Verifying Randomized Consensus Protocols with Common Coins
验证使用公共硬币的随机化共识协议

高嵩，詹博华，吴志林，张立军

发表于国际学术会议 International Conference on Dependable Systems and Networks (DSN 2024)

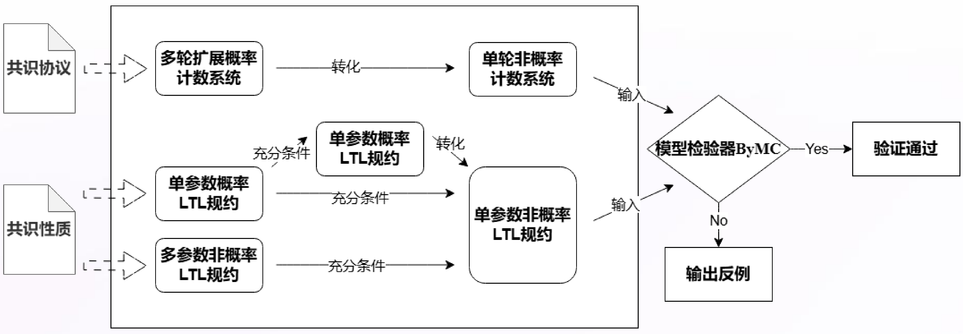
联系方式：高嵩 gaos@ios.ac.cn 18813135282

背景介绍

共识协议是分布式系统的基石，其中随机化共识协议在效率、容错、去中心化等方面具有独特的优势，适用于区块链等场景，而公共硬币是为其提供随机性的一种重要抽象。本文提出了一种对使用公共硬币的随机化共识协议进行**形式化建模**并**参数化验证**的方法。

论文创新点

1. 基于阈值自动机提出可处理公共硬币的**概率计数系统模型的扩展**
2. 证明多轮扩展概率计数系统模型上的共识性质参数化验证问题可以**转化**为已解决的单轮非概率计数系统上的验证问题
3. 提出并证明概率终止性对应的单参数非概率**充分条件**



整体思路

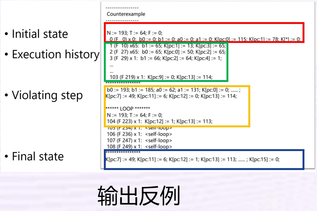
实验结果

实验基准由8个使用公共硬币的随机化共识协议组成，使用**模型检验器ByMC**对协议的共识性质，即**一致性**、**有效性**和**概率终止性**，进行参数化验证。对于其中7个协议成功验证了在任意规模的系统中都满足共识性质，对于一个已知存在终止性缺陷的协议则能够自动地找出反例：

N-阈值自动机					一致性		有效性
协议	类别	$\|\mathcal{L}\|$	$\|\mathcal{R}\|$	SMT 查询数量	运行时间	SMT 查询数量	运行时间
Rabin83	(*A*)	10	15	6	0.25	2	0.20
CC85(a)	(*B*)	9	18	342	4.93	42	0.50
CC85(b)	(*B*)	10	17	6	0.25	2	0.20
FMR05	(*B*)	10	16	6	0.23	2	0.21
KS16	(*B*)	11	26	18	0.75	5	0.31
MMR14	(*C*)	17	35	28918	298.90	1442	8.74
Miller18	(*C*)	22	48	$> 10^7$	**TO**	$> 10^5$	**TO**
ABY22	(*C*)	22	49	$> 10^7$	**TO**	$> 10^5$	**TO**
Miller18(mpi)	(*C*)	22	48	$> 10^8$	605	253534	226
ABY22(mpi)	(*C*)	22	49	$> 10^8$	583	106098	71

P-阈值自动机					概率终止性	
协议	类别	$\|\mathcal{L}\|$	$\|\mathcal{R}\|$	SMT 查询数量（总和）	运行时间（总和）
Rabin83	(*A*)	10	11	8	0.43
CC85(a)	(*B*)	9	16	171.5	3.36
CC85(b)	(*B*)	10	15	8	0.40
FMR05	(*B*)	10	11	2	0.41
KS16	(*B*)	11	28	15	1.02
MMR14	(*C*)	17	34	⊗	⊗
Miller18	(*C*)	22	47	$> 10^5$	**TO**
ABY22	(*C*)	22	48	$> 10^5$	**TO**
Miller18(mpi)	(*C*)	22	47	$> 10^8$	16h 08m 18s
ABY22(mpi)	(*C*)	22	48	$> 10^8$	13h 36m 57s

三个共识性质的参数化验证实验结果



输出反例