

## 1 Background

- Software errors can be very costly
- Testing is useful, but not a silver bullet
- Model checking is a formal verification technique that can help
- mCRL2 is a modelling language with an accompanying toolset
- The toolset allows model checking with modal  $\mu$ -calculus formulae

## 2 Modal $\mu$ -Calculus

- It is a temporal logic
- It includes fixed-point operators that allow definition of recursive predicates
- Very expressive, but potentially at the cost of performance and understandability

### Example

As an example consider the following formula:

$$\mu X(s, e) := (s = e) \vee \exists i, (edge(s, i) \wedge X(i, e))$$

This formula defines a reachability relation  $X(s, e)$  from  $s$  to  $e$  in a graph.  $e$  is reachable from  $s$  if they are the same node, or if there is an edge from  $s$  to an intermediate node  $i$  that can reach  $e$ .

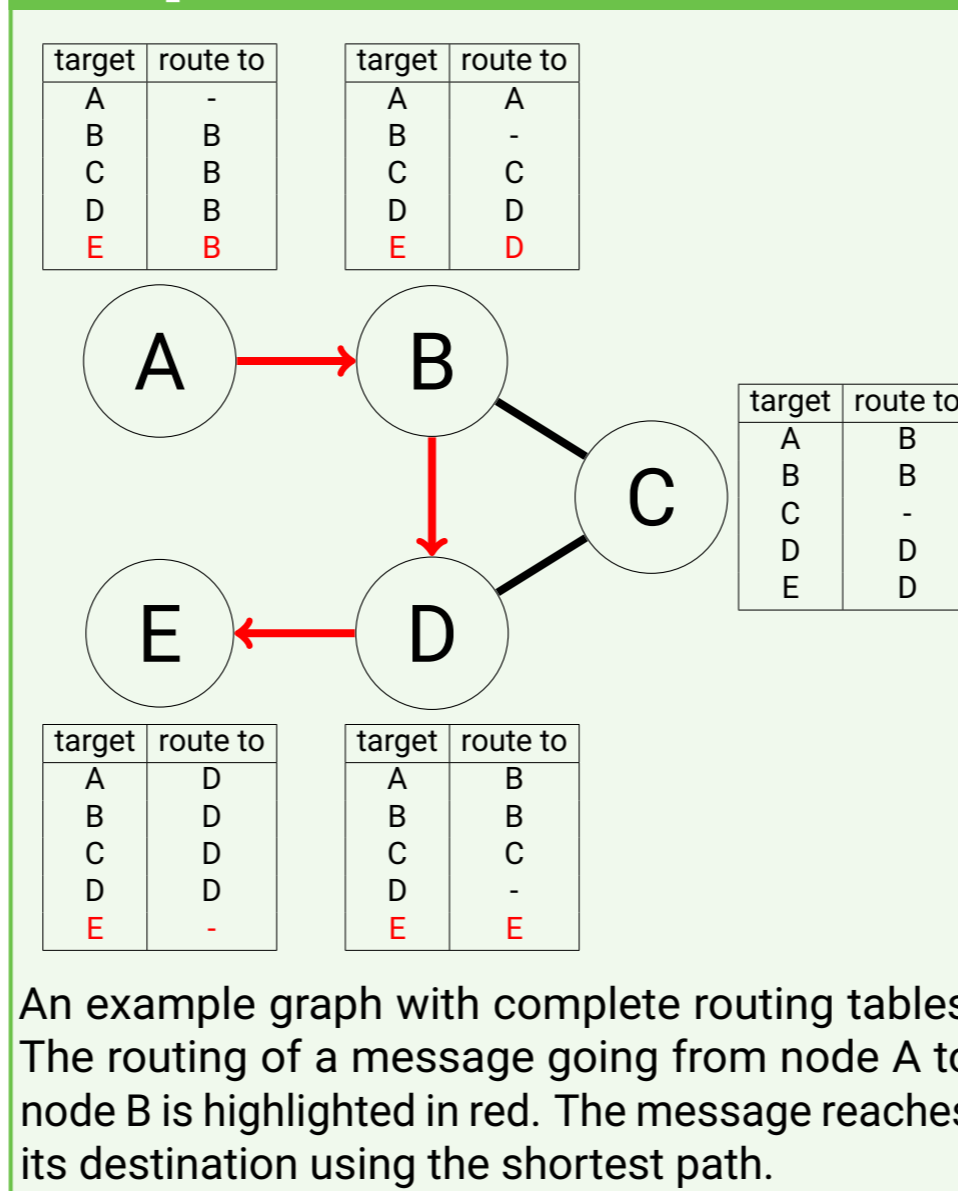
### Research question

What are the advantages and disadvantages of using fixed-point operators to express a property compared to using helper functions when verifying distance-vector routing protocols in mCRL2?

## 3 Case Study

- We investigate four distance-vector routing protocols, used for networking
- Each node in a network computes a routing table by communicating with its neighbors
- When messages follow the tables they should reach their destination, using the shortest path

### Example



## 4 Results

### 4.1 Fixed-Point Operator Advantages

- Around two times faster verification for this problem
- Overall size of code/expressions that need to be trusted is lower

### 4.2 Fixed-Point Operator Disadvantages

- Heavier reliance on logical expressions, harder to handle for the average programmer
- Errors in properties are less likely to be detected during verification.

Property variant	Property 1	Property 2	Property 3
fixed-point based	129	149	160
helper function based (excluding function size)	96	112	120
helper function based (including function size)	343	407	559

Table: The syntax tree sizes for the properties we considered in our case study.

## 5 Future Work

- More case studies to generalize the findings
- Surveys and similar methods to gather a wider range of opinions
- Investigating more complicated properties with potentially different outcomes