15 Lecture 03.21

On 03.21, we began to look more closely at the use of automorphisms of a structure as a tool for counting the number of structures that satisfy a given schema. The ideas we developed will also be very important in connection with our upcoming study of definability.

We focused our attention on a concrete example. Let S be the conjunction of SG and $\mathsf{1reg}$, that is, a graph A satisfies S if and only if A is a 1-regular, simple graph. As we discussed earlier, every such finite graph A has an even number, say $2n$, of nodes; moreover, if $A, B \models S$ and $|U^A| = |U^B|$, then A is isomorphic to B. (Recall that A *is isomorphic to* B if and only if there is an isomorphism h from A onto B; and that h is an isomorphism from A onto B if and only if h is a bijection from U^A onto U^B such that for all $a, b \in U^A$, $\langle a, b\rangle \in L^A$ if and only if $\langle h(a), h(b)\rangle \in L^B$.) We devoted the class to calculating the value of $\mathsf{mod}(S, 2n)$ in two ways, both for the intrinsic interest of each, and for the opportunity to "check our work."

Our first calculation involved an excursion through the concept of a *group action*, though in class, we stuck to the concrete example quite closely, and may not even have uttered this phrase. But in this memoir, memoirs being what they are, we will take the liberty to invent an alternative past. So let's take a deep breath, or several shallow cleansing breaths, and ....

For every positive integer k we write $[k]$ for $\{1, \ldots, k\}$ and $\mathbb{S}_k$ for the set of bijections from $[k]$ onto $[k]$ (also called the *permutation group on* or the *symmetric group on* $[k]$). These latter terms emphasize the following algebraic aspect: we may think of $\mathbb{S}_k$ as an algebra with a binary operation $\circ$, a unary operation $^{-1}$, and a distinguished element e, where, for permutations $f, g \in \mathbb{S}_k$, $f \circ g$ is the permutation resulting from the composition of f and g, that is, $f \circ g = h$ if and only if for every $i \in [k]$, $h(i) = f(g(i))$; f^{-1} is the permutation which is the inverse of f; and e stands for the identity function on $[k]$. With these understandings, you can verify that $\mathbb{S}_k$ is a group:

- $\circ$ is an associative operation, that is, $(f \circ g) \circ h = f \circ (g \circ h)$, for all $f, g \in \mathbb{S}_k$;
- e is an identity with respect to $\circ$, that is, $e \circ f = f \circ e = f$, for all $f \in \mathbb{S}_k$; and
- $f \circ f^{-1} = f^{-1} \circ f = e$, for all $f \in \mathbb{S}_k$.

We write $\mathbb{G}_k$ for the set of simple graphs A with $U^A = [k]$. For each $f \in \mathbb{S}_k$ and $A \in \mathbb{G}_k$, we define $f[A]$ to be the graph with universe $[k]$ such that for all $i, j \in [n]$, $\langle f(i), f(j)\rangle \in L^{f([A])}$ if and only if $\langle i, j\rangle \in L^A$. Note that f is an isomorphism of A onto $f[A]$. This is an example of a *group action* – the group $\mathbb{S}_k$ *acts on* the set $\mathbb{G}_k$ via the assignment of $f[A]$ to A. Verify that for all $A \in \mathbb{G}_k$ and $f, g \in \mathbb{S}_k$,

- $(f \circ g)[A] = f[g[A]]$, and
- $e[A] = A$.

Recall that $\mathsf{Aut}(A)$ is the set of automorphisms of A. In the current context, for $A \in \mathbb{G}_k$, $\mathsf{Aut}(A)$ is often called the *stabilizer* of A, since $f \in \mathsf{Aut}(A)$ if and only if $f[A] = A$. The *orbit of* A under the action of $\mathbb{S}_k$ (written $\mathsf{orb}(A, \mathbb{S}_k)$) is $\{h[A] \mid h \in \mathbb{S}_k\}$. The following result is a special case of the *Orbit-Stabilizer Theorem.*

Theorem 1 *For all* $A \in \mathbb{G}_n$,

$$|\mathbb{S}_n| = |\mathsf{orb}(A, \mathbb{S}_n)| \cdot |\mathsf{Aut}(A)|.$$

I present the proof, because several questions that arose yesterday suggest to me that you may find it illuminating.

Proof: Let $A \in \mathbb{G}_k$. We define an equivalence relation $\sim$ on $\mathbb{S}_k$: for all $f, g \in \mathbb{S}_k$, $f \sim g$ if and only if $(f^{-1} \circ g) \in \mathsf{Aut}(A)$. (You should verify that $\sim$ is an equivalence relation, for example, it is reflexive, that is, $f \sim f$, because $f^{-1} \circ f = e$ and $e \in \mathsf{Aut}(A)$; continue and show $\sim$ is symmetric and transitive.) We establish the following two claims about $\sim$ from which the Theorem follows immediately.

1. each equivalence class of $\sim$ has size $|\mathsf{Aut}(A)|$, and

2. the number of equivalence classes of $\sim$ is $|\mathsf{orb}(A, \mathbb{S}_k)|$.

Ad claim 1: Fix $f \in \mathbb{S}_k$. For each $h \in \mathsf{Aut}(A)$ there is a unique $g \in \mathbb{S}_k$ such that $f^{-1} \circ g = h$. (Verify!) It follows at once that there is a bijection between $\{g \mid f \sim g\}$ and $\mathsf{Aut}(A)$.

Ad claim 2: We show that for every $f, g \in \mathbb{S}_k$ $f[A] = g[A]$ if and only if $f \sim g$. We prove each direction of the bi-conditional. So suppose $f \sim g$. Then $f^{-1} \circ g \in \mathsf{Aut}(A)$. Hence, $(f^{-1} \circ g)[A] = A$. Hence, $f[(f^{-1} \circ g)[A]] = f[A]$. Hence, $(f \circ (f^{-1} \circ g))[A] = f[A]$. Hence, $((f \circ f^{-1}) \circ g)[A] = f[A]$. Hence, $(e \circ g)[A] = f[A]$. Hence, $g[A] = f[A]$. In the other direction, suppose $f[A] = g[A]$. Then, $f^{-1}[f[A]] = f^{-1}[g[A]]$. Hence, $(f^{-1} \circ f)[A] = (f^{-1} \circ g)[A]$. Hence, $(f^{-1} \circ g)[A] = e[A] = A$. Hence, $f^{-1} \circ g \in \mathsf{Aut}(A)$, that is, $f \sim g$. Thus, there is a bijection between the equivalence classes of $\sim$ and $\mathsf{orb}(A, \mathbb{S}_k)$. ■

We return to calculating the value of $|\mathsf{mod}(S, 2n)|$. As noted above, if $A, B \in \mathsf{mod}(S, 2n)$, then $A \cong B$. Let $A \in \mathsf{mod}(S, 2n)$. It follows at once that $\mathsf{mod}(S, 2n) = \mathsf{orb}(A, \mathbb{S}_{2n})$. Let's calculate $|\mathsf{Aut}(A)|$, since Theorem 1 will then allow us to calculate $|\mathsf{mod}(S, 2n)|$. Observe that A consists of n independent edges. Imagine them standing upright and lined up horizontally in some order. Now any permutation of the edges generates an automorphism of A. Moreover, in the process of permuting the edges, we may choose to "flip" any subset of them having those land on the edge to which they are permuted "head to foot" and "foot to head". Since there are $n!$ permutations of the n edges, and 2^n choices of which set of edges to flip, there are a total of $n! \cdot 2^n$ automorphisms of A. It therefore follows from Theorem 1 that $|\mathsf{mod}(S, 2n)| = (2n)!/n! \cdot 2^n$.

We also discussed a second direct method of calculating $|\mathsf{mod}(S, 2n)|$ which, thankfully, yielded the same result. We thought of constructing a member A of $\mathsf{mod}(S, 2n)$ as follows. We successively choose the n independent edges that constitute A. So for the first edge, we have $\binom{2n}{2}$ choices of a pair of nodes between which to place an edge, and for the second edge, we have $\binom{2n-2}{2}$ choices, ... So the number of ways we can choose a sequence of n independent edges is

$$\binom{2n}{2} \cdot \binom{2n-2}{2} \cdots \binom{4}{2} \cdot \binom{2}{2} = \frac{(2n)!}{2^n}.$$

Now any *set* of n edges chosen via this process will appear as the result of $n!$ such sequences of choices; thus, the total number of members of $\mathsf{mod}(S, 2n)$ we can construct is

$$\frac{(2n)!}{n! \cdot 2^n}.$$