Contribution ID: **81** Type: **not specified**

Cumulative Memory Lower Bounds for Randomized and Quantum Computation

Thursday, July 13, 2023 12:10 PM (20 minutes)

Paul Beame and Niels Kornerup

Abstract: Cumulative memory—the sum of space used over the steps of a computation—is a fine-grained measure of time-space complexity that was introduced to analyze cryptographic applications more precisely. It is a more accurate cost measure for algorithms with infrequent spikes in memory usage in the context of technologies such as cloud computing that allow dynamic allocation and de-allocation of resources during their execution.

We give the first lower bounds on cumulative memory complexity that apply to general sequential classical algorithms. We also prove the first such bounds for bounded error quantum circuits. Moreover, we develop general paradigms for bounding cumulative memory complexity inspired by the standard paradigms for proving time space tradeoff lower bounds, which only lower bound the maximum space used during an execution.

With these new paradigms we obtain lower bounds on cumulative memory that are essentially as strong as the best time-space tradeoff lower bounds which are known to be tight in many cases. Among many possible applications, we show that any classical sorting algorithm with success probability at least $1/\mathrm{poly}(n)$ requires cumulative memory $\tilde{\Omega}(n^2)$, any classical matrix multiplication algorithm requires cumulative memory $\Omega(n^6/T)$, any quantum sorting circuit requires cumulative memory $\Omega(n^3/T)$, and any quantum circuit that finds k disjoint collisions in a random function requires cumulative memory $\Omega(k^3n/T^2)$.

Presenter: KORNERUP, Niels

Session Classification: Track A-1