THREE QUESTIONS ON MSTD, MDTS AND BALANCED SUBSETS OF DICYCLIC GROUPS, ANSWERED IN THE NEGATIVE

KOREA SUPERINTELLIGENCE LABS

Abstract. For a subset A of a finite group one writes $A+A=\{a_1a_2 : a_1,a_2\in A\}$ and $A-A=\{a_1a_2^{-1} : a_1,a_2\in A\}$, and calls A *sum-dominant* (MSTD), *balanced*, or *difference-dominant* (MDTS) according as $|A+A|$ exceeds, equals, or falls short of $|A-A|$. Writing $\mathrm{S}_{\mathrm{Dic}_{4n}}(m)$, $\mathrm{D}_{\mathrm{Dic}_{4n}}(m)$, $\mathrm{B}_{\mathrm{Dic}_{4n}}(m)$ for the numbers of m-element subsets of the dicyclic group Dic_{4n} of each type, Mandal and Neetu recently determined all three counts for $m=2$, and for $m=3$ with n odd, and closed their paper with three questions: whether 4 divides $\mathrm{S}_{\mathrm{Dic}_{4n}}(m)$ for every admissible m and every $n\geq 3$; whether $4n$ divides $\mathrm{S}_{\mathrm{Dic}_{4n}}(m)$ for every $m\geq 2$; and whether all three counts are always even. We answer all three in the negative. One cell suffices: the four-element subsets of Dic_{12} split as $(\mathrm{S}_{\mathrm{Dic}_{12}}(4),\mathrm{D}_{\mathrm{Dic}_{12}}(4),\mathrm{B}_{\mathrm{Dic}_{12}}(4))=(126,228,141)$, where 126 is divisible by neither 4 nor 12 and 141 is odd. A second, independent counterexample lies in Dic_{28}, outside the range tabulated in the source: $(\mathrm{S}_{\mathrm{Dic}_{28}}(4),\mathrm{D}_{\mathrm{Dic}_{28}}(4),\mathrm{B}_{\mathrm{Dic}_{28}}(4))=(5586,7560,7329)$. We also compute $\gcd\{\mathrm{S}_{\mathrm{Dic}_{12}}(m) : m\geq 2\}=6$; we give the complete profiles $(\mathrm{S},\mathrm{D},\mathrm{B})$ of Dic_{4n} for $n\leq 7$ over the ranges searched, including the balanced counts, which the source does not tabulate; and we show that the failure is not uniform in n, since at Dic_{20} and Dic_{24} the size-four counts do satisfy both divisibility questions. Two of the three refuting values are entries of the source's own tables, and had already been published a year earlier by Neetu, Shetty and Shankar, so what is new here is the observation rather than the arithmetic; the cells at Dic_{24} and Dic_{28} appear in neither paper. Every theorem below is machine-checked in Lean 4.

1. Introduction

Let G be a finite group, written multiplicatively, and let $A\subseteq G$. Following the convention of Miller and Vissuet [2] for non-abelian groups, which the present paper adopts throughout, the *sumset* and the *difference set* of A are

$$A+A \;=\; \{a_1a_2 \;:\; a_1,a_2\in A\},\qquad A-A \;=\; \{a_1a_2^{-1} \;:\; a_1,a_2\in A\}.$$

In a non-abelian group $A+A$ is thus the set of left-to-right products and $A-A$ the set of right quotients. A set A is *MSTD* (more sums than differences, or sum-dominant) if $|A+A|>|A-A|$, *balanced* if $|A+A|=|A-A|$, and *MDTS* (more differences than sums, or difference-dominant) if $|A+A|<|A-A|$.

For subsets of $\mathbb{Z}$ the study of the sum-dominant phenomenon is by now extensive; Martin and O'Bryant [5] showed that a positive proportion of the subsets of $\{0,1,\ldots,n-1\}$ are MSTD, and Zhao [7] gave an algorithm computing the limiting proportion. In finite groups the counting question was raised by Nathanson [4], who used MSTD sets in finite abelian groups to construct MSTD sets of integers, and was carried further for abelian groups by Zhao [6]; Miller and Vissuet [2] began the non-abelian study with the dihedral groups, and Ascoli et al. [8] refined it by cardinality.

The dicyclic groups and the counts. For $n\geq 1$ the *dicyclic group* of order $4n$ is

$$\mathrm{Dic}_{4n} \;=\; \langle\, a,b \;:\; a^{2n}=1,\; a^n=b^2,\; b^{-1}ab=a^{-1}\,\rangle, \tag{1}$$

whose $4n$ elements are $1,a,\ldots,a^{2n-1},b,ab,\ldots,a^{2n-1}b$. For $m\in\mathbb{N}$ write

$$\mathrm{S}_{\mathrm{Dic}_{4n}}(m),\qquad \mathrm{D}_{\mathrm{Dic}_{4n}}(m),\qquad \mathrm{B}_{\mathrm{Dic}_{4n}}(m)$$

for the number of MSTD, MDTS and balanced subsets of Dic_{4n} of cardinality m. Since every subset is of exactly one of the three kinds, these three numbers sum to $\binom{4n}{m}$.

Mandal and Neetu [1] determined all three counts for $m = 2$ and every $n \geq 2$ (their Theorem 1.4), and for $m = 3$ and every odd $n \geq 3$, in two cases according as $3 \mid n$ or not (their Theorem 1.6). For $m = 2$ and odd n, for instance, $\mathrm{S}_{\mathrm{Dic}_{4n}}(2) = 4n(n-1)$, $\mathrm{D}_{\mathrm{Dic}_{4n}}(2) = 0$ and $\mathrm{B}_{\mathrm{Dic}_{4n}}(2) = 2n(2n+1)$. They also tabulate S and D for $\mathrm{Dic}_8, \mathrm{Dic}_{12}, \mathrm{Dic}_{16}, \mathrm{Dic}_{20}$ and all sizes $2 \leq m \leq 10$ (their Tables 1 and 2), and prove lower bounds in the boundary case $m = 2n$ for $n \geq 6$ (their Theorems 1.8 and 1.9). Their concluding section asks three questions, which we quote verbatim:

> **Question 6.1.** For any fixed integer m with $2 \leq m \leq 2n$, is 4 a divisor of $\gcd\left\{\mathrm{S}_{\mathrm{Dic}_{4n}}(m) : n \geq 3\right\}$?
>
> **Question 6.2.** For any fixed integer $n \geq 3$, is $4n$ a divisor of $\gcd\left\{\mathrm{S}_{\mathrm{Dic}_{4n}}(m) : m \geq 2\right\}$?
>
> **Question 6.3.** Is it true that $\mathrm{S}_{\mathrm{Dic}_{4n}}(m), \mathrm{D}_{\mathrm{Dic}_{4n}}(m)$ and $\mathrm{B}_{\mathrm{Dic}_{4n}}(m)$ are even integers for any positive integers n, m with $n \geq 3$ and $2 \leq m \leq 2n$?

Each is introduced by the observation that motivates it. Question 6.1 generalises the fact that $4 \mid \mathrm{S}_{\mathrm{Dic}_{4n}}(m)$ for $m = 2, 3$ and odd $n \geq 3$; Question 6.2 generalises $4n \mid \gcd\{\mathrm{S}_{\mathrm{Dic}_{4n}}(m) : m = 2, 3\}$ for odd $n \geq 3$; Question 6.3 generalises the evenness of all three counts for odd $n \geq 3$ and $m = 2, 3$. In each case the evidence is exactly the two closed-form theorems, that is, the sizes $m = 2$ and $m = 3$. Every numbered result of [1] cited here — Theorems 1.4, 1.6, 1.8 and 1.9, Corollary 1.1, Questions 6.1–6.3 and Tables 1 and 2 — carries the numbering of its arXiv version v1, which is its only version to date.

Results. All three questions have the answer *no*, and a single cell settles all three.

Theorem 1.1. *Among the* 495 *four-element subsets of* Dic_{12} *there are exactly* 126 *MSTD sets,* 228 *MDTS sets and* 141 *balanced sets. Since* $4 \leq 2 \cdot 3$*, the pair* $(n, m) = (3, 4)$ *is admissible in all three questions, and*

$$126 \;=\; 2 \cdot 3^2 \cdot 7 \quad \textit{is divisible by neither } 4 \textit{ nor } 4n = 12, \qquad 141 \textit{ is odd.}$$

Hence Questions 6.1, 6.2 and 6.3 of [1] *are all false.*

The refutation does not depend on the smallest case. A second counterexample occurs at $n = 7$, a group outside the range tabulated in [1]: among the 20 475 four-element subsets of Dic_{28} there are 5586 MSTD sets and 7329 balanced sets, and $5586 = 2 \cdot 3 \cdot 7^2 \cdot 19$ is divisible by neither 4 nor 28, while 7329 is odd (Theorem 4.3). In its own gcd form, Question 6.2 at $n = 3$ reads $\gcd\{\mathrm{S}_{\mathrm{Dic}_{12}}(m) : m \geq 2\} = 6$, and $12 \nmid 6$ (Theorem 4.2). Both refuting cells have n odd, so the questions fail also under the more cautious reading in which n is restricted to the odd integers, the case from which they were extrapolated.

We state at once the one thing a reader should know about the provenance of the numbers in Theorem 1.1. The values $\mathrm{S}_{\mathrm{Dic}_{12}}(4) = 126$ and $\mathrm{D}_{\mathrm{Dic}_{12}}(4) = 228$ are the Dic_{12} entries at size 4 of Tables 1 and 2 of [1] itself, and $\mathrm{B}_{\mathrm{Dic}_{12}}(4) = 495 - 126 - 228 = 141$ is one subtraction away from them. They are older than that again. The paper of Neetu, Shetty and Shankar [9] on the groups of order 12, published in 2025 and cited by [1], proves in its Lemma 3.1 that Dic_{12} has exactly 126 MSTD subsets of size 4, and records in the paragraph after that lemma that it has 228 MDTS subsets of that size. The counterexample therefore lies not merely inside the published data of the paper it refutes, but inside the published literature of the year before: what is new here is the observation, not the arithmetic. The questions were extrapolated from the closed forms at $m = 2, 3$ without being tested against the table printed four pages earlier, or against [9], which [1] cites for the fact that subsets of more than half a group are balanced. Neither paper prints $\mathrm{B}_{\mathrm{Dic}_{12}}(4) = 141$; both print the two numbers it is one subtraction away from. What appears in neither is the rest: the cells at $n = 6$ and $n = 7$, the sizes $m = 11, 12$ of Dic_{12}, and every balanced count except $\mathrm{B}_{\mathrm{Dic}_{12}}(2) = 42$, which [9] does give.

A literature check current as of 2026-08-28: [1] stands at v1, with no later version and no journal reference; a Semantic Scholar citation query for it returns no citing works; an arXiv full-text query for papers mentioning both dicyclic groups and MSTD sets returns [1] and nothing else; and of the papers with `MSTD` in the abstract, none postdating [1] concerns dicyclic groups. One item we have not been able to consult is Neetu and B. R. Shankar, *Sum and difference sets in generalized quaternion groups*, Proc. Jangjeon Math. Soc. **27** (2024), no. 4, 773–780, which [9] describes as a first step on these questions for the generalized quaternion groups Q_{4n}; for n a power of two Q_{4n} is Dic_{4n}, and some authors use the name for the presentation (1) at every n, so that paper may well contain further counts of the kind reproduced here. It cannot bear on Questions 6.1–6.3, which postdate it by two years.

The failure is genuinely cell-by-cell rather than a blanket property of the size $m = 4$. At $n = 5$ one has $\mathrm{S}_{\mathrm{Dic}_{20}}(4) = 1380 = 4 \cdot 345 = 20 \cdot 69$ and at $n = 6$ one has $\mathrm{S}_{\mathrm{Dic}_{24}}(4) = 1944 = 4 \cdot 486 = 24 \cdot 81$, both divisible by 4 and by $4n$, so neither cell refutes the two divisibility questions; and $\mathrm{B}_{\mathrm{Dic}_{24}}(4) = 3906$ is even, so the cell $n = 6$, $m = 4$ refutes none of the three (Sections 3 and 5). Two further remarks delimit what is being claimed. First, at the sizes the source actually proved, $m = 2$ and $m = 3$, all three questions do hold at $n = 3$ (Proposition 5.1): the refutations are about the extrapolation past $m = 3$, not about a misreading of the hypotheses. Second, in every cell computed here — that is, $2 \le n \le 7$ over the ranges of Section 3 — the counts S and D are *even*, and only B is ever odd. Question 6.3 restricted to S and D therefore survives all the evidence assembled here, and we do not settle it (Remark 5.5). Nothing below bears on the two asymptotic conjectures of [1], which are not finitely decidable.

Section 2 fixes the group and the counting functions, Section 3 presents the computed profiles and the searches behind them, Section 4 proves the refutations, Section 5 bounds their scope, and Section 6 describes the formal verification.

2. Preliminaries

Every element of Dic_{4n} is uniquely of the form $a^k b^e$ with $k \in \mathbb{Z}/2n\mathbb{Z}$ and $e \in \{0, 1\}$. Written in this normal form, the relations (1) force the multiplication table

$$a^k \cdot a^l = a^{k+l}, \qquad a^k \cdot a^l b = a^{k+l} b, \qquad a^k b \cdot a^l = a^{k-l} b, \qquad a^k b \cdot a^l b = a^{k-l+n}, \tag{2}$$

with all exponents read modulo $2n$, and the inversion rule $(a^k)^{-1} = a^{-k}$, $(a^k b)^{-1} = a^{n+k} b$; these are the consequences of (1) that [1] quotes from [3, Lemma 2.6].

Lemma 2.1. *For every $n \ge 1$, the set of formal symbols $a^k b^e$ with $k \in \mathbb{Z}/2n\mathbb{Z}$ and $e \in \{0, 1\}$, under the multiplication (2), is a group of order $4n$ in which $a^{2n} = 1$, $a^n = b^2$ and $b^{-1}ab = a^{-1}$. Moreover every element outside $\langle a \rangle$ squares to a^n, and hence has order 4.*

The last clause is what distinguishes Dic_{4n} from the dihedral group of the same order, in which the elements outside the cyclic subgroup are involutions; it is used only as a check that the object under study is the right one. The proof of Lemma 2.1 is a direct verification for all n simultaneously — eight cases of associativity over the ring $\mathbb{Z}/2n\mathbb{Z}$, the only delicate one being $(a^k b \cdot a^l b) \cdot a^j b$, which uses $a^n \cdot a^n = 1$. No enumeration over n is involved.

Lemma 2.2. *Let A be a finite subset of a group G. Then $z \in A + A$ if and only if $z = xy$ for some $x, y \in A$, and $z \in A - A$ if and only if $z = xy^{-1}$ for some $x, y \in A$. Moreover exactly one of "A is MSTD", "A is MDTS", "A is balanced" holds.*

The first assertion is a triviality that we record because the whole paper depends on reading the convention of [2, 1] correctly: in a non-abelian group $A + A$ is the pointwise product $A \cdot A$ and $A - A$ is the pointwise quotient $A \cdot A^{-1}$, not any symmetrised variant. The second is the trichotomy of $|A + A|$ against $|A - A|$; it gives at once

$$\mathrm{S}_{\mathrm{Dic}_{4n}}(m) + \mathrm{D}_{\mathrm{Dic}_{4n}}(m) + \mathrm{B}_{\mathrm{Dic}_{4n}}(m) = \binom{4n}{m}, \tag{3}$$

and (3) is checked directly at the cells of Tables 1 and 2 below, and at the Dic_{28} cells of Table 3, so that in those rows no subset can have been counted twice or dropped.

3. The counts

Two computations. The counts were produced twice. The first computation ranges over the subsets of the group itself, forming the pointwise sets $A \cdot A$ and $A \cdot A^{-1}$ and comparing their cardinalities; it is the faithful transcription of the definitions, and it is expensive. The second represents Dic_{4n} on the integers $\{0, 1, \ldots, 4n-1\}$ through the bijection

$$a^k b^e \longmapsto 2ne + k \qquad (0 \le k < 2n,\ e \in \{0,1\}), \tag{4}$$

and a subset by the corresponding bit pattern, so that a whole sumset is accumulated by shifts and disjunctions on a single integer. This is what makes the larger cells affordable, and it is legitimate only because of the following.

Proposition 3.1. *The map* (4) *is a bijection from* Dic_{4n} *onto* $\{0, 1, \ldots, 4n-1\}$*, and for* $2 \le n \le 7$ *the integer operations used in the second computation are exactly the multiplication and inversion of* Dic_{4n} *transported along it. At every cell at which both computations were run they return the same triple* $(\mathrm{S}, \mathrm{D}, \mathrm{B})$.

The profiles. Tables 1, 2 and 3 give the complete profiles. Each entry is exact and is obtained by exhaustive enumeration of the $\binom{4n}{m}$ subsets of the stated size; no sampling, no symmetry reduction and no closed form is involved.

Table 1. $(\mathrm{S}, \mathrm{D}, \mathrm{B})$ for Dic_8 and Dic_{12}. Sizes $m > 8$ are vacuous for Dic_8.

	Dic_8			Dic_{12}		
m	S	D	B	S	D	B
2	0	0	28	24	0	42
3	0	24	32	24	48	148
4	16	24	30	126	228	141
5	0	0	56	120	264	408
6	0	0	28	60	48	816
7	0	0	8	0	0	792
8	0	0	1	0	0	495
9				0	0	220
10				0	0	66
11				0	0	12
12				0	0	1

Table 2. $(\mathrm{S}, \mathrm{D}, \mathrm{B})$ for Dic_{16} and Dic_{20}, sizes $2 \le m \le 10$.

	Dic_{16}			Dic_{20}		
m	S	D	B	S	D	B
2	32	0	88	80	0	110
3	96	160	304	400	200	540
4	392	832	596	1380	2080	1385
5	752	2016	1600	3840	7160	4504
6	1368	3344	3296	9520	19920	9320
7	992	1888	8560	14480	31760	31280
8	288	296	12286	11920	23520	90530
9	0	0	11440	5360	7080	155520
10	0	0	8008	1080	480	183196

TABLE 3. (S, D, B) for Dic_{24} and Dic_{28}, sizes $2 \le m \le 4$. These groups are not tabulated in [1].

	Dic_{24}			Dic_{28}		
m	S	D	B	S	D	B
2	96	0	180	168	0	210
3	576	384	1064	1512	532	1232
4	1944	4776	3906	5586	7560	7329

Proposition 3.2. *The* Dic_8 *columns of Table 1 at sizes* $2 \le m \le 8$*, and its* Dic_{12} *columns at sizes* $m = 2, 3, 4$*, are correct. In particular*

$$\big(\mathrm{S}_{\mathrm{Dic}_{12}}(4), \mathrm{D}_{\mathrm{Dic}_{12}}(4), \mathrm{B}_{\mathrm{Dic}_{12}}(4)\big) = (126, 228, 141), \qquad 126 + 228 + 141 = 495 = \binom{12}{4}.$$

Proof sketch. Exhaustive enumeration over the group itself, in the sense of the first computation described above: for each of the 247 subsets of Dic_8 of size between 2 and 8, and each of the 781 subsets of Dic_{12} of size 2, 3 or 4, the sets $A \cdot A$ and $A \cdot A^{-1}$ are formed and their cardinalities compared. The entire claim rests on that finite computation, which was carried out inside the Lean kernel (Section 6). □

Proposition 3.3. *All entries of Tables 1 and 2 are correct, and each row satisfies* (3)*. The* S *and* D *entries agree with the* $\mathrm{Dic}_8, \mathrm{Dic}_{12}, \mathrm{Dic}_{16}, \mathrm{Dic}_{20}$ *columns of Tables 1 and 2 of* [1] *at every one of the* 68 *non-vacuous cells; the remaining four published cells,* Dic_8 *at sizes* 9 *and* 10 *in each of the two tables, are vacuous because* $|\mathrm{Dic}_8| = 8$*, and the source prints* 0 *there.*

Proof sketch. Exhaustive enumeration in the index model of (4), licensed by Proposition 3.1: 4083 subsets for Dic_{12} at sizes $2 \le m \le 12$, 58 634 for Dic_{16} and 616 645 for Dic_{20} at sizes $2 \le m \le 10$, and the 247 subsets of Dic_8 again. The agreement with [1] is a comparison of 68 integers, and the row identities (3) are 36 further integer identities. Nothing here is proved by a general argument. □

One feature of the tables is not accidental. For every $m > 2n$, that is for subsets of more than half the group, the counts $\mathrm{S}_{\mathrm{Dic}_{4n}}(m)$ and $\mathrm{D}_{\mathrm{Dic}_{4n}}(m)$ vanish and every subset is balanced. This is the theorem of Neetu, Shetty and Shankar [9, Theorem 2.1], quoted in [1], that $|A| > |G|/2$ implies $|A + A| = |A - A|$ in any finite group G. Above $m = 2n$ there is thus nothing to count, which is presumably why Questions 6.1 and 6.3 stipulate $m \le 2n$; Question 6.2 does not.

Proposition 3.3 is a reproduction of published data, and we claim no novelty for the S and D entries; its role is to make the reading of the convention in Lemma 2.2 an empirical fact rather than an interpretation, since a different reading of $A+A$ or $A-A$ would not reproduce 68 published integers. The balanced counts B are not printed in [1], but they are forced by (3) from the two published rows, so they are new only in the weakest sense.

Proposition 3.4. *All entries of Table 3 are correct, and each* Dic_{28} *row satisfies* (3)*.*

Proof sketch. Exhaustive enumeration in the index model over the 12 926 subsets of Dic_{24} and the 24 129 subsets of Dic_{28} of sizes 2, 3 and 4. □

These two groups lie outside the tables of [1], but not entirely outside its theorems: the size-two entries are predicted by its Theorem 1.4, and the size-three entries of Dic_{28} by its Theorem 1.6 for odd n with $3 \nmid n$. Every value so predicted agrees, namely $4n(n-2) = 96$ and $2n(2n+3) = 180$ at $n = 6$; and $4n(n-1) = 168$, $2n(2n+1) = 210$, $4n(n-1)(2n-5) = 1512$, $2n(n-1)(2n+5)/3 = 532$ and $2n(2n^2 + 27n - 23)/3 = 1232$ at $n = 7$. This is a check of the computation against closed forms at cells that no table covers. For $m = 4$ the source has no formula, and those six values appear neither in [1] nor in [9]. Altogether the distinct cells enumerated in this section comprise 716 664 subsets.

4. The three questions

We first fix the reading of each question. A positive integer d divides $\gcd S$, for a set S of non-negative integers, precisely when d divides every member of S; so each question is a universally quantified divisibility or parity statement, and refuting it means exhibiting one member of the relevant set that fails. Explicitly:

(5) Q6.1 : for all $m \geq 2$ and all $n \geq 3$ with $m \leq 2n$, $\quad 4 \mid \mathrm{S}_{\mathrm{Dic}_{4n}}(m)$;

(6) Q6.2 : for all $n \geq 3$ and all $m \geq 2$, $\quad 4n \mid \mathrm{S}_{\mathrm{Dic}_{4n}}(m)$;

(7) Q6.3 : for all $n \geq 3$ and all m with $2 \leq m \leq 2n$, $\quad \mathrm{S}_{\mathrm{Dic}_{4n}}(m)$, $\mathrm{D}_{\mathrm{Dic}_{4n}}(m)$, $\mathrm{B}_{\mathrm{Dic}_{4n}}(m)$ are even.

In Question 6.1 the constraint $2 \leq m \leq 2n$ contains the bound variable n of the gcd, so a literal reading has to attach it either to the fixed m or to the range of n; (5) takes the second, more generous option, under which the assertion is weakest. The counterexample below has $m = 4$ and $n = 3$, hence $2 \leq m \leq 2n = 6$, so it refutes the question under either reading.

Theorem 4.1. *Statements* (5), (6) *and* (7) *are all false. Each fails at $n = 3$, $m = 4$:*

$$\mathrm{S}_{\mathrm{Dic}_{12}}(4) = 126 = 2 \cdot 3^2 \cdot 7, \qquad \mathrm{D}_{\mathrm{Dic}_{12}}(4) = 228, \qquad \mathrm{B}_{\mathrm{Dic}_{12}}(4) = 141.$$

Indeed $4 \nmid 126$ *refutes* (5) *at $m = 4$; $12 \nmid 126$ refutes* (6) *at $n = 3$; and* 141 *is odd, which refutes* (7).

Proof. The three values are Proposition 3.2, which rests on the exhaustive enumeration of the 495 four-element subsets of Dic_{12} described there. The cell is admissible: $n = 3 \geq 3$ and $2 \leq 4 \leq 6 = 2n$. The three arithmetic facts $126 = 4 \cdot 31 + 2$, $126 = 12 \cdot 10 + 6$ and $141 = 2 \cdot 70 + 1$ then contradict (5), (6) and (7) respectively. □

Theorem 4.2. $\gcd\{\mathrm{S}_{\mathrm{Dic}_{12}}(m) \ : \ 2 \leq m \leq 12\} = 6$. *Consequently* $\gcd\{\mathrm{S}_{\mathrm{Dic}_{12}}(m) : m \geq 2\} = 6$ *as well, and $4n = 12$ does not divide it: Question 6.2 fails at $n = 3$ in its own* gcd *form.*

Proof. By Proposition 3.3 the row of MSTD counts of Dic_{12} is $(24, 24, 126, 120, 60, 0, 0, 0, 0, 0, 0)$ for $m = 2, \ldots, 12$, whose gcd is 6. For $m > 12$ the group Dic_{12} has no subset of size m at all, so $\mathrm{S}_{\mathrm{Dic}_{12}}(m) = 0$ and the gcd over all $m \geq 2$ is unchanged. Finally $6 < 12$, so $12 \nmid 6$. □

Theorem 4.3. *Among the* 20 475 *four-element subsets of* Dic_{28} *there are exactly* 5586 *MSTD sets,* 7560 *MDTS sets and* 7329 *balanced sets. Since*

$$5586 = 2 \cdot 3 \cdot 7^2 \cdot 19 \quad \textit{is divisible by neither } 4 \textit{ nor } 4n = 28, \qquad \textit{and } 7329 \textit{ is odd},$$

the cell $n = 7$, $m = 4$ refutes (5), (6) *and* (7) *independently of Theorem 4.1.*

Proof. The three values are the last row of Table 3 (Proposition 3.4), obtained by exhaustive enumeration of the $\binom{28}{4} = 20\,475$ four-element subsets; their sum is 20 475, as (3) requires. The cell is admissible, $n = 7 \geq 3$ and $2 \leq 4 \leq 14 = 2n$. Finally $5586 = 4 \cdot 1396 + 2$ and $5586 = 28 \cdot 199 + 14$, and 7329 is odd. □

Remark 4.4. Both refuting cells have n odd. The sentences of [1] that motivate the three questions all speak of odd n, the questions themselves having dropped that hypothesis; the counterexamples above therefore refute the odd-n readings as well. Note also that Theorem 4.1 refutes Questions 6.1 and 6.2 through the same integer, $\mathrm{S}_{\mathrm{Dic}_{12}}(4)$, and that this integer is printed in Table 1 of [1].

5. How far the failure reaches

Three propositions delimit the refutation. The first says that the questions are true on the evidence from which they were extrapolated, so that what fails is the extrapolation and not a misreading of the hypotheses.

Proposition 5.1. *At $n = 3$ and $m = 2$ the three counts are $(24, 0, 42)$, and at $n = 3$ and $m = 3$ they are $(24, 48, 148)$. Hence at these two cells 4 and $4n = 12$ both divide $\mathrm{S}_{\mathrm{Dic}_{12}}(m)$ and all six counts are even: statements* (5), (6) *and* (7) *hold there. Moreover* $\mathrm{S}_{\mathrm{Dic}_{12}}(3) = 24 < 48 = \mathrm{D}_{\mathrm{Dic}_{12}}(3)$, *so the exception at $n = 3$ in Corollary 1.1 of* [1] *is real.*

So all three questions are true at every cell the closed forms of [1] cover with $n = 3$, and all three are false at the very next size.

Proposition 5.2. $\mathrm{S}_{\mathrm{Dic}_{20}}(4) = 1380 = 4 \cdot 345 = 20 \cdot 69$ *is divisible by* 4 *and by* $4n = 20$*, so the cell* $n = 5$*,* $m = 4$ *refutes neither* (5) *nor* (6)*. On the other hand* $\mathrm{B}_{\mathrm{Dic}_{20}}(4) = 1385$ *is odd, so that cell does refute* (7)*.*

Together with Table 3, where $\mathrm{S}_{\mathrm{Dic}_{24}}(4) = 1944 = 4 \cdot 486 = 24 \cdot 81$ and $\mathrm{B}_{\mathrm{Dic}_{24}}(4) = 3906$ is even, this shows that the size $m = 4$ is not by itself fatal to any of the three questions. Over the cells computed here, statement (5) fails at $m = 4$ for $n = 3$ and $n = 7$ and holds there for $n = 4, 5, 6$, and statement (7) fails at $m = 4$ for $n = 3, 5, 7$ and holds there for $n = 4$ and $n = 6$. Any repair of Questions 6.1 and 6.3 must therefore be sensitive to n and not only to m.

Remark 5.3. Statement (6) fails at further cells still, and again inside the tables of [1]. At $n = 4$ those tables give $\mathrm{S}_{\mathrm{Dic}_{16}}(4) = 392 = 2^3 \cdot 7^2$ and $\mathrm{S}_{\mathrm{Dic}_{16}}(6) = 1368 = 2^3 \cdot 3^2 \cdot 19$, neither of which is divisible by $4n = 16$; both are divisible by 4, so Question 6.1 is untouched by them. These two failures do not survive the restriction to odd n from which Question 6.2 was extrapolated, whereas the failures at $n = 3$ and $n = 7$ in Theorems 4.1 and 4.3 do. Unlike the refutations of Section 4, this remark is an arithmetic consequence drawn by hand from the tabulated values of Proposition 3.3; the two divisibility failures it records are not themselves machine-checked.

Proposition 5.4. *The following hold in* Dic_{12}*, with* A *ranging over four-element subsets.*

(1) $A = \{1, a, a^4, b\}$ *has* $|A + A| = 11$ *and* $|A - A| = 10$*, so* A *is MSTD;* $A = \{1, a, a^2, b\}$ *has* $|A+A| = 10$ *and* $|A-A| = 11$*, so* A *is MDTS; and* $A = \{1, a, a^2, a^3\}$ *has* $|A+A| = |A-A| = 6$*, so* A *is balanced. In particular none of the three counts is vacuous, and the three properties are pairwise distinct.*

(2) *Not every subset of* Dic_{12} *is MSTD, and not every subset is balanced; and* $\mathrm{S}_{\mathrm{Dic}_{12}}(4) \neq \mathrm{D}_{\mathrm{Dic}_{12}}(4)$*,* $\mathrm{S}_{\mathrm{Dic}_{12}}(4) \neq 0$*,* $\mathrm{B}_{\mathrm{Dic}_{12}}(4) \neq 0$*.*

(3) Dic_{12} *is non-abelian, has exactly two solutions of* $x^2 = 1$*, and every element outside* $\langle a \rangle$ *has order* 4*.*

(4) *For* Dic_4 *one has* $(\mathrm{S}, \mathrm{D}, \mathrm{B}) = (0, 0, \binom{4}{m})$ *for* $1 \le m \le 4$*: the group is abelian and every subset is balanced.*

Item (3) is the point at which the object is pinned down: the dihedral group of order 12 has eight solutions of $x^2 = 1$, so the count 2 identifies the group as dicyclic; and non-commutativity is what makes $A + A$ and $A - A$ genuinely different constructions. Item (4) reproduces the remark in [1] that at $n = 1$ the group is $\mathbb{Z}/4\mathbb{Z}$ and all its subsets are balanced, which is the degenerate parameter of the problem.

Remark 5.5. In every cell of Tables 1–3 the counts $\mathrm{S}_{\mathrm{Dic}_{4n}}(m)$ and $\mathrm{D}_{\mathrm{Dic}_{4n}}(m)$ are even, and $\mathrm{B}_{\mathrm{Dic}_{4n}}(m)$ is the only one that is ever odd. Among the cells admissible in Question 6.3, namely $n \ge 3$ and $2 \le m \le 2n$, it is odd exactly at $(n, m) = (3, 4)$, $(5, 4)$ and $(7, 4)$; it is odd also at $(2, 8)$, $(3, 8)$ and $(3, 12)$, which lie outside that range. The refutation of Question 6.3 above is therefore a refutation of its balanced-set component only. Whether $\mathrm{S}_{\mathrm{Dic}_{4n}}(m)$ and $\mathrm{D}_{\mathrm{Dic}_{4n}}(m)$ are always even remains open, and the evidence here is consistent with it; we have no proof, and in particular we know of no type-preserving involution on m-subsets that would supply one.

The parity of B is not independent of the other two: by (3), B is odd exactly when $\binom{4n}{m} - \mathrm{S} - \mathrm{D}$ is odd, so over the range computed here, where S and D are even, $\mathrm{B}_{\mathrm{Dic}_{4n}}(m)$ is odd exactly when $\binom{4n}{m}$ is. Question 6.3 thus already fails, over this range, at every cell where $\binom{4n}{m}$ is odd — and $\binom{12}{4} = 495$ is odd. This is the shortest description of what went wrong: the parity question is in conflict with the parity of a binomial coefficient long before any group theory is used.

6. Verification

Every theorem, proposition and lemma in this paper has been formally verified in Lean 4 (toolchain `leanprover/lean4:v4.32.0`) against *Mathlib* [11, 10] at commit `81a5d257c8e410db227a6665ed08` `f64fea08e997`; the development contains no `sorry`, and each of them corresponds to a named declaration in it. The remarks are commentary, and Remark 5.3 in particular draws an arithmetic consequence from the machine-checked values of Proposition 3.3 without being checked separately. Lemmas 2.1 and 2.2, Propositions 3.1 and 3.2, Theorems 1.1 and 4.1, and Propositions 5.1 and 5.4 depend on no axioms beyond `propext`, `Classical.choice` and `Quot.sound`; in particular the refutation of all three questions at $n = 3$, $m = 4$, together with the value $(\mathrm{S}_{\mathrm{Dic}_{12}}(4), \mathrm{D}_{\mathrm{Dic}_{12}}(4), \mathrm{B}_{\mathrm{Dic}_{12}}(4)) = (126, 228, 141)$ on which it rests, is checked by the Lean kernel itself, evaluating the pointwise products $A \cdot A$ and quotients $A \cdot A^{-1}$ over subsets of the group as defined in Section 2. What is delegated to compiled evaluation, through Lean's `native_decide`, is exactly the enumerative sweeps: Propositions 3.3, 3.4 and 5.2, and hence Theorems 4.2 and 4.3, which quote their values. Those sweeps run in the index model of (4), whose identification with the group — for each of $n = 2, \ldots, 7$, a check of all $(4n)^2$ products and all $4n$ inverses, together with the bijectivity of (4) and the agreement of the two counting procedures at every overlapping cell — is Proposition 3.1 and is itself kernel-checked. The counts were also produced outside Lean, by a separate implementation in Python written before the formal statements: that implementation reproduces all 68 published cells of [1] and matches its closed forms at every $n \leq 7$ where they apply. Repository reference to be added at submission.

References

[1] S. Mandal and Neetu, *Exact and asymptotic counts of MSTD, MDTS, and balanced sets in dicyclic groups*, arXiv:2602.09073v1 (2026).

[2] S. J. Miller and K. Vissuet, *Most subsets are balanced in finite groups*, in: Combinatorial and additive number theory—CANT 2011 and 2012, 147–157, Springer Proc. Math. Stat., 101, Springer, New York, 2014.

[3] T. Cheng, L. Feng and H. Huang, *Integral Cayley graphs over dicyclic group*, Linear Algebra Appl. **566** (2019), 121–137.

[4] M. B. Nathanson, *Sets with more sums than differences*, Integers **7** (2007), A5, 24 pp.

[5] G. Martin and K. O'Bryant, *Many sets have more sums than differences*, in: Additive combinatorics, 287–305, CRM Proc. Lecture Notes, 43, Amer. Math. Soc., Providence, RI, 2007.

[6] Y. Zhao, *Counting MSTD sets in finite abelian groups*, J. Number Theory **130** (2010), no. 10, 2308–2322.

[7] Y. Zhao, *Sets characterized by missing sums and differences*, J. Number Theory **131** (2011), no. 11, 2107–2134.

[8] R. Ascoli, J. Cheigh, G. Zeus Dantas e Moura, R. Jeong, A. Keisling, A. Lilly, S. J. Miller, P. Ngamlamai and M. Phang, *Sum and difference sets in generalized dihedral groups*, in: Combinatorics and combinatorial computing, 1–30, Springer Proc. Math. Stat., 516, Springer, Cham; arXiv:2210.00669. Cited as "to appear" in [1]; the chapter appeared online on 15 September 2025.

[9] Neetu, A. Shetty and B. R. Shankar, *A note on sumsets and difference sets in groups of order 12*, Bol. Soc. Paran. Mat. (3) **43** (2025), no. 3, 1–12.

[10] L. de Moura and S. Ullrich, *The Lean 4 theorem prover and programming language*, in: Automated Deduction—CADE 28, 625–635, Lecture Notes in Comput. Sci., Springer, Cham, 2021.

[11] The mathlib Community, *The Lean mathematical library*, in: Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs (CPP 2020), 367–381, ACM, New York, 2020.