

Finding Safety Errors with ACO

Enrique Alba & Francisco Chicano
University of Málaga (Spain)



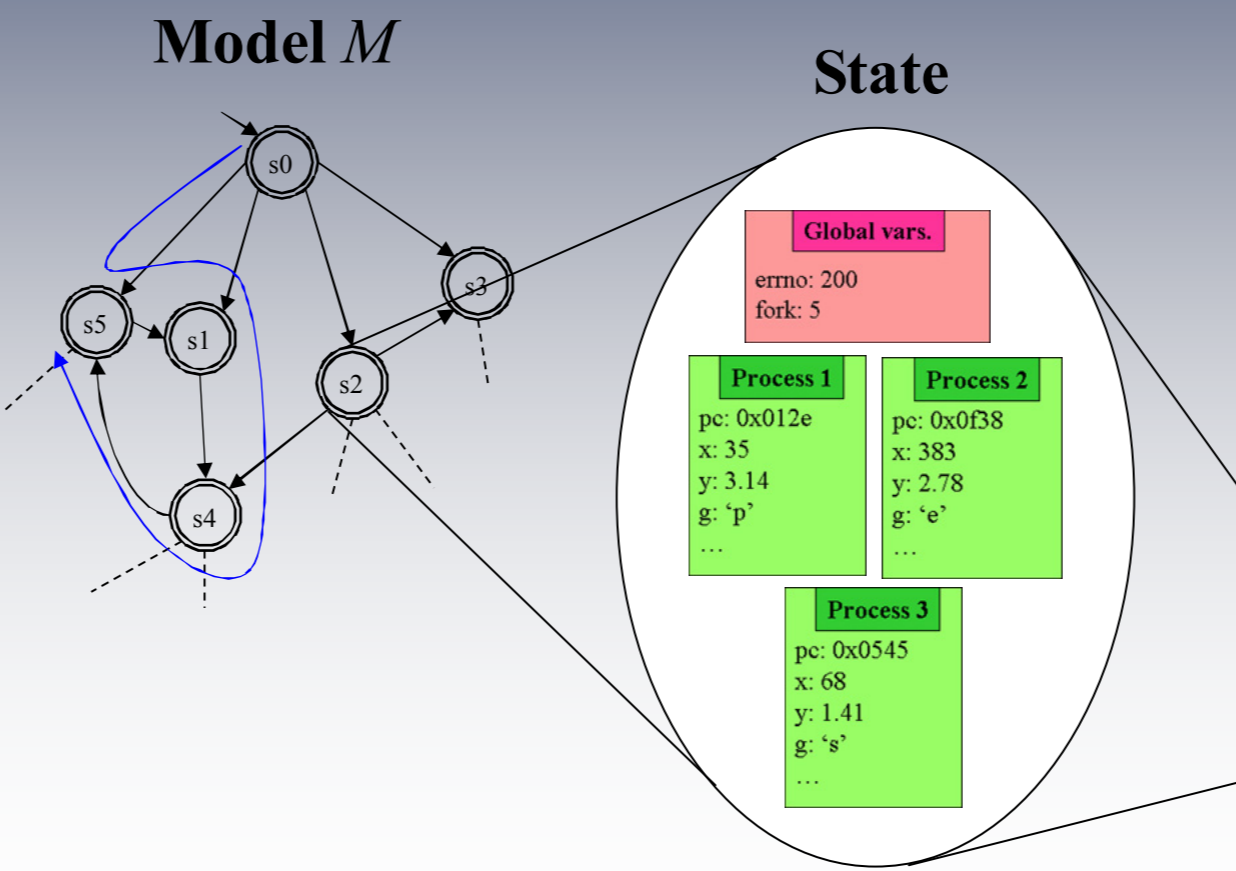
A software error can imply the lost of money...



... and even human lives

Model checking is a **fully automatic technique** for verifying concurrent systems

For **safety properties**, classical graph exploration algorithms can be applied



$$f = \square p$$



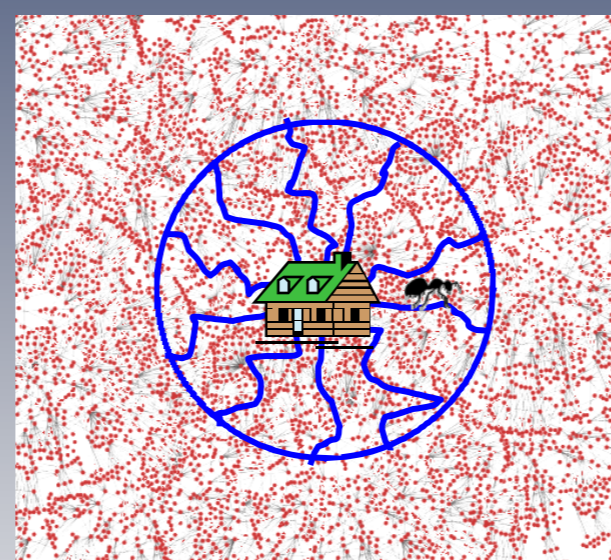
DFS BFS A* BF



Metaheuristics can manage the state explosion problem

Ant Colony Optimization

ACOhg



Missionary



```

Algorithm 1 ACOhg algorithm
1: init ← {}
2: next_init ← ∅
3: r ← initialize_pheromone()
4: step ← 1
5: stage ← 1
6: while step ≤ max_iter ∨ ∃ i, 1 ≤ i ≤ n such that |e_i| ∈ F do
7:   for k = 1 to n do
8:     a^k ← ∅
9:     a^k ← select_init_node_randomly(j^k)
10:    while |a^k| ≤ λ_max ∧ T(r, a^k) = a^k ≠ ∅ ∧ a^k ≠ j^k do
11:      node ← select_succesful(T(r, a^k), r, η)
12:      a^k ← a^k ∪ node
13:      τ ← local_pheromone_update(r, ζ)
14:    end while
15:    next_init ← select_best_paths(next_init, a^k)
16:    if f(a^k) < f(a^{k-1}) then
17:      a^{k-1} ← a^k
18:    end if
19:  end for
20:  τ ← pheromone_evaporation(r, ρ)
21:  r ← pheromone_update(r, a^{k-1})
22:  if step = 0 mod σ then
23:    init ← next_init
24:    next_init ← ∅
25:    stage ← stage + 1
26:    r ← pheromone_reset()
27:  end if
28:  step ← step + 1
29: end while
    
```

Traditional ACOs cannot deal with such a huge graph

NEW TECHNIQUE

Some results

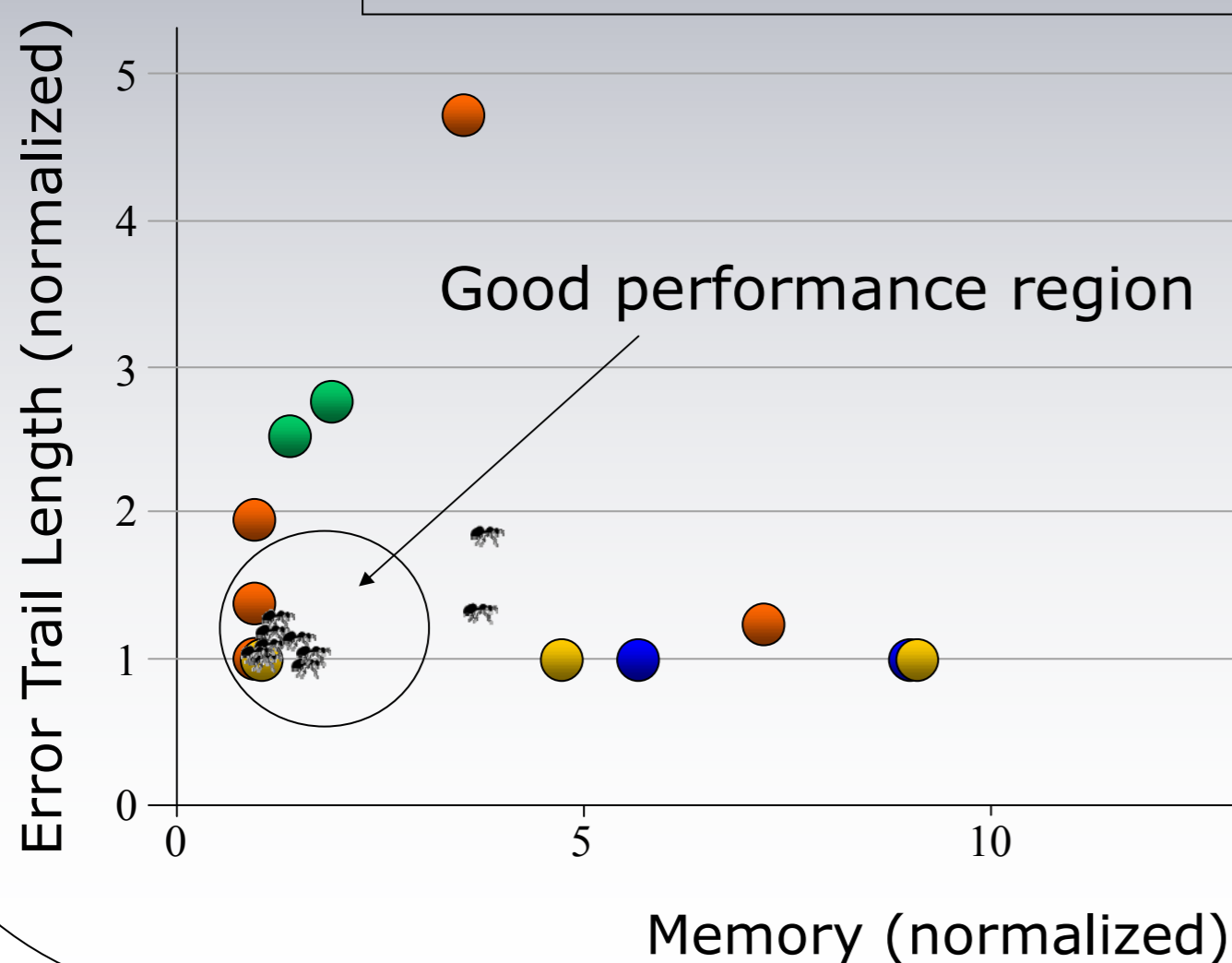
Models	BFS	DFS	A*	BF	ACOhg
giop22		●	●	●	🐜
needham	●	●	●	●	🐜
phil6			●	●	🐜
pots	●	●	●	●	🐜
marriers4				●	🐜
marriers20					🐜

ACOhg is the only one able of finding errors in very large models ...

Conclusions

- ACOhg is a newly developed ACO algorithm designed to deal with huge graphs
- It is able to find errors in **very large concurrent models**, in which traditional model checking techniques fail
- ACOhg **outperforms** the results of state-of-the-art algorithms in model checking

● BFS ● DFS ● A* ● BF 🐜 ACOhg



I want to learn more on this



Read the paper !!!

