

Ma 6 PSET 5

Victoria Liu

November 24, 2020

Problem 1

Proof. I believe this can be solved using permutations, by "disrupting" long cycles by a single transformation. Bob and Charlie should choose a strategy before the game, and we describe how Charlie and Bob should each act to win. We will start with Charlie (even though he acts after Bob) since his action is more straightforward. When Charlie comes in and hears Alice's number N , he should open the *box* number N . Say he finds a note with the number M on it, he should next look in box M , and so on. Now, the issue here is how many boxes will Charlie go through before he finds the box with card number N ? If Bob does not "transform" the boxes, Charlie may be unlucky and need to go through all 100 boxes before finding N , losing the game. Mathematically, needing to go through 100 boxes this would be the same as permutation with a single cycle, where all 100 numbers in the same cycle. To clarify the permutation idea more generally, the way Alice places the cards in the boxes will create a unique permutation when Charlie chooses boxes based on the card numbers he finds. The permutation will take a number A to the number B if and only if card B is found in box A , and the longest cycle here is 100. Notably, if Bob and Charlie can guarantee that the longest cycle in the permutation is 50 and Charlie knows which cycle to look through, then Charlie will be able to finish the cycle within 50 box openings, find N , and win. Bob can guarantee that the longest cycle in the permutation is 50 because he knows what cards are in what boxes. If Alice's original card placement does not create cycles greater than length 50, then Bob can choose not to switch any boxes (or if the game requires him to switch two boxes, he can just switch two boxes within the same cycle, thereby creating two even smaller cycles from that cycle). If Alice's original card placement creates a permutation with a cycle C greater than length 50 (and note, only once cycle could be greater than 50 since there only 100 boxes), Bob can always find two boxes in this cycle C to switch, such that the two resulting cycles are both less than 50. Bob's switch is the same as a transformation; we can think of Alice's original card placement as permutation α , and Bob's transformation as τ . If τ is done to two boxes within the same cycle, $\tau\alpha$ will split up the cycle that τ acted on. To ensure that the split-up cycles are both less than 50, Bob should choose two boxes that are "separated" by $\alpha^{\lceil |C|/2 \rceil}$ permutations, where $|C|$ represents the length of the cycle we are trying to break up (i.e. $|C| > 50$); the ceiling function is there to account for odd $|C|$. It is now evident that $\tau\alpha$ will result in a new permutation, the one that Charlie sees, where all the cycles are less than length 50. Now, how can we guarantee that Charlie will start looking in the cycle that contains N ? This is very easy—since he is starting with box number N , he is automatically in the right cycle. Thus, we have shown that a winning strategy exists, no matter how Alice plays.

□

Problem 2

Proof. We will do a bijective proof. We can split group G into G_E , the set of even permutations, and G_O , the set of odd permutations. We note that every element of G must fall into one of these two groups. We take $\beta \in G$ to be an odd permutation and $\alpha \in G$. If $\alpha \in G_E$, then the composition $\beta\alpha \in G_O$ because the sum of an odd and even number is odd. If $\alpha \in G_O$, then the composition $\beta\alpha \in G_E$. Without loss of generality, let's set $\alpha \in G_E$, and β maps α to some $\gamma \in G_O$. We will next show that β is a bijection between G_E and G_O , which would allow us to say that $|G_E| = |G_O|$.

Since G is a group, it has the Latin Square property, so that: $\gamma = \beta\alpha_1$ and $\gamma = \beta\alpha_2 \iff \alpha_1 = \alpha_2$. This can be clearly seen through the cancellation law, since:

$$\beta\alpha_1 = \beta\alpha_2 \tag{1}$$

$$\beta^{-1}\beta\alpha_1 = \beta^{-1}\beta\alpha_2 \tag{2}$$

$$\alpha_1 = \alpha_2 \tag{3}$$

Note that since G is a group, $\beta^{-1} \in G$. Now, we see that β maps $\alpha \in G_E$ to exactly one permutation $\gamma \in G_O$. Does it also connect every $\gamma \in G_O$ to exactly one permutation $\alpha \in G_E$? It does, since $\alpha = \beta^{-1}\gamma_1$ and $\alpha = \beta^{-1}\gamma_2 \iff \gamma_1 = \gamma_2$. This can again be seen through the cancellation law, since:

$$\beta^{-1}\gamma_1 = \beta^{-1}\gamma_2 \tag{4}$$

$$\beta\beta^{-1}\gamma_1 = \beta\beta^{-1}\gamma_2 \tag{5}$$

$$\gamma_1 = \gamma_2 \tag{6}$$

Now, we see that β^{-1} maps every $\gamma \in G_O$ to exactly one permutation $\alpha \in G_E$, and that β is a bijection between G_E and G_O . Thus, $|G_E| = |G_O|$, and exactly half the permutations are odd and exactly half the permutations are even.

□

Problem 3

Proof. We will do a proof by contradiction. Let's suppose that we can actually reach the sequence 2, 1, 3, 4, 5. We can think of rotations and reflections as permutations of the labeled vertices. For example, starting at 1, 2, 3, 4, 5, a clockwise rotation 75 degrees would result in 5, 4, 3, 2, 1. We can see that rotations shift every number by one, an operation that can be done by four transpositions. This means that rotations are all even permutations. In addition, reflections are also even permutations; a reflection will stabilize one vertex and transpose two pairs of vertices. In the example given in the problem, since we are reflecting over the line of symmetry passing through vertex 1, 1

is stabilized. The transpositions are then $(2, 5)(3, 4)$, which is even. Since all of the allowed permutations are even, all the compositions of permutations are even as well, and allowed sequences can only be reached through even permutations, meaning that $2, 1, 3, 4, 5$ must be reachable through an even permutation. However, that is not true, because we can visit $2, 1, 3, 4, 5$ using an odd permutation (i.e. the transposition $(1, 2)$), contradicting the stipulation that it can only be reached with even permutations.

□

Problem 4

4.a

Proof. We will do a direct proof. Let $\tau = (1\ 2)$ and $c = (1\ 2\ 3\ \dots\ n)$. Let's define the inverse of c as c^{-1} , where $c^{-1} = c^{n-1}$ because we are in effect shifting the cycle in the other direction. We can prove that $c^{-1} = c^{n-1}$ because:

$$c^{-1} \cdot c = 1 \tag{7}$$

$$c^{-1} \cdot c = c^n \tag{8}$$

$$c^{-1} \cdot c = c^{n-1} \cdot c \tag{9}$$

where 1 is the identity element.

Let's first show that compositions of τ and c can 'generate' all transpositions of the form $(k\ k+1)$, where $1 \leq k \leq n-1$. Intuitively, we will be composing c^{-1} onto itself $k-1$ times until $k \rightarrow 1$ and $k+1 \rightarrow 2$. Then, we switch 1 and 2 , which are in the original positions of k and $k+1$, respectively, with τ . Finally, we cycle back in the other direction by composing c onto itself $k-1$ times until we are back to our original sequence, except with k and $k+1$ switched. Mathematically, it looks like: $c^{k-1} \cdot \tau \cdot c^{1-k}$. This algorithm holds for all $1 \leq k \leq n-1$.

Now that we've shown that c and τ generate all "consecutive" transpositions, we will use induction to prove that the set of consecutive transpositions generate all transpositions $(p\ q)$ in S_n . Without loss of generality, we assume that $q > p$, and we can use induction on the difference between q and p . For our base case, when $q - p = 1$, it's evident that the consecutive transpositions can generate $(p\ q)$ because $(p\ q)$ would actually be a consecutive transposition. Now for our inductive hypothesis, suppose that all transpositions where $q - p \leq r$ can be generated by the "consecutive" transpositions, where $1 \leq r \leq n-2$. For $q - p = r + 1$, we can generate $(p\ q)$ as such:

$$(p\ p+1) \cdot (p+1\ q) \cdot (p\ p+1) \tag{10}$$

In this composition of transpositions, we ultimately switch p and q by using $p+1$ as an intermediary. Note that $(p\ p+1)$ is in our set of consecutive transpositions, and since $q - (p+1) = r$, the transposition $(p+1\ q)$ is guaranteed by our induction hypothesis. Thus, we've found a

composition of permutations for when $q - p = r + 1$, and our induction is complete; all sets of transpositions $(p \ q)$ can be "generated" from τ and c . We learned in class that all cycles and permutations can be decomposed into transpositions, so τ and c can "generate" all $(m \ n)$ where \square

4.b

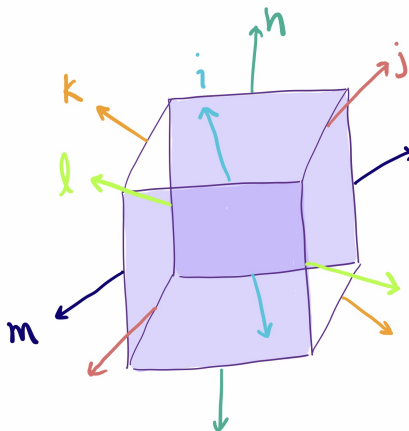
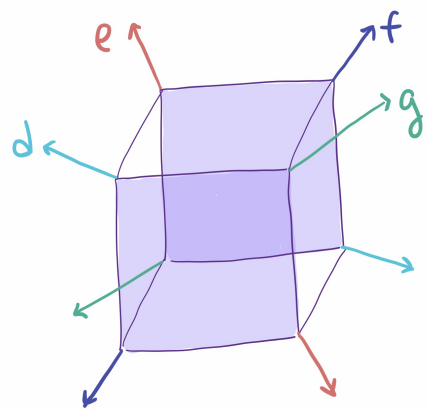
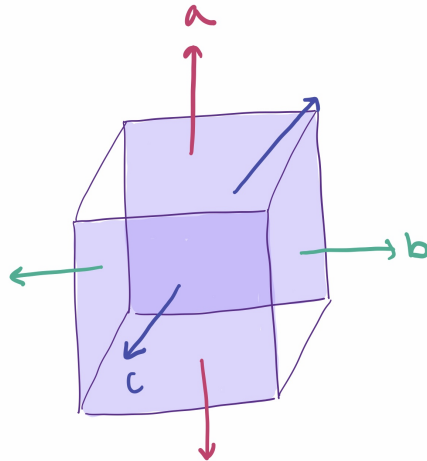
Proof. We will do a direct proof. It will be sufficient to show that the set of $\binom{n-1}{2} + 1$ transpositions can generate all transpositions in S_n , since all permutations in S_n can be decomposed into compositions of transpositions. We immediately note that a set T of $\binom{n-1}{2} + 1$ unique transpositions must have all n numbers (i.e. $1, 2, 3, \dots, n$) in at least one transposition, because the total number of unique transpositions in S_{n-1} is $\binom{n-1}{2}$, so adding 1 transposition would require including the n^{th} number. Now, how can we compose our current transpositions to 'generate' every transposition in S_n ? We can think of this in terms of graph theory; each number is a node, and each edge is a transposition in the set T . Since we have n numbers, there will be n nodes, and there will be $\binom{n-1}{2} + 1$ edges. Since every number is part of a transposition, this graph is connected; this fact can also be seen because the number of edges to fully connect any subset of $n - 1$ nodes is $\binom{n-1}{2}$, so $\binom{n-1}{2} + 1$ edges must connect an n^{th} node. Since the graph is connected, there exists a path between any two nodes, meaning that we can always find a composition of transpositions between two numbers. The algorithm to actually find the composition would be as follows: we run BFS to find the shortest distance between two nodes, and we start at one of our numbers in the transposition. Along each edge, we perform the transposition defined by that edge, and we do this until we reach the other number. Once we reach the second number, we go back the way we came from, "unperforming" each transposition until we get back to our original number. Note that we don't "unperform" the last transposition before reaching the second number; otherwise, we'd just be doing the identity element! We don't want any numbers to change positions except for the two in the transposition, and this is accomplished by "place-holding" along the forward path; each time we traverse an edge in the forward path (i.e. perform a transposition), one number will hold the place for the other number in transposition, allowing that number to go back to its original position in the backward path. However, the two original numbers (i.e. the number at the start and end of the path) don't have place-holders, and end up getting transposed. The connected nature of the graph guarantees a transposition between all pairs of numbers in S_n , so we are done. \square

Problem 5

Proof. The number of distinct vertex colorings is the same as the number of orbits / equivalence classes that the group of rotations G induces on the set of vertex colorings X . To find the number of distinct orbits, we will use the double counting theorem presented in lecture, namely that the number of orbits is:

$$\frac{1}{|G|} \sum_{g \in G} F(g) \quad (11)$$

There are 24 rotational symmetries, and let's start visualizing them by first seeing all the axes on which the rotations can occur.



We now make a table enumerating all 24 rotational symmetries, identifying them by axis and the degrees clockwise that we rotate in. Remember that symmetries map the cube vertices to themselves, so while each rotation will have vertices replaced by other vertices, the relative locations will remain the same. The third column of the table will have $F(g)$, which "counts the number of elements fixed by g ." For the identity element, $F(Id)$ is simply the total number of colorings, 4^8 .

Axis	Degrees	$F(g)$
ID	N/A	4^8
a	90	$\binom{4}{1}^2$
a	180	$\binom{4}{1}^4$
a	270	$\binom{4}{1}^2$
b	90	$\binom{4}{1}^2$
b	180	$\binom{4}{1}^4$
b	270	$\binom{4}{1}^2$
c	90	$\binom{4}{1}^2$
c	180	$\binom{4}{1}^4$
c	270	$\binom{4}{1}^2$
d	120	$\binom{4}{1}^4$
d	240	$\binom{4}{1}^4$
e	120	$\binom{4}{1}^4$
e	240	$\binom{4}{1}^4$
f	120	$\binom{4}{1}^4$
f	240	$\binom{4}{1}^4$
g	120	$\binom{4}{1}^4$
g	240	$\binom{4}{1}^4$
h	180	$\binom{4}{1}^4$
i	180	$\binom{4}{1}^4$
j	180	$\binom{4}{1}^4$
k	180	$\binom{4}{1}^4$
l	180	$\binom{4}{1}^4$
m	180	$\binom{4}{1}^4$

Now, substituting everything into our equation:

$$orbits = \frac{1}{|G|} \sum_{g \in G} F(g) \quad (12)$$

$$orbits = \frac{65536 + (16 + 256 + 16)(3) + (256 + 256)(4) + (256)(6)}{|24|} \quad (13)$$

$$orbits = 2916 \quad (14)$$

Thus, our final answer is that there are 2916 distinct ways to color the cube vertices with four colors, under rotational symmetries.

□