Extended transitive separation logic.

Summary: Separation logic (SL) is an extension of Hoare logic by operators and formulas for reasoning more flexibly about heap portions or linked object(record structures. In the present paper we give an algebraic extension of SL at the data structure level. At the same time we step beyond standard SL by studying not only domain disjointness of heap portions but also disjointness along transitive links. To this end we define operations that allow expressing assumptions about the linking structure. Phenomena to be treated comprise reachability analysis, (absence of) sharing, cycle detection and preservation of substructures under destructive assignments. We demonstrate the practicality of this approach with examples of in-place list-reversal, tree rotation and threaded trees.

Keywords: separation logic; reachability; sharing; strong separation; verification