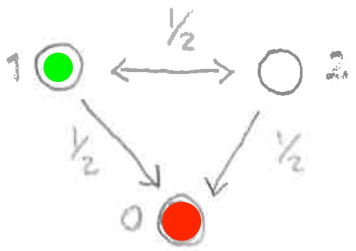
Carroll Morgan's "slides" for WG2.3
in Mooloolaba, 17-21/7/17.

PROBABILISTIC TERMINATION

1 20/7/17

1. The problem:



termination:
demonic – no
probabilistic – yes

No (standard) variant in either case.

Probabilistic termination is however only "almost sure", eqv. "with probability 1".

Trivial for mathematicians; puzzling for computer scientists

M : "It's just a..."
CS: "How do I <u>know</u> it's just a..."

The importance of source-level reasoning: no "cognitive gulf"; availability of mechanical provers. For the latter, the importance is their common source.

20/7/17

2. | A CS — solution (1996)
   | — but one of many.

[Integer variant s.t. $I \wedge G \Rightarrow$
bounded above and below;
guaranteed to decrease w.prob
at least some fixed $\varepsilon > 0$.

Previous page: variant is node-number. Easy.

M: d is probality of moving one step left eventually.

$d = \frac{1}{2} + \frac{1}{2} d^2$

CS: As recently as the beginning of 2017, this was beyond the reach of a number of sophisticated rules.

But we will do it today.

3. Today

20/7/17

a) Why does 1996 rule work?

b) Description of new rule (2017) (Andreas Lochbihler)

c) Sketch proof

---

but rigorous

d) arXiv paper gives sketch proof, and many examples * !

e) Since then have formalised it in pGCL

f) very quick description of pGCL

g) new rule in pGCL

---

h) Classical results (1950's, pre- CS)

i) 2d RW

4/

20/7/17

3a) Why does 1996 rule work?

[ ]

L H

t

i) never more than $H - L + 1$ steps from termination

ii) any consecutive run of t steps terminates w.prob at least $\varepsilon^t > 0$

↑
fixed

iii) prob of tN steps <u>not</u> terminating is no more than $(1-\varepsilon^t)^N$, goes to 0 as $N \to \infty$.

20/7/17

5/

3b) Description of new rule

i) real valued variant, non-negative and st. zero $\Rightarrow$ termination.

weaker requirement

No upper bound.

ii) parametrised progress: if $V = R$ then V decreases by at least $d(R)$ w.prob at least $p(R)$, for fixed, strictly positive antitone functions p, d.

weaker requirement

iii) V is a super-martingale.

stronger requirement

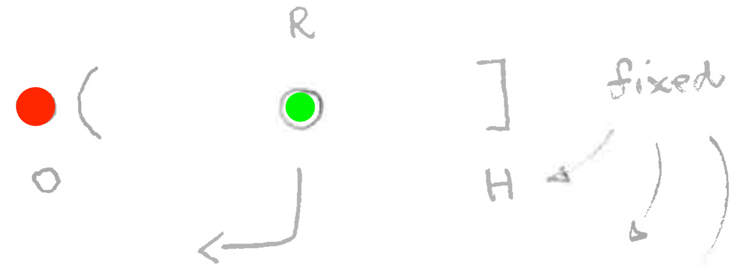
$d(v) = 1 \quad p(v) = 1/2 \quad$ and $\quad 1/2(n-1) + 1/2(n+1) \leq n$.

20/7/17

6/

3c) Sketch proof of new rule

i)



$d(R) \geq d(H)$

uprob $p(R) \geq p(H)$

Thus an instance of 1996 rule — but note escape can occur <u>above</u> H as well as at 0.

ii) If prob of escape above H is h, say, then expected value of V on termination (at either end) is at least hH. But by S-M we have $hH \leq R$

iii) So $H \to \infty$ makes $h \to 0$ hence $1-h \to 1$.

20/7/17

3d) arXiv paper gives more details, mentions demonic choice, contains many examples.

3e) Have since then formalised it in pGCL. (1983)

3f) What's pGCL? (1996/2005)

GCL $\quad pre \Rightarrow wp.C.post$

pGCL $\quad preE \leq wp.C.postE$

$\Rrightarrow$

real valued, its initial value

expected value of postE after executing (probabilistic) C.

$[pre] \leq wp.C.[post]$

or $\quad p\cdot[pre] \leq wp.C.[post]$

20/7/17

8/

3g)

probabilistic loop body

Boolean

$$\boxed{\text{loop: } \underline{\text{while}}\ G\ \underline{\text{do}}\ C\ \underline{\text{od}}}$$

define: $p, d : \mathbb{R}^+ \to \mathbb{R}^+$

V – $\mathbb{R}^{\geq}$– expression on state variables

I – Boolean invariant

i) $G \wedge I \Rightarrow V > 0$

ii) $p(R) \cdot [G \wedge I \wedge V = R]$

$\leq wp . C . [V \leq R - d(R)]$

arbitrary, captures V's initial value

iii) $V \geq [G \wedge I] \cdot wp(C, V)$

pGCL has been used within automated provers: McIver/Cecilia/Hurd – HOL

Cock – Isabelle

* Nice MSc project – prove this rule?

MSc Opportunity?

20/7/17

3h) Results of Foster Blackwell

on (deterministic) Markov chains (pre-CS, 1950's) anticipate this.

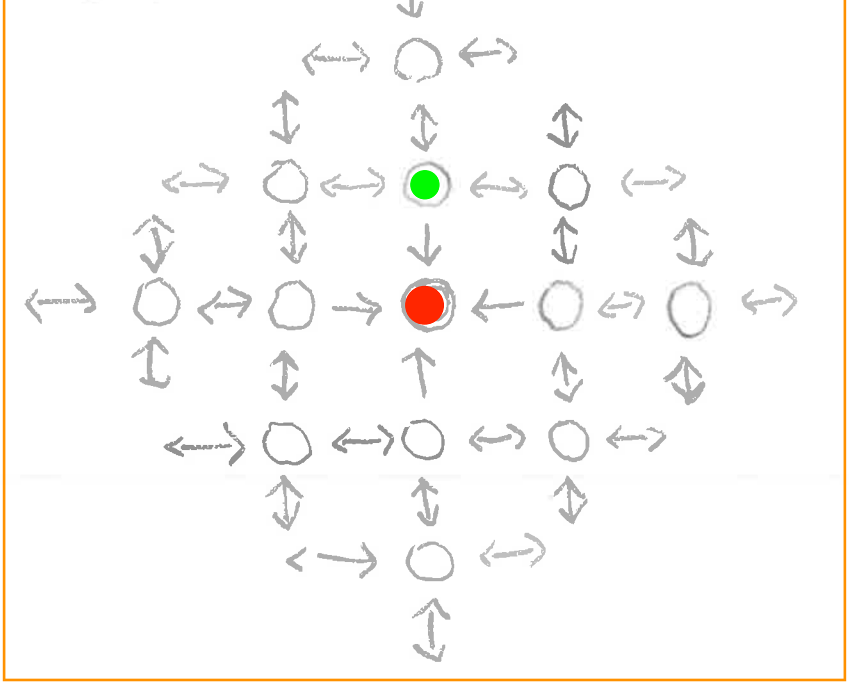
In particular, Foster gives sufficient conditions on an AST Markov chain for there to exist a variant in our style. It's a constructive proof, but not in closed form.

- 2dRW satisfies his conditions
- It terminates AS
- There is a variant/d/p that shows that
- WE DON'T KNOW WHAT THE VARIANT IS.

OPEN PROBLEM:
Termination proof for the two-dimensional random walk

10/ 20/7/17

3i)



Find a function from node to $R^{\geq}$ that

i) is 0 at centre (only).

ii) is a S-M: each node is $\geq$ average of its neighbours.

(iii) increases without bound as distance from centre increases.