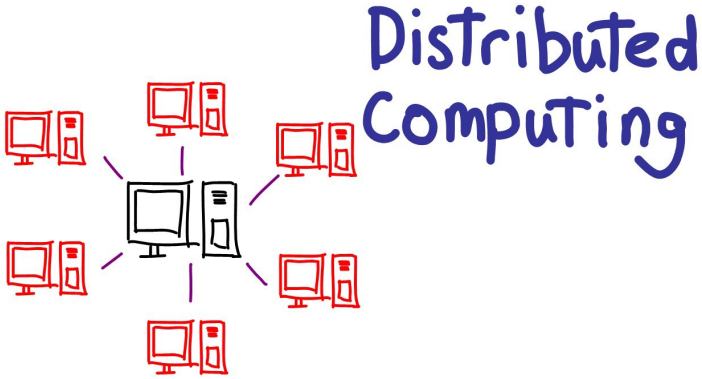
Android + 形式化方法 = ?

黄宇　　魏恒峰

南京大学计算机软件研究所

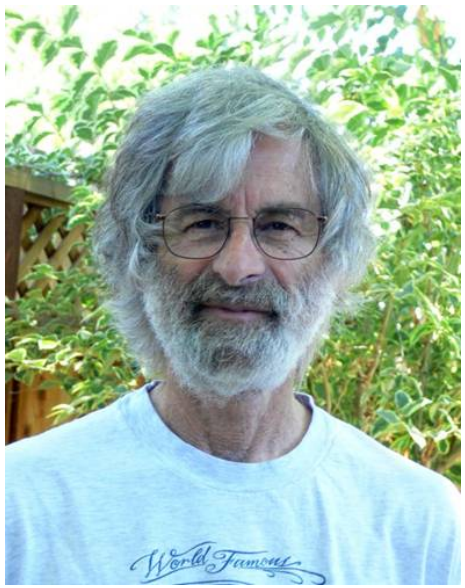
2019 年 03 月 28 日

用“逻辑”的方法保证系统的正确性



用“逻辑”的方法保证分布式协议的正确性

模型检验/定理证明: 使用 TLA+/TLAPS



TLA+ 小组: Disalg-ICS-NJU/tlaplus-projects@github

TLA+ 小组: Disalg-ICS-NJU/tlaplus-projects@github

Jupiter: 验证协同编辑应用核心协议的正确性

TPaxos: 验证腾讯所发表的 Consensus 协议的正确性

CRDT: 验证分布式数据结构的正确性

Engineers use TLA+ to prevent serious but subtle bugs from reaching production.

BY CHRIS NEWCOMBE, TIM RATH, FAN ZHANG, BOGDAN MUNTEANU, MARC BROOKER, AND MICHAEL DEARDEUFF

How Amazon Web Services Uses Formal Methods

Applying TLA+ to some of Amazon's more complex systems.

System	Components	Line Count (Excluding Comments)	Benefit
S3	Fault-tolerant, low-level network algorithm	804 PlusCal	Found two bugs, then others in proposed optimizations
	Background redistribution of data	645 PlusCal	Found one bug, then another in the first proposed fix
DynamoDB	Replication and group-membership system	939 TLA+	Found three bugs requiring traces of up to 35 steps
EBS	Volume management	102 PlusCal	Found three bugs
Internal distributed lock manager	Lock-free data structure	223 PlusCal	Improved confidence though failed to find a liveness bug, as liveness not checked
	Fault-tolerant replication-and-reconfiguration algorithm	318 TLA+	Found one bug and verified an aggressive optimization

"Engineers use TLA+ to prevent serious but subtle bugs from reaching production."


Model
Checking
Verification
Systems
Analysis
Logic
Distributed
Software
Testing
Runtime
Abstraction
Embedded
Languages
Algorithms
Representation
Succinct
Parameterized
Concurrent
Models
Program
Scheduling

挑战与机遇


THANK YOU