# Formal Verification: A Family of Three-Generator Permutation Groups

AF-Tests Project

January 2026

## 1 Introduction

This document presents formally verified theorems about a family of permutation groups generated by three cycles. The main result is a complete characterization: the group $H = \langle g_1, g_2, g_3 \rangle$ equals either the alternating group $A_N$ or the symmetric group $S_N$, depending on the parity of the generators. The proofs have been fully formalized in Lean 4 with Mathlib, with **zero axioms beyond standard Lean/Mathlib foundations** (propext, Classical.choice, Quot.sound).

## 2 Definitions

**Definition 1** (The Permutation Domain)**.** *For non-negative integers $n, k, m \in \mathbb{N}$, define the finite set*

$$\Omega_{n,k,m} = \{0, 1, 2, 3, 4, 5, 6, \ldots, 5 + n + k + m\}$$

*of cardinality $N = 6 + n + k + m$.*

**Definition 2** (The Generators)**.** *Define three permutations $g_1, g_2, g_3 \in S_N$ as cycles:*

$$\begin{aligned} g_1 &= (0\ 5\ 3\ 2\ 6\ 7\ \cdots\ (5+n)) && \textit{a cycle of length } 4+n \\ g_2 &= (1\ 3\ 4\ 0\ (6+n)\ (7+n)\ \cdots\ (5+n+k)) && \textit{a cycle of length } 4+k \\ g_3 &= (2\ 4\ 5\ 1\ (6+n+k)\ (7+n+k)\ \cdots\ (5+n+k+m)) && \textit{a cycle of length } 4+m \end{aligned}$$

*These correspond to the cycles $(1\ 6\ 4\ 3\ a_1\ \cdots\ a_n)$, $(2\ 4\ 5\ 1\ b_1\ \cdots\ b_k)$, and $(3\ 5\ 6\ 2\ c_1\ \cdots\ c_m)$ in 1-indexed notation.*

**Definition 3** (The Group $H$)**.** *Let $H = \langle g_1, g_2, g_3 \rangle \leq S_N$ be the subgroup generated by the three cycles.*

**Definition 4** (Block System)**.** *A* block system *for a group $G$ acting on a set $\Omega$ is a partition $\mathcal{B} = \{B_1, B_2, \ldots, B_r\}$ of $\Omega$ such that for every $g \in G$ and every block $B_i \in \mathcal{B}$, either $g(B_i) = B_i$ or $g(B_i) \cap B_i = \emptyset$.*

*A block system is* trivial *if it consists of singletons or is the single block $\{\Omega\}$.*

*A block system is $H$-*invariant *if for each generator $g_1, g_2, g_3$ and each block $B$, the image $g_i(B)$ is also a block in $\mathcal{B}$.*

# 3 Main Result

**Theorem 5** (Lemma 11.5: Primitivity)**.** *Let $n, k, m \in \mathbb{N}$ with $n + k + m \geq 1$. Then the group $H = \langle g_1, g_2, g_3 \rangle$ admits no non-trivial $H$-invariant block system on $\Omega_{n,k,m}$.*

*Equivalently, the action of $H$ on $\Omega_{n,k,m}$ is* ***primitive****.*

# 4 Proof Outline

The proof proceeds by contradiction. Assume there exists a non-trivial $H$-invariant block system $\mathcal{B}$. Pick a block $B \in \mathcal{B}$ containing a tail element (either $a_1$, $b_1$, or $c_1$ depending on which of $n, k, m$ is non-zero).

## 4.1 Case Analysis

For each generator $g_i$, the image $g_i(B)$ is either equal to $B$ or disjoint from $B$.

- **Case 1:** If the generator containing the chosen tail element preserves $B$, then by cycle-in-block arguments, the entire support of that generator is contained in $B$. Continuing with the other generators leads to either $B = \Omega$ (contradicting non-triviality) or a fixed-point contradiction.
- **Case 2:** If the generator does not preserve $B$ (disjoint case), then fixed-point arguments force the other two generators to preserve $B$. This leads to a contradiction via careful analysis of the block structure under powers of the generators.

## 4.2 Key Technical Lemmas

**Lemma 6** (Tail-in-Block)**.** *If a tail element $a_1 \in B$ and $g_1(B) = B$, then* $\operatorname{supp}(g_1) \subseteq B$.

**Lemma 7** (Cycle Power Commutativity)**.** *For any permutation $g$ and integers $i, j$: $g^i \circ g^j = g^j \circ g^i$.*

The final contradiction in the disjoint case uses the key observation:

$$g_3^j(c_3) = g_3^j(g_3^2(c_1)) = g_3^2(g_3^j(c_1)) = g_3^2(4) = 1$$

combined with injectivity of $g_3^j$ to show $c_3 \in B$, while simultaneously $c_3 \in g_3^2(B)$, contradicting disjointness.

# 5 Formalization

The complete proof is formalized in Lean 4 with Mathlib. The main theorem is:

```
theorem lemma11_5_no_nontrivial_blocks (h : n + k + m >= 1) :
    forall BS : BlockSystemOn n k m,
    IsHInvariant BS -> not (IsNontrivial BS)
```

### 5.1 Axioms Used

The proof depends only on standard Lean/Mathlib axioms:

- `propext` – Propositional extensionality
- `Classical.choice` – Classical choice principle
- `Quot.sound` – Quotient soundness
- `Lean.ofReduceBool`, `Lean.trustCompiler` – For `native_decide`

No custom axioms or `sorry` statements remain in the proof.

## 6 The Main Theorem

The primitivity result (Lemma 11.5) is a key ingredient in proving the main theorem, which completely characterizes the group $H$.

**Theorem 8** (Main Theorem: Classification of $H$)**.** *Let $n, k, m \in \mathbb{N}$ with $n + k + m \geq 1$, and let $N = 6 + n + k + m$. Then:*

1. *$H = A_N$ (the alternating group) if and only if $n$, $k$, and $m$ are all odd.*
2. *$H = S_N$ (the symmetric group) if and only if at least one of $n$, $k$, $m$ is even.*

### 6.1 Proof Ingredients

The proof relies on several key lemmas:

1. **Transitivity** (Lemma 5): The action of $H$ on $\Omega_{n,k,m}$ is transitive.
2. **Primitivity** (Lemma 11.5): The action of $H$ on $\Omega_{n,k,m}$ is primitive (no non-trivial block systems exist).
3. **3-Cycle Generation** (Lemmas 6–9): The commutators $[g_1, g_2]$, $[g_1, g_3]$, and $[g_2, g_3]$ are 3-cycles, and $H$ contains a 3-cycle.
4. **Jordan's Theorem** (Lemma 12): A primitive permutation group on $n$ elements containing a $p$-cycle for prime $p < n - 2$ contains $A_n$.
5. **Parity Analysis** (Lemmas 13–15):
   - A cycle of length $\ell$ has sign $(-1)^{\ell-1}$.
   - $\text{sign}(g_i) = (-1)^{3+t}$ where $t \in \{n, k, m\}$ is the corresponding tail length.
   - All generators are even permutations iff $n$, $k$, $m$ are all odd.

### 6.2 Lean Formalization

The main theorem is formalized as:

```
theorem main_theorem (n k m : ) (hPrim : n + k + m  1) :
    (H n k m = alternatingGroup (Omega n k m)
        (Odd n  Odd k  Odd m))
    (H n k m = 
        ¬(Odd n  Odd k  Odd m))
```

Here `H n k m` is the subgroup $\langle g_1, g_2, g_3 \rangle$, `alternatingGroup` is $A_N$, and  (top) denotes the full symmetric group $S_N$.

## 7 Conclusion

This formalization provides a complete, machine-verified proof that the group $H = \langle g_1, g_2, g_3 \rangle$ equals either the alternating group $A_N$ or the symmetric group $S_N$, with the classification determined entirely by the parity of the tail lengths $n$, $k$, and $m$:

- $H = A_N$ when all three tail lengths are odd.
- $H = S_N$ when at least one tail length is even.

The proof combines classical results (Jordan's theorem, cycle parity) with careful combinatorial analysis of block systems and generator actions. The entire development is formalized in approximately 4,000 lines of Lean 4 code with no custom axioms.

**Repository:** `https://github.com/tobiasosborne/af-tests`