MONA/PALE

Motivation

- Verify graph datastructures

How it works.

Describe store with PAL: M2L-Tree + graph types

Input: program with
- pre
- post
- loop invariants

Verifies each hoare triple which is loop free

Encode to M2L-Tree

Store predicates

ptr_p(v) "does p point to v" $p \rightarrow v$

succ_T_next(w, v) "does field next of w point to v" $w \xrightarrow{next} v$

Updates

- similar to weakest precondition but in forward manner

$p := q.next$

~~$p(v)$~~

$\Phi\ ptr\_p(v) = \exists w : ptr\_q(w) \wedge succ\_T\_next(w, v)$

Use Mona as decision engine with verification conditions generated by expressing pre/post using store predicates at end points.

Classification

Sound and complete
- ignoring frame problem

Scales OK
- Hoare triples are generally small, but inherit $2^{2^{2^{\cdots}}}$

Expresiveness

M2L-Tree