Abstract

Computing the simulation preorder of a given Kripke structure (i.e., a directed graph with \( n \) labeled vertices) has crucial applications in model checking of temporal logic. It amounts to solving a specific two-players reachability game, called simulation game. We offer the first conditional lower bounds for this problem, and we relate its complexity (for computation, verification, and certification) to some variants of \( n \times n \) matrix multiplication. We show that any \( O(n^\alpha) \)-time algorithm for simulation games, even restricting to acyclic games/structures, can be used to compute \( n \times n \) boolean matrix multiplication (BMM) in \( O(n^\alpha) \) time. In the acyclic case, we match this bound by presenting the first subcubic algorithm, based on fast BMM, and running in \( n^{\omega+o(1)} \) time (where \( \omega < 2.376 \) is the exponent of matrix multiplication). For both acyclic and cyclic structures, we point out the existence of natural and canonical \( O(n^2) \)-size certificates, that can be verified in truly subcubic time by means of matrix multiplication. In the acyclic case, \( O(n^2) \) time is sufficient, employing standard \((+,\times)\)-matrix product verification. In the cyclic case, a min-edge witness matrix multiplication (EWMM) is used, i.e., a matrix multiplication on the semi-ring \((\max,\times)\) where one matrix contains only 0’s and 1’s, which is computable in truly subcubic \( n^{(3+\omega)/2+o(1)} \) time. Finally, we show a reduction from EWMM to cyclic simulation games which implies a separation between the cyclic and the acyclic cases, unless EWMM can be verified in \( n^{\omega+o(1)} \) time.