. Let the common difference of B be d. Then the common difference of the arithmetic progressions $n^i B$, A_i, and $A_i + n^i B$ is $n^i d$.

Since $u \not\equiv 1 \pmod q$, we can find A_j, $j \neq i$, with $|A_j| = |A_i| = \lceil \frac{u}{q} \rceil$. By a similar argument to that above, we are done unless $A_j + n^j B$ is an arithmetic progression with common difference $n^j d$. Notice that $n^i d \not\equiv \pm n^j d \pmod p$, since no power of n is congruent to -1 modulo p. However, since

$$2 \leqslant \left\lceil \frac{u}{q} \right\rceil + v - 1 \leqslant p - 2,$$

we apply Lemma 8 to conclude that $A_i + n^i B \neq A_j + n^j B$. Since these sets have the same cardinality of $\lceil \frac{u}{q} \rceil + v - 1$ yet are not equal, we conclude that $|(A_i + n^i B) \cup (A_j + n^j B)| \geqslant \lceil \frac{u}{q} \rceil + v$. □

In order to determine $\mu_G(r,s)$ for nonabelian groups of order pq, we will analyze several possible scenarios. One such case is slightly more involved than the others, so we discuss this scenario in the lemma below. (Recall the notation established earlier which we will use when referring to nonabelian groups of order pq.) In particular, we analyze the possibility that A and B each have the form of a union of cosets of N with at most $p-2$ elements removed from these cosets. In other words, $|AN| \leqslant |A| + p - 2$ and $|BN| \leqslant |B| + p - 2$. (Since N is normal, it does not matter whether we discuss left or right cosets.)

Lemma 10. *Let A and B be subsets of G such that $|AN| \leqslant |A| + |N| - 2$ and $|BN| \leqslant |B| + |N| - 2$. Then $|AB| \geqslant \min\{f_1(|A|,|B|), f_p(|A|,|B|), pq\}$.*

Proof. Since N is normal, we see that $|BN| = |NB|$. Therefore, there exist $N_1, \ldots, N_u \subseteq N$ and $N'_1, \ldots, N'_v \subseteq N$ with $\sum_{i=1}^{u} |N \backslash N_i| \leqslant p - 2$ and $\sum_{j=1}^{v} |N \backslash N'_j| \leqslant p - 2$ such that

$$A = x^{m_1} N_1 \cup x^{m_2} N_2 \cup \cdots \cup x^{m_u} N_u \quad \text{and} \quad B = N'_1 x^{m'_1} \cup N'_2 x^{m'_2} \cup \cdots \cup N'_v x^{m'_v},$$

where $|A| = r$, $|B| = s$, $u = \lceil \frac{r}{p} \rceil$, and $v = \lceil \frac{s}{p} \rceil$. (All m_i are distinct modulo q and all m'_j are distinct modulo q.) Our goal is to show that $|AB| \geqslant \min\{f_1(r,s), f_p(r,s), pq\}$.

We first examine the case u = 1. If all $1 \leqslant j \leqslant v$ satisfy $N_1 N'_j = N$, then AB is a union of $v = \lceil \frac{s}{p} \rceil$ cosets of N. Hence

$$|AB| = p\left\lceil \frac{s}{p} \right\rceil = p\left(\left\lceil \frac{s}{p} \right\rceil + \left\lceil \frac{r}{p} \right\rceil - 1\right) = f_p(r,s).$$

Assume that for some $1 \leqslant w \leqslant v$ it is the case that $N_1 N'_w \neq N$. Without loss of generality, say $N_1 N'_v \neq N$. Then (by applying the Cauchy–Davenport theorem to $N_1 N'_v$, where N_1 and N'_v are viewed as subsets of $N \cong \mathbb{Z}/p\mathbb{Z}$) we obtain

$$|AB| = \sum_{j=1}^{v} |N_1 N'_j| \geqslant \left(\sum_{j=1}^{v-1} |N'_j|\right) + |N_1 N'_v| \geqslant \left(\sum_{j=1}^{v-1} |N'_j|\right) + \left(|N_1| + |N'_v| - 1\right) = r + s - 1 = f_1(r,s).$$

This concludes the case $u = 1$. The case $v = 1$ is analogous.

We now consider the case $u, v \geqslant 2$. Without loss of generality, assume that N_u has minimum cardinality among all N_i and N'_j. Let

$$\bar{A} = x^{m_1} N_1 \cup x^{m_2} N_2 \cup \cdots \cup x^{m_{u-1}} N_{u-1}.$$

We now claim that $\bar{A}B$ is a union of cosets of N. It suffices to show that for all $1 \leqslant i \leqslant u-1$ and for all $1 \leqslant j \leqslant v$, it is true that $N_i N'_j = N$. Notice that

$$|N_i| + |N'_j| \geqslant |N_i| + |N_u| \geqslant 2p - (p-2) = p + 2,$$

where $|N_i| + |N_u| \geqslant p+2$ follows from the formula $\sum_{k=1}^{u} |N \backslash N_k| \leqslant p-2$. Since $|N_i| + |N'_j| \geqslant p+2$, we conclude by the Cauchy–Davenport theorem that $N_i N'_j = N$. Therefore, $\bar{A}B$ is a union of cosets of N.

From the Cauchy–Davenport theorem applied to $G/N \cong \mathbb{Z}/q\mathbb{Z}$, we see that $|\bar{A}B/N| \geqslant \min\{(u-1)+v-1, q\}$. If $|\bar{A}B/N| = q$, then (as $\bar{A}B$ is a union of cosets of N) we have

$$|AB| \geqslant |\bar{A}B| = pq,$$

and we are done. Therefore, we may assume $|\bar{A}B/N| < q$. Furthermore, if $|\bar{A}B/N| \geqslant u+v-1$, then

$$|AB| \geqslant |\bar{A}B| \geqslant p(u+v-1) = p\left(\left\lceil \frac{r}{p} \right\rceil + \left\lceil \frac{s}{p} \right\rceil - 1\right) = f_p(r,s).$$

Therefore the only remaining possibility is that $|\bar{A}B/N| = u+v-2$ and that $u+v-2 < q$. By applying the Cauchy–Davenport theorem to AB/N, we conclude

$$|AB/N| \geqslant \min\{u+v-1, q\} = u+v-1 > |\bar{A}B/N|.$$

Thus, there is some $N'_j x^{m'_j} \subset B$ such that $(x^{m_u} N_u)(N'_j x^{m'_j}) \not\subset \bar{A}B$, and thus $(x^{m_u} N_u)(N'_j x^{m'_j}) \cap \bar{A}B = \emptyset$. Therefore

$$|AB| \geqslant |\bar{A}B| + \left|N_u N'_j\right| \geqslant p(u+v-2) + \min\left\{|N_u| + \left|N'_j\right| - 1, p\right\}.$$

Assume without loss of generality that N'_v has minimum cardinality among the N'_j. Let $m(r)$ and $m(s)$ be the smallest positive integers congruent to r and s modulo p, respectively. In particular, we notice that $|N_u| \geqslant m(r)$ and $|N'_v| \geqslant m(s)$ (with equality only when $|N_i| = p$ for all $i \neq u$ and $|N'_j| = p$ for all $j \neq v$). We have the identity

$$p\left(\left\lceil \frac{r}{p} \right\rceil + \left\lceil \frac{s}{p} \right\rceil\right) = r + s + 2p - m(r) - m(s).$$

We now obtain the bound

$$\begin{aligned} |AB| &\geqslant p(u+v-2) + \min\left\{|N_u| + \left|N'_v\right| - 1, p\right\} \\ &\geqslant p\left(\left\lceil \frac{r}{p} \right\rceil + \left\lceil \frac{s}{p} \right\rceil - 2\right) + \min\left\{m(r) + m(s) - 1, p\right\} \\ &= \min\left\{f_1(r,s), f_p(r,s)\right\}. \end{aligned}$$

We therefore conclude that $|AB| \geqslant \min\{f_1(r,s), f_p(r,s), pq\}$. □

We are now ready to begin computing $\mu_G(r,s)$ in nonabelian groups of order pq. We first obtain a lower bound on $\mu_G(r,s)$, using the results of [5].

Lemma 11. *For all $1 \leqslant r, s \leqslant pq$, $\mu_G(r,s) \geqslant \kappa_G(r,s)$.*

Proof. The only divisors of pq are 1, q, p, and pq. We know that G contains a subgroup of each of these cardinalities, and thus $\mathcal{D}\kappa_G(r,s) = \kappa_G(r,s)$. From Theorem 4, we conclude that $\kappa_G(r,s) \leqslant \mu_G(r,s)$. □

We are now at the main theorem of this paper. We will prove that $\mu_G(r,s) = \mathcal{N}\kappa_G(r,s)$ for r and s that satisfy several conditions. The proof centers on obtaining a stronger lower bound on $\mu_G(r,s)$ than that of Lemma 11. In particular, we perform a careful case analysis to prove that when r and s meet specified criteria, the inequality $\mu_G(r,s) \geqslant \mathcal{N}\kappa_G(r,s)$ always holds.

Theorem 12. *Let G be a nonabelian group of order pq, where $p > q$ are odd primes with $p \equiv 1 \pmod q$. Let $q+1 \leqslant r, s \leqslant pq$ such that $\lceil \frac{r}{q} \rceil + \lceil \frac{s}{q} \rceil < p$. Furthermore, suppose r and s are both congruent to either* 0 *or $q-1$ modulo q, with at least one of them 0 modulo q. Then $\mu_G(r,s) = \mathcal{N}\kappa_G(r,s)$.*

Proof. We know from Theorem 4 that $\mu_G(r,s) \leqslant \mathcal{N}\kappa_G(r,s)$. All that remains is to prove that $\mu_G(r,s) \geqslant \mathcal{N}\kappa_G(r,s)$. If $\mu_G(r,s) \geqslant f_1(r,s)$, then we are done since $f_1(r,s) \geqslant \mathcal{N}\kappa_G(r,s)$, so assume $\mu_G(r,s) < r+s-1$. Similarly, assume $\mu_G(r,s) < pq$.

Let A and B be subsets of G that realize $\mu_G(r,s)$. By Theorem 6 there exists a proper subgroup K_A of G such that either $|K_A A| < |K_A| + r - 1$ or $|AK_A| < |K_A| + r - 1$. Similarly, there is a proper subgroup K_B of G such that either $|K_B B| < |K_B| + s - 1$ or $|BK_B| < |K_B| + s - 1$. Each of K_A and K_B have order either p or q.

Consider first the case $K_A = K_B = N$. Since $|AN| = |NA|$ and $|BN| = |NB|$, we have $|AN| < p+r-1$ and $|BN| < p+s-1$. We then apply Lemma 10 to conclude that $\mu_G(r,s) \geqslant \min\{f_1(r,s), f_p(r,s), pq\}$.

The remainder of this proof will show that $K_B \neq N$ implies $|AB| \geqslant \mathcal{N}\kappa_G(r,s)$. By the symmetries $|AB| = |B^{-1}A^{-1}|$ and $\mu_G(r,s) = \mu_G(s,r)$, the same arguments can be used to show that $K_A \neq N$ implies $|AB| \geqslant \mathcal{N}\kappa_G(r,s)$. Therefore, it suffices to show that if there exists a subgroup H' of order q such that either $|BH'| < q+s-1$ or $|H'B| < q+s-1$, then it follows that $|AB| \geqslant \mathcal{N}\kappa_G(r,s)$. By conjugating A and B by an appropriate power of y, we may assume without loss of generality that $H' = H$.

We first examine the possibility that $|BH| < q+s-1$. Since $s \equiv 0 \pmod q$ or $s \equiv q-1 \pmod q$, we see that by inserting at most one element to B we can obtain a union of left cosets of H. Thus, for some $\bar{H} \subseteq H$ with $|\bar{H}| \geqslant q-1$, it is the case that

$$B = y^{k_1}\bar{H} \cup y^{k_2}H \cup \cdots \cup y^{k_u}H,$$

where $u = \lceil \frac{s}{q} \rceil \geqslant 2$ and all k_i are distinct modulo p. We will first argue that AB must be a union of left cosets of H. This is obvious if $\bar{H} = H$, so we assume for the moment that $|\bar{H}| = q-1$. Pick an element $y^i x^j \in A$ arbitrarily. It suffices to show that $y^i x^j \cdot y^{k_1} H \subset AB$. Consider the possibility that $y^i x^j$ is the unique element $a_0 \in A$ such that $a_0 B \cap y^i x^j y^{k_1} H \neq \emptyset$. Then each element in $y^i x^j y^{k_1} \bar{H} \subset AB$ is written uniquely as $a_0 b_0$ with $a_0 \in A$, $b_0 \in B$, which implies $|AB| \geqslant r+s-1$ by Theorem 7 and contradicts our assumption about the size of AB. Therefore, there exists a $y^f x^g \in A$ with $y^f x^g \neq y^i x^j$ such that $y^f x^g B \cap y^i x^j y^{k_1} H \neq \emptyset$. Thus, for some coset $y^{k_c} H$ with $y^{k_c} H \cap B \neq \emptyset$ we have $y^f x^g y^{k_c} H \cap y^i x^j y^{k_1} H \neq \emptyset$. Since distinct left cosets are disjoint, this implies $y^f x^g y^{k_c} H = y^i x^j y^{k_1} H$. If $y^{k_c} H \subset B$, then clearly $y^i x^j y^{k_1} H = y^f x^g y^{k_c} H \subset AB$. Therefore, the only remaining possibility is that $y^{k_c} H = y^{k_1} H$ and hence $y^f x^g y^{k_1} H = y^i x^j y^{k_1} H$. Let h be the element in H which is not in $\bar{H}$. Then $y^i x^j y^{k_1} \bar{H}$ contains all of $y^i x^j y^{k_1} H$ except for $y^i x^j y^{k_1} h$. Similarly, $y^f x^g y^{k_1} \bar{H}$ contains all of $y^i x^j y^{k_1} H$ except for $y^f x^g y^{k_1} h$. As $y^f x^g \neq y^i x^j$, we see that $y^f x^g y^{k_1} h \neq y^i x^j y^{k_1} h$, and therefore AB contains $y^i x^j y^{k_1} \bar{H} \cup y^f x^g y^{k_1} \bar{H} = y^i x^j y^{k_1} H$. Thus, AB is a union of left cosets of H.

We now count the number of left cosets of H that are contained in AB. We define sets $C_0, C_1, \ldots, C_{q-1}$, and D, which are subsets of $\mathbb{Z}/p\mathbb{Z}$:

$$C_j = \{ i \mid y^i x^j \in A \}, \qquad D = \{ w \mid y^w H \cap B \neq \emptyset \}.$$

Notice that $y^i x^j \cdot y^w H = y^{i+n^j w} H$. Thus, the number of left cosets of H which are contained in AB is the number of distinct values of $i + n^j w \pmod p$, where $i \in C_j$ and $w \in D$, which is

$$\left| (C_0 + D) \cup (C_1 + nD) \cup (C_2 + n^2 D) \cup \cdots \cup (C_{q-1} + n^{q-1} D) \right|.$$

We see that $|D| = \lceil \frac{s}{q} \rceil \geqslant 2$. Also, $|C_0| + |C_1| + \cdots + |C_{q-1}| = r$. We recall our assumption in the statement of the theorem that $\lceil \frac{r}{q} \rceil + \lceil \frac{s}{q} \rceil < p$. Furthermore, since r is either 0 or $q-1$ modulo q and q is odd, we observe that $r \not\equiv 1 \pmod q$. We now apply Lemma 9 to conclude that AB contains at least $\lceil \frac{r}{q} \rceil + \lceil \frac{s}{q} \rceil$ cosets of H. Thus,

$$|AB| \geqslant q\left(\left\lceil \frac{r}{q} \right\rceil + \left\lceil \frac{s}{q} \right\rceil\right) \geqslant r + s > f_1(r,s) \geqslant \mathcal{N}\kappa_G(r,s).$$

We now analyze the case $|HB| < q + s - 1$. Since s is either 0 or $q-1$ modulo q, it is possible to insert at most one additional element to B and obtain a union of right cosets of H. Thus, for some $\bar{H} \subseteq H$ with $|\bar{H}| \geqslant q-1$, it is the case that

$$B = \bar{H}y^{b_1} \cup Hy^{b_2} \cup Hy^{b_3} \cup \cdots \cup Hy^{b_v},$$

where all b_i are distinct modulo p and $v = \lceil \frac{s}{q} \rceil \geqslant 2$. We will write all of the elements of A in the form $y^a x^m$. We observe

$$\left(y^a x^m\right)\left(Hy^b\right) = y^a H y^b = \left\{y^{a+b}, y^{a+nb}x, y^{a+n^2 b}x^2, \ldots, y^{a+n^{q-1}b}x^{q-1}\right\}.$$

We now define the following two subsets of $\mathbb{Z}/p\mathbb{Z}$:

$$C = \left\{a \mid y^a x^m \in A \text{ for some } m \in \mathbb{Z}/q\mathbb{Z}\right\}, \qquad D = \left\{b \mid Hy^b \subset B\right\}.$$

Consider first the case $s \equiv 0 \pmod q$. Then $\bar{H} = H$, and hence

$$|AB| = |C + D| + |C + nD| + \left|C + n^2 D\right| + \cdots + \left|C + n^{q-1} D\right|,$$

which is obtained by counting the number of elements of the form $y^i x^0 \in AB$, then elements of the form $y^i x^1 \in AB$, and so on.

We notice $|C| \geqslant \lceil \frac{r}{q} \rceil \geqslant 2$ and $|D| = \lceil \frac{s}{q} \rceil \geqslant 2$. We assume $|C| + |D| \leqslant p$, since otherwise $|AB| = pq$. By the hypothesis in the statement of the theorem, we recall that $\lceil \frac{r}{q} \rceil + \lceil \frac{s}{q} \rceil - 1 \leqslant p - 2$. In particular, by the Cauchy–Davenport theorem we conclude that $|C + n^i D| \geqslant \lceil \frac{r}{q} \rceil + \lceil \frac{s}{q} \rceil - 1$, with equality possible (by Vosper's Theorem) only if C and $n^i D$ have sizes $\lceil \frac{r}{q} \rceil$ and $\lceil \frac{s}{q} \rceil$, respectively, and are arithmetic progressions with the same common difference. However, by Lemma 8, C can have a common difference with at most one of the sets $n^i D$, since $|C| \leqslant p - |D| \leqslant p - 2$. Therefore

$$|AB| \geqslant \left(\left\lceil \frac{r}{q} \right\rceil + \left\lceil \frac{s}{q} \right\rceil - 1\right) + (q-1)\left(\left\lceil \frac{r}{q} \right\rceil + \left\lceil \frac{s}{q} \right\rceil\right) = q\left(\left\lceil \frac{r}{q} \right\rceil + \left\lceil \frac{s}{q} \right\rceil\right) - 1 \geqslant r + s - 1 = f_1(r,s).$$

Now consider the case $s \equiv q - 1 \pmod q$. Then $r \equiv 0 \pmod q$ by a hypothesis of the theorem. We therefore have two possibilities: either $|C| = \frac{r}{q}$ and A is a union of left cosets of H, or instead $|C| > \frac{r}{q}$. If A is a union of left cosets of H, then the same argument as when B is a union of right cosets of H can be applied to conclude that $|AB| \geqslant f_1(r,s)$. We will therefore consider the case $|C| \geqslant \lceil \frac{r}{q} \rceil + 1$. Notice that $|D| = \lceil \frac{s}{q} \rceil - 1$. We have the inequality

$$|AB| \geqslant |C + D| + |C + nD| + \left|C + n^2 D\right| + \cdots + \left|C + n^{q-1} D\right|.$$

If $|C| \geqslant \lceil \frac{r}{q} \rceil + 2$, then

$$\begin{aligned}|AB| &\geqslant \min\left\{q\left(\left\lceil \frac{r}{q} \right\rceil + 2 + \left\lceil \frac{s}{q} \right\rceil - 1 - 1\right), qp\right\}\\ &\geqslant \min\{r+s, pq\}\\ &\geqslant \min\bigl\{f_1(r,s), pq\bigr\}.\end{aligned}$$

The only remaining possibility is $|C| = \lceil \frac{r}{q} \rceil + 1$. Thus, r is congruent to 0 modulo q, and A contains elements from exactly $\frac{r}{q} + 1$ left cosets of H. We have

$$A = y^{c_1} H_1 \cup y^{c_2} H_2 \cup \cdots \cup y^{c_u} H_u,$$

where $H_i \subseteq H$, $\sum_{i=1}^{u} |H_i| = r$, $1 \leqslant |H_i| \leqslant q$, and $u = \lceil \frac{r}{q} \rceil + 1$. In particular, we notice that at most one H_i can have size exactly 1. Without loss of generality, assume $|H_i| \geqslant 2$ for all $i \geqslant 2$. Thus, for all $i \geqslant 2$ we have $H_i \bar{H} = H$, since $|\bar{H}| = q - 1$. Therefore, we let

$$D' = \bigl\{b \bigm| \bar{H} y^b \subset B\bigr\}$$

and notice that

$$|AB| \geqslant |C + D'| + |C + nD'| + \cdots + \bigl|C + n^{q-1} D'\bigr| - 1,$$

with the -1 term to account for the fact that $|H_1 \bar{H}|$ might have size $q-1$ instead of q. Since $|D'| = \lceil \frac{s}{q} \rceil$, we compute

$$\begin{aligned}|AB| &\geqslant \min\bigl\{q\bigl(|C| + |D'| - 1\bigr) - 1, qp - 1\bigr\}\\ &\geqslant \min\left\{q\left(\left\lceil \frac{r}{q} \right\rceil + 1 + \left\lceil \frac{s}{q} \right\rceil - 1\right) - 1, pq - 1\right\}\\ &\geqslant \min\{r+s-1, pq-1\}.\end{aligned}$$

Since $\lceil \frac{r}{q} \rceil + \lceil \frac{s}{q} \rceil < p$, we have that $q(\lceil \frac{r}{q} \rceil + \lceil \frac{s}{q} \rceil) < qp$, and hence $r + s < qp$. Thus, $f_1(r,s) = r + s - 1 < qp - 1$. We therefore see that $|AB| \geqslant f_1(r,s)$. □

Theorem 12 provides the value of $\mu_G(r,s)$ for many r and s. In particular, these values suffice to demonstrate that in all nonabelian groups of order pq there exist $1 \leqslant r, s \leqslant pq$ with $\mu_G(r,s) > \kappa_G(r,s)$. This improves upon the calculations in [6], where Eliahou and Kervaire use a computer search to provide a single example of a group G where $\mu_G(r,s)$ does not always equal $\kappa_G(r,s)$.

Theorem 13. *Let G be a nonabelian group of order pq, where $p > q$ are odd primes and $p \equiv 1 \pmod{q}$. Then there exist $1 \leqslant r, s \leqslant pq$ such that $\mu_G(r,s) > \kappa_G(r,s)$.*

Proof. From Theorem 12, it suffices to find $q + 1 \leqslant r, s \leqslant pq$ such that $r, s \equiv 0 \pmod{q}$, $\lceil \frac{r}{q} \rceil + \lceil \frac{s}{q} \rceil < p$, and $\mathcal{N}\kappa_G(r,s) > \kappa_G(r,s)$. Set $r = 2q$ and $s = 3q$. Then $\lceil \frac{r}{q} \rceil + \lceil \frac{s}{q} \rceil = 5 < p$. Furthermore, $f_q(2q, 3q) = 4q$, which is strictly less than $f_1(2q, 3q) = 5q - 1$ and $f_{pq}(2q, 3q) = pq$. All that remains is to show that $f_q(r,s) < f_p(r,s)$. Since $p \equiv 1 \pmod{q}$, we know that $p = mq + 1$, where m is even. If $m = 2$, then $f_p(2q, 3q) = p + 2p - p = 4q + 2 > f_q(2q, 3q)$. If $m > 2$, then $p \geqslant 4q + 1$, and hence $f_p(2q, 3q) = p \geqslant 4q + 1 > f_q(2q, 3q)$. Therefore $\mathcal{N}\kappa_G(2q, 3q) > \kappa_G(2q, 3q)$, and thus $\mu_G(2q, 3q) > \kappa_G(2q, 3q)$. □

Theorem 12 is our main tool for completely determining $\mu_G(r,s)$ when G is a nonabelian group of order $3p$. Before we can do this, however, it remains to calculate $\mu_G(r,s)$ in the cases where Theorem 12 does not apply. In particular, it is straightforward to calculate $\mu_G(r,s)$ when either $\lceil \frac{r}{q} \rceil + \lceil \frac{s}{q} \rceil \geqslant p$ or when $\min\{r,s\} \leqslant q$. We begin by considering the possibility that $\lceil \frac{r}{q} \rceil + \lceil \frac{s}{q} \rceil \geqslant p$.

Lemma 14. *Let $q+1 \leqslant r, s \leqslant pq$ such that $\lceil \frac{r}{q} \rceil + \lceil \frac{s}{q} \rceil \geqslant p$. Then $\mu_G(r,s) = \kappa_G(r,s)$.*

Proof. Consider first the case $\lceil \frac{r}{q} \rceil + \lceil \frac{s}{q} \rceil = p$. Then $f_q(r,s) = pq - q$. Let $r' = q\lceil \frac{r}{q} \rceil$ and $s' = q\lceil \frac{s}{q} \rceil$. We have $r' \geqslant r$, $s' \geqslant s$, and $f_q(r,s) = f_q(r',s')$. Furthermore, $r' + s' = pq$. By Theorem 5, there exist subsets A' and B' of G with $|A'| = r'$, $|B'| = s'$, and $|A'B'| \leqslant f_q(r',s')$. We pick A to be an arbitrary subset of A' of size r and B to be an arbitrary subset of B' of size s. Then $|AB| \leqslant |A'B'| \leqslant f_q(r',s') = f_q(r,s)$. Thus, $\mu_G(r,s) \leqslant f_q(r,s)$. Since $\mu_G(r,s) \leqslant \mathcal{N}\kappa_G(r,s)$ by Theorem 4, we have

$$\mu_G(r,s) \leqslant \min\{f_q(r,s), \mathcal{N}\kappa_G(r,s)\} = \kappa_G(r,s).$$

Since $\mu_G(r,s) \geqslant \kappa_G(r,s)$ by Lemma 11, we conclude $\mu_G(r,s) = \kappa_G(r,s)$.

Finally, consider the case $\lceil \frac{r}{q} \rceil + \lceil \frac{s}{q} \rceil > p$. Then $f_q(r,s) \geqslant pq = f_{pq}(r,s)$, and hence $\kappa_G(r,s) = \mathcal{N}\kappa_G(r,s)$. By Theorem 4 and Lemma 11, we conclude $\mu_G(r,s) = \kappa_G(r,s)$. □

We now show that if either r or s is at most q then $\mu_G(r,s) = \kappa_G(r,s)$.

Lemma 15. *Let $1 \leqslant r, s \leqslant pq$ such that at least one of r or s is at most q. Then $\mu_G(r,s) = \kappa_G(r,s)$.*

Proof. By Theorem 4 and Lemma 11, it suffices to find sets A and B with $|A| = r$, $|B| = s$, and $|AB| \leqslant f_q(r,s)$. Without loss of generality, assume $r \leqslant q$. Take A to be a subset of H with $|A| = r$. Let B be a set of s elements contained in the union of no more than $\lceil \frac{s}{q} \rceil$ right cosets of H, so $B \subseteq Hy^{k_1} \cup Hy^{k_2} \cup \cdots \cup Hy^{k_v}$ where $v = \lceil \frac{s}{q} \rceil$. Then $AB \subseteq Hy^{k_1} \cup Hy^{k_2} \cup \cdots \cup Hy^{k_v}$, so

$$|AB| \leqslant q\left\lceil \frac{s}{q} \right\rceil = q\left(\left\lceil \frac{r}{q} \right\rceil + \left\lceil \frac{s}{q} \right\rceil - 1\right) = f_q(r,s)$$

and therefore $\mu_G(r,s) = \kappa_G(r,s)$. □

The combination of Theorem 12, Lemma 14, and Lemma 15 enables us to compute $\mu_G(r,s)$ for many values of r and s. In particular, these three results allow us to completely determine $\mu_G(r,s)$ in the case that G is a nonabelian group of order $3p$. This provides a complete description of $\mu_G(r,s)$ for an infinite family of finite groups G for which the relation $\mu_G(r,s) = \kappa_G(r,s)$ does not always hold. Previously, only a single such group G was known for which $\mu_G(r,s)$ is not always equal to $\kappa_G(r,s)$.

Theorem 16. *Let G be a nonabelian group of order $3p$, where $p > 3$ is prime. Let $1 \leqslant r, s \leqslant 3p$. Then*

$$\mu_G(r,s) = \begin{cases} \mathcal{N}\kappa_G(r,s), & \text{if } r, s > 3 \text{ and } \lceil \frac{r}{3} \rceil + \lceil \frac{s}{3} \rceil < p; \\ \kappa_G(r,s), & \text{otherwise.} \end{cases}$$

Proof. The second case follows from Lemma 14 and Lemma 15. When $r, s > 3$ and $\lceil \frac{r}{3} \rceil + \lceil \frac{s}{3} \rceil < p$, if one of r or s is congruent to 0 modulo 3 and the other is congruent to either 0 or 2 modulo 3, then the equation $\mu_G(r,s) = \mathcal{N}\kappa_G(r,s)$ follows from Theorem 12. Otherwise,

$$f_3(r,s) = 3\left(\left\lceil \frac{r}{3} \right\rceil + \left\lceil \frac{s}{3} \right\rceil - 1\right) \geqslant r + s + 2 - 3 = f_1(r,s),$$

and hence $\kappa_G(r,s) = \mathcal{N}\kappa_G(r,s)$. The equality $\mu_G(r,s) = \mathcal{N}\kappa_G(r,s)$ then follows from Theorem 4 and Lemma 11. □

4. Future work

The techniques employed in Theorem 12 led to a complete determination of $\mu_G(r,s)$ when G is a nonabelian group of order $3p$. In this theorem, we placed a restriction on r and s, namely that one of the values was 0 modulo q and the other was either 0 or $q-1$ modulo q. We conjecture that Theorem 12 can be extended to remove this condition. Specifically, we believe that Theorem 12 can be extended to prove the following analogue of Theorem 16:

Conjecture 17. *Let G be a nonabelian group of order pq, where $p > q$ are odd primes. Let $1 \leqslant r, s \leqslant pq$. Then*

$$\mu_G(r,s) = \begin{cases} \mathcal{N}\kappa_G(r,s), & \textit{if } r, s > q \textit{ and } \lceil \frac{r}{q} \rceil + \lceil \frac{s}{q} \rceil < p; \\ \kappa_G(r,s), & \textit{otherwise.} \end{cases}$$

We notice that in nonabelian groups of order $3p$, $\mu_G(r,s)$ is always equal to either $\kappa_G(r,s)$ or $\mathcal{N}\kappa_G(r,s)$. This leads us to two further open questions:

(1) For all finite solvable groups G and all $1 \leqslant r, s \leqslant |G|$, is it the case that $\mu_G(r,s) = f_d(r,s)$ for some $d \in \mathcal{H}(G)$? (This was previously conjectured in [6].)

(2) Are there examples of finite solvable groups G and $1 \leqslant r, s \leqslant |G|$ where $\mu_G(r,s)$ is equal to neither $\kappa_G(r,s)$ nor $\mathcal{N}\kappa_G(r,s)$?

Acknowledgments

I would like to thank Joe Gallian for bringing this problem to my attention and for his many helpful suggestions. I would also like to thank Reid Barton and Ricky Liu for their advice and for their careful editing of this paper.

This research was done at the University of Minnesota Duluth supported by the National Science Foundation (grant number DMS-0447070-001) and the National Security Agency (grant number H98230-06-1-0013).

References

[1] A. Cauchy, Recherches sur les nombres, J. École Polytech. 9 (1813) 99–123.
[2] H. Davenport, On the addition of residue classes, J. London Math. Soc. 10 (1935) 30–32.
[3] S. Eliahou, M. Kervaire, Sumsets in vector spaces over finite fields, J. Number Theory 71 (1998) 12–39.
[4] S. Eliahou, M. Kervaire, Minimal sumsets in infinite abelian groups, J. Algebra 287 (2005) 449–457.
[5] S. Eliahou, M. Kervaire, Some extensions of the Cauchy–Davenport theorem, Electron. Notes Discrete Math. 28 (2007) 557–564.
[6] S. Eliahou, M. Kervaire, Some results on minimal sumset sizes in finite non-abelian groups, J. Number Theory 124 (2007) 234–247.
[7] S. Eliahou, M. Kervaire, Sumsets in dihedral groups, European J. Combin. 27 (2006) 617–628.
[8] S. Eliahou, M. Kervaire, A. Plagne, Optimally small sumsets in finite abelian groups, J. Number Theory 101 (2003) 338–348.
[9] J.H.B. Kemperman, On complexes in a semigroup, Indag. Math. 18 (1956) 247–254.
[10] G. Vosper, The critical pairs of subsets of a group of prime order, J. London Math. Soc. 31 (1956) 200–205.
[11] G. Zemor, A generalisation to noncommutative groups of a theorem of Mann, Discrete Math. 126 (1994) 365–372.