Boosting Automated Verification Using Cyclic Proof: Diagrammatic Workplan

J. Brotherston (PI), B. Cook (CI), N. Gorogiannis (RCI)

We propose to assign the two RAs to work on the various threads of the research programme outlined in the Case for Support during the months indicated by 'RA1' or 'RA2' in the table below, where 'RA1' denotes Gorogiannis. Each thread has been designated as belonging to one or more of the Research Themes (RT) A, B, C and D given in section 2.4 of the Case for Support.

Months	0–6	7–12	13–18	19–24	25–30	31–36
1. Separation logic entailment proving (RT A)	RA1	RA1				
2. First-order logic entailment proving (RT A)	RA2	RA2				
3. Cyclic-proof based components for program analysis (RT B)	Both	Both	Both			
4. Abduction of inductive predicates for verification (RT C)			RA1	RA1		
5. Integration of cyclic abduction with shape analysis (RT C)				RA2	RA2	RA2
6. Integration of cyclic methods into a compositional analysis (RT E)				Both	Both	Both
7. Cyclic proof for temporal program properties (RT D)					RA1	RA1

Milestones

6 months: Initial studies into lemma application and generalisation schemes completed in both separation logic and first-order contexts. Decision reached on whether to use Cyclist as implementation platform, or modifying an established theorem prover.

12 months: Separation and first-order logic provers ready to be used as program analysis backends.

18 months: Abstraction and frame inference ready for use in program analysis core.

24 months: First complete version of a compositional shape analysis for general inductive predicates.

30 months: Integration of inductive definition abduction into shape analysis from previous milestone.

36 months: Abductive shape analysis employing general inductive predicates tested on large code bases. First complete version of a temporal logic verifier for heap manipulating programs.

We plan to produce academic papers describing our work roughly in line with the above milestones.

We emphasise that the workplan above is simply one plausible sequence of events, and not a rigid schedule. The RAs will be given the flexibility to react appropriately to the inevitable surprises, damp squibs and new opportunities that arise during most research projects.