DISTINGUISHING SETS UNDER GROUP ACTIONS, THE WREATH PRODUCT ACTION

ALICE MARK

The distinguishing number of a set under a group action is a way of quantifying how the way elements move within the set under the action depends on the way other elements move. The goal of this paper is to provide some intuition for this idea through examples and computations.

1. Notation, Definitions, and Other Background

Notation 1.1. Throughout this paper, the following will be used:

(1) Right group actions will be denoted by exponentiation, so if G is a group acting on a set X, $g \in G, x \in X$ then x^g denotes the action of g on x.
(2) $[n]$ denotes the set with n elements, $\{1, \ldots, n\}$.

Definition 1.2 (Distinguishing number of a graph)**.** Let $\Gamma = (V, E)$ be a graph and let $f : V \to [r]$ be a coloring of the set of vertices by r colors. The map f need not be surjective, in fact when $r > |V|$ it cannot be surjective. We say that f is r-distinguishing if the only automorphism of Γ that fixes the coloring f is the trivial automorphism. The distinguishing number of Γ is denoted by $D(\Gamma)$ and is equal to $\min\{r \mid \exists f : V \to [r]$ such that f is r-distinguishing$\}$.

More generally, we can also talk about the distinguishing number of a set under a group action.

Definition 1.3 (Distinguishing number of a set under a group action)**.** Let G be a group that acts on a set X. We say that an r-coloring $f : X \to [r]$ (not surjective for the reason given in definition 1.2) is r-distinguishing if the only element of G whose action preserves the labeling (i.e., $f(x^g) = f(x)$ for all $x \in X$) is the identity. The distinguishing number of X under the action by G is denoted $D_G(X)$ and is equal to $\min\{r \mid \exists f : X \to [r]$ such that f is r-distinguishing$\}$.

Definition 1.4 (Faithful group action)**.** Let G be a group that acts on a set X. We say that the action of G is faithful if for every $g \in G$ that is not the identity, there exists $x \in X$ such that $x^g \neq x$.

Remark 1.5. The notion of distinguishing number makes no sense in the context of a non-faithful group action, since if the action of a group G on a set X is not faithful, that means that there is some $1 \neq g \in G$ such that for all $x \in X$, $x^g = x$. This implies that no coloring is distinguishing. For the rest of this paper, all actions are faithful.

Here are some examples of how the distinguishing number of a set under a group action can be computed:

Date: 16 August 2007.

Example 1.6. The symmetric group on k elements is the permutation group of the set $[k]$. The group acts on the set by permuting the elements. The distinguishing number of this action $D_{S_k}([k]) = k$. This is because if we color the elements of $[k]$ with $k-1$ colors, there must be 2 with the same color since there are k elements total. There is a transposition element of S_k that switches these two, while holding all others fixed. Therefore the coloring is not distinguishing, so we need at least k colors. Of course, we need at most k colors since there are only k elements.

Remark 1.7. The distinguishing number cannot possibly be any higher than in example 1.6 for a finite set. Any finite set must be distinguished under a faithful action if each element is assigned a distinct label. This is because if for $g \in G$ and $x \in X$, $x^g \neq x$ different colors are assigned to x and x^g. We are guaranteed that such an x exists for each g since the action is faithful. This is an easy upper bound on the distinguishing number for a finite set.

Example 1.8. Consider the alternating group $A_k = \{\sigma \in S_k \mid \sigma \text{ is an even permutation}\}$ in its action on $[k]$. The transpositions are odd, so they are not in A_k. Let C be a distinguishing coloring of $[k]$ under A_k. If for $x, y \in [k]$ we have $C(x) = C(y)$, any permutation that switches them will also switch another pair. Therefore there cannot be any other pairs with the same color. If there is a third point colored the same as x and y then there is a 3-cycle that permutes them. Therefore there can be at most two elements with the same color and all others must be distinct, so $D_{A_k}([k]) = k-1$

Definition 1.9 (Transitive group action)**.** The action of a group G on a set X is called transitive if X is the only orbit, that is for all $x, y \in X$, there exists $g \in G$ such that $x^g = y$.

Examples 1.10. Some transitive group actions:

(1) The symmetric group S_n acts transitively on the set of n elements $[n]$, since each number is moved to each spot by some group element.
(2) The dihedral group D_n acts transitively on the set of vertices of the n-gon, since each vertex can be taken to each other vertex by a rotation.

Definition 1.11 (Regular group action)**.** The action of a group G on a set X is called regular if for all $1 \neq g \in G$, we have $x^g \neq x$ for all $x \in X$.

Example 1.12. A group G acts regularly on itself by left or right multiplication.

Remark 1.13. The distinguishing number of any regular action is 2. Let G act regularly on X. Let $x \in X$, define $f : X \to \{1, 2\}$ by $f(x) = 1$, $f(y) = 2$ for $x \neq y \in X$. Since no $1 \neq g \in G$ fixes x, $f(x) \neq f(x^g)$ for all $g \in G$. Therefore f is a distinguishing coloring. Since there is no distinguishing 1-coloring, the distinguishing number is 2.

Definition 1.14 (Imprimitive group action)**.** Let G be a group that acts faithfully and transitively on a set X. Call $X' \subseteq X$ an imprimitive block if $X' \neq \emptyset$, $X' \neq X$, and if for each $g \in G$, either $X'^g = X'$ or $X'^g \cap X' = \emptyset$. The action of G on X is said to be imprimitive if such a block can be found.

Example 1.15. Let (V, E) be a graph, $n \in \mathbb{N}$ and let

$$\Gamma = \bigsqcup_{i=1}^{n} (V, E)$$

Then the action of $\mathrm{Aut}(\Gamma)$ on Γ is imprimitive, and each copy of the original (V, E) is an imprimitive block.

Definition 1.16 (Primitive group action)**.** A group action is called primitive if no imprimitive block can be found.

Definition 1.17 (Semi-direct product of groups)**.** Let G and H be groups. Let $\phi : H \to \mathrm{Aut}(G)$ be a homomorphism. H acts on G by this homomorphism in the following way: for $h \in H, g \in G$ $g^h = g^{\phi(h)}$. The semidirect product $G \rtimes_\phi H$ is the group made up of the elements of $G \times H$ and with internal law of composition $(g, h)(g', h') = (gg'^{h^{-1}}, hh')$.

Definition 1.18 (Wreath product of groups)**.** Let G and H be groups acting on the right faithfully on sets X and Y. Let G^Y be the set of functions $f : Y \to G$. This can be considered a group with composition law $(ff')(y) = f(y)f'(y)$. The wreath product $G \wr_Y H$ is the semidirect product $G^Y \rtimes_\phi H$ where ϕ is the homomorphism $\phi : H \to \mathrm{Aut}(G^y)$ defined as follows: for $f \in G^Y, h \in H$ ϕh $f^h(y) = f(y^{h^{-1}})$. The wreath group $G \wr_Y H$ acts on the set $X \times Y$ by $(x, y)^{(f,h)} = (x^{f(y)}, y^h)$.

Remark 1.19. What the wreath action $G \wr_Y H$ on $X \times Y$ does is create an imprimitive action where the blocks are all copies of X and the set of blocks is a copy of Y. An element of the group (f, h) will take an element of the set (x, y) to the block designated y^h and then will act on the block by $f(y)$.

Every imprimitive action may be embedded in a wreath product action, which allows us to put an upper bound on the distinguishing number of any imprimitive action.

Remark 1.20. Since G and H act on the right, the wreath action is a right wreath action, so we have the group $G^Y \rtimes_\phi H$. In this group, elements are composed from the right, so $(f, h)(f', h') = (ff'^{h^{-1}}, hh')$. If the actions of G and H were left actions we would have the group $H \ltimes_\phi G^Y$. In this group, composition is done from the left, so $(h, f)(h', f') = (hh', f^{h'^{-1}} f')$.

2. A theorem about the distinguishing number of the wreath action

Chan proves the following theorem in [1]:

Theorem 2.1. *Let G and H be finite groups acting transitively (and faithfully) on the finite sets X and Y respectively. For each r, let n_r be the number of distinguishing r-colorings of X. Let $S = \{r \mid n_r \geq D_H(Y) \cdot |G|\}$. Then $D_{G \wr_Y H}(X \times Y) = \min S$*

Summary and Explanation of Proof. First note that if $|G|$, X and Y are required to be finite, $S \neq \emptyset$. This is true because of several facts. First, we have $D_H(Y)|G| < \infty$ (see remark 1.7). We also have that $n_r > 0$ since X is finite and the action G is faithful. The fact that coloring maps are surjective gives us that n_r increases without bound.

The proof constructs a coloring on $X \times Y$ by $k = \min S$ colors. First, consider the action of G on the set A of k distinguishing colorings of X, where G acts on A by $a^g(x) = a(x^{g^{-1}})$, so the color assigned to $x \in X$ by a^g is the same as the color assigned to $x^{g^{-1}}$ by a. Since each $a \in A$ is a distinguishing coloring, $\mathrm{Stab}(a) = \{1\}$ for all a. Therefore by the orbit stabilizer theorem, each element has orbit length

$|G|$. The number of orbits times $|G|$ equals $|A|$ since orbits are disjoint. Therefore, the number of orbits is equal to $\frac{|A|}{|G|} = \frac{n_k}{|G|}$. Since $k \in S$, $\frac{n_k}{|G|} \geq D_H(Y)$, so there are at least $D_H(Y)$ distinguishing k-colorings of X that are in different orbits of the action of G on A. Select these colorings, and label them $a_1, \ldots, a_{D_H(Y)}$. Let b be a distinguishing coloring of Y using $D_H(Y)$ colors. Define a coloring C of $X \times Y$ as follows: $C(x, y) = a_{b(y)}(x)$, so the color assigned to $(x, y) \in X \times Y$ is the same as the color assigned to x by the coloring $a_{b(y)}$.

Intuitively, what this is doing is coloring each block of $X \times Y$ using one of the a_i. This makes sense since each block looks like X. Then each coloring a_i is treated as a color. Since the action on the blocks looks like the action of H on Y, these colorings distinguish the blocks.

There are two things to check about this coloring. First, we need to make sure it is distinguishing, second that there is no distinguishing coloring with fewer than k colors.

To show that it is distinguishing, we first assume that for some $(f, h) \in G_{\wr Y} H$, $C(x, y) = C((x, y)^{(f,h)})$ for all pairs $(x, y) \in X \times Y$ and show that $(f, h) = (1, 1)$. By construction, the assumption means that $a_{b(y)}(x) = a_{b(y^h)}(x^{f(y)})$, so by the definition of the action of G on A, $a_{b(y^h)}^{f(y)^{-1}} = a_{b(y)}$. This implies that $a_{b(y^h)}$ and $a_{b(y)}$ are in the same orbit of that action, but since the a_i were chosen from distinct orbits, they must be the same, so $b(y^h) = b(y)$. Since b is distinguishing, $h = 1$. Now we have that $C(x, y) = C((x, y)^{(f,1)})$ for all pairs $(x, y) \in X \times Y$, but this necessarily means $f(y) = 1 \forall y$ since $a_{b(y)}(x^{f(y)}) = a_{b(y)}(x)$ since $a_{b(y)}$ is distinguishing. Therefore our coloring C is distinguishing.

Now all that remains to be shown is that there is no distinguishing coloring with fewer than k colors. Here we implicitly use the fact that the wreath action is imprimitive. Suppose we have a distinguishing l-coloring of $X \times Y$, C'. For each $y \in Y$, define an l-coloring of X, a_y where for $x \in X$, $a_y : x \mapsto C'(x, y)$. Now suppose $g \in G$ preserves a_y. Take $f \in G^Y$ such that $f(y) = g$, and $f(y') = 1$ for $y' \neq y$. Then $C'((x, y')^{(f,1)}) = C'(x^{f(y')}, y) = C'(x^1, y) = C'(x, y')$, so $(f, 1)$ preserves C'. Since we assumed that C' is distinguishing, we must have $f = 1$ which means $g = 1$ which means that a_y is a distinguishing coloring of X for each y. Now, as in the first part of the proof, let A' be the set of all distinguishing l-colorings of X, and consider the action of G on A' as before. Again, note that we have that the number of orbits is $\frac{|A'|}{|G|} = \frac{n_l}{|G|}$. This fact will come up later. Each of the colorings a_y is contained in one and only one of the orbits of this action since the orbits of an action are always disjoint. Let d be the number of orbits of the action of G on A', and index the orbits by $[d]$. Define b, a coloring of Y, as follows: $b : Y \to [d]$ by $b(y) = i$ if a_y is in the i-th orbit. Suppose we have $h \in H$ that preserves b. If this is the case, then $\forall y \in Y$ we have $b(y) = b(y^h)$ which by the way we defined b means that a_y and a_{y^h} are in the same orbit, so $\exists g_y \in G$ st $a_y^{g_y} = a_{y^h}$. Let $f \in G^Y$ be the function $f(y) = g_y$. Then for $(x, y) \in X \times Y$ we have $C'((x, y)^{(f,h)}) = C'(x^{f(y)}, y^h) = C'(x^{g_y}, y^h) = a_{y^h}(x^{g_y}) = a_{y^h}^{g_y^{-1}}(x) = a_y(x) = C'(x, y)$ which implies that $(f, h) = (1, 1)$ since C' is distinguishing. Since $h = 1$ we have that b is a distinguishing coloring of Y, so $d \geq D_H(Y)$. Therefore the number of orbits of the action $\frac{n_l}{|G|} d \geq D_H(Y)$ so $n_l \geq D_H(Y) \cdot |G|$. Therefore $l \in S$ so $l \geq \min S = k$, so every distinguishing coloring uses at least k colors.[1]

Remark 2.2. If we allow infinite groups and sets, we can get that $S = \emptyset$. This happens when either the action of G on X or the action of H on Y cannot be finitely distinguished, or when $|G|$ is infinite. In these cases, the distinguishing number of the wreath action on $X \times Y$ is infinite. This is because, as the proof has shown, if there is some k-coloring of $X \times Y$ for some finite k then we would get $n_k \geq D_H(Y)|G|$.[1]

3. Some examples of wreath actions

Example 3.1 (Symmetric Groups)**.** Consider the symmetric groups S_k and S_m and their respective actions on $[k]$ and $[m]$. The distinguishing number of the wreath action of $S_{k \wr [m]} S_m$ on $[k] \times [m]$ can be computed directly for certain m and k.

Claim. $D_{S_{k \wr [m]} S_m}([k] \times [m]) = k + 1$ if $m \leq k + 1$

Proof. Suppose for contradiction that we have a distinguishing coloring C of $[k] \times [m]$that uses k colors. For each $y \in [m]$, the set $A_y = \{(x, y) | x \in [k]\}$ is a "copy" of $[k]$, and the action of $\{(f, 1) | f \in G^Y\}$ on A_y is "isomorphic" to the action of S_K on $[k]$. Therefore, k colors are required to distinguish each set A_y, so the coloring C must assign the same k colors to each A_y, and all of them must be used for each A_y.

Now consider A_y and $A_{y'}$, and let σ be a permutation in S_m such that $y^\sigma = y' \neq y$. For each $(x, y) \in A_y$, there exists a unique $(x', y') \in A_{y'}$ such that $C(x, y) = C(x', y')$, and there exists $\pi \in S_k$ such that $x^\pi = x'$. Since there exists $f \in G^Y$ such that $f(y) = \pi$, we have $C(x, y) = C(x', y') = C(x^\pi, y^\sigma) = C(x^{f(y)}, y^\sigma) = C((x, y)^{(f,\sigma)})$ so C is not distinguishing, so more than k colors are required.

To see that $k + 1$ colors is enough, assign a coloring as follows: $\binom{k+1}{k} = k + 1$ so there are $k + 1$ ways to choose k colors. Since $m \leq k + 1$, there are at most $k + 1$ sets A_y, so each one may be assigned a different k colors taken from the original $k + 1$ colors. If we use all k colors for each A_y, the claim is that we have a distinguishing coloring. If for (f, σ), $C(x, y) = C(x, y)^{(f,\sigma)}$ for all (x, y) we have two cases to check. First suppose $\sigma \neq 1$, let $y \in [m]$ such that $y^\sigma \neq y$. There exists x such that $C(x, y) \neq C(x^{f(y)}, y^\sigma)$ since A_y is colored by a different set of k colors than A_{y^σ}, so this case will not happen. If $\sigma = 1$, we have $C(x, y) = C((x, y)^{(f,1)} = C(x^{f(y)}, y) \forall y \in [m]$, but since $(x^{f(y)}, y) \in A_y$ and each element of A_y is colored a different color, we must have $(x^{f(y)}, y) = (x, y)$ which implies that $x = x^{f(y)}$ for all $x \in [k]$ so $f = 1$. So we have $(f, \sigma) = (1, 1)$ so C is distinguishing. □

Using the theorem, we arrive at the same result much more quickly. The function $n_r = \binom{r}{k} k!$, since from r colors we want to select k of them, and then we can assign them to $[k]$ in $k!$ many ways. Then $S = \{r \mid \binom{r}{k} k! \geq mk!\}$ so $\min S$ is the minimal r such that $\binom{r}{k} \geq m$. As we saw before, this must be $k + 1$.

What happens when $m - k$ is a fairly large number? It is not as easy to compute $D_{S_{k \wr [m]} S_m}([k] \times [m])$ when $m \geq k + 2$. The reason for this becomes apparent when we try to use the theorem to compute it.

It is clear that for fixed m and k, $\binom{r}{k}$ is eventually greater than m as r increases, so $S \neq \emptyset$. It turns out that we can't compute this number because that would involve solving a large degree polynomial. The number we are looking for is the smallest integer r such that $\binom{r}{k} \geq m$. The sequence of numbers $a_{kr} = \binom{r}{k}$ is the k-th diagonal sequence of Pascal's triangle, where the first diagonal sequence $a_{1r} = 1$,

the second $a_{2r} = r$ and in general

$$a_{kr} = \sum_{i=1}^{r-1} a_{k-1i}$$

The closed form of this formula is

$$a_{kr} = \prod_{i=1}^{k-2} (i + r)$$

which is a polynomial in r of degree $k - 2$.

There is no easy way to compute the exact value of r from this, but we can approximate. We want $\binom{r}{k} \geq m > \binom{r-1}{k}$. We can bound $\binom{r}{k}$ in the following way:

$$\binom{r}{k} = \frac{r(r-1)\dots(r-k+1)}{k!}$$

The numerator is a product of k terms, so it can be bounded above by the largest:

$$\binom{r}{k} < \frac{r^k}{k!}$$

Similarly, $\binom{r-1}{k}$ can be bounded below:

$$\binom{r-1}{k} > \frac{(r-k)^k}{k!}$$

so we want

$$\frac{r^k}{k!} > m > \frac{(r-k)^k}{k!}$$

Which means that

$$r > (mk!)^{\frac{1}{k}} > r - k$$

So the r we want is an integer in the interval $((mk!)^{\frac{1}{k}}, (mk!)^{\frac{1}{k}})$.

Example 3.2 (Dihedral Groups)**.** The dihedral group on k elements is defined here to be the automorphism group of the k cycle C_k. It is isomorphic to the symmetry group of the k-gon. For the purposes of this paper, C_k refers to the vertex set of the k-cycle, although it might as well refer to the edges. The distinguishing number

$$D_{D_k}(C_k) = \begin{cases} 3 & \text{if } 3 \leq k \leq 5 \\ 2 & \text{if } 5 < k \end{cases}$$

This should be clear in the $k \leq 5$ cases. The $k = 6$ and $k = 7$ cases are pictured below. For larger k, the pattern can continue with longer sections colored all by 2. The 6-cycle is included in figure 1 because it has interesting unavoidable symmetry.

FIGURE 1. distinguishing 2-colorings of C_6 and C_7

If colors 1 and 2 are switched in the 6-cycle coloring, the resulting graph is the same as it would be if it were reflected across the axis that splits the graph from the top left edge through the bottom right edge. There is an element of D_6 that acts on the graph in this way. Other even cycles can be two colored in distinguishing ways with this kind of symmetry or not, but with a 6-cycle there is no other distinct distinguishing 2-coloring.

Consider the wreath action of $D_{k\wr C_m} D_m$ on $C_k \times C_m$. Unlike symmetric groups, it is easier to count the distinguishing number for large k and m.

Claim. For $k \geq 7$, $m > 6$, $D_{D_{k\wr C_m} D_m}(C_k \times C_m) = 2$

Proof. Since one color is clearly not enough, all we need is to construct a 2-coloring that works. For $y \in C_m$ let $A_y = \{(x, y) | x \in C_k\}$. A_y is a copy of C_k within $C_k \times C_m$, and for any $h \in D_m$, $\{(f, h) | f \in D_k^{C_m}\}$ acts on A_{y^h} in the same way D_k acts on C_k. Therefore only 2 colors are needed to distinguish A_y for each y. The wreath group acts on the set of sets A_y in the same way D_m acts on C_m. In order to distinguish the set of sets A_y, we need 2 distinct 2-distinguishing colorings, where distinct means that the number of elements colored by color 1 in the first coloring is different from the number of elements colored by color 1 in the second coloring. Two distinct colorings exist for $k > 7$, all we need is to take one without the symmetry of the C_6 coloring and switch the color of each vertex. □

Using the theorem, we should get the same result.

Claim. Same as above.

Proof. If $k > 7$, $n_2 \geq 2k \cdot 2 = 4k$ where $2k = |D_k|$ is the number of colorings we get by acting on C_k with D_k. It is multiplied by 2 since when we switch one color with the other we get a distinct coloring. There are even more ways, as described earlier, however we don't even need to count them since $D_{D_m} C_m \cdot |D_k| = 2 \cdot 2k$ so the numbers are already equal. Since $n_1 = 0$, we have $\min S = 2$. □

This deals with most cases. The theorem makes the others a lot simpler. For $3 < m < 5$, we have $D_{D_m}(C_m) = 3$ and $|D_k| = 2k$ so $S = \{r | n_r \geq 6k\}$. For $m > 5$ we have $D_{D_m}(C_m) = 2$ and $|D_k| = 2k$ so $S = \{r | n_r \geq 4k\}$, so we need to compute n_r, at least partially, for these cases.

In the case where $k = 3$, the function $n_r = \binom{r}{3} 3!$ since $D_3 \cong S_3$. If $3 \leq m \leq 5$, $\min S$ is the minimal r such that $6\binom{r}{3} \geq 6 \cdot 3$ so the r we want is 4. If $5 < m$ $\min S$ is the minimal r such that $6\binom{r}{3} \geq 4 \cdot 3$, so again the r we want is 4.

In the case where $k = 4$, the function n_r is more complicated since it is the sum of the number of 3-colorings plus the number of 4-colorings. The number of 3-colorings by r colors is $24\binom{r}{3}$. A distinguishing 3-coloring of C_4 is shown in figure 2. First we choose 3 colors, then choose which one will be used for two vertices. Note that the two with the same color must be next to each other as in the figure, since there are group elements that switch each pair of opposite corners while holding the other pair fixed. Then there are 4 ways this can be rotated, and the two colors used only once can be flipped, so the whole thing is multiplied by $3 \cdot 4 \cdot 2 = 24$

The number of distinguishing 4-colorings is simply $24\binom{r}{4}$ since we choose 4 colors and then place them in 4 distinct spots. Therefore $n_r = 24(\binom{r}{3} + \binom{r}{4})$.

If $3 \leq m \leq 5$, $\min S = \min\{r \mid 24(\binom{r}{3} + \binom{r}{4}) \geq 6 \cdot 4\}$ So the r we want is 3 (note that if $r < k$, $\binom{r}{k} := 0$). This is also the result when $m > 5$ since $4 \cdot 4 < 6 \cdot 4$ and

FIGURE 2. distinguishing 3-coloring of C_4

with $r < 3$ $n_r = 0$. Computing n_r explicitly wasn't even necessary, since already there are enough 3-colorings that we need not even consider the 4-colorings.

In the case where $k = 5$, n_r is the sum of the number of distinguishing 3,4, and 5-colorings. As before, however, we can find enough 3-colorings that we need not even consider 4 and 5-colorings. The number of distinguishing 3-colorings is $72\binom{r}{3}$. There are a few different kinds of distinguishing 3-colorings of C_5, shown in figure 3. In all cases, we first choose 3 colors. In cases (a) and (c), there are 3 choices for which color is used 3 times, there are 2 ways to order the remaining 2 colors, and there are 5 ways to place them to make a picture like (a) and 5 ways to place them to make a picture like (c). Therefore we multiply by $3 \cdot 2 \cdot 10 = 60$. To get (c) and (d), first we have 3 choices for the one single color, then we must order the pairs. There are 2 ways if vertices of the same color are next to each other(c), and 2 ways if they are not (d). Therefore the whole thing is multiplied by $3 \cdot 4 = 12$. This gives us that the total number of 3-colorings of C_5 is $60\binom{r}{3} + 12\binom{r}{3} = 72\binom{r}{3}$

FIGURE 3. ways to color C_5 with 3 colors

All that we need to notice is that the terms describing the number of 4 and 5-colorings will be $a\binom{r}{4}$ and $b\binom{r}{5}$ respectively for some constants a and b. When $r = 1$ or 2, all three terms will be 0. Therefore the smallest nonzero value of n_r occurs when $r = 3$, at which point the 4 and 5 terms are 0 and the 3 term is 72. This will be plenty of colorings, since if $3 \leq m \leq 5$ we want $n_r \geq 6 \cdot 5 = 30$ and when $m > 5$ we want $n_r \geq 4 \cdot 5 = 20$, so with 3 colors we have enough colorings.

We can also see that this is true if we think about this problem in terms of distinct colorings, where two colorings C and C' are distinct if there is no $g \in D_5$ with $C(C_5) = C'(C_5^g)$. No m will require more than 3 distinct distinguishing colorings, and figure 3 shows that we have 4 distinct distinguishing colorings of C_5.

In the case where $k = 6$, n_r is the sum of the number of 2, 3, 4, 5, and 6-colorings of C_6. Once again, it will not be necessary to compute this entirely.

The total number of distinguishing 2-colorings by r colors is $12\binom{r}{2}$, since there is only 1 distinct 2-coloring and $|D_6| = 12$. The number of distinguishing 3-colorings

FIGURE 4. 3 distinct 2-colorings of C_k for $k \geq 7$

of D_6 by r colors is going to be larger than the number of distinguishing 3-colorings of D_5 by r colors, since each distinct 5-coloring gives rise to at least 1 6-coloring, and there is a way to do this such that the 6-colorings generated will all be distinct. So it will be $a\binom{r}{3}$ where $a > 72$. Following a similar argument to the $k = 5$ case, we find that $r = 3$ both when $3 \leq m \leq 5$ and when $m > 5$.

Finally in the case where $k \geq 7$, we need only consider what happens when $3 \leq m \leq 5$, since we have already done the other case. It should be clear that there are at least 3 distinct 2-colorings of C_k from figure 4

It turns out that for all k, $\min S$ is the same no matter what m is. This is because n_r goes up in such big jumps that there is no case where $6k > n_r \geq 4k$.

Everything is summarized in table 1.

TABLE 1. Table of cases. Note that if $k > r$, $\binom{r}{k} := 0$. $D_{D_k \wr C_m} D_m C_k \times C_m = \min S$

k	3	4	5	6	≥ 7
$\min S$	4	3	3	3	2

Example 3.3 (Symmetric and Dihedral groups)**.** It is interesting what happens with the wreath action of a symmetric and a dihedral group. Let S_K be the symmetric group acting on the set $[k]$, and let D_m be the automorphism group of the m-cycle C_m. It should not be surprising that $D_{S_k \wr C_m} D_m([k] \times C_m)$ is not the same as $D_{D_m \wr [k]} S_k(C_m \times [k])$.

In the first case, the blocks look like symmetric groups and the action on the blocks looks like a dihedral action. We therefore need either 3 or 2 distinct colorings of the symmetric group on k elements, depending on whether $3 \leq m \leq 5$ or $m > 5$. Either way, if $k > 1$ we have $\binom{k+1}{k} = k + 1 \geq 3$ so the distinguishing number will be $k + 1$

In the second case the blocks look like dihedral groups, so 2 or 3 colors are needed to distinguish each one depending on whether $3 \leq m \leq 5$ or $m > 5$. We need k distinct colorings of the blocks, however, since the wreath group acts on the blocks in the way S_k acts on $[k]$. For small k this will be easy to solve for, and we can use much the same method as when both were dihedral groups. When k is very large, however, it is necessary to compute explicitly what n_r will be for a given m. This is possible, and can be done using combinatorial arguments, but the process is long and repetitive.

4. Acknowledgements

Thanks to Ian Shipman, Laci Babai, and Michael Geline for their explanations, suggestions, and comments.

References

[1] Melody Chan. The distinguishing number of the direct product and wreath product action. Yale University. 2005.