QUOTIENT-REALIZABLE MULTISETS IN A FINITE GROUP: THE CLASSIFICATION IN S_3, COUNTEREXAMPLES IN D_8 AND Q_8, AND THE ABELIANIZATION OBSTRUCTION IN EVERY FINITE NONABELIAN GROUP

KOREA SUPERINTELLIGENCE LABS

Abstract. A multiset A of $|G|$ elements of a finite group G is *quotient-realizable* if $A = \{b(i)c(i)^{-1}\}$ for two enumerations b, c of G; equivalently, if $A = \{\varphi(x)x^{-1} : x \in G\}$ for some permutation φ of G. Hall proved in 1952 that for abelian G the obvious necessary condition — that the elements of A have trivial product in $G/[G,G]$ — is also sufficient, and Aliabadi recently showed that it is not sufficient for S_3 and asked a list of questions about the nonabelian case. We answer four of them outright — his Problems 7.1, 7.2, 7.3 and 7.6 — and, with Hall's theorem, a fifth, his Problem 7.5. First, the obstruction fails to be sufficient in *every* finite nonabelian group: one commutator together with $|G| - 1$ copies of the identity is a witness, so the groups in which the abelianization obstruction is the only obstruction are exactly the finite abelian groups. Second, we classify the quotient-realizable multisets of cardinality 6 in S_3: there are 146 of them, and they are the two-sided translates of ten explicit representatives. Third, for D_8 and for Q_8 we exhibit multisets that pass not only the abelianization test but also the strictly stronger product-one-ordering test that Aliabadi's S_3 example was built to pass, and are still not quotient-realizable; each comes with a human proof as well as an exhaustive one. Finally we count: of the 6435 multisets of cardinality 8, exactly 1423 are quotient-realizable in D_8 and exactly 1415 in Q_8, so this count separates two groups that share their order, their abelianization and their character degrees. The numbered results below are machine-checked in Lean 4 against Mathlib apart from four exceptions; Section 8 names those, says which of the remaining statements rest on exhaustive computation and how large each search was, and says which entries of the census are measurements rather than theorems.

1. Introduction

The objects. Let G be a finite group. Hall's theorem [2] concerns multisets of $|G|$ elements of a finite *abelian* G: such a multiset $A = \{a_1, \dots, a_n\}$, $n = |G|$, can be written as $a_i = b_i - c_i$ for two enumerations b, c of G if and only if $a_1 + \cdots + a_n = 0$. Ullman and Velleman [9] give an expository account of the abelian question. Aliabadi [1] asks the multiplicative question for nonabelian G, and we quote his Definition 2.1 verbatim.

Definition 1.1 ([1, Definition 2.1])**.** Let A be a multiset of cardinality $|G|$ whose elements belong to G. We say that A is *quotient-realizable* in G if there exist bijections $b, c : \{1, \dots, |G|\} \to G$ such that $A = \{b(i)c(i)^{-1} : 1 \le i \le |G|\}$ as multisets.

His Lemma 2.2 collapses the pair of bijections to a single permutation, again verbatim:

> Let A be a multiset of cardinality $|G|$ in G. Then A is quotient-realizable in G if and only if there exists a permutation $\varphi \in \mathrm{Sym}(G)$ such that $A = \{\varphi(x)x^{-1} : x \in G\}$.

So the quotient-realizable multisets are exactly the multisets of symbols read off the $|G|!$ diagonals — one cell in each row and each column — of the table $L(y, x) = yx^{-1}$. Two necessary conditions sit above quotient-realizability, in this order. The first is Aliabadi's abelianization obstruction, his Proposition 2.3, verbatim:

> Let A be a quotient-realizable multiset in G, and let $\pi : G \to G_{\mathrm{ab}} = G/[G,G]$ be the canonical projection. Then $\prod^{\mathrm{mult}}_{a \in A} \pi(a) = 1$ in G_{ab}.

(The superscript is the source's own notation for a product taken with multiplicity.)

The second is that some ordering of the elements of A has product 1 in G itself. It implies the first, and it is implied by quotient-realizability because each cycle of φ contributes a word whose product telescopes to 1. For abelian G the two conditions coincide with each other and, by Hall's theorem, with quotient-realizability. Aliabadi shows that they do not coincide with it in S_3: his Propositions 5.2 and 5.4 say that $\{s, s, t, t, t, t\}$, for $s = (1\,2)$ and $t = (2\,3)$, has an ordering with product 1 — hence also satisfies the abelianization condition — and is not quotient-realizable.

The questions. Section 7 of [1] poses seven further problems, numbered 7.1 to 7.7 there; we quote the five that concern us verbatim.

> **7.1.** Classify all quotient-realizable multisets of cardinality 6 in S_3.
>
> **7.2.** Let D_8 be the dihedral group of order 8. Find a multiset A of cardinality 8 satisfying the abelianization condition but not quotient-realizable, or prove that no such multiset exists.
>
> **7.3.** Do the same for the quaternion group Q_8.
>
> **7.5.** For which finite groups G is the abelianization obstruction sufficient for quotient-realizability?
>
> **7.6.** Does every finite nonabelian group admit a multiset A of cardinality $|G|$ satisfying the abelianization obstruction but not quotient-realizable?

The source's own comment on 7.6 is that "a positive answer would characterize finite abelian groups as precisely those finite groups for which the abelianization obstruction is the only obstruction".

What is settled here.

- *Problems 7.6 and 7.5* (Theorem 3.2 and Corollary 3.3). The answer to 7.6 is yes, for every finite nonabelian group at once, and the witness is as small as it could be: a nontrivial commutator together with $|G| - 1$ copies of the identity. Combined with Hall's theorem this answers 7.5: the abelianization obstruction is sufficient exactly for the finite abelian groups.
- *Problem 7.1* (Theorem 4.1 and Theorem 4.2). A multiset is quotient-realizable in S_3 if and only if some two-sided translate gAh is one of ten explicit multisets, listed in Section 4. There are 146 quotient-realizable multisets in all, out of 462 of cardinality 6.
- *Problems 7.2 and 7.3* (Theorems 5.2 and 6.2). In D_8 the multiset $\{s, s, sr, sr, sr, sr, sr, sr\}$, and in Q_8 the multiset $\{a, a, x, x, x, x, x, x\}$ for two elements of order 4 generating different cyclic subgroups, satisfy the abelianization condition, admit an ordering with product 1, and are not quotient-realizable.
- *Counts and two-letter lemmas* (Theorems 5.4, 5.5, 6.4 and 6.5). Of the 6435 multisets of cardinality 8, exactly 1423 are quotient-realizable in D_8 and exactly 1415 in Q_8. In each of D_8 and Q_8, a quotient-realizable multiset supported in the two letters of the counterexample above carries 0, 4 or 8 copies of the first letter — the analogue of [1, Lemma 6.1], which is the same statement for S_3 with $\{0, 3, 6\}$ in place of $\{0, 4, 8\}$.

An honest reading of Problems 7.2 and 7.3. Problems 7.2 and 7.3 ask, literally, for a multiset satisfying the abelianization condition and not quotient-realizable. Read that way they are corollaries of Theorem 3.2, with the trivial witnesses $\{r^2\} \cup \{1\}^7$ in D_8 and $\{-1\} \cup \{1\}^7$ in Q_8; the proof is two lines and is given in Section 3. We say so plainly, because it changes how Theorems 5.2 and 6.2 should be read.

Aliabadi's own S_3 example is not $\{c\} \cup \{1\}^5$ for a 3-cycle c, which would have answered the literal question there; it is $\{s, s, t, t, t, t\}$, and his Proposition 5.4 records that this multiset also admits an ordering with product 1. That second condition is strictly stronger than the abelianization condition (Remark 2.6), and it is what makes his counterexample interesting: it survives a test the trivial witnesses fail, since a multiset with one non-identity element has no product-one ordering at all. Theorems 5.2 and 6.2 answer Problems 7.2 and 7.3 at that stronger reading, with witnesses that are the exact D_8 and Q_8 analogues of the source's S_3 multiset. The source nowhere says which of the two readings it intends, and the argument for the stronger one is ours; so both are answered here, the literal one in Remark 3.4 and the stronger one in Sections 5 and 6.

What is not claimed. We do not classify the quotient-realizable multisets of D_8 or Q_8 up to translation, as Theorem 4.1 does for S_3; only the counts and the two-letter cases are settled there. We do not treat any group of order larger than 8: the searches below are exhaustions over $\mathrm{Sym}(G)$, of size $|G|!$, and Section 8 says where that stops being affordable. In particular we make no claim whatever about D_{10}, about D_{12}, about the dicyclic group of order 12, or about A_4 — the one of those four whose commutator subgroup is not cyclic, and so the interesting one — and whether any of them carries a counterexample of the kind of Theorems 5.2 and 6.2 is left open. Nothing here bears on Problems 7.4 and 7.7 of [1]. Finally, Section 4 also reproduces results of [1] itself (Propositions 4.4 and 4.5); those are not new, and are included because they were used as a check on the definitions and because the new statements are stated against them.

Provenance. The notion of Definition 1.1 appears to be introduced in [1]. The work reported here was done on 3 September 2026 from the LaTeX source of arXiv v2 (26 June 2026), which was and remains the current arXiv version; the published version in *Utilitas Mathematica* was consulted afterwards, and its statements and its numbering of definitions, lemmas, propositions, theorems, corollaries and problems agree item for item with v2. All quotations above and all numbered references to [1] are to that common numbering. (The numbering of arXiv v1 differs from v2 in Section 5 only, that section having gained a remark in v2; nothing else moved.) A full-text arXiv search for the string *quotient-realizable* returns [1] and three unrelated stemming matches; a full-text snapshot of arXiv sources held locally contains the phrase only in the shard carrying [1] itself; and a web search for the phrase together with *multiset*, *finite group* and *bijections* returns only the source. A citation query against OpenAlex for the work returns a citation count of zero and an empty list of citing works. The corresponding query to Semantic Scholar also returned an empty list, but its positive control was rate-limited on three attempts, so that particular zero is weak evidence and the OpenAlex query is what carries the check. The twelve items in the bibliography of [1] were read; the two that bear on the finite case are [2], which is the abelian contrast, and [3], whose complete mappings are the special case of Definition 1.1 in which every element of G occurs once and which we use as an independent control in Section 7. No search returned counts of quotient-realizable multisets in any group; queries to the OEIS for $146, 1423, 1415$ and for $462, 236, 191, 146$ return nothing, while the control sequence $1, 1, 2, 5, 14, 42$ returns the Catalan numbers, so the endpoint was working.

2. Preliminaries

Throughout, G is a finite group written multiplicatively, 1 is its identity, and $\pi : G \to G_{\mathrm{ab}} = G/[G,G]$ is the canonical projection. Multisets over G are written inside braces, with exponents indicating multiplicity: $\{s^2, t^6\}$ is the multiset with two copies of s and six of t. For $g, h \in G$ we write gAh for the multiset $\{gah : a \in A\}$, counted with multiplicity, and A^{-1} for $\{a^{-1} : a \in A\}$.

For a permutation φ of the set G put

$$Q(\varphi) \;=\; \{\, \varphi(x)x^{-1} \;:\; x \in G \,\},$$

a multiset of cardinality $|G|$.

Proposition 2.1. *A multiset A over G is quotient-realizable in the sense of Definition 1.1 if and only if $A = Q(\varphi)$ for some permutation φ of G.*

Proof. This is [1, Lemma 2.2]. Given bijections b, c with $A = \{b(i)c(i)^{-1}\}$, the permutation $\varphi = b \circ c^{-1}$ satisfies $\varphi(c(i))c(i)^{-1} = b(i)c(i)^{-1}$, and as i runs over the index set $c(i)$ runs over G, so $Q(\varphi) = A$. Conversely, given φ, let c be any enumeration of G and put $b = \varphi \circ c$. $\square$

We use Proposition 2.1 without further comment and say that A is *realized* by φ. Note that a realizable multiset automatically has cardinality $|G|$.

Definition 2.2. A multiset A over G *satisfies the abelianization condition* if $\prod_{a\in A}\pi(a)=1$ in G_{ab} (the product is well defined because G_{ab} is commutative), and *admits a product-one ordering* if its elements can be listed in some order $a_1,\dots,a_n$ with $a_n\cdots a_1=1$.

Proposition 2.3. *If A is quotient-realizable in G then A satisfies the abelianization condition; and if A admits a product-one ordering then A satisfies the abelianization condition.*

Proof. The first assertion is [1, Proposition 2.3]: for $A=Q(\varphi)$,

$$\prod_{a\in A}\pi(a) \;=\; \prod_{x\in G}\pi(\varphi(x))\pi(x)^{-1} \;=\; \Big(\prod_{x\in G}\pi(\varphi(x))\Big)\Big(\prod_{x\in G}\pi(x)\Big)^{-1} \;=\; 1,$$

the middle step because G_{ab} is commutative and the last because φ permutes G. The second is the image under the homomorphism π of a product equal to 1. ☐

Proposition 2.4. *Let A be quotient-realizable in G. Then so are gAh for all $g,h\in G$, and A^{-1}, and $\alpha(A)$ for every $\alpha\in\mathrm{Aut}(G)$.*

Proof. If $A=Q(\varphi)$ then $gAh=Q(\psi)$ for $\psi(x)=g\,\varphi(hx)$, since $\psi(x)x^{-1}=g\,\varphi(hx)(hx)^{-1}h$ and $x\mapsto hx$ is a permutation of G; $A^{-1}=Q(\varphi^{-1})$, because $(\varphi(x)x^{-1})^{-1}=x\varphi(x)^{-1}$ and $x\mapsto\varphi(x)$ is a permutation; and $\alpha(A)=Q(\alpha\varphi\alpha^{-1})$. ☐

Proposition 2.4 is elementary, and we make no novelty claim for it; it is recorded because it is what turns the answer to Problem 7.1 from a list of 146 multisets into a list of ten. The group it generates acts on the multisets of cardinality $|G|$ over G, and the quotient-realizable ones are a union of orbits.

Finally we record the combinatorial form of realizability that the human proofs of Sections 5 and 6 use. A *word* over G is a finite sequence $w=(a_1,\dots,a_\ell)$ of elements of G; its *partial products* are $p_0=1$ and $p_j=a_ja_{j-1}\cdots a_1$; its *letter multiset* is $\{a_1,\dots,a_\ell\}$. Call w a *product-one word* if $p_\ell=1$, *simple* if $p_0,\dots,p_{\ell-1}$ are pairwise distinct, and write $P(w)=\{p_0,\dots,p_{\ell-1}\}$, a subset of G of size ℓ containing 1.

Lemma 2.5. *A multiset A of cardinality $|G|$ over G is quotient-realizable if and only if there are simple product-one words $w_1,\dots,w_m$ over G and elements $g_1,\dots,g_m$ of G such that A is the disjoint union of the letter multisets of $w_1,\dots,w_m$ and G is the disjoint union of the sets $P(w_1)g_1,\dots,P(w_m)g_m$.*

Proof. Let $A=Q(\varphi)$ and let $(x,\varphi x,\dots,\varphi^{\ell-1}x)$ be a cycle of φ. Put $a_j=\varphi^j(x)\,\varphi^{j-1}(x)^{-1}$ for $1\le j\le\ell$; then $p_j=\varphi^j(x)x^{-1}$, so $p_\ell=1$, the p_j with $j<\ell$ are distinct because the points of the cycle are, and $P(w)x$ is the support of the cycle. The letters contributed by all cycles together are exactly the quotients $\varphi(y)y^{-1}$, $y\in G$. Conversely, given such w_i and g_i, define φ on $P(w_i)g_i$ by $\varphi(p_jg_i)=p_{j+1}g_i$ with indices mod ℓ_i; the sets $P(w_i)g_i$ partition G, so φ is a permutation, and $\varphi(p_jg_i)(p_jg_i)^{-1}=p_{j+1}p_j^{-1}=a_{j+1}$, so $Q(\varphi)$ is the union of the letter multisets, namely A. ☐

Lemma 2.5 is [1, Theorem 3.4], the source's cycle-tiling criterion, with its Definitions 3.1 and 3.3 — of a simple product-one word and of a cycle-tiling decomposition — written into the statement; the two agree word for word once those definitions are unfolded. We have reproduced the proof only to keep this paper self-contained, and it uses nothing beyond Definition 1.1.

Remark 2.6. Quotient-realizability implies the existence of a product-one ordering: concatenate the words w_i of Lemma 2.5, each of which has product 1. Together with Proposition 2.3 this gives the chain

$$\text{quotient-realizable} \implies \text{product-one ordering} \implies \text{abelianization condition},$$

and both implications are strict in each of S_3, D_8 and Q_8: strictness of the first is Proposition 4.4 and Theorems 5.2 and 6.2, strictness of the second is witnessed by the multisets of Theorem 3.2, which have no product-one ordering at all, because they contain exactly one element different from 1. The implication displayed on the left of the chain is not formalized; see Section 8.

3. The abelianization obstruction is never the only one

Lemma 3.1. *Let G be a finite group and $g \in G$ with $g \neq 1$. Then the multiset $\{g\} \cup \{1\}^{|G|-1}$ is not quotient-realizable in G.*

Proof. A permutation φ realizing it would satisfy $\varphi(x)x^{-1} = 1$, that is $\varphi(x) = x$, for all but exactly one $x \in G$. No permutation has support of size 1. □

Theorem 3.2. *Let G be a finite nonabelian group. Then there is a multiset A of cardinality $|G|$ over G that satisfies the abelianization condition and is not quotient-realizable in G. Explicitly, one may take $A = \{g\} \cup \{1\}^{|G|-1}$ for any $g = aba^{-1}b^{-1} \neq 1$ with $a, b \in G$.*

Proof. Choose $a, b \in G$ with $ab \neq ba$ and put $g = aba^{-1}b^{-1}$, so that $g \neq 1$. Since g is a commutator, $\pi(g) = 1$, and the remaining $|G| - 1$ elements of A are the identity, so $\prod_{a \in A} \pi(a) = 1$ and A satisfies the abelianization condition. By Lemma 3.1, A is not quotient-realizable. □

This answers Problem 7.6 in the affirmative, for every finite nonabelian group at once. With Hall's theorem it answers Problem 7.5.

Corollary 3.3. *For a finite group G, the abelianization condition is sufficient for quotient-realizability — that is, every multiset of cardinality $|G|$ over G satisfying it is quotient-realizable — if and only if G is abelian.*

Proof. If G is abelian then $G_{\mathrm{ab}} = G$ and π is the identity, so the abelianization condition says that the elements of A have product 1; that this is sufficient is Hall's theorem [2], written multiplicatively. If G is nonabelian, apply Theorem 3.2. □

The direction of Corollary 3.3 that comes from [2] is quoted, not reproved; see Section 8.

Remark 3.4. Taking $G = D_8$ and $g = r^2$, and $G = Q_8$ and $g = -1$, Theorem 3.2 produces the multisets $\{r^2\} \cup \{1\}^7$ and $\{-1\} \cup \{1\}^7$, which settle Problems 7.2 and 7.3 as literally posed. Neither admits a product-one ordering, and the point of Sections 5 and 6 is to answer those two problems at the stronger reading discussed in the introduction.

4. The classification in S_3

Write S_3 for the symmetric group on $\{1, 2, 3\}$, with $s = (1\,2)$, $t = (2\,3)$, $u = (1\,3)$ and $c = st = (1\,2\,3)$, permutations composing as functions. There are $\binom{11}{5} = 462$ multisets of cardinality 6 over S_3. Put, writing each multiset out in full so that no exponent has to be read as a multiplicity,

$$\begin{aligned}
R_1 &= \{1,1,1,1,1,1\}, & R_2 &= \{1,1,1,c^2,c^2,c^2\},\\
R_3 &= \{1,1,1,1,u,u\}, & R_4 &= \{1,1,u,u,c^2,c^2\},\\
R_5 &= \{1,1,1,t,u,c^2\}, & R_6 &= \{1,1,t,u,c^2,c^2\},\\
R_7 &= \{1,1,u,u,c,c^2\}, & R_8 &= \{1,1,t,u,c,c^2\},\\
R_9 &= \{1,1,1,1,c,c^2\}, & R_{10} &= \{1,1,c,c,c^2,c^2\}.
\end{aligned}$$

Theorem 4.1. *A multiset A over S_3 is quotient-realizable in S_3 if and only if there are $g, h \in S_3$ with $gAh \in \{R_1, \ldots, R_{10}\}$.*

Proof. For the "if" direction, each R_i is quotient-realizable — checked by exhibiting a realizing permutation for each of the ten, which the formal development does by searching $\mathrm{Sym}(S_3)$, of size 720 — and then $A = g^{-1}(gAh)h^{-1}$ is quotient-realizable by Proposition 2.4. The "only if" direction is an exhaustive computation: for each of the 720 permutations φ of S_3, the multiset $Q(\varphi)$ is formed and one of the 36 translates $gQ(\varphi)h$ is found in the list. This is the whole of the finite search behind the theorem: 720 permutations, and at most 36 translations each. □

Theorem 4.2. *Exactly* 146 *multisets over* S_3 *are quotient-realizable; that is,* 146 *of the* 462 *multisets of cardinality* 6 *over* S_3 *are quotient-realizable.*

Proof. The quotient-realizable multisets are by definition the image of the map $\varphi \mapsto Q(\varphi)$ on $\mathrm{Sym}(S_3)$, so the count is the number of distinct values taken by that map over the 720 permutations. The computation is again exhaustive; in the formal development the multisets are compared through their multiplicity vectors $(\#\{a \in A : a = g\})_{g\in S_3} \in \mathbb{N}^6$, which determine the multiset, so that the deduplication is a comparison of lists of natural numbers rather than a permutation test. The count is independent of Theorem 4.1, and agrees with it: the ten orbits represented by $R_1, \dots, R_{10}$ have sizes $6, 6, 18, 18, 36, 18, 18, 18, 6, 2$, summing to 146. That agreement is a check on the two theorems and not a step in either proof; the orbit sizes themselves are computed outside the formal development, see Remark 4.3. □

Remark 4.3. The following are computations made alongside the formal development but outside it, and no claim in this paper rests on them. Under two-sided translation alone the 462 multisets fall into 27 orbits, of which the ten listed are the quotient-realizable ones; adjoining inversion merges two of the 27, leaving 26, and the quotient-realizable multisets are still the same ten orbits, which is why Theorem 4.1 is stated with translations only. Automorphisms add nothing here, $\mathrm{Aut}(S_3)$ being inner. Each representative contains the identity, which is no accident: replacing A by $a^{-1}A$ for any $a \in A$ puts 1 in the multiset. Stratifying by the number k of transpositions in A — the abelianization condition for S_3 says exactly that k is even, and left translation by an odd permutation exchanges k with $6-k$ — gives $146 = 10+63+63+10$ for $k = 0, 2, 4, 6$. Every figure in this remark — the orbit sizes, the counts 27 and 26, the order of $\mathrm{Aut}(S_3)$ and the stratification — was computed twice, by two programs written independently of one another; none of it is kernel-checked.

The next two propositions are results of [1], reproduced here. They are not new; they were recomputed from Definition 1.1 before anything else in this paper, as a check that the definitions had been transcribed correctly, and they are quoted because Theorems 5.2 and 6.2 are modelled on them.

Proposition 4.4 ([1, Propositions 5.2 and 5.4])**.** *The multiset* $\{s^2, t^4\} = \{s, s, t, t, t, t\}$ *is not quotient-realizable in* S_3*, although* $sstttt = 1$*, so that it admits a product-one ordering and satisfies the abelianization condition.*

Proof. The product-one ordering is the displayed one, s and t being involutions. Non-realizability is an exhaustion over the 720 permutations of S_3. □

Proposition 4.5 ([1, Lemma 6.1])**.** *For* $0 \le q \le 6$*, the multiset* $\{s^q, t^{6-q}\}$ *is quotient-realizable in* S_3 *if and only if* $q \in \{0, 3, 6\}$.

Proof. Seven exhaustions over the 720 permutations of S_3, one for each q. □

5. A counterexample in D_8

Let $D_8 = \langle r, s \mid r^4 = s^2 = 1,\ srs^{-1} = r^{-1}\rangle$ be the dihedral group of order 8. Its four reflections are s, sr, sr^2, sr^3; the product of two of them is r^{j-i} for sr^i and sr^j, which has order 4 when $j-i$ is odd and order 2 when $j - i = 2$. Its commutator subgroup is $\langle r^2\rangle$ and $(D_8)_{\mathrm{ab}} \cong C_2 \times C_2$.

Throughout this section s and t denote two reflections with st of order 4; concretely $t = sr$, so that $st = r$.

Lemma 5.1. *Let* s, t *be reflections of* D_8 *with* st *of order* 4*. The simple product-one words with letters in* $\{s, t\}$ *are exactly* (s, s)*,* (t, t)*, and the two alternating words of length* 8*. Moreover* $P((s, s)) = \langle s\rangle$ *and* $P((t, t)) = \langle t\rangle$*, while the letter multiset of an alternating word of length* 8 *is* $\{s^4, t^4\}$.

Proof. Let $w = (a_1, \dots, a_\ell)$ be simple and product-one with letters in $\{s, t\}$. If $a_{j+1} = a_j$ for some $1 \le j < \ell$ then, both letters being involutions, $p_{j+1} = a_j a_j p_{j-1} = p_{j-1}$; as $j + 1 \le \ell - 1$ would put two equal elements among $p_0, \dots, p_{\ell-1}$, this forces $j + 1 = \ell$, and then $p_\ell = p_{\ell-2}$, so $p_{\ell-2} = 1 = p_0$ and $\ell = 2$, giving (s, s) or (t, t). Otherwise w alternates. An alternating word of odd length has as product a single reflection, which is not 1, so $\ell = 2m$ is even and $p_\ell = (a_2 a_1)^m \in \{(st)^m, (ts)^m\}$, which is 1 exactly when $4 \mid m$. Since $P(w)$ has ℓ distinct elements in a group of order 8, we have $\ell \le 8$, so $m = 4$ and $\ell = 8$; and then $P(w)$ is all of D_8 and w carries four copies of each letter. Conversely each of the four listed words is simple and product-one, and $P((s, s)) = \{1, s\} = \langle s \rangle$, $P((t, t)) = \{1, t\} = \langle t \rangle$. □

Theorem 5.2. *The multiset $A = \{s, s, sr, sr, sr, sr, sr, sr\}$ has cardinality $8 = |D_8|$, admits an ordering with product 1 — hence satisfies the abelianization condition — and is not quotient-realizable in D_8.*

This answers Problem 7.2, with a witness of the same shape as Aliabadi's S_3 example: two copies of one reflection and six copies of another whose product with it has order 4.

Proof. Write $t = sr$. Both s and t are involutions, so $s\,s\,t\,t\,t\,t\,t\,t = 1$ and A admits a product-one ordering; by Proposition 2.3 it satisfies the abelianization condition. Non-realizability is settled in the formal development by an exhaustive search over the $8! = 40320$ permutations of D_8: none of them has $Q(\varphi) = A$. We also give a human proof.

Suppose A were quotient-realizable and take a decomposition as in Lemma 2.5. All letters lie in $\{s, t\}$, so by Lemma 5.1 each word is (s, s), (t, t) or alternating of length 8. An alternating word carries four copies of s and A carries two, so no alternating word occurs, and the decomposition consists of α copies of (s, s) and β copies of (t, t) with $2\alpha = 2$ and $2\beta = 6$; thus $\alpha = 1$ and $\beta = 3$, and D_8 is partitioned into one right coset of $\langle s \rangle$ and three right cosets of $\langle t \rangle$.

Project along $D_8 \to D_8/\langle r^2 \rangle \cong C_2 \times C_2$, writing $\bar{\ }$ for images. The four classes have two preimages each, $\bar{s} \ne \bar{t}$ are distinct involutions and $\bar{s}\bar{t} = \bar{r}$. The image of a right coset $\langle s \rangle g = \{g, sg\}$ is the coset $\{\bar{g}, \bar{s}\bar{g}\}$ of $\{\bar{1}, \bar{s}\}$, and it meets two distinct classes in one element each; similarly for $\langle t \rangle$. Since the four tiles cover each of the eight elements once, each class is covered exactly twice. Let α_1, α_2 be the numbers of $\langle s \rangle$-tiles lying over the two cosets $\{\bar{1}, \bar{s}\}$ and $\{\bar{t}, \bar{r}\}$ of $\{\bar{1}, \bar{s}\}$, and β_1, β_2 the numbers of $\langle t \rangle$-tiles over $\{\bar{1}, \bar{t}\}$ and $\{\bar{s}, \bar{r}\}$. Counting the covers of the classes $\bar{1}, \bar{s}, \bar{t}, \bar{r}$ gives

$$\alpha_1 + \beta_1 = \alpha_1 + \beta_2 = \alpha_2 + \beta_1 = \alpha_2 + \beta_2 = 2,$$

whence $\alpha_1 = \alpha_2$ and $\alpha = \alpha_1 + \alpha_2$ is even. But $\alpha = 1$. □

Proposition 5.3. *The product $s \cdot sr^2 = r^2$ has order 2, and the multiset $\{s^2, (sr^2)^6\}$, with two copies of s and six of sr^2,* is *quotient-realizable in D_8.*

Proof. The order is a computation in D_8; realizability is exhibited by a permutation found in the same exhaustive search over $\mathrm{Sym}(D_8)$. □

Proposition 5.3 says that the hypothesis $\mathrm{ord}(st) = 4$ in Theorem 5.2 is doing work: the counterexample is not an artefact of the shape "two copies of one reflection and six of another".

Theorem 5.4. *For $0 \le q \le 8$, the multiset $\{s^q, (sr)^{8-q}\}$ is quotient-realizable in D_8 if and only if $q \in \{0, 4, 8\}$.*

Proof. Nine exhaustions over the 40320 permutations of D_8, one for each q. (For $q \in \{0, 8\}$ realizability also follows from Lemma 2.5: a constant multiset $\{g^{|G|}\}$ is realized by left translation by g.) □

This is the D_8 analogue of [1, Lemma 6.1], which is Proposition 4.5 above; the answer set is $\{0, |G|/2, |G|\}$ in both cases.

Theorem 5.5. *Exactly 1423 of the $\binom{15}{7} = 6435$ multisets of cardinality 8 over D_8 are quotient-realizable.*

Proof. As in Theorem 4.2: the number of distinct values of $\varphi \mapsto Q(\varphi)$ over the 40320 permutations of D_8, computed with multisets represented by their multiplicity vectors in $\mathbb{N}^8$. $\square$

6. A counterexample in Q_8

Let $Q_8 = \langle a, x \mid a^4 = 1,\ x^2 = a^2,\ xax^{-1} = a^{-1}\rangle$ be the quaternion group of order 8, with central involution $-1 = a^2 = x^2$. Its commutator subgroup is $\{1, -1\}$ and $(Q_8)_{\mathrm{ab}} \cong C_2 \times C_2$, generated by the images of a and x. The six elements of order 4 are $a^{\pm 1}, x^{\pm 1}, (ax)^{\pm 1}$, and $\langle a\rangle \neq \langle x\rangle$.

Lemma 6.1. *Let $a, x \in Q_8$ have order 4 with $\langle a\rangle \neq \langle x\rangle$. Then:*

1. *every product-one word with letters in $\{a, x\}$ carries an even number of each letter;*
2. *there is no simple product-one word of length 1, 2 or 3 with letters in $\{a, x\}$;*
3. *there is no simple product-one word with letter multiset $\{a^2, x^6\}$;*
4. *the only word with letter multiset $\{x^4\}$ is (x, x, x, x); it is simple and product-one, and $P((x, x, x, x)) = \langle x\rangle$;*
5. *the simple product-one words with letter multiset $\{a^2, x^2\}$ are exactly the four below, with the partial-product sets shown, and none of these sets is $\langle x\rangle$:*

$$\begin{array}{llll} (a,a,x,x) & \{1,a,a^2,xa^2\} & (x,a,a,x) & \{1,x,xa^3,xa^2\} \\ (a,x,x,a) & \{1,a,xa,a^3\} & (x,x,a,a) & \{1,x,a^2,a^3\} \end{array}$$

Proof. (1) is Proposition 2.3 applied to the word. The images $\bar{a}, \bar{x}$ are nontrivial in $(Q_8)_{\mathrm{ab}} \cong C_2 \times C_2$, and they are distinct: $\bar{a} = \bar{x}$ would put $x \in \{a, a^{-1}\}$ and force $\langle a\rangle = \langle x\rangle$. So $\bar{a}, \bar{x}$ form a basis of $(Q_8)_{\mathrm{ab}}$, and a product equal to 1 needs both exponent sums even. For (2), a word of length 1 has $p_1 = a_1 \in \{a, x\}$, which is not 1; by (1) a product-one word has even length, so length 3 is excluded, and the length-2 candidates are (a, a) and (x, x), with $p_2 = a^2 \neq 1$ and $p_2 = x^2 \neq 1$.

For (3), suppose w has length 8 with two letters a, in positions $i < k$, and six letters x. Simplicity means $p_0, \ldots, p_7$ are the eight elements of Q_8, so four of them lie in the subgroup $\langle x\rangle$ of index 2 and four in the other coset. Modulo $\langle x\rangle$, the class of p_j is nontrivial exactly when an odd number of a's occur among $a_1, \ldots, a_j$, that is exactly for $i \le j \le k-1$; so $k-i = 4$, and in particular $1 \le i \le 4$. Now $x^3 = xx^2 = xa^2 = a^{-2}x = a^2x$, and $xa = a^{-1}x$ gives $ax^3a = a(a^2x)a = a^3(xa) = a^3a^3x = a^2x = x^3$, so

$$p_8 \;=\; x^{4-i}\left(a\,x^3\,a\right)x^{i-1} \;=\; x^{4-i}x^3x^{i-1} \;=\; x^6 \;=\; x^2 \;\neq\; 1,$$

and w is not product-one. Item (4) is immediate, $\langle x\rangle = \{1, x, x^2, x^3\}$ being the set of partial products of (x, x, x, x). For (5), the six orderings of $\{a, a, x, x\}$ are checked one by one; (a, x, a, x) and (x, a, x, a) have $p_4 = x^2 \neq 1$ and $p_4 = a^2 \neq 1$, and the other four are as listed. Finally $\langle x\rangle = \{1, x, a^2, xa^2\}$, and each of the four listed sets contains an element outside it: the two words beginning with a give sets containing a, while those of (x, a, a, x) and (x, x, a, a) contain $xa^3 = ax$ and a^3. $\square$

Theorem 6.2. *The multiset $A = \{a, a, x, x, x, x, x, x\}$, for $a, x \in Q_8$ of order 4 with $\langle a\rangle \neq \langle x\rangle$, has cardinality $8 = |Q_8|$, admits an ordering with product 1 — hence satisfies the abelianization condition — and is not quotient-realizable in Q_8.*

This answers Problem 7.3 at the same reading as Theorem 5.2 answers Problem 7.2.

Proof. The ordering $a\,a\,x\,x\,x\,x\,x\,x$ has product $a^2x^6 = (-1)(-1) = 1$, so A admits a product-one ordering and, by Proposition 2.3, satisfies the abelianization condition. Non-realizability is settled in the formal development by an exhaustive search over the $8! = 40320$ permutations of Q_8. The human proof runs as follows.

Take a decomposition of A as in Lemma 2.5. All letters lie in $\{a, x\}$, so by Lemma 6.1(1) and (2) each word has even length at least 4, and the lengths sum to 8: either one word of length 8, excluded by Lemma 6.1(3), or two words of length 4. Each length-4 word has even letter counts, so its letter multiset is $\{a^4\}$, $\{a^2, x^2\}$ or $\{x^4\}$; the only pair summing to $\{a^2, x^6\}$ is $\{a^2, x^2\}$ together with $\{x^4\}$. By Lemma 6.1(4) one tile is $\langle x\rangle g$, a right coset of $\langle x\rangle$; since the two tiles partition Q_8, the other is the complementary right coset $\langle x\rangle g'$. So $P(w)h = \langle x\rangle g'$ for the $\{a^2, x^2\}$-word w and some h, making $P(w)$ a right coset of $\langle x\rangle$; as $1 \in P(w)$, that coset is $\langle x\rangle$ itself. Lemma 6.1(5) says no $\{a^2, x^2\}$-word has $P(w) = \langle x\rangle$. □

Proposition 6.3. *Since* $a^2 = x^2 = -1$ *one has* $xa^2 = x^3$*, and the multiset* $\{x, x, x^3, x^3, x^3, x^3, x^3, x^3\}$ is *quotient-realizable in* Q_8*.*

Proof. The identity is a computation in Q_8; realizability is exhibited by a permutation found in the exhaustive search over $\mathrm{Sym}(Q_8)$. □

So the hypothesis $\langle a\rangle \neq \langle x\rangle$ in Theorem 6.2 is doing work: replacing the second letter by another generator of the *same* cyclic subgroup makes the multiset quotient-realizable.

Theorem 6.4. *For* $0 \leq q \leq 8$*, the multiset* $\{a^q, x^{8-q}\}$ *— q copies of a and* $8 - q$ *copies of x, for* a, x *as in Theorem 6.2 — is quotient-realizable in* Q_8 *if and only if* $q \in \{0, 4, 8\}$*.*

Proof. Nine exhaustions over the 40320 permutations of Q_8, one for each q. □

The answer set is the same as in D_8 (Theorem 5.4), and the same as in S_3 with 3 in place of 4 (Proposition 4.5), although the two letters are involutions in the first two cases and elements of order 4 here.

Theorem 6.5. *Exactly* 1415 *of the* $\binom{15}{7} = 6435$ *multisets of cardinality* 8 *over* Q_8 *are quotient-realizable — eight fewer than in* D_8*.*

Proof. As in Theorem 5.5, over the 40320 permutations of Q_8. □

Remark 6.6. D_8 and Q_8 have the same order, isomorphic abelianizations $C_2 \times C_2$ and the same multiset of irreducible character degrees $\{1, 1, 1, 1, 2\}$. Theorems 5.5 and 6.5 give an invariant that separates them: the number of quotient-realizable multisets of cardinality $|G|$ is 1423 for one and 1415 for the other.

7. Controls, and the three-column census

A *complete mapping* of a group G is, in the sense of [3], a bijection $\theta : G \to G$ for which $y \mapsto y\theta(y)$ is also a bijection. The single multiset in which every element of G occurs exactly once is quotient-realizable precisely when G admits one. Indeed, that multiset is $Q(\varphi)$ exactly when φ is a permutation of G for which $x \mapsto \varphi(x)x^{-1}$ is a permutation as well, and $\theta(y) = \varphi^{-1}(y)^{-1}$ turns such a φ into a complete mapping and back: θ is a bijection, φ is recovered from it as the inverse of $y \mapsto \theta(y)^{-1}$, and $y\theta(y) = \varphi(x)x^{-1}$ for $x = \varphi^{-1}(y)$, so one of the two maps $y \mapsto y\theta(y)$ and $x \mapsto \varphi(x)x^{-1}$ is a bijection if and only if the other is. By the Hall–Paige theorem, a finite group admits a complete mapping if and only if its Sylow 2-subgroup is trivial or non-cyclic. Hall and Paige [3] proved the necessity and conjectured the sufficiency; Wilcox [4] reduced the conjecture to the simple groups and proved it for the groups of Lie type apart from the Tits group, Evans [5] settled the Tits group and all the sporadic groups except J_4, and the remaining case is documented in [6]. We quote the criterion and prove nothing about it; it is used only as a check on the computations of the previous sections, against a theorem they know nothing about.

Proposition 7.1. *The multiset listing each element of the group exactly once is quotient-realizable in* D_8 *and in* Q_8*, and is not quotient-realizable in* S_3*.*

Proof. Three exhaustive searches, over $\mathrm{Sym}(S_3)$, $\mathrm{Sym}(D_8)$ and $\mathrm{Sym}(Q_8)$. The outcome agrees with Hall–Paige: the Sylow 2-subgroup of S_3 is cyclic of order 2, while D_8 and Q_8 are their own Sylow 2-subgroups and are not cyclic. □

Remark 7.2 (computed outside the formal development). The three necessary conditions of Remark 2.6 were counted for all three groups by a separate program, which enumerates every multiset of cardinality $|G|$ and tests each condition directly. Only the last column is part of the formal development (Theorems 4.2, 5.5 and 6.5); the middle two are measurements, reported here for orientation and not used in any proof.

G	multisets of card $\lvert G\rvert$	abelianization	product-one ordering	quotient-realizable
S_3	462	236	191	146
D_8	6435	1635	1521	1423
Q_8	6435	1635	1517	1415

Both inclusions are strict in every row. Among the multisets that satisfy the abelianization condition but are not quotient-realizable there are 90 in S_3, 212 in D_8 and 220 in Q_8; of these, 45, 98 and 102 respectively also admit a product-one ordering. In D_8 exactly 8 of the last group have support of size 2, and they are the multisets $\{y^2, z^6\}$ for the four unordered pairs $\{y, z\}$ of reflections whose product has order 4, each pair contributing two multisets; the witness of Theorem 5.2 is one of them. In Q_8 exactly 24 have support of size 2, and they are the $\{y^2, z^6\}$ for the $6 \times 4 = 24$ ordered pairs of elements of order 4 generating different cyclic subgroups; the witness of Theorem 6.2 is one of them. Every figure in this remark was produced twice, by two programs written independently of one another, the second of them building S_3 from permutations of three points, D_8 from the symmetries of a square and Q_8 from the unit quaternions, so that it shares no group encoding with the formal development; the last column of the table agrees with the formally verified counts of Theorems 4.2, 5.5 and 6.5. The middle two columns are not kernel-checked.

8. Formal verification

Every lemma, proposition, theorem and corollary above is formalized and machine-checked in Lean 4 [7] against Mathlib [8], with four exceptions named below. Definition 1.1 and the abelianization condition of Definition 2.2 are the development's own definitions; the product-one-ordering condition is not a named predicate there, and enters only through the explicit orderings exhibited in Theorems 5.2 and 6.2 and Proposition 4.4. The development is four files: a general one, carrying Definition 1.1, Propositions 2.1, 2.3 and 2.4, Lemma 3.1 and Theorem 3.2; and one file each for S_3, D_8 and Q_8. The groups are Mathlib's own `Equiv.Perm (Fin 3)`, `DihedralGroup 4` and `QuaternionGroup 2`, so nothing depends on a hand-built multiplication table. There is no incomplete proof anywhere in the development.

What rests on exhaustive computation, and how large each search is. Theorem 3.2, Lemma 3.1 and Propositions 2.1, 2.3 and 2.4 are proved symbolically for an arbitrary finite group, with no computation and no group-specific input; their axiom sets contain only propositional extensionality, quotient soundness and choice. (Corollary 3.3 is the combination of Theorem 3.2 with a quoted theorem, and is discussed below.) Every other statement about a specific group is decided by evaluating a decision procedure over the whole of $\mathrm{Sym}(G)$ — 720 permutations for S_3, $8! = 40320$ for D_8 and for Q_8 — inside the compiled evaluator, which contributes one additional axiom per such evaluation asserting that the evaluator's verdict is correct. Concretely: the "only if" half of Theorem 4.1 (one sweep of 720 permutations, each of the resulting multisets tested against the 36 translates of the ten representatives) and the realizability of the ten representatives (one sweep); Theorems 4.2, 5.5 and 6.5 (one sweep each, the multisets being deduplicated through their multiplicity vectors); Propositions 4.4, 5.3 and 6.3 and the non-realizability halves of Theorems 5.2 and 6.2 (one sweep each); Proposition 7.1 (three sweeps, one per group); and Proposition 4.5 and Theorems 5.4 and 6.4 (seven and nine sweeps each, one per value of q). The product-one orderings and the order computations in D_8 and Q_8 are decided by the kernel itself, without the evaluator.

The four exceptions are these. Lemma 2.5 and the human proofs of Theorems 5.2 and 6.2, together with Lemmas 5.1 and 6.1 on which they rest, are not formalized; what is formalized for those two theorems is the exhaustive search, which is logically independent of the human argument, so each theorem has two proofs of which one is machine-checked. The implication "quotient-realizable ⇒

product-one ordering" of Remark 2.6 is not formalized either; it is used nowhere else, every product-one ordering needed in this paper being exhibited explicitly. Hall's theorem, quoted for one direction of Corollary 3.3, is not formalized; the other direction, which is the new one, is. And Remarks 4.3 and 7.2 are computations made outside the development, labelled as such where they appear. Before any Lean was written, six results of [1] — its Lemma 5.1, Propositions 5.2 and 5.4, Lemma 6.1, Theorem 3.4 and Theorem 4.1 — were recomputed from Definition 1.1 by an independent program, as a check that the definitions had been transcribed correctly; for Theorem 3.4 that means agreement of the cycle-tiling criterion with realizability on all 462 multisets of cardinality 6 over S_3, and for Theorem 4.1 agreement on all multisets supported in $\langle s \rangle$ and in A_3. The counts of Theorems 4.2, 5.5 and 6.5 were obtained three times: by that program, by a second one that builds the three groups from constructions independent of Mathlib's, and inside Lean. The whole development elaborates in about seven minutes and its memory use is dominated by loading the library.

The cost of these searches scales as $|G|!$, and that is what confines the census to groups of order at most 8: for a group of order 10 one sweep runs over $10! = 3\,628\,800$ permutations, and for a group of order 12 over $12! = 479\,001\,600$, which is past the compute budget adopted here. So the cells beyond order 8 are open rather than merely unaddressed: for D_{10}, for D_{12}, for the dicyclic group of order 12, and for A_4 — whose commutator subgroup, alone among these, is not cyclic — this paper decides nothing, and in particular whether A_4 carries a multiset that passes the product-one-ordering test and is not quotient-realizable is left open. The repository is private; repository reference to be added at submission.

References

[1] M. Aliabadi, *A nonabelian twist on differences of bijections*, *Utilitas Mathematica* **128** (2026), 375–397; DOI `10.61091/um128-18`. Preprint: arXiv:2605.16478 (v1 15 May 2026, v2 26 June 2026), math.GR and math.CO. All quotations in this paper are from the LaTeX source of v2, read in full on 3 September 2026, and all numbered references are to the numbering of the published version, which agrees item for item with that of v2.

[2] M. Hall, Jr., *A combinatorial problem on abelian groups*, Proc. Amer. Math. Soc. **3** (1952), 584–587; DOI `10.1090/S0002-9939-1952-0050579-7`.

[3] M. Hall, Jr. and L. J. Paige, *Complete mappings of finite groups*, Pacific J. Math. **5** (1955), 541–549; DOI `10.2140/pjm.1955.5.541`.

[4] S. Wilcox, *Reduction of the Hall–Paige conjecture to sporadic simple groups*, J. Algebra **321** (2009), no. 5, 1407–1428; DOI `10.1016/j.jalgebra.2008.11.033`.

[5] A. B. Evans, *The admissibility of sporadic simple groups*, J. Algebra **321** (2009), no. 1, 105–116; DOI `10.1016/j.jalgebra.2008.09.028`.

[6] J. N. Bray, Q. Cai, P. J. Cameron, P. Spiga and H. Zhang, *The Hall–Paige conjecture, and synchronization for affine and diagonal groups*, J. Algebra **545** (2020), 27–42; DOI `10.1016/j.jalgebra.2019.02.025`.

[7] L. de Moura and S. Ullrich, *The Lean 4 theorem prover and programming language*, in: Automated Deduction — CADE 28, Lecture Notes in Computer Science 12699, Springer, 2021, pp. 625–635; DOI `10.1007/978-3-030-79876-5_37`.

[8] The mathlib Community, *The Lean mathematical library*, in: Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs (CPP 2020), ACM, 2020, pp. 367–381; DOI `10.1145/3372885.3373824`.

[9] D. H. Ullman and D. J. Velleman, *Differences of bijections*, Amer. Math. Monthly **126** (2019), no. 3, 199–216; DOI `10.1080/00029890.2019.1546077`. Cited for the expository account of the abelian question; no result of this paper depends on it.