Trees and Wreaths: Solution

For each of the seven $(1 + 2 + 4 = 7)$ vertices above the last row, we have a binary choice of whether or not to swivel the subtree below it. Thus, the number of swivellable permutations of the last row of vertices is $2^7 = 128$.

It may not be obvious why this exhausts all possibilities; what about the order in which we swivel subtrees, or the option to swivel multiple times at a vertex (just not in a row), why don't these lead to more permutations?

Consider the general problem of counting the number W_n of permutations possible if our tree has n levels (our situation is $n = 3$). The permutations are of two kinds: those where the left half of the numbers remain on the left and the right half of numbers remain on the right, or those where the opposite is true. There are an equal number of each, because swivelling below the top vertex converts permutations of the one kind to the other and then back.

The number of permutations of the first kind is $W_{n-1} \times W_{n-1}$, because there are W_{n-1} permutations possible for the first half of numbers and W_{n-1} also for the second half. Therefore, we have the recursion

$$W_n = 2W_{n-1}^2.$$

The first couple values are $W_0 = 1$ and $W_1 = 2$ by inspection, which leads to $W_2 = 2^3 = 8$ and $W_3 = 2^7 = 128$. The general formula we then guess is

$$W_n = 2^{1+2+\cdots+2^{n-1}} = 2^{2^n-1}.$$

We can verify this is true by induction: this satisfies $W_0 = 1$ and $W_n = 2W_{n-1}^2$.

This means swivelling in different orders or multiple times at vertices achieves no more permutations than if we always swivel the vertices in the same order at most once each. Indeed, each permutation can be interpreted as a function of $\{1, 2, 3, 4, 5, 6, 7, 8\}$ which means we have a **permutation group**: a set of invertible functions on a set which is closed under composition and inverses.

To understand the structure of this permutation group, it's necessary to understand **wreath products**. One way to understand the wreath products (and direct products) of permutation groups is with the *product action*. Suppose G is a permutation group acting on the set $\{1, \cdots, m\}$ and H is a permutation group acting on the set $\{1, \cdots, n\}$. Make a table with m rows and n columns, filling the entries with the numbers 1 through $m \times n$:

	1	2	3	$\cdots$	n
1	1	$\cdot$	$\cdot$	$\cdots$	$\cdot$
2	$\cdot$	$\cdot$	$\cdot$	$\cdots$	$\cdot$
3	$\cdot$	$\cdot$	$\cdot$	$\cdots$	$\cdot$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
m	$\cdot$	$\cdot$	$\cdot$	$\cdots$	mn

The direct product $H^m = \overbrace{H \times \cdots \times H}^{m}$ (in some contexts called a direct sum, for which we will use the shorthand $mH = H \oplus \cdots \oplus H$) is a permutation group acting on $\{1, \cdots, mn\}$, the set of labels in the table. The elements of H^m are attained by using permutations from H on each row individually.

The wreath product $H \wr G$ is a larger permutation group, containing H^m as a subgroup, acting on $\{1, \cdots, mn\}$. The functions of $H \wr G$ are attained by using row-permutations from H^m followed by using a permutation from G to shuffle the rows amongst each other. This means the order (cardinality) of the wreath product is $|H \wr G| = |H|^m |G|$.

The permutation group which cycles the elements $\{1, 2, \cdots, p\}$ around in a circle we can denote $\mathbb{Z}_p$. The permutation group of order 2^7 we found acting on $\{1, \cdots, 8\}$ is actually a **wreath power** $\mathbb{Z}_2^{\wr 3} = \mathbb{Z}_2 \wr \mathbb{Z}_2 \wr \mathbb{Z}_2$ (we don't need to distinguish between $\mathbb{Z}_2 \wr (\mathbb{Z}_2 \wr \mathbb{Z}_2)$ and $(\mathbb{Z}_2 \wr \mathbb{Z}_2) \wr \mathbb{Z}_2$ because the wreath product, as an operation on permutation groups, is associative).

Wreath powers yield **Sylow subgroups** of symmetric groups. The first Sylow theorem asserts that if a finite group G has order n and p^k is the largest power of a prime p dividing n, then G has a subgroup of order p^k, called a Sylow subgroup (this is a partial converse to Lagrange's theorem, which says the order of any subgroup H is a divisor of n; the full converse is false in general).

In particular, our $\mathbb{Z}_2^{\wr 3}$ is a Sylow subgroup of S_{2^3}. In general, a Sylow subgroup P of S_n can be constructed as a direct sum of wreath powers analogous to representing n in base-p. Specifically, if $n = \sum n_k p^k$ (with digits n_k taken from $\{0, 1, \cdots, p-1\}$) is n's base-p representation, then $P = \bigoplus n_k \mathbb{Z}_p^{\wr k}$. This can be verified a Sylow subgroup with Legendre's formula from number theory.