

Möbius Cube-Square Refinement of Commuting Triples in Dihedral Groups

Augusto Rehfeldt

Text generated by language models in the mathforge pipeline; not reviewed by a person.

Abstract

For the dihedral group D_n of order $2n$, we count ordered commuting triples (x, y, z) jointly by the number $k \in \{0, 1, 2, 3\}$ of reflections among the entries and by the order d of the rotation part $\langle x, y, z \rangle \cap \langle r \rangle$. If $d \nmid n$ the count $T(n, k, d)$ is 0. If $d \mid n$ and $k = 0$ it is $\sum_{e \mid d} \mu(d/e) e^3$. If $k = 1$ or $k = 2$ it is $3n \sum_{e \mid d} \mu(d/e) e^2$ when $d \mid \gcd(n, 2)$ and 0 otherwise. If $k = 3$ it is $n \sum_{e \mid d} \mu(d/e) e^2$ when $d \mid \gcd(n, 2)$ and 0 otherwise. The formula was verified by exhaustive enumeration for $1 \leq n \leq 12$ with no counterexample, confirmed by an independent check, and formalized in Lean 4 to the level of compiles with `sorry` with a faithful statement back-translation.

1. Introduction

Context

Commuting-pair probabilities and total numbers $|\text{Hom}(\mathbb{Z}^r, G)|$ of commuting r -tuples for finite groups, including dihedral groups, are known. The dihedral centralizer facts used here are elementary: a rotation commutes with a reflection only when the rotation has order dividing 2, and two reflections commute only when their product has order dividing 2. Counting generating tuples of a cyclic group by Möbius inversion, i.e. Jordan's totient $J_m(d) = \sum_{e \mid d} \mu(d/e) e^m$, is standard.

What is new

What is new is the exact joint refinement for commuting triples in D_n by both the reflection number k and the exact order d of the generated rotation subgroup, with a cube law for $k = 0$ versus a square law with prefactors $3n$ for $k = 1, 2$ and n for $k = 3$, and a vanishing condition outside $d \mid \gcd(n, 2)$ for $k \geq 1$. The novelty assessment is `APPARENTLY_NEW` on the basis of a bounded automated search described in Section 5, not a full literature review. The $k = 0$ case alone is standard; the full $k = 1, 2, 3$ refinement with $3n$ versus n prefactors is the claimed new part.

2. Notation

D_n is the group of order $2n$ presented as $\langle r, s \mid r^n = 1, s^2 = 1, srs = r^{-1} \rangle$; $\langle r \rangle$ is its cyclic rotation subgroup of order n and elements outside $\langle r \rangle$ are reflections; $\langle x, y, z \rangle$ is the subgroup generated by x, y, z ; $|\cdot|$ is group order; $\gcd$ is greatest common divisor; e dividing d means e is a positive divisor of d ; μ is the Möbius function with $\mu(1) = 1$, $\mu(m) = (-1)^t$ if m is a product of t distinct primes, and $\mu(m) = 0$ otherwise.

3. Results

Theorem (Möbius cube-square refinement). *For every integer $n \geq 1$, every $k \in \{0, 1, 2, 3\}$ and every integer $d \geq 1$, let $T(n, k, d)$ be the number of ordered triples (x, y, z) in D_n^3 such that $xy = yx$, $xz = zx$, $yz = zy$, exactly k of x, y, z lie outside the rotation subgroup $\langle r \rangle$, and the order of $\langle x, y, z \rangle \cap \langle r \rangle$ equals d . Then if d*

does not divide n , $T(n, k, d) = 0$; if d divides n and $k = 0$, $T(n, k, d)$ equals the sum over e dividing d of $\mu(d/e)e^3$; if $k = 1$ or $k = 2$, $T(n, k, d)$ equals $3n$ times the sum over e dividing d of $\mu(d/e)e^2$ when d divides $\gcd(n, 2)$ and equals 0 otherwise; if $k = 3$, $T(n, k, d)$ equals n times the sum over e dividing d of $\mu(d/e)e^2$ when d divides $\gcd(n, 2)$ and equals 0 otherwise.

Full proof, verbatim from the verified proof:

Proof of the commuting-triple formula for D_n . We prove the theorem stated below. Let $n \geq 1$ and

$$D_n = \langle r, s \mid r^n = 1, s^2 = 1, srs = r^{-1} \rangle.$$

Write $C = \langle r \rangle$. An element of D_n in C is called a rotation; an element outside C is called a reflection. For $(x, y, z) \in D_n^3$, write $\langle x, y, z \rangle$ for the subgroup they generate. For integers $n \geq 1$, $k \in \{0, 1, 2, 3\}$, $d \geq 1$, let $T(n, k, d)$ be the number of ordered triples $(x, y, z) \in D_n^3$ such that $xy = yx$, $xz = zx$, $yz = zy$, exactly k of x, y, z lie outside C , and $|\langle x, y, z \rangle \cap C| = d$.

□

Theorem. *If $d \nmid n$ then $T(n, k, d) = 0$. If $d \mid n$ and $k = 0$ then*

$$T(n, k, d) = \sum_{e \mid d} \mu(d/e) e^3.$$

If $k = 1$ or $k = 2$ then $T(n, k, d) = 3n \sum_{e \mid d} \mu(d/e) e^2$ when $d \mid \gcd(n, 2)$ and $T(n, k, d) = 0$ otherwise. If $k = 3$ then $T(n, k, d) = n \sum_{e \mid d} \mu(d/e) e^2$ when $d \mid \gcd(n, 2)$ and $T(n, k, d) = 0$ otherwise. Here μ is the Möbius function.

Lemma 1 (Structure of D_n). *D_n has order $2n$. The subgroup $C = \langle r \rangle$ is cyclic of order n , normal of index 2. Every element of D_n is uniquely of the form r^b or sr^a with $a, b \in \mathbb{Z}_n$, and $(sr^a)^2 = 1$ for every a .*

Proof. Let $V = \mathbb{Z}_n \times \{+1, -1\}$ with multiplication

$$(b_1, \epsilon_1)(b_2, \epsilon_2) = (b_1 + \epsilon_1 b_2, \epsilon_1 \epsilon_2),$$

where ϵ_i acts on $\mathbb{Z}_n$ by multiplication by ± 1 . A direct verification shows V is a group. Put $r_V = (1, +1)$ and $s_V = (0, -1)$. Then $r_V^n = (0, +1)$, $s_V^2 = (0, +1)$, and $s_V r_V s_V = (0, -1)(1, +1)(0, -1) = (-1, +1) = r_V^{-1}$. Every element of V equals $r_V^b = (b, +1)$ or $s_V r_V^a = (a, -1)$, so $|V| = 2n$.

In any group satisfying the three defining relations, $s^{-1} = s$ from $s^2 = 1$, and $srs = r^{-1}$ gives $sr^b s^{-1} = r^{-b}$ for all integers b , whence $r^b s = sr^{-b}$. Therefore every word in r, s reduces to r^i or sr^i , and reducing exponents modulo n shows there are at most $2n$ elements. Hence the relations present a group of order at most $2n$, while V is a model of order exactly $2n$ satisfying them. So $D_n \cong V$ has order $2n$, and the normal form is unique. In particular $|C| = n$ and $[D_n : C] = 2$, so C is normal. Moreover $sr^a sr^a = r^{-a} r^a = 1$ using $sr^a s^{-1} = r^{-a}$ and $s^2 = 1$, so $(sr^a)^2 = 1$.

□

Henceforth exponents are read modulo n , and rotations are r^b , reflections sr^a .

Lemma 2 (Commutation criteria). *Rotations commute with each other. A rotation r^b commutes with a reflection sr^a if and only if $2b = 0$ in $\mathbb{Z}_n$. Two reflections sr^a and sr^b commute if and only if $2(b - a) = 0$ in $\mathbb{Z}_n$.*

Proof. Rotations lie in the cyclic group C and hence commute. Using $r^b s = sr^{-b}$ from Lemma 1,

$$(sr^a)r^b = sr^{a+b}, \quad r^b(sr^a) = r^b sr^a = sr^{-b} r^a = sr^{a-b}.$$

By uniqueness of the normal form, these are equal if and only if $a + b = a - b$ in $\mathbb{Z}_n$, i.e. $2b = 0$. Similarly,

$$(sr^a)(sr^b) = sr^a sr^b = r^{-a} r^b = r^{b-a}, \quad (sr^b)(sr^a) = r^{a-b},$$

both rotations, and equality holds if and only if $r^{b-a} = r^{a-b}$, i.e. $2(b-a) = 0$ in $\mathbb{Z}_n$. □

Lemma 3 (Annihilator of 2). *Let $A = \{b \in \mathbb{Z}_n : 2b = 0\}$. Then A is a subgroup of the additive group $\mathbb{Z}_n$ of order $g = \gcd(n, 2)$. Explicitly, if n is odd $A = \{0\}$; if n is even $A = \{0, n/2\}$.*

Proof. A is the kernel of the endomorphism $b \mapsto 2b$ and hence a subgroup. Write $g = \gcd(n, 2)$. Then $2b = 0 \pmod n$ means $n \mid 2b$. Dividing by g , $(n/g) \mid (2/g)b$ with $\gcd(n/g, 2/g) = 1$, so $(n/g) \mid b$. Conversely every multiple of n/g satisfies $2b = 0 \pmod n$ since $2(n/g) = (2/g)n$. Thus A consists of the g residues $0, n/g, 2n/g, \dots, (g-1)n/g$. For $g = 1$ this is $\{0\}$; for $g = 2$ it is $\{0, n/2\}$. □

Under $b \leftrightarrow r^b$, A corresponds to $\{h \in C : h^2 = 1\}$, the unique subgroup of C of order g .

Lemma 4 (Möbius inversion). *For $m \geq 1$, $\sum_{c \mid m} \mu(c)$ equals 1 if $m = 1$ and 0 if $m > 1$. Consequently, if F, A are functions on positive divisors with $A(e) = \sum_{e' \mid e} F(e')$ for all $e \mid N$, then $F(d) = \sum_{e \mid d} \mu(d/e) A(e)$ for all $d \mid N$.*

Proof. For $m = 1$ the sum is $\mu(1) = 1$. Let $m > 1$ with $t \geq 1$ distinct prime factors. Only squarefree divisors contribute, since μ vanishes otherwise. There are $\binom{t}{j}$ squarefree divisors with j primes, each contributing $(-1)^j$. Hence the sum is $\sum_{j=0}^t \binom{t}{j} (-1)^j = (1-1)^t = 0$.

For inversion, fix $d \mid N$ and expand:

$$\sum_{e \mid d} \mu(d/e) A(e) = \sum_{e \mid d} \mu(d/e) \sum_{e' \mid e} F(e') = \sum_{e' \mid d} F(e') \sum_{c \mid (d/e')} \mu(c),$$

writing $c = d/e$. The inner sum is 1 when $d/e' = 1$, i.e. $e' = d$, and 0 otherwise by the first assertion. Hence the total equals $F(d)$. □

Lemma 5 (Exact generation counts in cyclic groups). *Let C_N be cyclic of order N , $m \geq 1$ fixed. For $e \mid N$ let U_e be the unique subgroup of order e . Let $F_m(e)$ be the number of m -tuples in U_e^m generating exactly U_e . Then $e^m = \sum_{e' \mid e} F_m(e')$, and for $d \mid N$,*

$$F_m(d) = \sum_{e \mid d} \mu(d/e) e^m.$$

If $d \nmid N$ there is no subgroup of order d and the number of m -tuples generating a subgroup of order d is 0.

Proof. C_N has a unique subgroup of each order dividing N . Every m -tuple with entries in U_e generates a subgroup of U_e , hence exactly $U_{e'}$ for a unique $e' \mid e$. Partitioning the e^m tuples by the order generated gives $e^m = \sum_{e' \mid e} F_m(e')$. Lemma 4 then yields the formula for $d \mid N$. If $d \nmid N$, C_N has no subgroup of order d , so the count is 0. □

Lemma 6 (Rotation part of a subgroup generated with one reflection). *Let $a \in \mathbb{Z}_n$ and $K_0 \leq C$. Let $H = \langle sr^a, K_0 \rangle$. Then $K_0 \triangleleft H$, H/K_0 has order 2 generated by the coset of sr^a , and $H \cap C = K_0$.*

Proof. Every subgroup of the abelian group C is preserved by inversion. Conjugation by sr^a acts on C as inversion, since $(sr^a)r^t(sr^a)^{-1} = r^{-t}$ (using $(sr^a)^{-1} = sr^a$ and $sr^t sr^{-t}$ computation as in Lemma 2). Hence K_0 is normalized by sr^a and by itself, so $K_0 \triangleleft H$. The quotient H/K_0 is generated by the image of sr^a , whose square is $1 \in K_0$, so $|H/K_0| \leq 2$. Since $sr^a \notin C \supseteq K_0$, the coset is nontrivial and $|H/K_0| = 2$. As $K_0 \leq H \cap C \leq H$ with $[H : K_0] = 2$ and $H \cap C \neq H$ (because $sr^a \in H \setminus C$), equality $H \cap C = K_0$ follows. $\square$

Proof of the theorem. If $H \leq D_n$ then $H \cap C \leq C$ has order dividing $|C| = n$ by Lagrange's theorem. Hence if $d \nmid n$ no triple has $|\langle x, y, z \rangle \cap C| = d$, so $T(n, k, d) = 0$ for all k . Assume henceforth $d \mid n$.

Write $g = \gcd(n, 2)$ and A as in Lemma 3. Let $U_g \leq C$ be the unique subgroup of order g ; under $b \leftrightarrow r^b$, $U_g = \{r^b : b \in A\}$.

Case $k = 0$. All entries are rotations, which commute pairwise by Lemma 2. Since $\langle x, y, z \rangle \leq C$, we have $\langle x, y, z \rangle \cap C = \langle x, y, z \rangle$. Counting ordered triples in C^3 generating a subgroup of order d is Lemma 5 with $N = n$, $m = 3$: it is 0 if $d \nmid n$ and $\sum_{e|d} \mu(d/e)e^3$ if $d \mid n$.

Case $k = 1$. Permuting coordinates preserves pairwise commutation, the number of reflections, and the generated subgroup. Hence the three position patterns for the single reflection have equal counts and are disjoint. Fix the pattern (sr^a, r^b, r^c) . By Lemma 2, commutation holds if and only if $2b = 2c = 0$, i.e. $b, c \in A$, while $a \in \mathbb{Z}_n$ is unrestricted. Thus commuting triples of this pattern are in bijection with $\mathbb{Z}_n \times A \times A$.

For such a triple, $H = \langle sr^a, r^b, r^c \rangle = \langle sr^a, K_0 \rangle$ with $K_0 = \langle r^b, r^c \rangle$, so Lemma 6 gives $H \cap C = K_0 = \langle r^b, r^c \rangle$, independent of a . Since $b, c \in A$, $K_0 \leq U_g$. The number of pairs $(b, c) \in A^2$ with $\langle r^b, r^c \rangle$ of order d is the number of pairs in U_g^2 generating order d : it is 0 if $d \nmid g$ (subgroups of U_g have orders dividing g), and $\sum_{e|d} \mu(d/e)e^2$ if $d \mid g$ by Lemma 5 with $N = g$, $m = 2$. For each such pair there are n choices of a . Hence one position contributes $nF(d)$, where $F(d)$ is that pair count, and the three positions give $T(n, 1, d) = 3nF(d)$. Since $g \mid n$, $d \mid g$ implies $d \mid n$. This is exactly $3n \sum_{e|d} \mu(d/e)e^2$ when $d \mid g$ and 0 otherwise.

Case $k = 2$. Again the three patterns (choice of the rotation position) are symmetric and disjoint. Fix (sr^a, sr^b, r^c) . By Lemma 2, commutation holds if and only if $2(b - a) = 0$ and $2c = 0$, i.e. $t = b - a \in A$ and $c \in A$. Thus data are equivalent to $(a, t, c) \in \mathbb{Z}_n \times A \times A$ via $b = a + t$. Let $K_0 = \langle r^{b-a}, r^c \rangle = \langle r^t, r^c \rangle$. Then $r^{b-a} = (sr^a)(sr^b) \in H$ and $sr^b = (sr^a)r^{b-a}$, so $H = \langle sr^a, sr^b, r^c \rangle = \langle sr^a, K_0 \rangle$. Lemma 6 gives $H \cap C = K_0 = \langle r^t, r^c \rangle$, depending only on (t, c) . As before the number of $(t, c) \in A^2$ generating order d is $F(d)$, 0 unless $d \mid g$. With n choices of a per (t, c) and three patterns, $T(n, 2, d) = 3nF(d)$, the same formula as for $k = 1$.

Case $k = 3$. Triples (sr^a, sr^b, sr^c) commute pairwise if and only if the three pairwise differences are annihilated by 2 by Lemma 2. Since A is a subgroup, $b - a \in A$ and $c - a \in A$ imply $c - b \in A$, and conversely. Hence with $t_1 = b - a$, $t_2 = c - a$, commuting triples are in bijection with $(a, t_1, t_2) \in \mathbb{Z}_n \times A \times A$. Let $K_0 = \langle r^{b-a}, r^{c-a} \rangle = \langle r^{t_1}, r^{t_2} \rangle$. Then $(sr^a)(sr^b) = r^{b-a} \in H$, $(sr^a)(sr^c) = r^{c-a} \in H$, and $sr^b = (sr^a)r^{b-a}$, $sr^c = (sr^a)r^{c-a}$, so $H = \langle sr^a, K_0 \rangle$. Lemma 6 gives $H \cap C = K_0$. The number of (t_1, t_2) generating order d is $F(d)$ as above, and a has n independent choices. There is only one position pattern, so $T(n, 3, d) = nF(d)$, i.e. $n \sum_{e|d} \mu(d/e)e^2$ when $d \mid g$ and 0 otherwise.

This establishes all asserted formulas. $\square$

4. Computational verification

The search space was: for each n with $1 \leq n \leq 12$, construct D_n as permutations or as pairs (a, i) with $a \in \mathbb{Z}_n$ and $i \in \{0, 1\}$, enumerate all $(2n)^3$ ordered triples, keep those with pairwise commuting entries, compute k as the count of entries with $i = 1$, compute G as the subgroup generated by the triple by closure, compute d as the size of G intersected with the rotation subgroup, tabulate observed $T(n, k, d)$ for all $k \in \{0, 1, 2, 3\}$ and all d dividing n , and compare to the formula. Any mismatch is a counterexample.

The falsification run exited with code 0 and reported: Möbius values check OK for $\{1 : 1, 2 : -1, 3 : -1, 4 : 0, 5 : -1, 6 : 1, 7 : -1, 8 : 0, 9 : 0, 10 : 1, 30 : -1, 12 : 0\}$; commute cross-check for $n = 1$ to 12 OK; totals $D_1 = 8$ and $D_2 = 64$ plus subgroup cross-check OK; NO COUNTEREXAMPLE checked $n=1..12$ $k=0..3$ $d|n$ cases=140 triples=48672. No repairs were needed.

The independent check exited with code 0 and reported Lemma 1 OK through Lemma 6 OK and Theorem OK, followed by ALL CHECKS PASSED, with no repairs.

Lean 4 status for the theorem: compiles with `sorry` (not attempted / failed to compile / compiles with `sorry` / machine-checked sorry-free). Concretely, the Lean file compiled with exit code 0, `compiles: true`, `sorry_free: false`, 8 sorries, with warnings that the declaration uses `sorry` and that `main_theorem` depends on axioms [`propext`, `sorryAx`, `Classical.choice`, `Quot.sound`] including the unexpected axiom `sorryAx`. No repairs were made. A sorry-free Lean proof would certify the Lean statement, which still has to be read against the informal one.

Back-translation faithfulness verdict on the Lean statement: FAITHFUL, with no differences noted and `trivialized: false`. The back-translation reads the Lean formalization as counting ordered triples in $Dih\ n$ cubed that pairwise commute, have exactly k entries with flip true, and whose generated subgroup intersected with the rotation subgroup has cardinality d , with the six conjuncts covering $d \nmid n$, $k = 0$, $k = 1$ or 2 with and without $d \mid \gcd(n, 2)$, and $k = 3$ with and without $d \mid \gcd(n, 2)$, using divisor sums of Möbius times powers.

5. Limitations and open questions

The enumeration covers only $1 \leq n \leq 12$ and only the stated (k, d) tabulation; larger n , unrefined totals beyond the sanity checks, and other families such as dicyclic or semidihedral groups were not searched. The proof is specific to triples and to dihedral groups with cyclic rotation subgroup of index two. No ## GAP markers remain in the verified proof, and the referee reported no issues; there are therefore no hidden gaps to carry forward beyond the general limits of the verification described above.

Novelty

The automated novelty search returned verdict APPARENTLY_NEW. The closest known results noted were Jordan's totient identity $J_m(d) = \sum_{e|d} \mu(d/e)e^m$ for generating tuples of a cyclic group, the aggregated total commuting-tuple count $|\text{Hom}(\mathbb{Z}^r, G)|$ for groups with abelian normal subgroup and cyclic quotient including the P_r formula for dihedral groups, and the elementary centralizer description in D_n .

The exact queries run were:

1. Number of commuting triples in the dihedral group D_n with a prescribed number of reflections and prescribed order of the subgroup generated inside the cyclic rotation subgroup, expressed with Jordan totient functions by Möbius inversion.
2. Enumeration of commuting m -tuples and homomorphisms from $\mathbb{Z}^m$ to finite groups, especially dihedral groups, metacyclic groups and groups with a cyclic subgroup of index two.
3. Möbius inversion on the divisor lattice for counting generating tuples of a cyclic group and evaluating Jordan's totient function J_k .

These returned 21 hits in total (7 arXiv, 12 Crossref, 2 OpenAlex), listed in the verification record, with 0 matching hits. This is a bounded automated search over those indexes only, not a literature review, and it is blind to books, journals outside them, and anything phrased differently. The evidence base for this result is retrieval, not memory-only, so novelty does not rest on model recall alone; nevertheless absence from these hits does not prove novelty.

Open questions include whether analogous cube-versus-square divisor-sum refinements hold for commuting m -tuples with $m > 3$, for other reflection-like cosets in metacyclic groups, and whether the $3n$ versus n prefactors have a character-theoretic explanation.

Models

Mobius cube-square refinement of commuting triples in dihedral groups (verified)

- Proposed the claim: muse-spark-1.3-contributor-free
- Counterexample search: muse-spark-1.3-contributor-free
- Wrote the proof: muse-spark-1.3-contributor-free
- Referee: muse-spark-1.3-contributor-free
- Independent check script: muse-spark-1.3-contributor-free
- Lean formalization: muse-spark-1.3-contributor-free
- Faithfulness judge: muse-spark-1.3-contributor-free