発表概要

配列を入力引数とする関数の検証のための分離論理の拡張

水谷 慎之介[1,a)]　西田 直樹[1,b)]　酒井 正彦[1,c)]

2016年6月9日発表

C 言語などにおいて配列を入力引数とする関数は入力配列の先頭のアドレスのみを受け取ることで間接的に配列を受け取る．そのため，そのような関数は様々なサイズの配列を受け取る可能性がある．そのような関数を検証するにあたって入力配列のサイズを任意ととらえ，事前条件においても任意のサイズのヒープに関する性質の記述が必要である．分離論理では線形リストを表現する再帰定義された述語を応用すればそのようなヒープを表現することは可能だが，連続するヒープをわざわざそのような述語を用いて検証するのは冗長である．本発表では，整数式でサイズを表したヒープ表現を導入することで分離論理を拡張し，その拡張に応じて分離論理の推論規則も拡張する．

Extension of Separation Logic toward Verification of Functions Passed Arrays as Arguments

Shinnosuke Mizutani[1,a)]　Naoki Nishida[1,b)]　Masahiko Sakai[1,c)]

Presented: June 9, 2016

As in the C programming language, a function passed an array as one of its arguments receives only a pointer to the first element of the array, and acts as if the entire array is recieved. For this reason, we cannot expect the fixed size of arrays that the function receives. To verify the function, considering the array size unknown, we must write assertions for e.g., pre-/post- conditions that specify properties on arrays (i.e., heaps) with the arbitrary size. In the framework of separation logic, we can specify such heaps by using a recursively-defined predicate indicating that a given pointer refers to the first element of a linear list. Though, such a predicate would be overspecified for representing heaps for arrays where each element is located at the next cell of the previous element. In this presentation, we extend separation logic by introducing a notation for heaps, the size of which can be specified by non-ground expressions over the integers. We also extend inference rules of separation logic for the extension of the syntax.

[1] 名古屋大学大学院情報科学研究科
Graduate School of Information Science, Nagoya University, Nagoya 464–8603, Japan
[a)] mizutani_s@trs.cm.is.nagoya-u.ac.jp
[b)] nishida@is.nagoya-u.ac.jp
[c)] sakai@is.nagoya-u.ac.jp