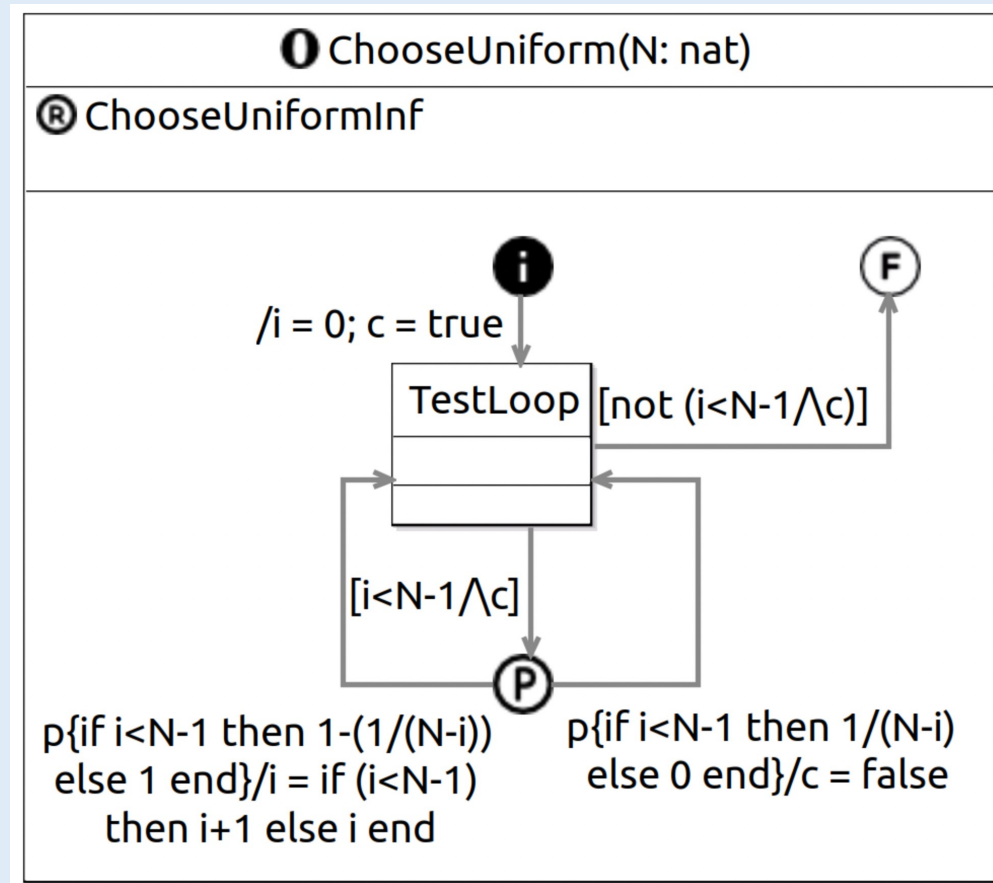


Probabilistic modelling and verification in RoboChart

Probabilistic junctions to model randomness in robot control algorithms, such as

- Localisation and mapping (RANSAC, SLAM)
- Control and planning (PRM)



Properties

Qualitative	Will the robot <i>never</i> collide with obstacles	?
Quantitative	How likely a robot will	
Quality of Service	On average, how many deliveries the robot can	

Probabilistic property language

PRISM PCTL*
(Probabilistic CTL + LTL) enriched with RoboChart elements

```

prob property P_1:
  Forall [Globally (Finally (fd==2) and (Next (fd==0)))]

prob property P_goodfit:
  Prob=? of [Finally ransacMOD::ransacCTRL::stm_ref0
    is in ransacMOD::ransacCTRL::stm_ref0::goodFit]
    
```

Probabilistic Models

Probabilistic Properties

Formal Verification Techniques

Probabilistic Model Checking

- "Exact" (numerical) results,
- Medium and large finite models
- Fully automated

Statistical Model Checking

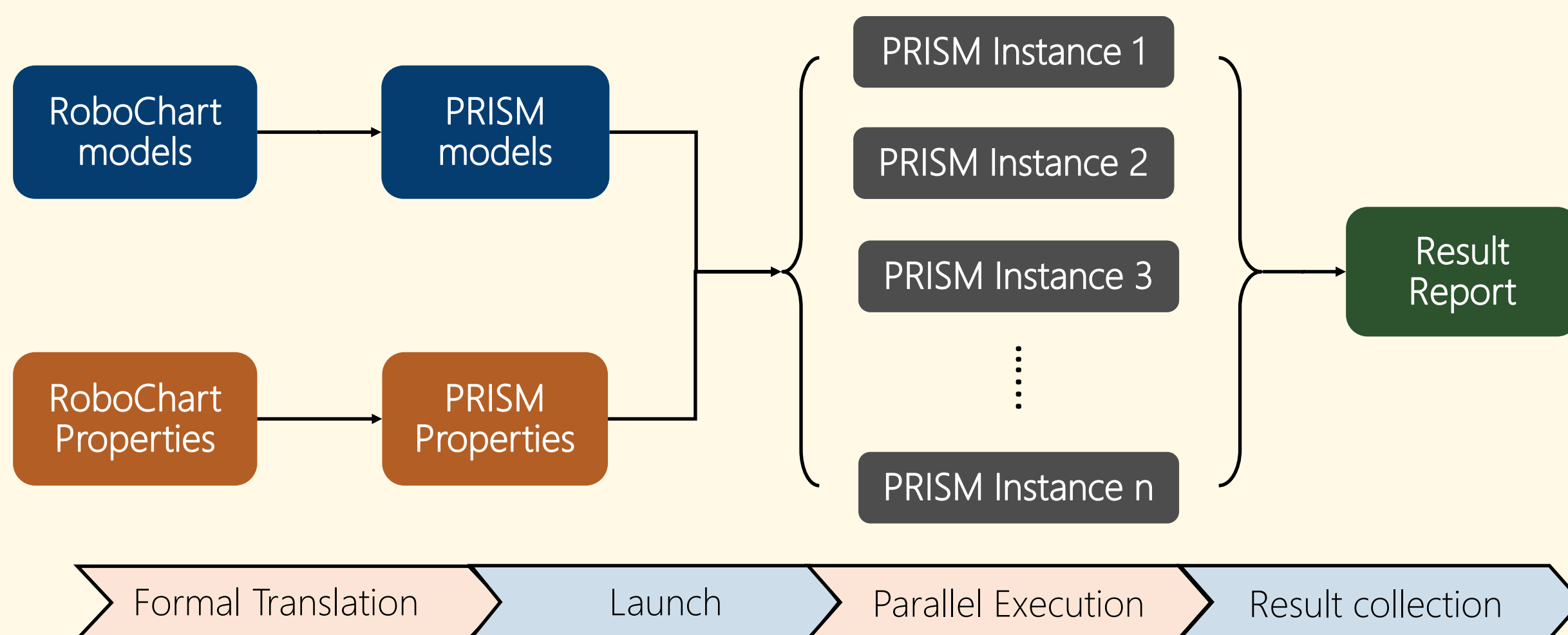
- Approximate results on sampling
- Very large finite models
- Fully automated

Theorem Proving

- Exact results
- Infinite large models
- Largely automated

Verification Tool Support

RoboTool



Isabelle/UTP

```

Lemma robot_localisation: "
  ((( init || scale_door) ;
    move_right || scale_door) ;
  move_right || scale_wall)
  =
  prfun_of_rvfun (
    1/18 * [[bel^ = 0]]_e +
    8/9 * [[bel^ = 1]]_e +
    1/18 * [[bel^ = 2]]_e
  )_e"
apply (simp add: robot_localisation_def)
apply (simp add: move_right_2_simp believe_3_def)
apply (simp add: scale_wall_def door_def pfun_defs)
apply (simp add: move_right_2_dist)
apply (simp add: move_right_2_def dist_defs)
apply (expr simp 1)
apply (rule HOL.arg_cong[where f="prfun_of_rvfun"]1)
apply (simp add: ring_distrib(2))
apply (subst fun_eq_iff, rule allI)
apply (auto)
by (simp add: believe_3_sum)+
    
```

Verification results

Assertion: P_deadlock_free

Assertion	states	transitions	result	checkTime
P_deadlock_free	3322	3742	true	0.004 seconds

Assertion: P_nr_of_tries

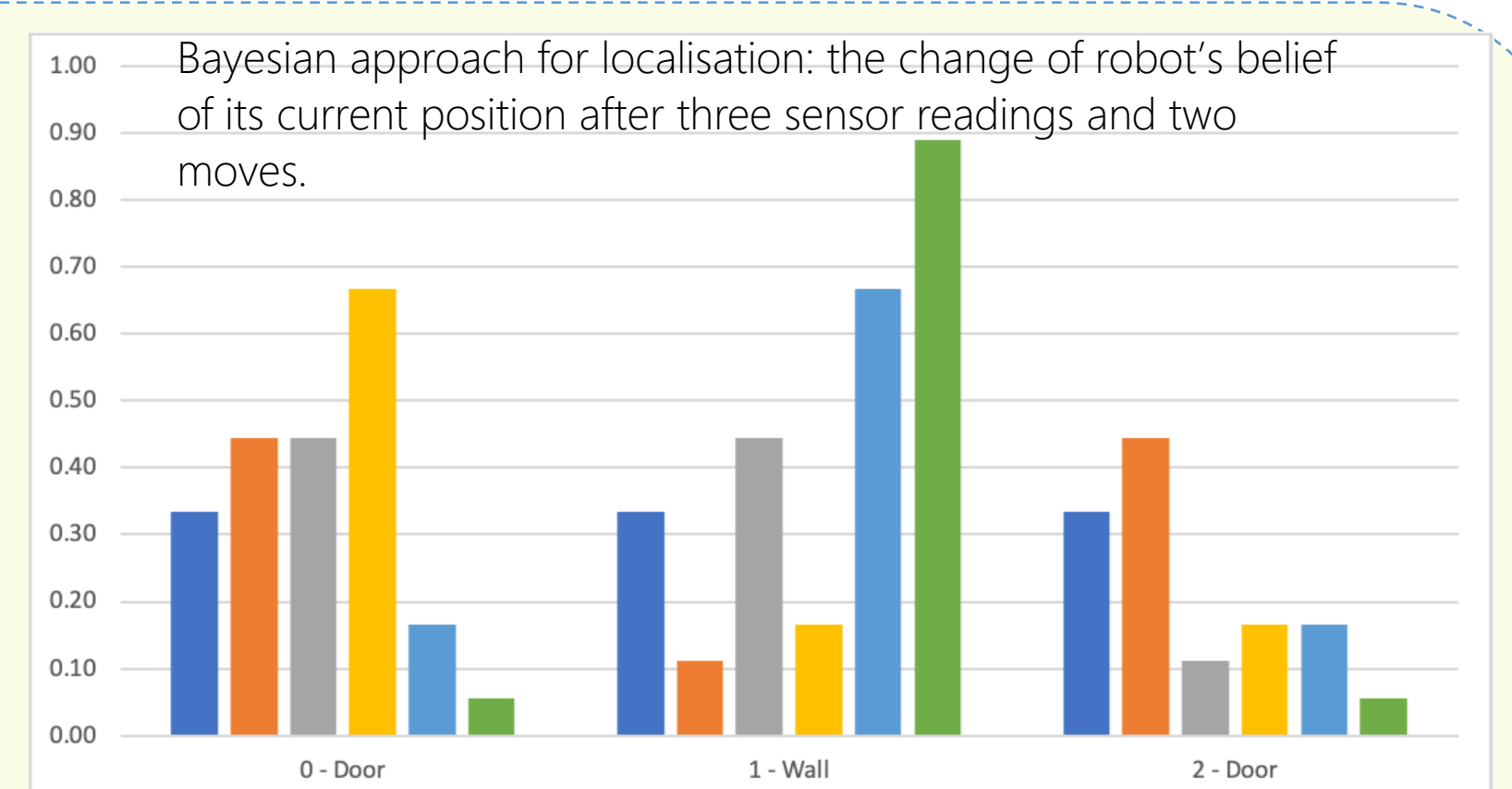
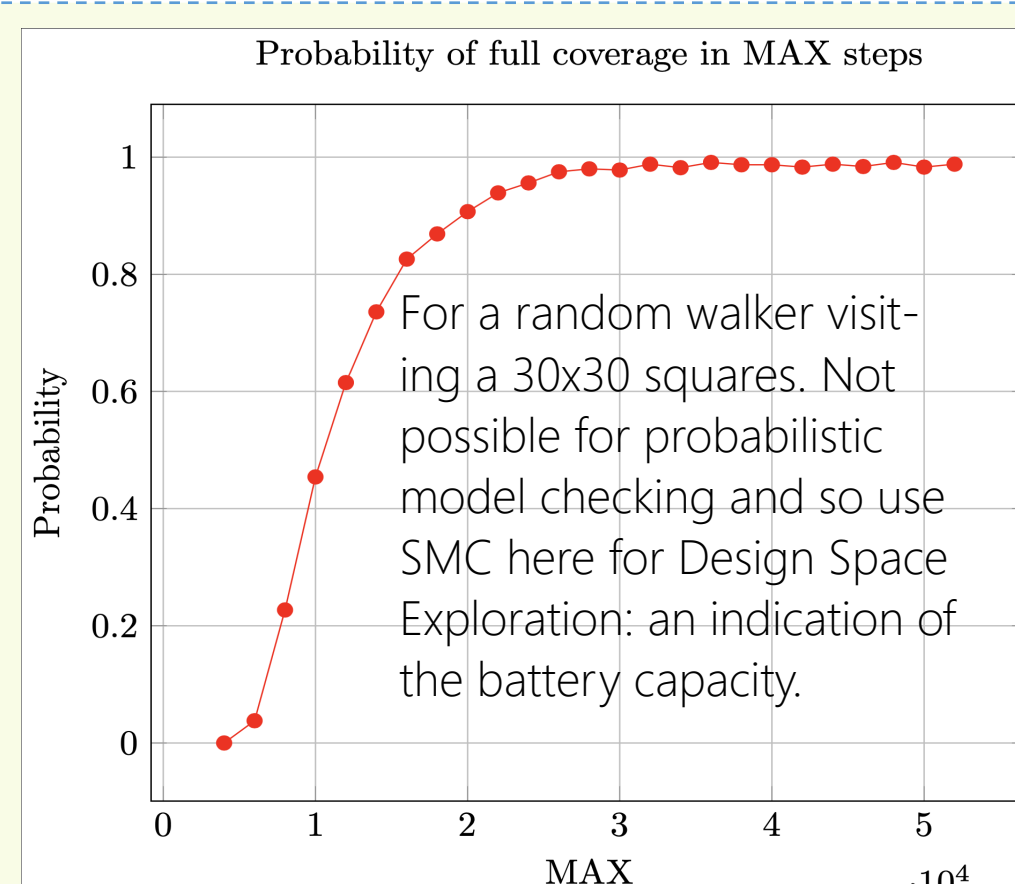
Assertion	states	transitions	result	checkTime
P_nr_of_tries	3322	3742	1.6998561958204306	0.055 seconds

Assertion: P_nr_of_choices

Assertion	states	transitions	result	checkTime
P_nr_of_choices	3322	3742	2.6998527952527036	0.092 seconds

Assertion: P_goodfit

Assertion	states	transitions	result	checkTime
P_goodfit	3322	3742	1.0	0.029 seconds



	Probabilistic Model Checking	Statistical Model Checking	Theorem Proving
Qualitative	✓	✓	✓
Quantitative	= 5.56 %	≈ 5.45 %	= 1/18
Quality of Service	= 4.286	≈ 4.351	= 30/7

