A classification of solvable spinning-switches puzzles

P. Graham
https://orcid.org/0009-0007-8493-1505

October 31, 2026

Abstract

Spinning-switches puzzles ask for a predetermined sequence of moves that works despite hidden permutations of the switches. Kagey formulated the problem using a finite group of switch states and a permutation group of positions, proved solvability when both groups are p-groups for one prime p, and classified the case of abelian switch groups. We prove the converse without an abelian hypothesis: for nontrivial finite groups G and H, with H acting faithfully on a finite set Ω, a surjective strategy for $G \wr_\Omega H$ exists exactly when G and H are p-groups for the same prime. This answers Kagey's Open Question 31. The necessity proof restricts the adversary to a prime-order element and tracks excluded configurations by cosets of prime-power subgroups. We also give a central-series proof of the known sufficient condition. The classification and its consequences for $S_3 \wr C_2$ and $A_4 \wr C_3$ are formalized in Lean.

This work has not yet been reviewed by experts. The proofs, the Lean formalization and the text were produced by AI models (from OpenAI and Anthropic), working under the author's direction.

MSC 2020: 20D15, 05E18. **Keywords:** spinning switches, wreath products, finite groups.

1 Introduction

A player changes hidden switches while an adversary permutes their positions. The player must choose the moves in advance. Kagey's model [1] assigns a group G to each switch and lets a group H act on the set of positions Ω. Write $K = G^\Omega$ for the configuration group, with pointwise multiplication, and put

$$(\alpha_h x)(\omega) = x(h^{-1}\omega), \qquad W = K \rtimes_\alpha H, \qquad (x,h)(y,a) = (x\alpha_h(y), ha).$$

A move is an arbitrary element of K; in particular, it may change several switches at once. For fixed moves $k_1, \dots, k_N$ and adversary choices $h_1, \dots, h_N$, put $P_0 = 1$ and $P_j = (k_1, h_1) \cdots (k_j, h_j)$. Write $P_j = (b_j, a_j)$. Following Definition 9 of [1, arXiv v1], the moves form a *surjective strategy* if, for every adversary sequence, $\{b_j : 0 \le j \le N\} = K$. Equivalently, from every initial configuration x_0, some $x_0 b_j$ equals 1. No observation of the spins is available.

Theorem 1. *Let G and H be nontrivial finite groups, and let H act faithfully on a finite set Ω. There is a surjective strategy for $G \wr_\Omega H$ if and only if there is a prime p for which both G and H are p-groups.*

The action need not be transitive. A p-group here means a finite group whose order is a power of p. The nontriviality assumptions matter: trivial switches need no moves, and a trivial adversary

permits a tour of any finite configuration group. If N is the kernel of the action, each b_j depends only on the images of the h_i in H/N, so $G \wr_\Omega H$ has a surjective strategy if and only if $G \wr_\Omega (H/N)$ does. Hence in general a surjective strategy exists if and only if $G = 1$, or H acts trivially, or G and H/N are p-groups for one prime p.

All statement numbers below refer to arXiv:2210.09408v1, posted October 17, 2022, of Kagey's 2023 paper [1]. Theorem 22 gives the sufficient condition in Theorem 1. Theorem 23 gives the equivalence when G is abelian. Open Question 31 asks for the finite wreath products admitting a surjective strategy. Our contribution is necessity for arbitrary finite switch groups, including nonabelian groups; Section 3 reproves the known sufficiency for a complete formal proof. Earlier rotating-table and blind-bartender puzzles were studied by Bar Yehuda, Etzion and Moran [3] and Ehrenborg and Skinner [4]; Rabinovich's linear-action criterion [5], stated as Theorem 13 of [1, arXiv v1], says that a faithful linear action on a finite-field vector space of characteristic p admits a strategy exactly when the acting group is a p-group. That linear setting does not cover nonabelian switch groups; our coset invariant supplies necessity in this case.

Theorem 26 of that version asserts solvability for $G \wr C_2$ when G is generated by involutions. This assertion was already corrected: ndkrempel reported on MathOverflow on December 7, 2025 that Theorem 26 fails, and Kagey acknowledged the error there on December 8, 2025, noting that Example 27 fails [2]. The classification, not that correction, is the claim of this paper. For example, it implies that $S_3 \wr C_2$, with C_2 interchanging two positions, is unsolvable, refuting Conjecture 32 (already implicit in the Theorem 26 correction). It refutes Conjecture 33 for every $n \geq 4$: $A_n \wr C_3$ on three cyclically permuted positions is unsolvable because $|A_n|$ is even; the $n = 3$ case holds by Theorem 22. For a nontrivial p-group H acting faithfully, it settles Conjecture 34 exactly: a strategy exists precisely when G is a p-group; the trivial adversary case is always solvable, as above. The formalized negative instances are $S_3 \wr C_2$ and $A_4 \wr C_3$, with group orders $6, 2$ and $12, 3$, respectively.

2 The prime-order obstruction

Fix a prime q, an element $h \in H$ of order q, and a position ω that h moves. Its orbit O has q elements. Restrict the adversary to $\langle h \rangle$. For $k \in K$ and $E \subseteq K$, define

$$T_k(E) = \{1\} \cup \{y \in K : (a \mapsto y(h^n a))k^{-1} \in E \text{ for every } n \geq 0\}. \tag{1}$$

For a move sequence, set $E_0 = \{1\}$ and $E_i = T_{k_i}(E_{i-1})$. These are configurations excluded from surviving play, expressed in the adversary's moving coordinates.

Lemma 2. *If $E_N \neq K$, the moves $k_1, \ldots, k_N$ are not a surjective strategy.*

Proof. Choose $z_N \notin E_N$. Recursively, (1) gives n_i such that $z_{i-1} = (a \mapsto z_i(h^{n_i} a))k_i^{-1} \notin E_{i-1}$. Every z_i is nonidentity. Set $h_i = h^{-n_i}$ and $x_0 = z_0$. The multiplication in W gives, inductively,

$$\begin{aligned} x_0 b_i &= x_0 b_{i-1} \alpha_{a_{i-1}}(k_i) = \alpha_{a_{i-1}}(z_{i-1} k_i), \\ \alpha_{a_i^{-1}}(x_0 b_i) &= \alpha_{h_i^{-1}}(z_{i-1} k_i) = z_i, \end{aligned} \tag{2}$$

since $a_i = a_{i-1} h_i$. Thus $x_0 b_i \neq 1$ for every prefix, so the base projections miss x_0^{-1}. □

Say that $y \in K$ is *P-aligned on O*, for a subgroup $P \leq G$, if $y(a)^{-1} y(b) \in P$ for all $a, b \in O$. This means its values on O lie in one left coset of P.

Lemma 3. *If every member of E is P-aligned on O for a q-subgroup $P \leq G$, then there is a q-subgroup $P' \leq G$ such that every member of $T_k(E)$ is P'-aligned on O.*

Proof. For $y \in T_k(E)$ with $y \neq 1$, rotate any $t \in O$ to any $a \in O$ in (1) and apply alignment at t, ht. This gives

$$k(t)(y(a)^{-1}y(ha))k(ht)^{-1} \in P \qquad (a, t \in O). \tag{3}$$

Put

$$R = \bigcap_{t \in O} k(t)^{-1}Pk(t), \qquad C = \bigcap_{t \in O} k(t)^{-1}Pk(ht).$$

If $T_k(E) = \{1\}$, take $P' = 1$. Otherwise (3) supplies $c \in C$. We have $C = Rc$: indeed, $d \in C$ exactly when $dc^{-1} \in R$. Also c normalizes R. To see this, write $v_t = k(t)ck(ht)^{-1} \in P$; for $r \in R$,

$$k(t)crc^{-1}k(t)^{-1} = v_t(k(ht)rk(ht)^{-1})v_t^{-1} \in P.$$

This proves $cRc^{-1} \subseteq R$, hence equality by finiteness. Multiplying $v_t v_{ht} \cdots v_{h^{q-1}t}$ shows $k(t)c^q k(t)^{-1} \in P$, so $c^q \in R$.

The subgroup R is a q-group, being contained in a conjugate of P. Consequently $P' = \langle R, c\rangle = R\langle c\rangle$ is a q-group: R is normal in P' and P'/R is cyclic of order dividing q. Equation (3) puts every consecutive difference $y(a)^{-1}y(ha)$ in $C \subseteq P'$. Multiplying consecutive differences around O gives $y(a)^{-1}y(b) \in P'$ for all $a, b \in O$. The identity configuration satisfies the same conclusion. □

Necessity in Theorem 1. Suppose a surjective strategy exists. For any prime q dividing $|H|$, Cauchy's theorem supplies an element h of order q; faithfulness supplies a position it moves. Starting with the trivial subgroup and $E_0 = \{1\}$, Lemma 3 gives a q-subgroup P_N such that all of E_N is P_N-aligned on O. Lemma 2 forces $E_N = K$. For each $g \in G$, choose a configuration with value 1 at ω and g at $h\omega$. Alignment forces $g \in P_N$. Thus $G = P_N$ is a q-group.

Choose a prime $p \mid |H|$, possible since $H \neq 1$. Then G is a p-group. Because $G \neq 1$, it cannot also be a q-group for a different prime q. Every prime divisor of $|H|$ is therefore p, and H is a p-group as well. □

3 Sufficiency and the formal theorem

Here is a self-contained proof of Kagey's sufficient condition. For the full adversary, replace (1) by

$$T_k^H(E) = \{1\} \cup \{y : \alpha_a(y)k^{-1} \in E \text{ for all } a \in H\}.$$

Let $E^H(s)$ be the result of applying these operations to $\{1\}$ along a sequence s. If a play from x_0 never reaches 1, its moving configuration $z_j = \alpha_{a_j^{-1}}(x_0 b_j)$ stays outside the corresponding excluded set: using (2) with $a = h_j$ in the universal condition gives $\alpha_{h_j}(z_j)k_j^{-1} = z_{j-1}$, so induction excludes z_j from $T_{k_j}^H(E^H(k_1, \ldots, k_{j-1}))$. Hence $E^H(s) = K$ implies that s is surjective.

Lemma 4. *Let $M \lhd K$ be H-invariant. Suppose a sequence s of moves in M satisfies $M \subseteq E^H(s)$. If $u \in K \setminus M$ commutes modulo M with every element of W, the same assertion holds for the strictly larger normal, H-invariant subgroup $L = M\langle u\rangle$.*

Proof. The commutator hypothesis makes L normal in K and H-invariant, and makes H fix each coset Mu^j. Form a sequence consisting of r copies of s separated by the move u^{-1}, where r is the order of u. After $i+1$ copies, the excluded set contains $M \cup Mu^{-1} \cup \cdots \cup Mu^{-i}$. This follows by induction. The separating move sends each guaranteed coset Mu^{-j} to $Mu^{-(j+1)}$ in the recurrence. Each subsequent move in s preserves these shifted cosets, because they are H-invariant and closed under right multiplication by M. Meanwhile the block s restores M: every excluded set contains 1, and the recurrence is monotone in E. After r copies all of L is excluded. All moves used lie in L. □

Sufficiency in Theorem 1. If G and H are p-groups, then W is a finite p-group and so is nilpotent. Begin with $M = 1$ and the empty sequence. For $M \neq K$, let $Z_i(W)$ be the upper central series, and choose the least i with $K \cap Z_i(W) \not\subseteq M$. Choose u in this difference. Its commutators with W lie in $K \cap Z_{i-1}(W) \subseteq M$. Lemma 4 enlarges M while preserving the sequence property. Finiteness makes this process reach $M = K$, giving a sequence with $E^H(s) = K$, hence a surjective strategy. □

The accompanying Lean project proves the full statement, in namespace `SpinningSwitches`, with the following parameters and type:

```
variable {G H Ω : Type*} [Group G] [Group H] [MulAction H Ω]
theorem classification [Finite G] [Finite H] [Finite Ω]
    [FaithfulSMul H Ω] [Nontrivial G] [Nontrivial H] :
    (∃ ks : List (Ω → G), IsSurjectiveStrategy H ks) ↔
      ∃ p : ℕ, p.Prime ∧ IsPGroup p G ∧ IsPGroup p H
```

Here `IsSurjectiveStrategy` quantifies over every equally long list of adversary moves and every base configuration, requiring a prefix index from zero through the list length whose base projection equals that configuration. It is exactly the definition in Section 1. For finite groups, Mathlib's `IsPGroup` is equivalent to having prime-power order. The development also checks the two unsolvable examples stated above. It does not assert an optimal strategy length.

To reproduce the check, install elan, Git, and a C compiler, enter `lean/` in the accompanying bundle, and run `lake exe cache get`, then `lake build`. The project pins Lean 4.34.0 and its Mathlib dependencies. The build checks the proof, its statement type, small examples, and axiom guards. The theorem uses only Lean's standard axioms `propext`, `Classical.choice`, and `Quot.sound`; no compiled evaluation is used. This relies on Lean's kernel and the stated formal definitions. The formalization uses Mathlib's finite-group and nilpotency libraries [6]. A cached build takes several minutes.

References

[1] P. Kagey, *Spinning switches on a wreath product*, Journal of Combinatorial Theory, Series A **200** (2023), 105795. doi:10.1016/j.jcta.2023.105795. Statement numbers refer to arXiv:2210.09408v1, October 17, 2022.

[2] ndkrempel and P. Kagey, comments of December 7 and December 8, 2025, on Kagey's answer to *Game on groups (generalization of spinning switches puzzle)*, MathOverflow, https://mathoverflow.net/a/423643.

[3] R. Bar Yehuda, T. Etzion and S. Moran, *Rotating-table games and derivatives of words*, Theoretical Computer Science **108** (1993), 311–329. doi:10.1016/0304-3975(93)90196-Z.

[4] R. Ehrenborg and C. M. Skinner, *The blind bartender's problem*, Journal of Combinatorial Theory, Series A **70** (1995), 249–266. doi:10.1016/0097-3165(95)90092-6.

[5] Y. Rabinovich, *A generalization of the Blind Rotating Table game*, Information Processing Letters **176** (2022), 106233. doi:10.1016/j.ipl.2021.106233.

[6] The mathlib Community, *The Lean mathematical library*, Proceedings of CPP 2020, 367–381. doi:10.1145/3372885.3373824.