Sumsets in dihedral groups

Shalom Eliahou, Michel Kervaire

Abstract

Let $D_n$ be the dihedral group of order $2n$. For all integers $r, s$ such that $1 \leq r, s \leq 2n$, we give an explicit upper bound for the minimal size $\mu_{D_n}(r, s) = \min |A \cdot B|$ of sumsets (product sets) $A \cdot B$, where $A$ and $B$ range over all subsets of $D_n$ of cardinality $r$ and $s$ respectively. It is shown by construction that $\mu_{D_n}(r, s)$ is bounded above by the known value of $\mu_G(r, s)$, where $G$ is any abelian group of order $2n$. We conjecture that this upper bound is sharp, and prove that it really is if $n$ is a prime power.

© 2005 Elsevier Ltd. All rights reserved.

1. Introduction

Let $G$ be a finite group of order $g$ and let $r, s$ be two integers satisfying $1 \leq r, s \leq g$. We are interested in the smallest possible size $\mu_G(r, s)$ of the product set (sumset) $A \cdot B = \{x \cdot y \mid x \in A, y \in B\}$ of two subsets $A, B \subseteq G$ of cardinalities $r$ and $s$ respectively.

In formula,

$$\mu_G(r, s) = \min \left\{ |A \cdot B| : A \in \binom{G}{r}, B \in \binom{G}{s} \right\},$$

E-mail addresses: eliahou@lmpa.univ-littoral.fr (S. Eliahou), Michel.Kervaire@math.unige.ch (M. Kervaire).

0195-6698/$ - see front matter © 2005 Elsevier Ltd. All rights reserved.
where \(|X|\) denotes the cardinality of the set \(X\) and \(\left\{ \frac{G}{t} \right\} = \{ X \subset G : |X| = t \}\) is the set of subsets of \(G\) of cardinality \(t\).

The nature of the function \(\mu_G\) is fairly well understood when \(G\) is a finite abelian group. In that case, \(\mu_G(r, s)\) is given by the following formula.

**Theorem (\cite{4}).** Let \(G\) be a finite abelian group of order \(g\). Then

\[
\mu_G(r, s) = \min_{d \mid g} \left( \left\lceil \frac{r}{d} \right\rceil + \left\lfloor \frac{s}{d} \right\rfloor - 1 \right) d,
\]

for all positive integers \(r, s \leq g\).

In the above formula, the minimum is taken over all positive divisors \(d\) of \(g\). The notation \(\left\lceil \xi \right\rceil\), for a real number \(\xi \in \mathbb{R}\), stands for the smallest integer \(x\) such that \(\xi \leq x\).

It is also known that this formula cannot hold in general for non-abelian groups. Indeed, it is proved in \cite{4, Proposition in Section 5}, that for an arbitrary group \(G\) and positive integer \(r\), the equality \(\mu_G(r, r) = r\) is equivalent to the existence in \(G\) of a subgroup of order \(r\). Since obviously \(\mu_G(r, r) \geq r\), because any product set \(A \cdot B\) contains at least the subset \(A \cdot \{b\}\) of the same cardinality as \(A\) for any \(b \in B\), it follows that we have \(\mu_G(r, r) > r\) if \(G\) does not contain any subgroup of order \(r\).

Thus, if \(r\) is a positive divisor of the order \(g\) of \(G\) but is not the order of a subgroup of \(G\), then

\[
\min_{d \mid g} \left( \left\lceil \frac{r}{d} \right\rceil + \left\lfloor \frac{s}{d} \right\rfloor - 1 \right) d \leq \left( \left\lceil \frac{r}{s} \right\rceil + \left\lfloor \frac{r}{s} \right\rfloor - 1 \right) r = r < \mu_G(r, r).
\]

For instance, in the alternating group \(A_4\) of order 12, there is no subgroup of order 6 and thus \(\mu_{A_4}(6, 6) > 6 = \min_{d \mid 12} \{ \left\lceil \frac{6}{d} \right\rceil + \left\lfloor \frac{6}{d} \right\rfloor - 1 \} d\} \).

In \cite[Theorem 4.2]{2}, it was proved that if \(r + s = |G|\), then \(\mu_G(r, s) = |G| - h(s)\), where \(h(s)\) is the largest order of a subgroup of \(G\), dividing \(s\). Hence, \(\mu_{A_4}(6, 6) = 9\), since here \(h(6) = 3\).

However, the formula for \(\mu_G(r, s)\) in the abelian case may fail for \(G\) a non-abelian finite group even if \(G\) has a subgroup of order \(d\) for every positive divisor of \(|G|\).

This last phenomenon occurs with the polycyclic group \(P = C_7 \times C_3\) of order 21 with presentation \(\langle x, y : x^7 = y^3 = 1, yxy^{-1} = x^2 \rangle\).

Here, \(\mu_P(6, 8) = 13\) but \(\min_{d \mid 21} \{ \left\lceil \frac{6}{d} \right\rceil + \left\lfloor \frac{8}{d} \right\rfloor - 1 \} d\} = 12\). (This example is presented in \cite[Section 5]{2}.)

In the present note, we study the function \(\mu_G\) for \(G\) the finite dihedral group \(D_n = \langle a, b : a^n = b^2 = 1, bab^{-1} = a^{-1} \rangle\) of order \(2n\).

We obtain an upper bound for \(\mu_{D_n}\) which is valid for all \(n\). This upper bound is sharp if \(n\) is a power of a prime number. Thus we give a complete description of \(\mu_{D_n}\) when \(n\) is a prime power. In the general case, when \(n\) is composite, the upper bound for \(\mu_{D_n}(r, s)\) may not be sharp for some \(r, s\), although we conjecture that it always is.

It is convenient to introduce, as in \cite{2}, the following notation.

**Notation.** \(G\) being a finite group, set

\[
\kappa_G(r, s) = \min_{h \in \mathcal{H}(G)} \left( \left\lceil \frac{r}{h} \right\rceil + \left\lfloor \frac{s}{h} \right\rfloor - 1 \right) h,
\]

where the minimum is taken over the set \(\mathcal{H}(G)\) of all orders \(h\) of subgroups \(H \subset G\).
Although in the case of $G = D_n$ the set of orders of subgroups is exactly the same as the set of divisors of $|D_n| = 2n$, we keep the above $\kappa$-notation which is more significant in general as explained above in the case $G = A_4$.

However, in Section 4, where we want to stress the fact that $\kappa_{D_n}(r, s)$ only depends on the set of divisors of $2n = |D_n|$, we introduce the simplified notation

$$\kappa_m(r, s) = \min_{d|m} \left( \left\lceil \frac{r}{d} \right\rceil + \left\lceil \frac{s}{d} \right\rceil - 1 \right) d.$$ (Thus, $\kappa_G(r, s) = \kappa_8(r, s)$ whenever $\mathcal{H}(G)$ coincides with the set of divisors of $g = |G|$.)

We shall prove the following results.

**Theorem 1.1.** For every positive integer $n$, one has the inequality

$$\mu_{D_n}(r, s) \leq \kappa_{D_n}(r, s)$$

for all positive integers $r, s \leq 2n$.

The proof is given in Section 2.

In Section 3 we prove the reverse inequality for $n$ a prime power.

**Theorem 1.2.** Let $D_q$ be the dihedral group of index $q = p^\nu$, a prime power. Let $r, s$ be integers such that $1 \leq r, s \leq 2q$. Then $\mu_{D_q}(r, s) \geq \kappa_{D_q}(r, s)$.

Combining the two results, we get the corollary:

**Corollary.** When $q$ is a prime power, then $\mu_{D_q}(r, s) = \kappa_{D_q}(r, s)$.

Very probably, the equality $\mu_{D_n} = \kappa_{D_n}$ holds for all $n$. In fact, we conjecture that the inequality $\mu_G(r, s) \geq \kappa_G(r, s)$ holds for any finite group and all positive integers $r, s \leq |G|$ (see [2]).

In Section 4, we make some remarks concerning the hypothesis in Lemma 3.1 which yields Theorem 1.2. The validity of formula (2) in this lemma is a purely arithmetical question which seems to require an essential use of Additive Number Theory.

2. Proof of Theorem 1.1

In this section we shall prove the inequality $\mu_{D_n}(r, s) \leq \kappa_{D_n}(r, s)$ for the dihedral group $D_n$ in the following equivalent form.

**Proposition 2.1.** Let $r, s$ be a pair of integers satisfying $1 \leq r, s \leq 2n$. Let $h$ be the order of a subgroup of $D_n$. Then, there exist subsets $A, B \subset D_n$ with cardinalities $|A| = r, |B| = s$ such that $|A \cdot B| \leq \left( \left\lceil \frac{r}{h} \right\rceil + \left\lceil \frac{s}{h} \right\rceil - 1 \right) h$.

We begin with a lemma which is valid in any finite solvable group.

**Lemma 2.2.** Let $G$ be a finite solvable group and $1 \leq r, s \leq |G|$. Let $k$ be the order of a normal subgroup $K$ of $G$. Then

$$\mu_G(r, s) \leq \left( \left\lceil \frac{r}{k} \right\rceil + \left\lceil \frac{s}{k} \right\rceil - 1 \right) k.$$
Proof of the Lemma. Let $G_0 = G/K$ and $r_0 = \lceil \frac{r}{k} \rceil$, $s_0 = \lceil \frac{s}{k} \rceil$. By definition, $r_0$ is the smallest integer satisfying $r_0 \geq \frac{r}{k}$. Since $g_0 = \frac{r}{k}$ is an integer and $g_0 \geq \frac{r}{k}$, we have $g_0 \geq r_0$. Similarly, $g_0 \geq s_0$.

Since $G_0 = G/K$ is solvable, $\mu_{G_0}(r_0, s_0) \leq r_0 + s_0 - 1$ by Theorem 2.2 of [3]. Let $A_0, B_0 \subset G_0$ be subsets in the quotient group $G_0$, of cardinalities $r_0$ and $s_0$ respectively, such that $|A_0 \cdot B_0| = \mu_{G_0}(r_0, s_0) \leq r_0 + s_0 - 1$.

Now, let us define

$$A' = \pi^{-1}(A_0) \quad \text{and} \quad B' = \pi^{-1}(B_0),$$

where $\pi : G \to G_0$ denotes the natural projection.

We have

$$|A'| = r' = r_0 \cdot k, \quad |B'| = s' = s_0 \cdot k.$$ 

Thus,

$$|A' \cdot B'| = (r_0 + s_0 - 1)k = \left( \left\lceil \frac{r}{k} \right\rceil + \left\lceil \frac{s}{k} \right\rceil - 1 \right) k.$$ 

Since $r_0 = \lceil \frac{r}{k} \rceil \geq \frac{r}{k}$ and $s_0 = \lceil \frac{s}{k} \rceil \geq \frac{s}{k}$, we have

$$r' = r_0 \cdot k \geq r \quad \text{and} \quad s' = s_0 \cdot k \geq s.$$ 

Let $A \subset A'$ and $B \subset B'$ be subsets of cardinalities $|A| = r$, $|B| = s$. We have $A \cdot B \subset A' \cdot B'$ and thus

$$\mu_G(r, s) \leq |A \cdot B| \leq |A' \cdot B'| = \left( \left\lceil \frac{r}{k} \right\rceil + \left\lceil \frac{s}{k} \right\rceil - 1 \right) k. \quad \Box$$

Note that the following statement is a corollary of the lemma.

Corollary 2.3. Suppose $G$ is a solvable group and for some $r, s$ the minimum $\kappa_G(r, s) = \min_h((\left\lceil \frac{r}{h} \right\rceil + \left\lceil \frac{s}{h} \right\rceil - 1)h)$ is attained at the order $h$ of a normal subgroup $H \subset G$, then $\mu_G(r, s) \leq \kappa_G(r, s)$.

We now proceed to prove the proposition.

Proof of Proposition 2.1. For the dihedral group $D_n$, we use the presentation

$$D_n = \langle a, b : a^n = b^2 = 1, bab^{-1} = a^{-1} \rangle.$$ 

In view of the lemma, we may suppose that the given $h$ is the order of a non-invariant subgroup $H$ of $D_n$. Hence, we may assume that $H = \langle a^m, a^ib \rangle$ for some $i$, where $h = 2k$ with $k = \frac{m}{2}$ some proper divisor of $n$.

Writing $C$ for the cyclic subgroup $C = \langle a \rangle \subset D_n$, we shall denote by $K = \langle a^m \rangle$ the cyclic subgroup $K = H \cap C$ of $H$ generated by $a^m$, of order $k$. Note that $K$ is a normal subgroup of $D_n$ since $zbz^{-1} = z^{-1}$ for every $z \in C$.

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

Our objective is to prove that there exist subsets $A, B \subset D_n$ of cardinality $r$ and $s$ respectively such that $|A \cdot B| \leq f_{2k}(r, s)$. Again by the above lemma, we may assume that $f_{2k}(r, s) < f_k(r, s)$. Indeed, if we had $f_k(r, s) \leq f_{2k}(r, s)$, then applying the lemma to $k$ which is the order of the invariant
subgroup $K \subset D_n$ we would conclude

$$\mu_{D_n}(r, s) \leq f_k(r, s) \leq f_{2k}(r, s)$$

as desired.

In order to exploit the assumption $f_{2k}(r, s) < f_k(r, s)$, we perform the euclidean division of $r$ and $s$ by $h = 2k$ with non-positive remainder:

$$r = \left\lceil \frac{r}{2k} \right\rceil 2k - \varrho_h(r), \quad s = \left\lceil \frac{s}{2k} \right\rceil 2k - \varrho_h(s),$$

with $0 \leq \varrho_h(r) < 2k$, and $0 \leq \varrho_h(s) < 2k$. We write

$$\begin{cases} 
\varrho_h(r) = \alpha k + r_1 \text{ with } \alpha \in \{0, 1\} \text{ and } 0 \leq r_1 < k, \\
\varrho_h(s) = \beta k + s_1 \text{ with } \beta \in \{0, 1\} \text{ and } 0 \leq s_1 < k.
\end{cases}$$

We use the notation $u$ and $v$ for the ceilings $u = \left\lceil \frac{r}{k} \right\rceil$, $v = \left\lceil \frac{s}{k} \right\rceil$.

Comparing the above with the defining formulas for $\left\lceil \frac{r}{k} \right\rceil$ and $\left\lceil \frac{s}{k} \right\rceil$ given by euclidean division by $k$, namely

$$r = \left\lfloor \frac{r}{k} \right\rfloor k - \varrho_k(r), \quad s = \left\lfloor \frac{s}{k} \right\rfloor k - \varrho_k(s),$$

with $0 \leq \varrho_k(r) < k$, and $0 \leq \varrho_k(s) < k$, we see that

$$r_1 = \varrho_k(r), \quad s_1 = \varrho_k(s), \quad \text{and} \quad \left\lceil \frac{r}{k} \right\rceil = 2u - \alpha, \quad \left\lceil \frac{s}{k} \right\rceil = 2v - \beta.$$

Therefore,

$$f_{2k}(r, s) = f_k(r, s) + (\alpha + \beta - 1)k.$$  

The assumption $f_{2k}(r, s) < f_k(r, s)$ yields the inequality $\alpha + \beta < 1$, hence $\alpha = \beta = 0$.

We can then write

$$r = (2u - 1) \cdot k + x, \quad s = (2v - 1) \cdot k + y$$  \hspace{1cm} (1)

with $1 \leq u, v \leq m$ and $1 < x = k - \varrho_k(r), y = k - \varrho_k(s) \leq k$.

In order to produce the formulas defining the sets $A, B \subset D_n$ which satisfy $|A \cdot B| \leq f_{2k}(r, s)$, we need some more notation. For $0 \leq w \leq m$, let $X_w$ be the set

$$X_w = \{1, a, \ldots, a^{w-1}\},$$

of cardinality $w$. Note that if $w = 0$, then we have $X_w = \emptyset$.

We will use also

$$K_j = \{1, a^m, \ldots, a^{(j-1)m}\} \subset K,$$

for $1 \leq j \leq k$. Note that $K_k = K = \langle a^m \rangle$.

Finally, for $X \subset \langle a \rangle$ any subset of $\langle a^m \rangle$, we denote by $\overline{X}$ the set

$$\overline{X} = bXb^{-1} = \{z^{-1} \mid z \in X\}.$$

Note that $a^{w-1}\overline{X_w} = X_w$ and $\overline{K} = K$.

As defining formulas for $A$ and $B$ we take

$$A = (K \cdot X_u) \cup (K \cdot X_{u-1} \cup K_s a^{u-1}) a^{v-1} b,$$
Let \( \mu \) then we have \(|\mathcal{A}| = ku + k(u - 1) + x = r \) and \( |\mathcal{B}| = s \).

The product set of \( \mathcal{A} = \mathcal{A}_0 \cup \mathcal{A}_1 \subset D_n \) and \( \mathcal{B} = \mathcal{B}_0 \cup \mathcal{B}_1 \subset D_n \) is given by

\[
\mathcal{A} \cdot \mathcal{B} = (\mathcal{A}_0 \cdot \mathcal{B}_0 \cup \mathcal{A}_1 \cdot \overline{\mathcal{B}_1}) \cup (\mathcal{A}_0 \cdot \mathcal{B}_1 \cup \mathcal{A}_1 \cdot \overline{\mathcal{B}_0})b.
\]

Using the product formulas \( \mathcal{K} \cdot \mathcal{K}_j = \mathcal{K} \), and

\[
\mathcal{K} \cdot \mathcal{X}_l \cdot \mathcal{X}_w = \begin{cases} 
\mathcal{K} \cdot \{1, a, \ldots, a^{t+w-1}\} & \text{if } t + w - 1 \leq m, \\
\mathcal{K} \cdot \{1, a, \ldots, a^{m-1}\} = \langle a \rangle & \text{if } t + w - 1 > m,
\end{cases}
\]

that is \( \mathcal{K} \cdot \mathcal{X}_l \cdot \mathcal{X}_w = \mathcal{K} \cdot \mathcal{X}_{\min(t+w-1,m)} \), we then verify the desired inequality \(|\mathcal{A} \cdot \mathcal{B}| \leq \kappa_{D_n}(r, s)\). Indeed,

\[
\mathcal{A} \cdot \mathcal{B} = (\mathcal{K} \cdot \mathcal{X}_u \cdot \mathcal{X}_v \cup \mathcal{K} \cdot \mathcal{X}_{u-1} \cdot \mathcal{X}_{v-1} \cup \mathcal{K} \cdot \mathcal{X}_{u-1} a^u \cup \mathcal{X}_v \cdot \overline{\mathcal{K}_x a^{u-1}})
\]

\[
\cup (\mathcal{K} \cdot \mathcal{X}_u \cdot \mathcal{X}_{v-1} \cup \mathcal{K} \cdot \mathcal{X}_u \cdot a^{v-1} \cup \mathcal{K} \cdot \mathcal{X}_{u-1} \cdot \mathcal{X}_v \cup \mathcal{K} \cdot \mathcal{X}_v a^{u-1}) \cdot b.
\]

Therefore,

\[
\mathcal{A} \cdot \mathcal{B} = \mathcal{K} \cdot \mathcal{X}_{\min(u+v-1,m)} \cup \mathcal{K} \cdot \mathcal{X}_{\min(u+v-1,m)}b
\]

and \(|\mathcal{A} \cdot \mathcal{B}| \leq 2k(u + v - 1) = f_n(r, s). \quad \square
\]

### 3. Proof of Theorem 1.2

Conjecturally, the inequality \( \mu_{D_n}(r, s) \geq \kappa_{D_n}(r, s) \) holds for every positive integer \( n \).

However, we only have a complete proof in the case where \( n \) is a prime power: \( n = q = p^\nu \).

We prove a preliminary statement which is valid for all \( n \) and on which we return with some comments in Section 4.

Using the presentation \( D_n = \langle a, b : a^n = b^2 = 1, bab^{-1} = a^{-1} \rangle \), let \( C \) be the cyclic subgroup \( C = \langle a \rangle \subset D_n \) of order \( n \). We also use \( D \) to denote the group \( D_n \) itself.

We introduce the notation

\[
M_C(r_0, r_1, s_0, s_1) = \max\{\kappa_C(r_0, s_0), \kappa_C(r_1, s_1)\} + \max\{\kappa_C(r_0, s_1), \kappa_C(r_1, s_0)\},
\]

where \( r_0, r_1, s_0, s_1 \) are positive integers less than or equal to \( n \) and call \( M_C(r_0, r_1, s_0, s_1) \) the decomposition function.

**Lemma 3.1.** Given the positive integers \( n \) and \( r, s \). If for every choice of positive integers \( r_0, r_1, s_0, s_1 \leq n \) satisfying \( r_0 + r_1 = r \) and \( s_0 + s_1 = s \) we have the inequality

\[
M_C(r_0, r_1, s_0, s_1) \geq \kappa_{D_n}(r, s),
\]

then \( \mu_{D_n}(r, s) \geq \kappa_{D_n}(r, s) \).

**Proof.** Let \( A, B \subset D \) be any two subsets of the dihedral group with respective cardinalities \( r, s \). Our objective is to prove that \(|A \cdot B| \geq \kappa_{D_n}(r, s)\). We write \( A = A_0 \cup A_1b \) and \( B = B_0 \cup B_1b \), where \( A_0, A_1, B_0, B_1 \) are subsets of the cyclic group \( C \). Set \( r_0 = |A_0|, r_1 = |A_1| \) and \( s_0 = |B_0|, s_1 = |B_1| \).
We have
\[ A \cdot B = (A_0 \cdot B_0 \cup A_1 \cdot \overline{B}_1) \cup (A_0 \cdot B_1 \cup A_1 \cdot \overline{B}_0)b. \]

Therefore,
\[ |A \cdot B| = |A_0 \cdot B_0 \cup A_1 \cdot \overline{B}_1| + |A_0 \cdot B_1 \cup A_1 \cdot \overline{B}_0|. \]

It follows that
\[ |A \cdot B| \geq \max(|A_0 \cdot B_0|, |A_1 \cdot \overline{B}_1|) + \max(|A_0 \cdot B_1|, |A_1 \cdot \overline{B}_0|). \]

By the result of [4] recalled in the Introduction, we have \( \mu_C = \kappa_C \) in the abelian group \( C \). It follows that
\[ |A \cdot B| \geq \max[\kappa_C(r_0, s_0), \kappa_C(r_1, s_1)] + \max[\kappa_C(r_0, s_1), \kappa_C(r_1, s_0)] \]
\[ = M_C(r_0, r_1, s_0, s_1), \]

at least if none of the sets \( A_0, A_1, B_0, B_1 \) is empty.

Then the inequality (2) implies \( |A \cdot B| \geq \kappa_{D_n}(r, s) \).

It remains to prove that even if one of the sets \( A_0, A_1, B_0, B_1 \subset C \) is empty, we still have \( |A \cdot B| \geq \kappa_{D_n}(r, s) \), as desired.

Consider the abelian group \( G = C \times \langle c \rangle \), direct product of \( C \), cyclic of order \( n \), with a cyclic group of order 2, whose generator is denoted by \( c \). Let \( X, Y \subset G \) be subsets of \( G \) with cardinalities \( r, s \geq 1 \) respectively. By the formula \( \mu_G = \kappa_G \) in the abelian group \( G \), we have \( |X \cdot Y| \geq \kappa_G(r, s) \). Moreover, since \( G \) has order \( 2n \) and the orders of the subgroups of \( G \) are all the positive divisors of \( 2n \), as is the case for the non-abelian group \( D_n \), we have \( \kappa_G(r, s) = \kappa_{D_n}(r, s) \).

We are going to show that if anyone of \( r_0, r_1 \) or \( s_0, s_1 \) vanishes, then one can construct subsets \( X, Y \subset G \) of cardinalities \( r = r_0 + r_1 \) and \( s = s_0 + s_1 \) respectively such that \( |X \cdot Y| = |A \cdot B| \), thus implying
\[ |A \cdot B| = |X \cdot Y| \geq \kappa_G(r, s) = \kappa_{D_n}(r, s). \]

As above in Section 2, we use the notation \( \overline{Z} = \{z^{-1} \mid z \in Z\} \), if \( Z \) is any subset of \( C \).

Observe that for subsets \( X, Y \subset G, X = X_0 \cup X_1c \) and \( Y = Y_0 \cup Y_1c \), where \( X_0, X_1, Y_0, Y_1 \) are subsets of \( C \), we have
\[ X \cdot Y = (X_0 \cdot Y_0 \cup X_1 \cdot Y_1) \cup (X_0 \cdot Y_1 \cup X_1 \cdot Y_0)c, \]

and
\[ |X \cdot Y| = |X_0 \cdot Y_0 \cup X_1 \cdot Y_1| + |X_0 \cdot Y_1 \cup X_1 \cdot Y_0|. \]

Typically, if \( A_0 = \emptyset \), we may take \( X = A_1c \subset G, Y = \overline{B}_0 \cup \overline{B}_1c \subset G \), where, by a slight abuse of notation, we identify the two copies of \( C \) sitting in \( G \) and \( D_n \). Note that \( |X| = |A_1| = r, |Y| = s \). Taking the product of \( X \) and \( Y \) in \( G \), we have
\[ X \cdot Y = A_1 \cdot \overline{B}_1 \cup A_1 \cdot \overline{B}_0c, \]

and
\[ |X \cdot Y| = |A_1 \cdot \overline{B}_1| + |A_1 \cdot \overline{B}_0| = |A \cdot B|. \]
We leave it to the reader to verify that if \( A_1 = \emptyset \), or \( B_0 = \emptyset \), or \( B_1 = \emptyset \), then one gets \(|X \cdot Y| = |A \cdot B|\) with \( X, Y \subseteq G \) by taking for the pair \((X, Y)\) the pairs \((A_0, B_0 \cup B_1c), (A_0 \cup A_1c, B_1c)\) and \((A_0 \cup A_1c, B_0)\), respectively.

This finishes the proof of Lemma 3.1. □

As we shall see now, the inequality (2), in the hypothesis of Lemma 3.1, holds true when \( n \) is a prime power.

**Theorem 3.2.** Let \( p \) be a prime number and \( \nu \in \mathbb{N} \) a positive integer. For every \( 1 \leq r_0, r_1, s_0, s_1 \leq p^\nu \), one has

\[
M_C(r_0, r_1, s_0, s_1) \geq \kappa_D(r_0 + r_1, s_0 + s_1),
\]

where \( C \) stands for the cyclic group of order \( p^\nu \) and \( D \) stands for the dihedral group of order \( 2p^\nu \).

**Proof.** Let \( H \) be any abelian group of order \( p^\nu \). It follows from [4] that \( \mu_H(x, y) = \kappa_C(x, y) \) for all \( 1 \leq x, y \leq |H| \), where \( C \) is a cyclic group of order \( p^\nu \). Similarly, if \( G \) is any abelian group of order \( 2p^\nu \), we have \( \mu_G(x, y) = \kappa_D^{2p^\nu}(x, y) \) for all \( 1 \leq x, y \leq |G| \) as the orders of the subgroups of \( G \) and \( D_{p^\nu} \) coincide. Both consist exactly of the positive divisors of \( 2p^\nu \).

From now on we shall fix very specifically such groups \( H \) and \( G \). Namely, \( H \) will be the additive group of the finite field \( \mathbb{F}_q \) of order \( q = p^\nu \), and \( G \) will be the direct product \( G = H \times \mathbb{Z}/2\mathbb{Z} \). Temporarily, we write these abelian groups additively.

Let \( c = (0, 1) \in G \), which is of order 2. By a slight abuse of notation, we consider \( H \) as a subgroup of \( G \), and hence \( G \) as the disjoint union of the two cosets \( H \) and \( H + c \).

Assume we are given the subsets \( A_0, A_1, B_0, B_1 \subseteq H \) of cardinalities \( r_0, r_1, s_0, s_1 \) respectively. We then form the subsets \( A, B \subseteq G \) defined by \( A = A_0 \cup (A_1 + c) \) and \( B = B_0 \cup (B_1 + c) \). Since these unions are disjoint, we have \(|A| = r_0 + r_1\) and \(|B| = s_0 + s_1\). Consider the sumset \( A + B \subseteq G \). Since \( 2c = 0 \), we have \( A + B = U \cup V \), where \( U = (A_0 + B_0) \cup (A_1 + B_1) \) and \( V = [(A_0 + B_1) \cup (A_1 + B_0)] + c \). Obviously, we have

\[
|U| + |V| = |A + B| \geq \mu_G(r_0 + r_1, s_0 + s_1) = \kappa_D(r_0 + r_1, s_0 + s_1),
\]

where the last equality holds because the groups \( G = H \times \mathbb{Z}/2\mathbb{Z} \) and \( D = D_{p^\nu} \) have the same set of orders of subgroups.

It remains to apply this formula to well chosen subsets \( A_0, A_1, B_0, B_1 \). We choose the subsets \( A_0, A_1, B_0, B_1 \subseteq H \) such that \(|U| + |V|\) realizes the minimum of the left hand side \( M_C(r_0, r_1, s_0, s_1) \) in formula (2).

Here we appeal to our description of \( H \) as the additive group of \( \mathbb{F}_{p^\nu} \) and to the (reverse) lexicographical order on \( H \), viewed as a vector space over \( \mathbb{F}_p \). In [1] this order is described as the natural order in the interval of integers \([0, p^\nu - 1]\), where the \( \mathbb{F}_p \)-vector space addition is given by the \( p \)-adic Nim sum (see page 17 of [1]).

Given \( 1 \leq t < p^\nu \), let us denote by \( IS_t \) the initial segment of \( H \) of cardinality \( t \), for that total ordering. Given any two initial segments \( IS_t, IS_u \) \((1 \leq t, u < p^\nu)\), it follows from Proposition (3.1) of [1], that their sumset \( IS_t + IS_u \) is optimally small,
i.e. \(|IS_t + IS_u| = \mu_H(t, u)|. More precisely,

\[ IS_t + IS_u = IS_{\mu_H(t, u)}, \]

as the sumset of two initial segments of \(H\) is proved in [1] to be again an initial segment. A simple but crucial observation for what follows is that either \(IS_t\) contains \(IS_u\) or \(IS_u\) contains \(IS_t\). In fact, we have \(IS_t \cup IS_u = IS_{\max\{t, u\}}\).

Now, our specific choice of subsets \(A_0, A_1, B_0, B_1\) will be to take initial segments of the required cardinalities. That is, \(A_0 = IS_{r_0}, A_1 = IS_{r_1}, B_0 = IS_{s_0},\) and \(B_1 = IS_{s_1}\).

For simplicity, let \(\mu_{i, j} = \mu_H(r_i, s_j) = \kappa_C(r_i, s_j)\) for \(i, j \in \{0, 1\}\). Since \(A_i + B_j = IS_{r_i} + IS_{s_j} = IS_{\mu_{i, j}}\), we have \(U = (A_0 + B_0) \cup (A_1 + B_1) = IS_{\max\{\mu_{0,0}, \mu_{1,1}\}}\) and similarly, \(V = (A_0 + B_1) \cup (A_1 + B_0) = IS_{\max\{\mu_{0,1}, \mu_{1,0}\}}\). Thus, \(|U| + |V| = \max\{\mu_{0,0}, \mu_{1,1}\} + \max\{\mu_{0,1}, \mu_{1,0}\}\). By the above inequality \(|U| + |V| \geq \kappa_D(r_0 + r_1, s_0 + s_1)\), it follows

\[ \max\{\mu_{0,0}, \mu_{1,1}\} + \max\{\mu_{0,1}, \mu_{1,0}\} \geq \kappa_D(r_0 + r_1, s_0 + s_1), \]

as desired. □

4. Remarks on the decomposition function

In this section, we discuss the validity of the inequality (2) occurring in the hypothesis of Lemma 3.1, in Section 3.

We are given a positive integer \(n\) and a quadruple of integers \((r_0, r_1, s_0, s_1)\) such that \(1 \leq r_i, s_j \leq n\) for \(i, j \in \{0, 1\}\).

The decomposition function \(M_C(r_0, r_1, s_0, s_1)\) is the expression

\[ M(r_0, r_1, s_0, s_1) = \max\{\kappa_n(r_0, s_0), \kappa_n(r_1, s_1)\} + \max\{\kappa_n(r_0, s_1), \kappa_n(r_1, s_0)\}, \]

where \(\kappa_g(r, s) = \min_{d \mid g} \left\{ \left\lceil \frac{r}{d} \right\rceil + \left\lceil \frac{s}{d} \right\rceil - 1 \right\} \cdot d\).

The hypothesis in Lemma 3.1 was the inequality

\[ M(r_0, r_1, s_0, s_1) \geq \kappa_{2n}(r_0 + r_1, s_0 + s_1), \]

labelled formula (2).

In Section 3, Theorem 3.2, we have proved that this inequality holds for all \((r_0, r_1, s_0, s_1)\) with \(1 \leq r_0, r_1, s_0, s_1 \leq n\), if \(n\) is a prime power. Although the inequality is a purely arithmetical statement, the only proof we have, as given in Section 3, relies in an essential way on Additive Number Theory.

In this section, we show that the inequality (2) is definitely false for at least one quadruple \((r_0, r_1, s_0, s_1)\) with \(1 \leq r_0, r_1, s_0, s_1 \leq n\), if \(n\) is divisible by two distinct primes.

Proposition 4.1. Assume \(n = u \cdot v\), where \(u, v\) are relatively prime integers with \(u, v \geq 2\), then

\[ \max\{\kappa_n(r_0, s_0), \kappa_n(r_1, s_1)\} + \max\{\kappa_n(r_0, s_1), \kappa_n(r_1, s_0)\} < \kappa_{2n}(r, s), \]

for \(r_0 = u, r_1 = v, s_0 = n - u, s_1 = n - v\).
For the proof we shall use from [2, Corollary 3.2] the formula satisfied by the function $\kappa_G(r, s)$ for $1 \leq r, s \leq g - 1$:

$$\kappa_G(x, y) = \min\{x + y - h_G(\gcd(x, y)), \kappa_G(x + 1, y), \kappa_G(x, y + 1)\},$$

where $g$ is the order of the group $G$ and $h_G(t)$ is the largest order of a subgroup of $G$, dividing $t$.

In the present context, this formula becomes

$$\kappa_G(x, y) = \min\{x + y - \gcd(x, y, g), \kappa_G(x + 1, y), \kappa_G(x, y + 1)\},$$

(4)

for $1 \leq x, y \leq g - 1$.

**Proof of the Proposition.** We may assume $u < v$.

For simplicity of the notation, we let $\mu_{i,j} = \kappa_n(r_i, s_j)$ for $i, j \in \{0, 1\}$. That is $\mu_{0,0} = \kappa_n(u, n - u), \mu_{1,1} = \kappa_n(v, n - v), \mu_{0,1} = \kappa_n(u, n - v),$ and $\mu_{1,0} = \kappa_n(v, n - u)$.

We now prove the stated inequality

$$\max\{\mu_{0,0}, \mu_{1,1}\} + \max\{\mu_{0,1}, \mu_{1,0}\} < \kappa_{2n}(u + v, 2n - (u + v)).$$

We first list and prove 3 claims which will be used in evaluating the various terms in the above expression.

**Claim 1:** $\mu_{0,0} \leq n - u$.

Indeed, $\mu_{0,0} = \kappa_n(u, n - u) \leq n - \gcd(u, n - u, n)$ by (4). As $n = u \cdot v$, it follows that $\gcd(u, n - u, n) = u$. Therefore $\mu_{0,0} \leq n - u$, as claimed.

**Claim 2:** $\max\{\mu_{0,0}, \mu_{1,1}\} + \max\{\mu_{0,1}, \mu_{1,0}\} \leq 2n - u$.

Indeed, we have $\mu_{1,1} = \kappa_n(v, n - b) \leq n - v$, as above. Since $u < v$, it follows that $\max\{\mu_{0,0}, \mu_{1,1}\} \leq n - u$. As for $\mu_{0,1}$ and $\mu_{1,0}$, it suffices for our purposes to invoke the crude estimate $\max\{\mu_{0,1}, \mu_{1,0}\} \leq n$. The claim follows.

**Claim 3:** $\kappa_{2n}(u + v, 2n - (u + v)) \geq 2n - \varepsilon$, where $\varepsilon \in \{1, 2\}$ and $\varepsilon \equiv u + v \mod 2$.

Indeed, by (4) we have

$$\kappa_{2n}(u + v, 2n - (u + v)) \geq 2n - \gcd(u + v, 2n - (u + v), 2n)$$

$$= 2n - \gcd(u + v, 2uv).$$

Since $u, v$ are coprime integers, it follows that $\gcd(u + v, 2uv) = 1$ if $u + v$ is odd, and $\gcd(u + v, 2uv) = 2$ otherwise. This proves claim 3.

To complete the proof of the proposition, assume first that $u \geq 3$. Then $\max\{\mu_{0,0}, \mu_{1,1}\} + \max\{\mu_{0,1}, \mu_{1,0}\} \leq 2n - u$ by claim 2, whereas by claim 3, $\kappa_{2n}(u + v, 2n - (u + v)) \geq 2n - 3$, and the stated inequality follows.

It remains to examine the case where $u = 2$.

On the one hand, $\max\{\mu_{0,0}, \mu_{1,1}\} \leq 2n - 2$ by claim 2. On the other hand, $\kappa_{2n}(u + v, 2n - (u + v)) \geq 2n - 1$. This follows from claim 3 at $\varepsilon = 1$ whenever $u + v$ is odd, which is the case as $u = 2$ and $v$ is coprime to $u$. Thus, here again, the stated inequality follows. □

Even though formula (2) fails in general if $n$ is composite, Lemma 3.1 is very useful for machine experimentation with the conjecture $\mu_{D_n}(r, s) \geq \kappa_{D_n}(r, s)$.
Firstly, Lemma 3.1 implies that it is enough to verify \(|A \cdot B| \geq \kappa_{D_n}(r, s)|\) for the subsets \(A = A_0 \cup A_1 b, B = B_0 \cup B_1 b\) such that \(|A| = r, |B| = s\) with \(r_i = |A_i| \geq 1, s_j = |B_j| \geq 1\) and such that

\[M(r_0, r_1, s_0, s_1) < \kappa_{2n}(r_0 + r_1, s_0 + s_1).\]

Moreover, in view of the following lemma, we may also restrict the search to the quadruples \((r_0, r_1, s_0, s_1)\) satisfying \(r_i + s_j \leq n\) for all \(i, j\).

**Lemma 4.2.** If \(A = A_0 \cup A_1 b, B = B_0 \cup B_1 b\) is a pair of subsets \(A, B \subset D_n = C \cup Cb\), such that \(|A| + |B_j| > n\) for some indices \(i, j \in \{0, 1\}\), then

\[|A \cdot B| \geq \kappa_{D_n}(r, s),\]

where \(r = |A|, s = |B|\).

**Proof.** The product set \(A \cdot B\) of \(A = A_0 \cup A_1 b\) and \(B = B_0 \cup B_1 b\) is given by

\[A \cdot B = (A_0 \cdot B_0 \cup A_1 \cdot B_1) \cup (A_0 \cdot B_1 \cup A_1 \cdot B_0)b.\]

As seen above, thus,

\[|A \cdot B| = |A_0 \cdot B_0 \cup A_1 \cdot B_1| + |A_0 \cdot B_1 \cup A_1 \cdot B_0|.\]

By the theorem in [4], recalled in the Introduction, we have

\[|X \cdot Y| \geq \mu_G(r, s) = \kappa_{2n}(r, s) = \kappa_{D_n}(r, s).\]

Let \(X, Y \subset G = C \cup Cc\) be the two subsets \(X = A_0 \cup A_1 c\) and \(Y = B_0 \cup B_1 c\) of cardinalities \(r\) and \(s\) respectively. We have

\[X \cdot Y = (A_0 \cdot B_0 \cup A_1 \cdot B_1) \cup (A_0 \cdot B_1 \cup A_1 \cdot B_0)c,\]

and hence

\[|X \cdot Y| = |A_0 \cdot B_0 \cup A_1 \cdot B_1| + |A_0 \cdot B_1 \cup A_1 \cdot B_0|.\]

Thus, even though \(A, B\) and \(X, Y\) live in different groups, we see that if

\[|A_0 \cdot B_0 \cup A_1 \cdot B_1| \geq |A_0 \cdot B_0 \cup A_1 \cdot B_1|,\]

then

\[|A \cdot B| \geq |X \cdot Y| \geq \kappa_{D_n}(r, s).\]

Obviously, (5) holds true if \(A_0 \cdot B_0 = C\).

This happens if \(|A_0| + |B_0| > |C| = n\) by the well known Theorem 1.1 of [5]. (See also [2, Theorem 4.1].)

If \(|A_i| + |B_j| > n\) for some other pair of indices \(i, j \in \{0, 1\}\), we can reduce back to the case \(|A_0| + |B_0| > n\) by replacing if needed, \(A = A_0 \cup A_1 b\) by \(A' = bA = \overline{A}_1 \cup \overline{A}_0 b\) and/or \(B = B_0 \cup B_1 b\) by \(B' = Bb = B_1 \cup B_0 b\).

This finishes the proof of Lemma 4.2. □
Note that, in any case, searching for counter-examples to the conjecture $\mu_{D_n}(r, s) \geq \kappa_{D_n}(r, s)$, it suffices to examine subsets $A = A_0 \cup A_1 b \subset D_n$ and $B = B_0 \cup B_1 b \subset D_n$ such that $|A_0 \cdot B_0| \leq n - 1$. This follows from the above proof.

Using the theorems in Section 4 of [2] and the above lemmata, we have verified the conjecture $\mu_{D_n}(r, s) \geq \kappa_{D_n}(r, s)$ for $n$ composite by machine calculation up to 15, i.e. for $n = 6, 10, 12, 14$ and 15.

Acknowledgment

During the preparation of this paper, the first author has partially benefited from a research contract with the Fonds National Suisse pour la Recherche Scientifique.

References