Appendix : Model Checking of State Based Randomized Systems using Probabilistic Process Algebraic Tools

Contents

1 Embedding for Eventually operator of $PCTL$ 3

2 Tables of case studies 3
2.1 Bounded Retransmission Protocol . . . 4
2.2 Crowds Protocol . . . 5
2.3 Contract Signing Protocol . . . 5
2.4 Synchronous Leader Election Protocol . . . 5
2.5 NAND Multiplexing . . . 6

3 Properties 6
3.1 Bounded Retransmission Protocol . . . 6
3.1.1 Property 1 . . . 6
3.1.2 Property 2 . . . 7
3.1.3 Property 3 . . . 7
3.1.4 Property 4 . . . 7
3.1.5 Property 5 . . . 7
3.1.6 Property 6 . . . 8
3.2 Crowds Protocol . . . 8
3.3 Contract signing protocol . . . 8
3.3.1 Property 1 . . . 8
3.3.2 Property 2 . . . 9
3.4 Synchronous leader election protocol . . . 9
3.4.1 For the models having $N = 3$ . . . 9
3.4.2 For the models having $N = 4$ . . . 9
3.4.3 For the models having $N = 5$ . . . 9
3.4.4 For the models having $N = 6$ . . . 10
3.4.5 Bounded Until formula . . . 10
3.5 NAND multiplexing . . . 10

4 Tables and graphs of bounded until property of Case Study "Synchronous leader election protocol" 11

1 Embedding for Eventually operator of $PCTL$

As the *eventually* operator of $PCTL$ is a derived operator from the $Until$ operator, therefore the embedding of *eventually* operator can also be derived from the embedding of $Until$ operator.

The transformation for the Until operator of $PCTL \rightarrow APCTL$ is given by the following function.

$$\begin{aligned} aldl'\Big(P_J(\Phi \mathbf{U} \Phi')\Big) \quad =& P_J\Bigg(\Bigg(\Big(aldl'(\Phi) \wedge P_{[1,1]}\big(\mathbf{X}_{\neg\perp}\mathbf{true}\big)\Big) \vee \Big(\big(P_{(0,1]}(\mathbf{X}_{\perp}\mathbf{true})\big) \vee \big(P_{(0,1]}(\mathbf{X}_{\tau}\mathbf{true})\big)\Big)\Bigg)_{\mathbf{true}} \\ & \mathbf{U}\Big(aldl'(\Phi') \wedge P_{[1,1]}\big(\mathbf{X}_{\neg\perp}\mathbf{true}\big)\Big)\Bigg) \end{aligned}$$

Let us consider a PCTL formula for eventually requirement $P_J(true U \Phi)$ using the embedding for until operator we get the below:

$$\begin{aligned} aldl'\Big(P_J(true \mathbf{U} \Phi')\Big) \quad =& P_J\Bigg(\Bigg(\Big(aldl'(true) \wedge P_{[1,1]}\big(\mathbf{X}_{\neg\perp}\mathbf{true}\big)\Big) \vee \Big(\big(P_{(0,1]}(\mathbf{X}_{\perp}\mathbf{true})\big) \vee \big(P_{(0,1]}(\mathbf{X}_{\tau}\mathbf{true})\big)\Big)\Bigg)_{\mathbf{true}} \\ & \mathbf{U}\Big(aldl'(\Phi') \wedge P_{[1,1]}\big(\mathbf{X}_{\neg\perp}\mathbf{true}\big)\Big)\Bigg) \\ =& P_J\Bigg(\Bigg(\Big(true \wedge P_{[1,1]}\big(\mathbf{X}_{\neg\perp}\mathbf{true}\big)\Big) \vee \Big(\big(P_{(0,1]}(\mathbf{X}_{\perp}\mathbf{true})\big) \vee \big(P_{(0,1]}(\mathbf{X}_{\tau}\mathbf{true})\big)\Big)\Bigg)_{\mathbf{true}} \\ & \mathbf{U}\Big(aldl'(\Phi') \wedge P_{[1,1]}\big(\mathbf{X}_{\neg\perp}\mathbf{true}\big)\Big)\Bigg) \\ =& P_J\Bigg(\Bigg(\Big(P_{[1,1]}\big(\mathbf{X}_{\neg\perp}\mathbf{true}\big)\Big) \vee \Big(\big(P_{(0,1]}(\mathbf{X}_{\perp}\mathbf{true})\big) \vee \big(P_{(0,1]}(\mathbf{X}_{\tau}\mathbf{true})\big)\Big)\Bigg)_{\mathbf{true}} \\ & \mathbf{U}\Big(aldl'(\Phi') \wedge P_{[1,1]}\big(\mathbf{X}_{\neg\perp}\mathbf{true}\big)\Big)\Bigg) \\ =& P_J\Bigg(\Bigg(\Big(P_{[1,1]}\big(\mathbf{X}_{\neg\perp}\mathbf{true}\big) \vee \big(P_{(0,1]}(\mathbf{X}_{\perp}\mathbf{true})\big) \vee \big(P_{(0,1]}(\mathbf{X}_{\tau}\mathbf{true})\big)\Big)\Bigg)_{\mathbf{true}} \\ & \mathbf{U}\Big(aldl'(\Phi') \wedge P_{[1,1]}\big(\mathbf{X}_{\neg\perp}\mathbf{true}\big)\Big)\Bigg) \end{aligned}$$

From the above derivation, it is clear that for the embedding of a $PCTL$ formula having an eventually operator, the resultant $APCTL$ holds the property that the left portion from the until operator is Φ independent.

Further on the assumption that the Φ' no more goes to the probability operator of the PCTL syntax, we can say the below,

$$\begin{aligned} aldl'\Big(P_J(true \mathbf{U} \Phi')\Big) \quad =& P_J\Bigg(\Bigg(\Big(P_{[1,1]}\big(\mathbf{X}_{\neg\perp}\mathbf{true}\big) \vee \big(P_{(0,1]}(\mathbf{X}_{\perp}\mathbf{true})\big) \vee \big(P_{(0,1]}(\mathbf{X}_{\tau}\mathbf{true})\big)\Big)\Bigg)_{\mathbf{true}} \\ & \mathbf{U}\Big(\Phi' \wedge P_{[1,1]}\big(\mathbf{X}_{\neg\perp}\mathbf{true}\big)\Big)\Bigg) \end{aligned}$$

2 Tables of case studies

In every table, the first column lists the parameters and their corresponding values for each PRISM case study [**?**]. The next two columns present the model size in terms of states and transitions for the SDTMC (second column) and ADTMC (third column), respectively. The "Embed" column reports the embedding time in seconds (t_1) required to transform an SDTMC into the corresponding ADTMC for a

given model size. The column "Property number" is included for case studies with multiple probabilistic properties, where p_i denotes the i^{th} property. Next, we provide the model checking times for both tools: PRISM (t_2) and CADP (t_3). Here, t_3 represents the total time required to convert the model from the *.aut* format to the *.bcg* format of CADP and perform CADP model checking. Since the model *.aut* $\rightarrow$ *.bcg* is performed only once for a given model size, the first component of the reported values for t_3 remains identical in all properties. Finally, the last column presents the computed probability values corresponding to each property.

2.1 Bounded Retransmission Protocol

N MAX	Model size (state, trans) SDTMC	 ADTMC	Embed (t_1 in seconds)	Property number	Total model checking time (in seconds) PRISM (t_2)	 aut2bcg + CADP Model checking (t_3)	Prob
10^4 2	420005, 540003	840010, 960008	6.97	p_1	90.38	17.5+57.04	0
				p_2	95.35	17.5+57.19	0
				p_3	343.52	17.5+56.72	0.23251
				p_4	348.13	17.5+61.54	2.03E-5
				p_5	353.28	17.5+57.17	0.23228
				p_6	95.71	17.5+57.65	8.0E-6
10^4 4	680007, 900003	1360014, 1580010	11.75	p_1	151.01	37.37+156.61	0
				p_2	152.75	37.37+157.06	0
				p_3	580.27	37.37+153.1	2.35E-4
				p_4	575.41	37.37+160.26	2.35E-8
				p_5	594.5	37.37+154.27	2.35E-4
				p_6	160.71	37.37+161.64	3.2E-9
10^4 8	1200011, 1620003	2400022, 2820014	20.92	p_1	264.24	92.88+547.13	0
				p_2	290.64	92.88+537.96	0
				p_3	1063.26	92.88+523.73	1.85E-10
				p_4	1061.24	92.88+530.67	1.85E-14
				p_5	1073.18	92.88+530.4	1.85E-10
				p_6	285.55	92.88+538.68	5.12E-16
5×10^4 2	2100005, 2700003	4200010, 4800008	37.17	p_1	536.92	294+1795.77	0
				p_2	516.65	294+1879.73	0
				p_3	6964.02	294+1686.78	0.7337
				p_4	7084.17	294+1798.88	7.05E-6
				p_5	7018.42	294+1693.3	0.7335
				p_6	520.4	294+1858.47	8.0E-6
5×10^4 4	3400007, 4500003	6800014, 7900010	60.15	p_1	872.16	720.57+6634.53	0
				p_2	884.72	720.57+6803.15	0
				p_3	12050.36	720.57+6550.78	0.00117
				p_4	12034.98	720.57+6754.12	2.35E-8
				p_5	11956.9	720.57+6549.94	0.00117
				p_6	917.4	720.57+7056.78	3.2E-9
5×10^4 8	6000011, 8100003	12000022, 14100014	107.88	p_1	1437.88	2365.39+29418.92	0
				p_2	1400.75	2365.39+28902.74	0
				p_3	21546.87	2365.39+28484.5	9.27E-10
				p_4	21623.74	2365.39+29042.25	1.85E-14
				p_5	21069.6	2365.39+28149.49	9.26E-10
				p_6	1441.38	2365.39+28456.04	5.12E-16

Table 1: Results for the Bounded Retransmission Protocol

2.2 Crowds Protocol

TotalRuns, CrowdSize	Model size (state, trans)		Embed (t_1 in seconds)	Total model checking time (in seconds)		prob
	SDTMC	ADTMC		PRISM (t_2)	aut2bcg + CADP Model checking (t_3)	
10, 4	63922, 103962	127844, 167884	1.34	31.54	2.21+4.84	1
30, 2	80787, 110547	161574, 191334	1.53	35.63	2.88+4.43	1
40, 2	186182, 255062	372364, 441244	3.57	91.01	7.47+9.73	1
50, 2	357477, 490077	714954, 847554	6.93	170.96	16.77+27.62	1
20, 4	1321167, 2171247	2642334, 3492414	29.42	768.39	108.31+520.9	1
30, 4	8557737, 14122857	17115474, 22680594	164.75	5379.99	4884.8+59782.38	1

Table 2: Results for the Crowds protocol

2.3 Contract Signing Protocol

N L	Model size (state, trans)		Embed (t_1 in seconds)	Property number	Total model checking time (in seconds)		Prob
	SDTMC	ADTMC			PRISM (t_2)	aut2bcg + CADP Model checking (t_3)	
2 4	494, 509	988, 1003	0.01	p_1	1.43	0.11+2.11	0.625
				p_2	1.43	0.11+1.96	0.375
2 8	1006, 1021	2012, 2027	0.02	p_1	2.25	0.15+2.05	0.625
				p_2	2.33	0.15+2.12	0.375
2 16	2030, 2045	4060, 4075	0.05	p_1	4.52	0.26+2.17	0.625
				p_2	4.28	0.26+2.08	0.375
4 4	15102, 15357	30204, 30459	0.35	p_1	23.48	1.4+3.05	0.53125
				p_2	26.42	1.4+3.02	0.46875
4 8	31486, 31741	62972, 63227	0.73	p_1	61.87	3.02+4.18	0.53125
				p_2	72.59	3.02+4.13	0.46875
4 16	64254, 64509	128508, 128763	1.55	p_1	138.88	6.07+6.84	0.53125
				p_2	150.37	6.07+6.87	0.46875
8 2	3342334, 3407869	6684668, 6750203	82.61	p_1	6607.02	7029.01+5270.1	0.501953
				p_2	6972.67	7029.01+5492.24	0.498047
8 4	7536638, 7602173	15073276, 15138811	219.3	p_1	26121.04	26400.42+68253.31	0.501953
				p_2	22286.14	26400.42+46408.64	0.498047
8 8	15925246, 15990781	31850492, 31916027	401.1	p_1	53824.58	63348.52+227628.92	0.501953
				p_2	53857.49	63348.52+219431.09	0.498047

Table 3: Results for the Contract signing protocol

2.4 Synchronous Leader Election Protocol

N, K	Model size (state, trans)		Embed (t_1 in seconds)	Total model checking time (in seconds)		Prob
	SDTMC	ADTMC		PRISM (t_2)	aut2bcg + CADP Model checking (t_3)	
6, 2	335, 398	670, 733	0.01	0.85	0.08+1.89	1
6, 3	3759, 4487	7518, 8246	0.06	1.91	0.18+2	1
6, 4	20884, 24979	41768, 45863	0.36	7.49	0.73+2.85	1
6, 5	78784, 94408	157568, 45863	1.4	52.13	2.76+6.21	1
6, 6	234210, 280865	468420, 173192	4.19	307.38	17.52+22.42	1
6, 8	1312334, 1574477	2624668, 2886811	24.14	out of memory	453.61+638.43	1

Table 4: Results for the Synchronous leader election protocol

2.5 NAND Multiplexing

N, K	Model size (state, trans)		Embed (t_1 in seconds)	Total model checking time (in seconds)		Prob
	SDTMC	ADTMC		PRISM (t_2)	aut2bcg + CADP Model checking (t_3)	
2, 2	178, 243	356, 421	0.004	0.81	0.07+1.73	0.74342
5, 2	1728, 2505	3456, 4233	0.03	1.25	0.1+1.96	0.61125
10, 2	14322, 21567	28644, 35889	0.22	1.9	0.41+2.26	0.47284
20, 2	154942, 239832	309884, 394774	2.43	16.43	4.32+12.86	0.41286
20, 4	308162, 476472	616324, 784634	4.97	33.86	10.89+38.29	0.49415
20, 6	461382, 713112	922764, 1174494	7.41	51.59	17.12+79.92	0.51309
30, 2	681362, 1065797	1362724, 1747159	11.08	76.17	37.85+187.09	0.48760
30, 4	1358942, 2124557	2717884, 3483499	22.53	156.12	133.04+804.91	0.59635
30, 6	2036522, 3183317	4073044, 5219839	34.1	239.37	229.14+2127.94	0.61932
40, 2	2003082, 3150462	4006164, 5153544	33.9	257.29	283.97+1892.96	0.48380
40, 4	3999522, 6288542	7999044, 10288064	67.99	562.02	1100.87+12598	0.61868
40, 6	5995962, 9426622	11991924, 15422584	102.8	845.17	1965.94+34843	0.64387
50, 2	4679602, 7384827	9359204, 12064429	80.35	618.27	1551.19+20265.33	0.51128
50, 4	9348902, 14750427	18697804, 24099329	163.04	1314.16	6649.77+91082.95	0.66270
50, 6	14018202, 22116027	28036404, 36134229	239.84	1987.36	11675.94+213253.49	0.68803

Table 5: Results for the NAND multiplexing

3 Properties

3.1 Bounded Retransmission Protocol

PCTL formulas

$$p_1 : P =?[\, F\ (srep = 1\ \wedge\ rrep = 3\ \wedge\ recv)\,]$$
$$p_2 : P =?[\, F\ (srep = 3\ \wedge\ \neg(rrep = 3)\ \wedge recv)\,]$$
$$p_3 : P =?[\, F\ (s = 5)\,]$$
$$p_4 : P =?[\, F\ (s = 5\ \wedge\ srep = 2)\,]$$
$$p_5 : P =?[\, F\ (s = 5\ \wedge\ srep = 1\ \wedge\ i > 8)\,]$$
$$p_6 : P =?[\, F\ (\neg(srep = 0)\ \wedge \neg recv)\,]$$

APCTL in MCL syntax

3.1.1 Property 1

```
prob
(((if not(prob
{?act: String ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any
 where not(act = "BOT")}
is >= 1 end prob
or
prob
{?act: String ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any
 where act = "BOT"}
is > 0 end prob) then false end if)).true or tau)*.
if not(prob
{?act: String
 ?any
 ?srep:nat
 ?any ?any ?any ?any ?any ?any ?any
 ?rrep:nat
       ?any ?any ?any ?any
 ?recv:bool
 ?any ?any ?any
 where srep=1 and rrep=3 and recv and not(act="BOT")}
is >=1 end prob) then false end if
is >=? 0
end prob
```

3.1.2 Property 2

```
prob
(((if not(prob
{?act: String ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any
 where not(act = "BOT")}
is >= 1 end prob
or
prob
{?act: String ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any
 where act = "BOT"}
is > 0 end prob) then false end if)).true or tau)*.
if not(prob
{?act: String
 ?any
 ?srep:nat
 ?any ?any ?any ?any ?any ?any ?any
 ?rrep:nat
 ?any ?any ?any ?any
 ?recv:bool
 ?any
 ?any
 ?any
 where srep=3 and not(rrep=3) and recv and not(act="BOT")}
is >=1 end prob) then false end if
is >=? 0
end prob
```

3.1.3 Property 3

```
prob
(((if not(prob
{?act: String ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any
 where not(act = "BOT")}
is >= 1 end prob
or
prob
{?act: String ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any
 where act = "BOT"}
is > 0 end prob) then false end if)).true or tau)*.
if not(prob
{?act: String
 ?s:nat
 ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any
 where s=5 and not(act="BOT")}
is >=1 end prob) then false end if
is >=? 0
end prob
```

3.1.4 Property 4

```
prob
(((if not(prob
{?act: String ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any
 where not(act = "BOT")}
is >= 1 end prob
or
prob
{?act: String ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any
 where act = "BOT"}
is > 0 end prob) then false end if)).true or tau)*.
if not(prob
{?act: String
 ?s:nat
 ?srep:nat
 ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any
 where s=5 and srep=2 and not(act="BOT")}
is >=1 end prob) then false end if
is >=? 0
end prob
```

3.1.5 Property 5

```
prob
(((if not(prob
{?act: String ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any
 where not(act = "BOT")}
is >= 1 end prob
or
prob
{?act: String ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any
```

```
 where act = "BOT"}
is > 0 end prob) then false end if)).true or tau)*.
if not(prob
{?act: String
 ?s:nat
 ?srep:nat
 ?any
 ?i:nat
 ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any
 where s=5 and srep=1 and i>8 and not(act="BOT")}
is >=1 end prob) then false end if
is >=? 0
end prob
```

3.1.6 Property 6

```
prob
(((if not(prob
{?act: String ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any
 where not(act = "BOT")}
is >= 1 end prob
or
prob
{?act: String ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any
 where act = "BOT"}
is > 0 end prob) then false end if)).true or tau)*.
if not(prob
{?act: String
 ?any
 ?srep:nat
 ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any
 ?recv:bool
 ?any ?any ?any
 where not(srep=0) and recv=false and not(act="BOT")}
is >=1 end prob) then false end if
is >=? 0
end prob
```

3.2 Crowds Protocol

```
prob
(((if not(prob {?act: String ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any
?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any where not(act = "BOT")} is >= 1 end prob
or
prob {?act: String ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any
?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any where act = "BOT"}
is > 0 end prob) then false end if)).true or tau)*.
if not(prob {?act: String
 ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any
 ?observe0:int
 ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any
 where observe0 > 1 of int and not(act="BOT")}
is >=1 end prob) then false end if
is >=? 0
end prob
```

3.3 Contract signing protocol

3.3.1 Property 1

```
prob
(((if not(prob {?act: String ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any
 ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any
 ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any
 ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any
 ?any ?any ?any ?any where not(act = "BOT")} is >= 1 end prob
or
prob {?act: String
          ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any
 ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any
 ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any
 ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any
 ?any ?any where act = "BOT"} is > 0 end prob) then false end if)).true or tau)*.
if not(prob {?act: String
 ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any
          ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any
          ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any
          ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any
 ?knowB:bool
 ?knowA:bool
```

```
 where  not(knowA) and knowB and not(act="BOT")}
is >=1 end prob) then false end if
is >=? 0
end prob
```

3.3.2 Property 2

```
prob
(((if not(prob {?act: String ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any
 ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any
 ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any
 ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any
 ?any ?any ?any ?any where not(act = "BOT")} is >= 1 end prob
or
prob {?act: String ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any
 ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any
 ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any
 ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any
 ?any ?any where act = "BOT"} is > 0 end prob) then false end if)).true or tau)*.
if not(prob {?act: String
 ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any
          ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any
          ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any
          ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any
 ?knowB:bool
 ?knowA:bool
 where  not(knowB) and knowA and not(act="BOT")}
is >=1 end prob) then false end if
is >=? 0
end prob
```

3.4 Synchronous leader election protocol

3.4.1 For the models having $N = 3$

```
prob
(((if not(prob {?act: String ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any
 where not(act = "BOT")} is >= 1 end prob
or
prob {?act: String ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any where act = "BOT"}
 is > 0 end prob) then false end if)).true or tau)*.
if not(prob {?act: String
 ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any
 ?elected: bool
 where  elected=true and not(act="BOT")}
is >=1 end prob) then false end if
is >=? 0
end prob
```

3.4.2 For the models having $N = 4$

```
prob
(((if not(prob {?act: String ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any
 where not(act = "BOT")} is >= 1 end prob
or
prob {?act: String ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any
 where act = "BOT"} is > 0 end prob) then false end if)).true or tau)*.
if not(prob {?act: String
 ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any
 ?elected: bool
 where  elected=true and not(act="BOT")}
is >=1 end prob) then false end if
is >=? 0
end prob
```

3.4.3 For the models having $N = 5$

```
prob
(((if not(prob {?act: String ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any
 ?any ?any ?any ?any where not(act = "BOT")} is >= 1 end prob
or
prob {?act: String ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any
 ?any ?any where act = "BOT"} is > 0 end prob) then false end if)).true or tau)*.
if not(prob {?act: String ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any
      ?any ?any ?any
 ?elected: bool
```

```
 where  elected=true and not(act="BOT")}
is >=1 end prob) then false end if
is >=? 0
end prob
```

3.4.4 For the models having $N = 6$

```
prob
(((if not(prob {?act: String ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any
 ?any ?any ?any ?any ?any ?any ?any ?any where not(act = "BOT")} is >= 1 end prob
or
prob {?act: String ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any
 ?any ?any ?any ?any ?any ?any where act = "BOT"} is > 0 end prob) then false end if)).true or tau)*.
if not(prob {?act: String
 ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any ?any
          ?any ?any ?any
 ?elected: bool
 where  elected=true and not(act="BOT")}
is >=1 end prob) then false end if
is >=? 0
end prob
```

3.4.5 Bounded Until formula

This formula is for $N = 3$ and $L = 1$

```
prob
true{0 ... 8}.{!"BOT"
 ?any
 ?s1: nat
 ?any ?any ?any
 ?s2: nat
 ?any ?any ?any
 ?s3: nat
 ?any ?any ?any ?any
 where s1=3 and s2=3 and s3=3}
is >=? 0
end prob
```

This formula is for $N = 4$ and $L = 1$

```
 prob
 true{0 ... 10}.{!"BOT"
  ?any
  ?s1: nat
  ?any ?any ?any
  ?s2: nat
  ?any ?any ?any
  ?s3: nat
  ?any ?any ?any
  ?s4: nat
  ?any ?any ?any ?any
  where s1=3 and s2=3 and s3=3 and s4=3}
 is >=? 0
 end prob
```

3.5 NAND multiplexing

```
prob
(((if not(prob {?act: String ?any ?any ?any ?any ?any ?any ?any ?any where not(act = "BOT")} is >= 1 end prob
or
prob {?act: String ?any ?any ?any ?any ?any ?any ?any ?any where act = "BOT"} is > 0 end prob)
then false end if)).true or tau)*.
if not(prob {?act: String
 ?any
 ?any
 ?s:nat
 ?z:real
 ?any
 ?any
 ?any
 ?any
 where s=4 and z/2 of real < 0.1 of real and not(act="BOT")}
is >=1 end prob) then false end if
is >=? 0
end prob
```

Table 6: Table showing the upper bounds of the bounded until formula

N	K	L	Upper bound in PCTL	Upper bound in MCL
4	3	1	5	10
4	3	2	10	20
4	3	3	15	30
4	3	4	20	40
4	3	5	25	50
4	3	6	30	60
4	3	7	35	70
4	3	8	40	80
4	3	9	45	90
4	3	10	50	100
3	2	1	4	8
3	2	2	8	16
3	2	3	12	24
3	2	4	16	32
3	2	5	20	40
3	2	6	24	48
3	2	7	28	56
3	2	8	32	64
3	2	9	36	72
3	2	10	40	80

4 Tables and graphs of bounded until property of Case Study "Synchronous leader election protocol"

In this section, we compute the probability that a leader is elected within L rounds for $N = 3$, $N = 4$, and $N = 5$. For each value of N, we consider $K = 2, 3, 4, 5, 6$, and 8. For every combination of N and K, we vary L from 1 to 10.

$N = 3$ $\quad P =?[trueU <= L * (N + 1)(s1 = 3 \ \& \ s2 = 3 \ \& \ s3 = 3)]$

$N = 4$ $\quad P =?[trueU <= L * (N + 1)(s1 = 3 \ \& \ s2 = 3 \ \& \ s3 = 3 \ \& \ s4 = 3)]$

$N = 5$ $\quad P =?[trueU <= L * (N + 1)(s1 = 3 \ \& \ s2 = 3 \ \& \ s3 = 3 \ \& \ s4 = 3 \ \& \ s5 = 3)]$

In the graph, we have plotted the expected values with respect to L in the x-axis. **Models with value $N = 3$**

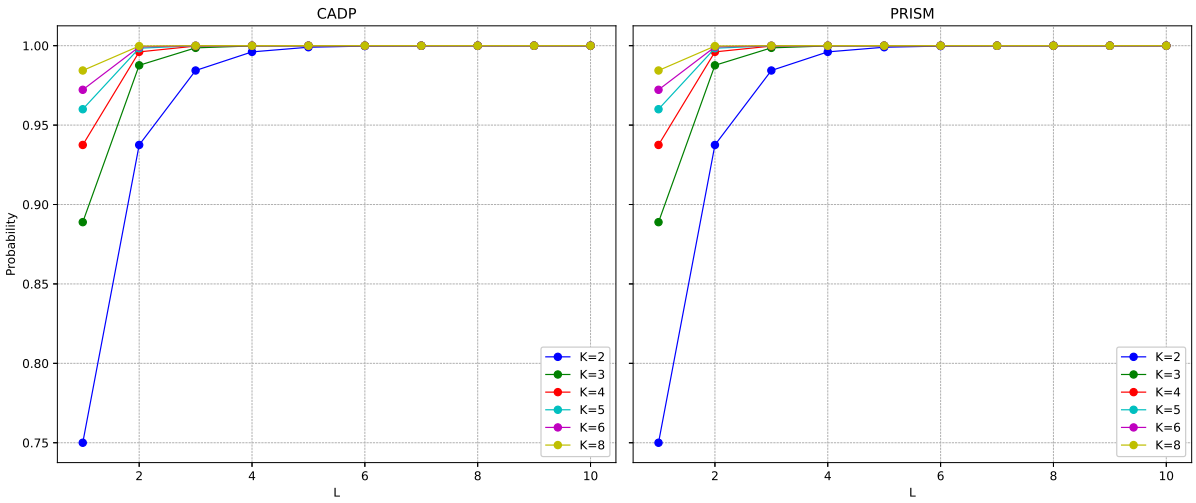

Figure 1: Table mapping the CADP and PRISM probabilities for model with parameter $N = 3$

Table 7: Probability values by CADP and PRISM for $N = 3$

N	K	L	CADP probability value	PRISM probability value
3	2	1	0.75	0.75
3	2	2	0.9375	0.9375
3	2	3	0.984375	0.984375
3	2	4	0.996094	0.99609375
3	2	5	0.999023	0.9990234375
3	2	6	0.999756	0.999755859375
3	2	7	0.999939	0.99993896484375
3	2	8	0.999985	0.9999847412109375
3	2	9	0.999996	0.9999961853027344
3	2	10	0.999999	0.9999990463256836
3	3	1	0.888889	0.8888888888888884
3	3	2	0.987654	0.9876543209876535
3	3	3	0.998628	0.9986282578875164
3	3	4	0.999848	0.9998475842097233
3	3	5	0.999983	0.9999830649121907
3	3	6	0.999998	0.9999981183235761
3	3	7	1	0.9999997909248411
3	3	8	1	0.999999976769426
3	3	9	1	0.9999999974188245
3	3	10	1	0.9999999997132021
3	4	1	0.9375	0.9375
3	4	2	0.996094	0.99609375
3	4	3	0.999756	0.999755859375
3	4	4	0.999985	0.9999847412109375
3	4	5	0.999999	0.9999990463256836
3	4	6	1	0.9999999403953552
3	4	7	1	0.9999999962747097
3	4	8	1	0.9999999997671694
3	4	9	1	0.9999999999854481
3	4	10	1	0.9999999999990905
3	5	1	0.96	0.9600000000000007
3	5	2	0.9984	0.9984000000000008
3	5	3	0.999936	0.9999360000000008
3	5	4	0.999997	0.999997440000001
3	5	5	1	0.9999998976000007
3	5	6	1	0.9999999959040008
3	5	7	1	0.9999999998361608
3	5	8	1	0.9999999999934472
3	5	9	1	0.9999999999997388
3	5	10	1	0.9999999999999903
3	6	1	0.972222	0.9722222222222251
3	6	2	0.999228	0.9992283950617316
3	6	3	0.999979	0.9999785665294953
3	6	4	0.999999	0.9999994046258223
3	6	5	1	0.9999999834618314
3	6	6	1	0.9999999995406093
3	6	7	1	0.999999999987242
3	6	8	1	0.9999999999996486
3	6	9	1	0.9999999999999931
3	6	10	1	1.0000000000000029
3	8	1	0.984375	0.984375
3	8	2	0.999756	0.999755859375
3	8	3	0.999996	0.9999961853027344
3	8	4	1	0.9999999403953552
3	8	5	1	0.9999999990686774
3	8	6	1	0.9999999999854481
3	8	7	1	0.9999999999997726
3	8	8	1	0.9999999999999964
3	8	9	1	1.0
3	8	10	1	1.0

Models with value $N = 4$

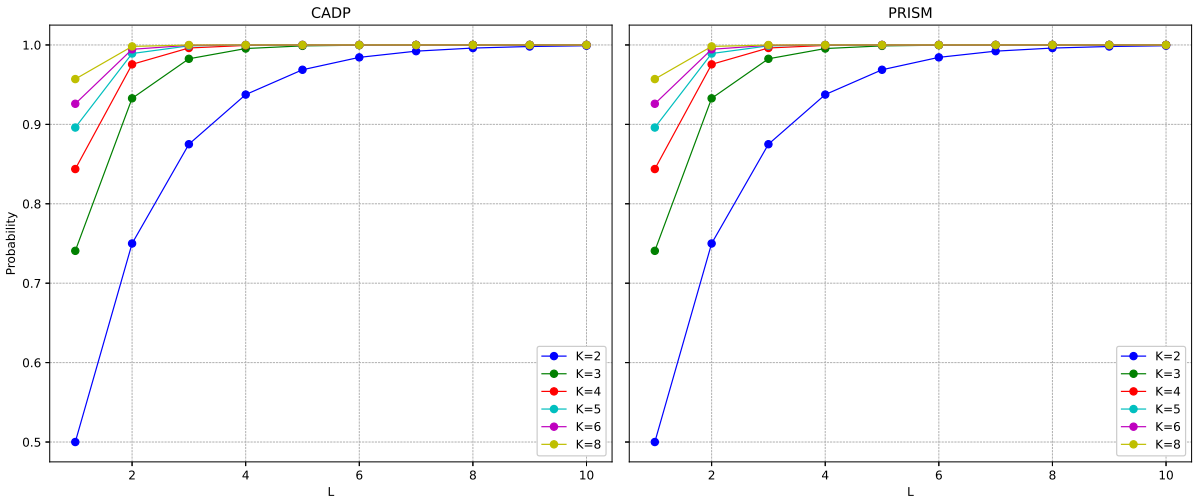

Figure 2: Table mapping the CADP and PRISM probabilities for the model with parameter $N = 4$

Table 8: Probability values by CADP and PRISM for $N = 4$

N	K	L	CADP probability value	PRISM probability value
4	2	1	0.5	0.5
4	2	2	0.75	0.75
4	2	3	0.875	0.875
4	2	4	0.9375	0.9375
4	2	5	0.96875	0.96875
4	2	6	0.984375	0.984375
4	2	7	0.992188	0.9921875
4	2	8	0.996094	0.99609375
4	2	9	0.998047	0.998046875
4	2	10	0.999023	0.9990234375
4	3	1	0.740741	0.7407407407407418
4	3	2	0.932785	0.9327846364883418
4	3	3	0.982574	0.9825737946451257
4	3	4	0.995482	0.995482094907996
4	3	5	0.998829	0.9988286912724443
4	3	6	0.999696	0.9996963273669313
4	3	7	0.999921	0.9999212700580946
4	3	8	0.99998	0.9999795885335816
4	3	9	0.999995	0.999994708138338
4	3	10	0.999999	0.9999986280358656
4	4	1	0.84375	0.84375
4	4	2	0.975586	0.9755859375
4	4	3	0.996185	0.996185302734375
4	4	4	0.999404	0.9994039535522461
4	4	5	0.999907	0.9999068677425385
4	4	6	0.999985	0.9999854480847716
4	4	7	0.999998	0.9999977262632456
4	4	8	1	0.9999996447286321
4	4	9	1	0.9999999444888488
4	4	10	1	0.9999999913263826
4	5	1	0.896	0.8960000000000092
4	5	2	0.989184	0.9891840000000127
4	5	3	0.998875	0.9988751360000127
4	5	4	0.999883	0.9998830141440133
4	5	5	0.999988	0.9999878334709892
4	5	6	0.999999	0.9999987346809942
4	5	7	1	0.9999998684068346
4	5	8	1	0.9999999863143206
4	5	9	1	0.9999999985766995
4	5	10	1	0.9999999998519886
4	6	1	0.925926	0.9259259259258992
4	6	2	0.994513	0.9945130315500353
4	6	3	0.999594	0.9995935578925635
4	6	4	0.99997	0.9999698931772002
4	6	5	0.999998	0.999997769864947
4	6	6	1	0.9999998348047807
4	6	7	1	0.9999999877632894
4	6	8	1	0.9999999990935462
4	6	9	1	0.9999999999328276
4	6	10	1	0.9999999999949966
4	8	1	0.957031	0.95703125
4	8	2	0.998154	0.9981536865234375
4	8	3	0.999921	0.999920666217804
4	8	4	0.999997	0.9999965911265463
4	8	5	1	0.9999998535249688
4	8	6	1	0.999999993706151
4	8	7	1	0.9999999997295635
4	8	8	1	0.9999999999883775
4	8	9	1	0.9999999999994967
4	8	10	1	0.9999999999999802

Models with value $N = 5$

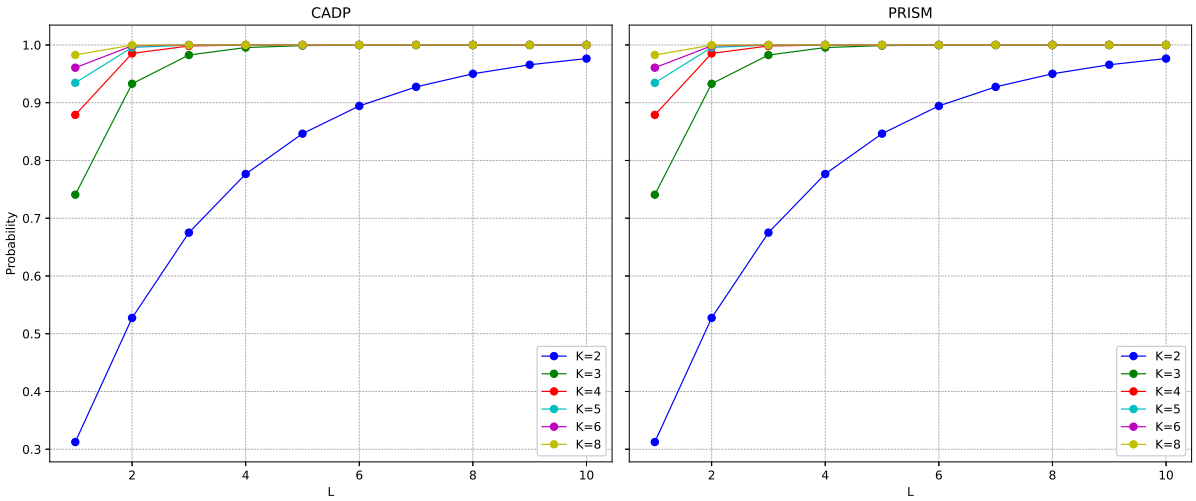

Figure 3: Table mapping the CADP and PRISM probabilities for the model with parameter $N = 5$

Table 9: Probability values by CADP and PRISM for $N = 5$

N	K	L	CADP probability value	PRISM probability value
5	2	1	0.3125	0.3125
5	2	2	0.527344	0.52734375
5	2	3	0.675049	0.675048828125
5	2	4	0.776596	0.7765960693359375
5	2	5	0.84641	0.846409797668457
5	2	6	0.894407	0.8944067358970642
5	2	7	0.927405	0.9274046309292316
5	2	8	0.950091	0.9500906837638468
5	2	9	0.965687	0.9656873450876446
5	2	10	0.97641	0.9764100497477557
5	3	1	0.740741	0.7407407407407387
5	3	2	0.932786	0.9327846364883379
5	3	3	0.982575	0.9825737946451223
5	3	4	0.995483	0.9954820949079933
5	3	5	0.99883	0.9988286912724397
5	3	6	0.999698	0.9996963273669253
5	3	7	0.999922	0.999921270058091
5	3	8	0.999981	0.9999795885335758
5	3	9	0.999996	0.9999947081383331
5	3	10	1	0.999998628035862
5	4	1	0.878906	0.87890625
5	4	2	0.985336	0.9853363037109375
5	4	3	0.998224	0.9982243180274963
5	4	4	0.999784	0.9997849760111421
5	4	5	0.999973	0.9999739619388492
5	4	6	0.999996	0.9999968469535325
5	4	7	0.999999	0.9999996181857798
5	4	8	0.999999	0.9999999537646866
5	4	9	0.999999	0.9999999944011939
5	4	10	0.999999	0.9999999993220174
5	5	1	0.9344	0.9343999999999674
5	5	2	0.995697	0.9956966399999704
5	5	3	0.999718	0.9997176995839668
5	5	4	0.999981	0.9999814810926732
5	5	5	0.999999	0.9999987851596481
5	5	6	1	0.9999999203064366
5	5	7	1	0.999999994772068
5	5	8	1	0.9999999996570184
5	5	9	1	0.9999999999774722
5	5	10	1	0.9999999999984861
5	6	1	0.960648	0.9606481481480117
5	6	2	0.998451	0.9984514317556756
5	6	3	0.999939	0.9999390609717145
5	6	4	0.999998	0.9999976019362344
5	6	5	1	0.9999999056315987
5	6	6	1	0.9999999962862788
5	6	7	1	0.9999999998537179
5	6	8	1	0.9999999999941
5	6	9	1	0.9999999999996296
5	6	10	1	0.9999999999998415
5	8	1	0.982667	0.982666015625
5	8	2	0.9997	0.9996995329856873
5	8	3	0.999996	0.9999947917094687
5	8	4	1	0.9999999097195733
5	8	5	1	0.9999999984350856
5	8	6	1	0.9999999999728808
5	8	7	1	0.999999999999543
5	8	8	1	0.999999999999997
5	8	9	1	1
5	8	10	1	1