XAVIER COITEUX-ROY, University of Calgary

Unconditional quantum advantage at the Razborov–Smolensky frontier

Constant-depth quantum circuits can solve relation problems that their classical counterparts provably cannot solve. Until now, the strongest complexity-theoretic separation for QNC^0-circuits was against AC^0, the class of constant-depth, polynomial-size classical circuits composed of unbounded fan-in AND and OR gates, as well as NOT gates. The classical lower bounds in all known demonstrations of that separation rely on random restrictions and switching lemmas. Here we extend the separation to $\mathrm{AC}^0[p]$, the class obtained by augmenting AC^0 with unbounded fan-in MOD_p gates. For each prime p, we give a relation problem that QNC^0-circuits over a fixed finite gate set can solve with probability at least $\frac{99}{100}$, but that cannot be solved by $\mathrm{AC}^0[p]$-circuits with probability $\frac{2}{3}$. The validity of a proposed solution can nevertheless be checked in $\mathrm{AC}^0[p]$. The classical hardness is proven by deriving a contradiction with the fundamental lower bound by Razborov–Smolensky that MOD_6 cannot be approximated by $\mathrm{AC}^0[p]$-circuits for any prime p. Since no lower bounds comparable to those of Razborov–Smolensky are known for even slightly stronger models such as $\mathrm{AC}^0[6]$, extending this unconditional quantum advantage to such models will require a breakthrough in classical circuit complexity.