Smallfoot

Motivation

- Verify datastructures
- Use Separation logic

How it works

Frame problem

$\{P\}\ S\ \{Q\}$ ← if true we do not know if other parts was changed

Heaplets

emp ← empty heaplet

$E \to F_1:E_1, \ldots, F_n:E_n$ ← one record heap

$P * Q$ ← two separated heaplets

We can avoid global reasoning:

$$\frac{\{P\}\ S\ \{Q\}}{\{P*R\}\ S\ \{Q*R\}}$$ R not changed!

Smallfoot

- like PALE: pre, post and loop invariants
- hardcoded predicates for list and tree
- Simple expression language

Example

```
list_reverse(i)   [list(i)]
      ⋮
while(...)        [list(i)*List(0)]
      ⋮
[list(0)]
```

- No elements lost
- List returned
- Other parts of heap not changed

Classification

Sound and incomplete

Scales = local reasoning, like PALE

Expresiveness lower than PALE