Kuncak, Viktor; Nguyen, Huu Hai; Rinard, Martin
Deciding Boolean algebra with Presburger arithmetic. (English) Zbl 1112.03011

Summary: We describe an algorithm for deciding the first-order multisorted theory BAPA, which combines Boolean algebras of sets of uninterpreted elements (BA) and Presburger arithmetic operations (PA). BAPA can express the relationship between integer variables and cardinalities of unbounded finite sets, and it supports arbitrary quantification over sets and integers. Our motivation for BAPA is deciding verification conditions that arise in the static analysis of data structure consistency properties. Data structures often use an integer variable to keep track of the number of elements they store; an invariant of such a data structure is that the value of the integer variable is equal to the number of elements stored in the data structure. When the data structure content is represented by a set, the resulting constraints can be captured in BAPA. BAPA formulas with quantifier alternations arise when verifying programs with annotations containing quantifiers or when proving simulation relation conditions for refinement and equivalence of program fragments. Furthermore, BAPA constraints can be used for proving the termination of programs that manipulate data structures, as well as in constraint database query evaluation and loop invariant inference. We give a formal description of an algorithm for deciding BAPA. We analyze our algorithm and show that it has optimal alternating time complexity and that the complexity of BAPA matches the complexity of PA. Because it works by a reduction to PA, our algorithm yields the decidability of a combination of sets of uninterpreted elements with any decidable extension of PA. When restricted to BA formulas, the algorithm can be used to decide BA in optimal alternating time. Furthermore, the algorithm can eliminate individual quantifiers from a formula with free variables and therefore perform projection onto a desirable set of variables. We have implemented our algorithm and used it to discharge verification conditions in the Jahob system for data structure consistency checking of Java programs; our experience suggest that a straightforward implementation of the algorithm is effective on nontrivial formulas as long as the number of set variables is small. We also report on a new algorithm for solving the quantifier-free fragment of BAPA.

MSC:
03B35 Mechanization of proofs and logical operations
03B25 Decidability of theories and sets of sentences
68P05 Data structures
68Q60 Specification and verification (program logics, model checking, etc.)

Keywords:
Boolean algebra; Presburger arithmetic; decision procedure; quantifier elimination; complexity; program verification

Software:
ML; Isabelle/HOL; UCLID; CVC Lite; PVS; HOL; MONA; Quaffle; VAMPIRE

Full Text: DOI

References:


