Oral Exam: Proposal

Peter Kagey

2020/07/28

This document will explore two ideas for dissertation chapters in two different sections. The first section explores how restricting the cycle structure of a permutation affects the expected value of its first letter. In particular, there seems to be a hidden relationship with derangements of n-dimensional hypercubes and the generalized symmetric group more broadly. The second section generalizes a puzzle, and develops (or proves the non-existence of) conditions under which there exists an algorithm for a certain kind of walk reaching every element of a finite group with a random (or an adversarial) player trying to prevent this.

Contents

1 Expected value of the first letter of a permutation

The genesis of this problem comes from a talk that Sami relayed to me during which the speaker described a surprising and elegant relationship between the number of descents in a permutation and the expected value of the first letter:

> Given some $\pi \in S_n$, let $\operatorname{des}(\pi)$ give the number of descents of π, that is
>
> $$\operatorname{des}(\pi) = \#\{i : \pi(i) > \pi(i+1)\}. \tag{1.0.1}$$
>
> For all n, the expected value of $\pi(1)$ for a permutation $\pi \in S_n$ with k descents is $k+1$.

Sami challenged me to look at other permutation statistics and to find other relationships.

1.1 Definitions, notation, and background

Definition 1.1.1. *A **permutation statistic** is simply a map* $\operatorname{st}\colon S_n \to \mathbb{Z}$.

Definition 1.1.2. *Given a permutation statistic* st*, let* $\mathbb{E}^{st}_{n,m}$ *denote the expected value of the first letter of a permutation taken uniformly at random from* $\{\pi \in S_n \mid \operatorname{st}(\pi) = m\}$.

1.2 Main conjecture

Perhaps the richest permutation statistic that I found was the three parameter family given by looking at permutations in S_n with exactly m k-cycles.

Definition 1.2.1. *Let* $\mathrm{cyc}_k(\pi)$ *be the number of* k*-cycles in the cycle decomposition of* π*.*

Conjecture 1.2.2. *For* $k > 1$*,*

$$\mathbb{E}_{n,m}^{cyc_k} = \begin{cases} \dfrac{n+1}{2} + \dfrac{(-1)^{n/k-m}}{2A320032(\frac{n}{k}-m,k)} & k \mid n \\ \dfrac{n+1}{2} & \textit{otherwise} \end{cases}, \tag{1.2.1}$$

where OEIS sequence $A320032(n,k)$ *is the number of derangements of the wreath product* $\mathbb{Z}_k \wr S_n$*, given by the expansion of the exponential generating function*

$$\frac{\exp(-x)}{1-kx}. \tag{1.2.2}$$

This conjecture was suggested by computational evidence, some of which is reflected in the following two tables.

Table 1.2.3. $\mathbb{E}_{n,m}^{cyc_2}$ *gives the expected value of the first letter of* $\pi \in S_n$*, given that* π *has* m 2*-cycles.*

		m					
		0	1	2	3	4	5
n	2	1/1	2/1				
	3	2/1	2/1				
	4	13/5	2/1	3/1			
	5	3/1	3/1	3/1			
	6	101/29	18/5	3/1	4/1		
	7	4/1	4/1	4/1	4/1		
	8	1049/233	130/29	23/5	4/1	5/1	
	9	5/1	5/1	5/1	5/1	5/1	
	10	12809/2329	1282/233	159/29	28/5	5/1	6/1

(1.2.3)

Table 1.2.4. $\mathbb{E}_{n,m}^{cyc_3}$ *gives the expected value of the first letter of* $\pi \in S_n$*, given that* π *has* m 3*-cycles.*

		m			
		0	1	2	3
n	2	3/2			
	3	7/4	5/2		
	4	5/2	5/2		
	5	3/1	3/1		
	6	46/13	13/4	4/1	
	7	4/1	4/1	4/1	
	8	9/2	9/2	9/2	
	9	1159/232	131/26	19/4	11/2

(1.2.4)

Note 1.2.5. *As mentioned in the conjecture the "error" term in the* $k \mid n$ *case is related to the wreath product* $\mathbb{Z}_k \wr S_n$*. Specializing to* $k = 2$*, this is the hyperoctahedral group, so the error is related to the number of isometries of the* n*-dimensional hypercube that move* $(n-1)$*-dimensional facets. (I don't know how to explain this phenomenon, but I'd like to find out.)*

1.3 Some recurrences

I've made some headway in proving this conjecture. In particular, I can compute $\mathbb{E}_{n,m}^{\mathrm{cyc}_k}$ with much lower computational complexity than brute force, I have useful related recurrences, and I have found a bijection that proves the "otherwise" part of the conjecture.

Definition 1.3.1. *Let $C_k(n,m)$ be the number of permutations $\pi \in S_n$ such that $\mathrm{cyc}_k(\pi) = m$.*

Definition 1.3.2. *Let $C_k^{(\ell)}(n,m)$ be the number of permutations $\pi \in S_n$ such that $\mathrm{cyc}_k(\pi) = m$ and $\pi(1) = \ell$.*

Lemma 1.3.3. *$C_k^{(1)}(n,m) = C_k(n-1,m)$ for all $k \geq 2$.*

Proof. Writing π as a word, consider the map $\pi_1\pi_2\ldots\pi_n \mapsto (\pi_2-1)\ldots(\pi_n-1)$. Since $\pi_1 = 1$, the inverse map is clear. □

Lemma 1.3.4. *$C_k^{(2)}(n,m) = \cdots = C_k^{(n)}(n,m)$.*

Proof. It is enough to show that $C_k^{(a)}(n,m) = C_k^{(b)}(n,m)$ for all $a,b > 1$. Since the permutations under consideration do not fix 1, conjugation by (ab) is an isomorphism which takes all words starting with a to words starting with b without changing the cycle structure. □

Lemma 1.3.5. *$C_k^{(1)}(n,m) = C_k(n-1,m)$ for all $k \geq 2$.*

Proof. Writing π as a word, consider the map $\pi_1\pi_2\ldots\pi_n \mapsto (\pi_2-1)\ldots(\pi_n-1)$. Since $\pi_1 = 1$, the inverse map is clear. □

Lemma 1.3.6. *$C_k^{(2)}(n,m) = \cdots = C_k^{(n)}(n,m)$.*

Proof. It is enough to show that $C_k^{(a)}(n,m) = C_k^{(b)}(n,m)$ for all $a,b > 1$. Since the permutations under consideration do not fix 1, conjugation by (ab) is an isomorphism which takes all words starting with a to words starting with b without changing the cycle structure. □

Lemma 1.3.7. *For all $2 \leq a \leq n$,*

$$C_k^{(a)}(n,m) = \frac{C_k(n,m) - C_k(n-1,m)}{n-1}. \tag{1.3.1}$$

Proof. Since

$$C_k(n,m) = C_k^{(1)}(n,m) + C_k^{(2)}(n,m) + \cdots + C_k^{(n)}(n,m) \tag{1.3.2}$$

using Lemma 1.3.6, for all values $2 \leq a \leq n$, this can be rewritten as

$$C_k(n,m) = C_k^{(1)}(n,m) + (n-1)C_k^{(a)}(n,m) \tag{1.3.3}$$

solving for $C_k^{(a)}(n,m)$ and using the substitution from Lemma 1.3.5 gives the desired result:

$$C_k^{(a)}(n,m) = \frac{C_k(n,m) - C_k(n-1,m)}{n-1}. \tag{1.3.4}$$

□

Theorem 1.3.8. *The base case, $C_k(n,0)$ is given by the expansion of the exponential generating function*

$$\frac{\exp(-x^k/k)}{(1-x)}, \tag{1.3.5}$$

and moreover,

$$C_k(n,0) = \sum_{i=0}^{\lfloor n/k \rfloor} \frac{n!(-1)^i}{i!\,k^i} = A122974(n,k). \tag{1.3.6}$$

Proof. A probabilistic proof can be found here. `http://capone.mtsu.edu/dwalsh/NOKCYCLB.pdf` □

Note 1.3.9. *I'd like to find a combinatorial proof of this fact, and I'd like to see if I can modify the probabilistic proof to prove Conjecture 1.2.2.*

Theorem 1.3.10. *For all $k > 0, m > 0$*

$$mC_k(n,m) = (k-1)!\binom{n}{k}C_k(n-k,m-1). \tag{1.3.7}$$

Proof. As an abuse of notation, let $C_k(n,m) = \{\pi \in S_n \mid \mathrm{cyc}_k(\pi) = m\}$. Then consider the two sets, whose cardinalities match the left- and right-hand sides of the equation above:

$$S^L_{n,m,k} = \{(\pi, c) \mid \pi \in C_k(n,m), c \text{ a distinguished } k\text{-cycle of } \pi\} \tag{1.3.8}$$

$$S^R_{n,m,k} = \{(\sigma, d) \mid \pi \in C_k(n-m,m-1), d \text{ an } n\text{-ary necklace of length } k\} \tag{1.3.9}$$

The first set, $S^L_{n,m,k}$, is constructed by taking a permutation in $C_k(n,m)$ and choosing one of its m k-cycles to be distinguished, so $S^L_{n,m,k} = mC_k(n,m)$.

In second set, $S^R_{n,m,k}$, the two parts of the tuple are independent. There are $C_k(n-k,m-1)$ choices for σ and $(k-1)!\binom{n}{k}$ choices for d. Thus $S^R_{n,m,k} = (k-1)!\binom{n}{k}C_k(n-k,m-1)$.

Now, consider the map $\phi\colon S^L_{n,m,k} \to S^R_{n,m,k}$ which in cycle notation does the following

$$(\pi_1\pi_2\ldots\pi_\ell, \pi_1) \mapsto (\pi'_2\ldots\pi'_\ell, \pi_1) \tag{1.3.10}$$

where π'_i is π_i after relabeling.

By construction, σ has one fewer k-cycle and k fewer letters than π. □

Example 1.3.11. *Suppose $\pi = (18)(\mathbf{37})(254)$ in cycle notation with (37) distinguished. Then*

$$((18)(37)(254),(37)) \mapsto ((16)(243),(37)) \tag{1.3.11}$$

under this bijection.

Theorem 1.3.12. *For $k > 1$, the expected value of the first letter of a permutation $\pi \in S_n$ with m k-cycles is given by*

$$E^{cyc_k}_{n,m} = \frac{n}{2}\left(1 - \frac{C_k(n-1,m)}{C_k(n,m)}\right) + 1. \tag{1.3.12}$$

Proof. By definition,

$$E^{\mathrm{cyc}_k}_{n,m} = \frac{\displaystyle\sum_{a=1}^{n} aC^{(a)}_k(n,m)}{C_k(n,m)}. \tag{1.3.13}$$

Using Lemma 1.3.6, we can consolidate all but the first term of the numerator

$$\sum_{a=1}^{n} aC^{(a)}_k(n,m) = C^{(1)}_k(n,m) + \sum_{a=2}^{n} aC^{(n)}_k(n,m) \tag{1.3.14}$$

$$= C^{(1)}_k(n,m) + C^{(n)}_k(n,m)\sum_{a=2}^{n} a \tag{1.3.15}$$

$$= C^{(1)}_k(n,m) + \frac{(n-1)(n+2)}{2}C^{(n)}_k(n,m) \tag{1.3.16}$$

$$\tag{1.3.17}$$

Now using the recurrences in Lemmas 1.3.5 and 1.3.7

$$\sum_{a=1}^{n} aC_k^{(a)}(n,m) = C_k(n-1,m) + \frac{(n-1)(n+2)}{2}\left(\frac{C_k(n,m) - C_k(n-1,m)}{n-1}\right) \tag{1.3.18}$$

$$= \left(\frac{n}{2}+1\right)C_k(n,m) - \frac{n}{2}C_k(n-1,m). \tag{1.3.19}$$

Lastly, dividing by the numerator yields the result

$$E_{n,m}^{\mathrm{cyc}_k} = \frac{\left(\frac{n}{2}+1\right)C_k(n,m) - \frac{n}{2}C_k(n-1,m)}{C_k(n,m)} = \frac{n}{2}\left(1 - \frac{C_k(n-1,m)}{C_k(n,m)}\right) + 1. \tag{1.3.20}$$

□

Note 1.3.13. *Theorem 1.3.12 together with Theorem 1.3.8 and Theorem 1.3.10 give a computationally inexpensive way to compute* $\mathbb{E}_{n,m}^{cyc_k}$.

1.4 A bijective proof

One plausible proof strategy is based on Theorem 1.3.12, namely making sense of the ratio $\frac{C_k(n-1,m)}{C_k(n,m)}$. In particular, to show the "$k \nmid n$" case of Conjecture 1.2.2, it is enough to show that the ratio is equal to n, or equivalently, that $nC_k(n-1,m) = C_k(n,m)$.

The nicest combinatorial proof of this fact would be a family of bijections $\varphi_k \colon [n] \times S_{n-1} \to S_n$ that preserves the number of k cycles when $k \nmid n$.

Note 1.4.1. *No such map can exist when $k \mid n$ because in that case there exist permutations in S_n consisting of n/k disjoint k-cycles, but no permutation in S_{n-1} can contain this many k-cycles.*

Theorem 1.4.2. *The exists a bijective map $\varphi_k \colon [n] \times S_{n-1} \to S_n$ that preserves k-cycles when $k \nmid n$.*

Proof. I will construct such a map and the inverse of such a map. The bijection is easy to implement but more difficult to write down. It will be clear from the construction that it preserves the number of k-cycles. In this section, the names of the arguments and output of the function will follow the convention $\varphi_k(i,\pi) = \pi'$, where π has cycles $c_1c_2\ldots c_N$. (And π' has cycles $c_1'c_2'\ldots c_{N'}'$.) The cycles themselves have letters $c_i = (c_{i,1}c_{i,2}\ldots c_{i,d_i})$, where $c_{i,d_i+1} = c_{i,1}$. Moreover the letters of each cycle chosen so that the smallest letter is first, after which the cycles are written in lexicographic order.

- The permutation π' sends $1 \mapsto i$.
- If the cycle that 1 is in is called the *initial cycle*, then if π has an initial ℓ cycle then
  - If $i = 1$, then $c_1' = (1)$,
  - if $|c_1| = k$, then $|c_1'| = k$,
  - if $|c_1| = k-1$ then $|c_1'| = k+1$,
  - otherwise, $|c_1'| = |c_1| + 1$.

These are choices so that the inverse map can recover the "added" letter and so that the combinatorics works.

(For the sake of simplicity, when describing the behavior of φ_k, assume that the arguments are normalized so that the letters are $[N]$, with the first argument being considered smaller in the case of a tie. For example, instead of talking about $\phi_k(3,(25)(93))$, I'll instead describe $\phi_k(2,(14)(53))$.)

- When $i = 1$, ϕ_k simply adds a 1-cycle to π: in cycle notation, $\pi' = (1)\pi$.
- When the $c_1 > k$ or $c_1 < k-1$, ϕ_k inserts i after 1 in the cycle. (e.g. $\phi_2(4,(1726)(53)) = (14726)(53)$.)
- When $|c_1| = k$, $\pi' = (c_{1,1}ic_{1,3}\ldots c_{1,d_1})\phi_k(c_{1,2},c_2\ldots c_N)$. (e.g $\phi_2(4,(17)(2653)) = (14)\phi_2(7,(2653))$.)

- The bijection is most complex when $|c_1| = k-1$.

When $|c_1| = k-1$, you "insert i and take from the next cycle". The "take from the next cycle" requires and auxillary function ψ_k which takes a $(k-1)$-cycle and a permutation and returns a permutation.

$$\psi_k((\alpha_1\alpha_2\dots\alpha_{k-1}),\pi) = \begin{cases} (\alpha_1 c_{1,1}\alpha_2\dots\alpha_{k-1})c_2\dots c_N & |c_1| = 1 \\ (\alpha_1 c_{1,2}\alpha_2\dots\alpha_{k-1})\psi_k((c_{1,1}c_{1,3}\dots c_{1,k}),c_2\dots c_N) & |c_1| = k \\ (\alpha_1 c_{1,2}\alpha_2\dots\alpha_{k-1})(c_{1,1}c_{1,3}\dots c_{1,d_1})c_2\dots c_N & \text{otherwise} \end{cases}. \tag{1.4.1}$$

Thus when $|c_1| = k-1$,

$$\varphi_k(i,\pi) = \begin{cases} (c_{1,1}ic_{2,1}c_{1,2}\dots c_{1,k-1})c_3\dots c_N & |c_2| = 1 \\ (c_{1,1}ic_{2,2}c_{1,2}\dots c_{1,k-1})\psi_k((c_{2,1}c_{2,3}\dots c_{2,k}),c_3\dots c_N) & |c_2| = k \\ (c_{1,1}ic_{2,2}c_{1,2}\dots c_{1,k-1})(c_{2,1})(c_{2,3}\dots c_{2,k+1})c_3\dots c_N & |c_2| = k+1 \\ (c_{1,1}ic_{2,2}c_{1,2}\dots c_{1,k-1})(c_{2,1}c_{2,3}\dots c_{2,d_2})c_3\dots c_N & \text{otherwise} \end{cases}. \tag{1.4.2}$$

□

This bijection φ_k preserves the number of k-cycles when $k \nmid n$, but can sometimes fail to preserve k-cycles when $k \mid n$, as explored in the next section.

1.5 Generating function

Theorem 1.4.2 takes care of the case where $k \nmid n$, but an analysis of where the bijection fails to preserve the number of k-cycles does not easily yield Conjecture 1.2.2.

I'm most interested in the case where $k = 2$, and moreover my previous results for this case have generalized easily to $k > 2$, so for the remainder of this section, I'll specialize to $k = 2$.

Definition 1.5.1. *Let the failure of the bijection to preserve k-cycles be measured by the function*

$$\text{Error}_k(n,m) := C_k(n,m) - nC_k(n-1,m). \tag{1.5.1}$$

Conjecture 1.5.2. *When $k = 2$ it appears that*

$$\text{Error}_2(2n,m) = (-1)^{n+m+1}(2n-1)!!\left(\binom{n-1}{m}\binom{n-1}{m-1}\right) \tag{1.5.2}$$

$$\text{Error}_2(2n+1,m) = 0 \tag{1.5.3}$$

where $(2n-1)!! = (2n-1)\cdot(2n-3)\cdots 5\cdot 3\cdot 1$.

My next steps for this project involve taking Conjecture 1.5.2 for granted and solving for $A320032$ in Equation 1.2.1, seeing if temporarily assuming the conjecture, using generating function tricks, and working backward is a viable proof strategy.

In particular, I'd like to prove

$$\mathbb{E}^{\text{cyc}_2}_{n,m} = n\left(1 - \frac{C_2(2n-1,m)}{C_2(2n,m)}\right) + 1 \tag{1.5.4}$$

$$= \frac{2n+1}{2} + \frac{(-1)^{n-m}}{2A320032(n-m,2)} \tag{1.5.5}$$

where Equation 1.5.4 follows from Theorem 1.3.12, and Equation 1.5.5 is Conjecture 1.2.2. Solving for $C_2(2n-1,m)$ gives

$$C_2(2n-1,m) = \frac{C_2(2n,m) + (-1)^{n+m}(2n-1)!!\left(\binom{n-1}{m}\binom{n-1}{m-1}\right)}{2n}, \tag{1.5.6}$$

so taking Conjecture 1.5.2 for granted, means that proving Conjecture 1.2.2 is equivalent to showing that

$$\frac{2n+1}{2} + \frac{(-1)^{n-m}}{2A320032(n-m,2)} = n\left(1 - \frac{C_2(2n,m) + (-1)^{n+m}(2n-1)!!\left(\binom{n-1}{m}\binom{n-1}{m-1}\right)}{2nC_2(2n,m)}\right) + 1. \tag{1.5.7}$$

If I haven't made any mistakes, solving for $A320032$ gives

$$A320032(n-m,2) = -\frac{C_2(2n,m)}{(2n-1)!!\left(\binom{n-1}{m}\binom{n-1}{m-1}\right)}, \tag{1.5.8}$$

which is a surprisingly simple rearrangment of Equation 1.5.7 above. Since I know several recurrences for $C_k(n,m)$, I have some hope of being able to solve this with generating function tricks.

1.6 Next steps

There are a few different things I'd like to explore next.

- I have a document with tables of other permutation statistics. Some of these don't look like they have much structure, but some of them might be amenable to this sort of analysis.
- I'm interested in specifying more data about the cycle structure. For example,
  - If the cycle structure is fully specified by a partition of n.
  - If the cycle structure is partly specified (e.g. π has exactly three fixed points and one transposition.)
- I'd like to make the connection to derangements of wreath products, and to derangements of the hyperoctahedral group in particular. (This is the case where $k = 2$).
- It appears that
$$nC_k(kn-1,m-1) = mC_k(kn,m) \tag{1.6.1}$$
and it would be nice to have a combinatorial proof for why.
- I'd like to prove (or disprove) that
$$C_k(kn,i) + C_k(kn,k-i) = kn(C_k(kn-1,i) + C_k(kn-1,k-i)) \tag{1.6.2}$$
and in particular when $i = 0$,
$$C_k(kn,0) - knC_k(kn-1,0) = C_k(kn,k). \tag{1.6.3}$$

2 Spinning Switches

The second problem is inspired by a puzzle that came up at the 2019 Graduate Student Combinatorics Conference in Philadelphia. I first saw the puzzle in Steve Miller's Math Riddles collection, I introduced the puzzle to a few attendees of the 2019 GSCC, and after a few days we were able to generalize the puzzle somewhat. It turns out that both the puzzle and the generalization that we found was in Peter Winkler's *Mathematical Puzzles: A Connoisseur's Collection*:

> Four identical, unlabeled switches are wired in series to a light bulb. The switches are simple buttons whose state cannot be directly observed, but can be changed by pushing; they are mounted on the corners of a rotatable square. At any point, you may push, simultaneously, any subset of the buttons, but then an adversary spins the square. Show that there is a deterministic algorithm that will enable you to turn on the bulb in at most some fixed number of steps.

(The generalization that we found and that exists in the book is that there also exists an algorithm for any rotating 2^n-gon.)

2.1 Definitions and notation

The language that I use to generalize this puzzle is the language of wreath products, which came up in the above section in Conjecture 1.2.2 where the number of derangements of the generalized symmetric group $(\mathbb{Z}_k \wr S_n)$ played a role in the error term. In the first section, you could get away without knowing what a wreath product is, but in this section it plays a more pivotal role. I'm defining *finite* wreath products because that's all we need, and it sidesteps some technical details.

Definition 2.1.1. *Let G and H be finite groups, and let Ω be a finite set with an H action. Next, define $K = \prod_{\omega\in\Omega} A_\omega$ (called the **base** of the wreath product) be the $|\Omega|$-fold product of G, indexed by elements of Ω. The H-action extends to K by $h \cdot \alpha_\omega = \alpha_{h^{-1}\cdot\omega}$ Then $G \wr_\Omega H$ is the semidirect product $K \rtimes H$ where the group multiplication is*

$$(k_1, h_1)(k_2, h_2) = (k_1(h_1 \cdot k_2), h_2h_2). \tag{2.1.1}$$

2.2 Generalization

I'm interested in determining criteria for when two finite groups G and H (together with a set Ω upon which H acts) have what I call a "switching strategy", which in terms of the above puzzle means that there is a deterministic finite algorithm that can turn on the bulb.

Definition 2.2.1. *Let $p\colon G \wr_\Omega H \to K$ be the projection map from the wreath product onto its base. A **switching strategy** is a finite sequence, $\{k_i \in K\}_{i=1}^N$, such that for every sequence $\{h_i \in H\}_{i=1}^N$,*

$$p(\{e_{G\wr H}, (k_1, h_1), (k_1, h_1) \cdot (k_2, h_2), \cdots, (k_1, h_1) \cdot (k_2, h_2) \cdots (k_N, h_N)\}) = K. \tag{2.2.1}$$

Definition 2.2.2. *A switching strategy is called **minimal** when $N = |K| - 1$.*

2.3 Motivating examples.

Example 2.3.1. *In the introductory example, $G = \mathbb{Z}_2$, $H = C_4$, and Ω is the vertices of a square, with H acting on Ω by rotation. Up to the action of H and the toggling of all of the switches, there are four distinct moves:*

- $k_a = (1, 1, 1, 1)$, *toggling all of the switches,*
- $k_b = (0, 0, 0, 1)$, *toggling just one of the switches,*
- $k_c = (0, 0, 1, 1)$, *toggling two adjacent switches,*
- $k_d = (0, 1, 0, 1)$, *toggling diagonally opposite switches.*

Then one solution is the fifteen move sequence

$$k_a, k_b, k_a, k_c, k_a, k_b, k_a, k_d, k_a, k_b, k_a, k_c, k_a, k_b, k_a. \tag{2.3.1}$$

Note 2.3.2. *The exact same strategy works if Example 2.3.1 is modified so that $H = D_4$ the dihedral group of the square.*

Example 2.3.3. *If $G = \mathbb{Z}_3$ and $H = C_3$, there are four possible moves up to toggling all switches and H-action:*

$$\underbrace{\begin{array}{ccc} & 1 & \\ / & & \backslash \\ 1 & — & 1 \end{array}}_{x} \quad \underbrace{\begin{array}{ccc} & 1 & \\ / & & \backslash \\ 0 & — & 0 \end{array}}_{A} \quad \underbrace{\begin{array}{ccc} & 0 & \\ / & & \backslash \\ 1 & — & 1 \end{array}}_{B} \quad \underbrace{\begin{array}{ccc} & 0 & \\ / & & \backslash \\ 1 & — & 2 \end{array}}_{C} \quad \underbrace{\begin{array}{ccc} & 0 & \\ / & & \backslash \\ 2 & — & 1 \end{array}}_{D} \tag{2.3.2}$$

By looking at the multiplication table in Figure 1, you can create the directed graph in Figure 2. If x denotes flipping all of the switches once, then one valid strategy is $((x^2C)^2x^2A)^2(x^2C)^2x^2$. This is the "top" strategy in the graph.

	A	B	C	D
A	$\{B\}$	$\{C, D\}$	$\{A\}$	$\{A\}$
B	$\{C, D\}$	$\{A\}$	$\{B\}$	$\{B\}$
C	$\{A\}$	$\{B\}$	$\{D\}$	$\emptyset$
D	$\{A\}$	$\{B\}$	$\emptyset$	$\{C\}$

Figure 1: Multiplication table for states/moves in K modulo rotations and toggling all switches.

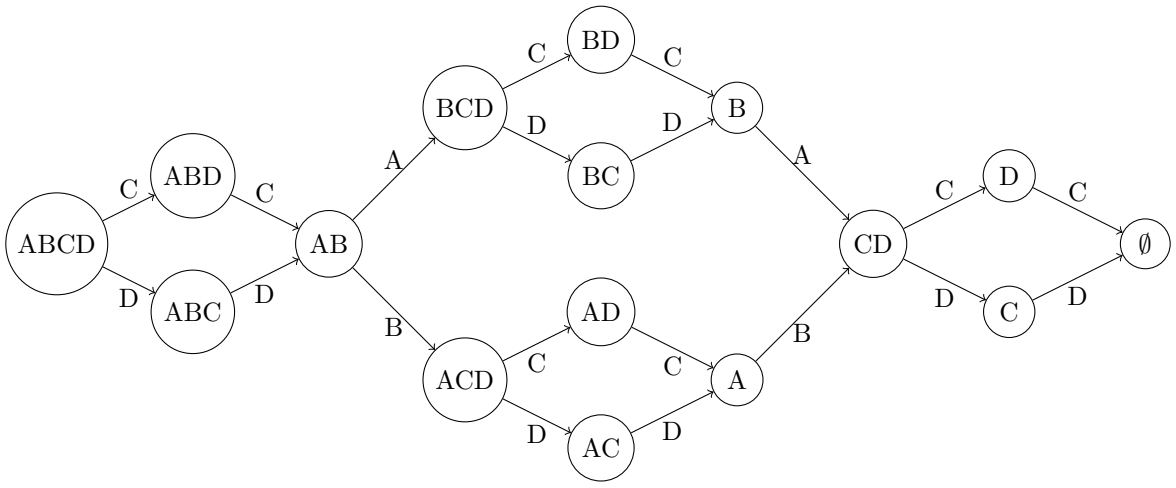

Figure 2: Switching strategy for $C_3 \wr C_3$. Notice that this diagram is 180° antisymmetric: flipping the picture around sends sets to their complements and moves to their inverses.

Example 2.3.4. *So far, G has always been abelian, so it's worth including an example where G is not abelian. Suppose that $G = D_8$, $H = \mathbb{Z}_2$ and Ω is a two element set upon which H acts non-trivially. Then using the following four moves:*

- *A_r: Apply r to both copies.*
- *A_f: Apply f to both copies.*
- *B: Apply r to one copy.*

- *C: Apply r^2 to one copy.*
- *D: Apply f to one copy.*

A strategy is $(A_r^3A_fA_r^3)B(A_r^3A_fA_r^3)C(A_r^3A_fA_r^3)B(A_r^3A_fA_r^3)D(A_r^3A_fA_r^3)B(A_r^3A_fA_r^3)C(A_r^3A_fA_r^3)B(A_r^3A_fA_r^3)$ *or if* $x = A_r^3A_fA_r^3$ *then the same strategy is* $xBxCxBxDxBxCxBx$

2.4 Conjectures

Conjecture 2.4.1. *$\{k_i\}_{i=1}^n$ is a switching strategy if and only if $\{k_{n-i+1}\}_{i=1}^n$ is a switching strategy.*

Conjecture 2.4.2. *$\{k_i\}_{i=1}^n$ is a switching strategy if and only if $\{k_i^{-1}\}_{i=1}^{|K|}$ is a switching strategy.*

Conjecture 2.4.3. *If there exists a strategy $\{k_i\}_{i=1}^n$, then there also exists a minimal strategy $\{k_i'\}_{i=1}^{|K|}$.*

2.5 Reduction

For some given G and H, there is a method to prove that no strategy exists, which I am calling **reduction** as an allusion to the notion of reduction in complexity theory. The idea is to show that there if there exists a strategy that strategy can be repurposed to solve a G' and H' that is known to have no solution. For example, when $G' = \mathbb{Z}_2$ and $H' = C_3$, there is no strategy because one could get stuck in a state where exactly one switch is in a different state than the other two. This means that there is also no strategy for $G = \mathbb{Z}_3$ and $H = C_6$, because if there were a switching strategy, you could "ignore" every other switch and come up with a switching strategy on $\mathbb{Z}_3 \wr C_3$.

More precisely, there exists a reduction from $G \wr H$ to $G' \wr H'$ if H' is isomorphic to a subset of H and if there exists a quotient group of G that is isomorphic to G'.

There are some additional details and hypothesis here, including how the H- and H'-actions relate to each other. This is something that I'm still trying to make sense of.

2.6 Next steps

There are a few different things I'd like to explore next.

- I still need to prove that a n-gon does not have a strategy with p^k-way switches unless n is a power of p. (I can prove the converse.)
- I have a very loose conjecture that given a transitive group action (and maybe some other natural conditions), $G \wr H$ has a switching strategy if and only if the cardinality of the wreath product, $|G \wr H|$, is a prime power.
- Concretely, I'd like to explore the case where the switches behave like the quaternion group (which is of order 2^3). I already know there's a switching strategy for both cyclic groups and dihedral groups of order 2^ℓ, so the quaternion group is the smallest group not yet checked.
- I'd like to prove or disprove the three conjectures above.
- Of course $G \wr \mathbb{1}$ has a switching strategy, but does it always have a palindromic switching strategy?
- I'd like to characterize the story for arbitrarily chosen G and H, and I'd like to better understand what role the group action plays.
- I'm interested in some analog where the different "switches" can behave differently. (E.g. a triangle with a three-way switch and two two-way switches.)
- If there is not a (deterministic) switching strategy, is there some useful notion of a "probabilistic" switching strategy that minimizes the expected number of moves. (Assuming that the adversary picks the sequence $h_i \in H_{i=1}^\infty$ according to some known distribution.)
- Given the prominence of groups of prime power order, I'm curious if there's some vector space phenomena going on under the hood. If there is, I'd like to be able to see it.