Symmetry and Hardness

Samuel Schlesinger

November 26, 2023

Given $f : \{0,1\}^n \to \{0,1\}$, define

$$Stab(f) = \{\sigma \mid \sigma \in S_n, \forall x \in \{0,1\}^n, f(\sigma(x)) = f(x)\}.$$

We define the orbit of $x \in \{0,1\}^n$,

$$Orb(f,x) = \{\sigma(x) \mid \sigma \in Stab(f)\}.$$

Given a function $g : \{0,1\}^n \to \{0,1\}^m$ with the property that

$$\forall x, y \in \{0,1\}^n, g(x) = g(y) \iff Orb(f,x) = Orb(f,y),$$

we know that there exists a function h such that precomposition with g yields f

$$h \circ g = f.$$

Why is that? Well, that is because the value of f is uniform within an orbit, so determining the orbit determines the value of f. From here, we simply need a function from m bits to 1, which we can make for the low-low price of $(1 + o(1))\frac{2^m}{m}$ via Lupanov's construction.

To put this idea to the test, what if $Stab(f)$ is the entire symmetric group S_n? Well, in this case we can write $g(x) = 1 - count(x)$, with $m = \lceil log_2(n) \rceil$. How big does a circuit have to be to compute $1 - count$? We can design a $1 - count$ circuit in linear size based on the addition circuit, and the rest is $O(\frac{2^{log_2(n)}}{log_2(n)}) = O(\frac{n}{log_2(n)})$, so we have a linear circuit overall for computing fully symmetric functions.

What we find when we put these ideas to the test and really analyze them, like Lazlo Babai et al. did in their paper "Symmetry and Complexity", is that there is a very strong connection between the number of orbits and the complexity of f. What is shown in that paper is that if there are s orbits of $\{0,1\}^n$ under $Stab(f)$, then we can compute f in circuits of polynomial size in s, depth polynomial in $log(s)$. Further, we can show that there are functions with s permutations which cannot be computed by circuits of size $\frac{s}{2log(s)}$, showing that this relationship is tight up to a logarithmic factor, which is typical for such separations.