Workshop: TLA$^+$ in Action

Hydraconf

Markus A. Kuppe (@lemmster)

Microsoft

June 2021

TLA+ Workshop material

The workshop material can be found at the following locations:

- https://git.io/JZxUh
- https://aka.ms/tlaewd998
- https://github.com/lemmy/ewd998
- => Please consider “starring” the Github repository

TLA+ Workshop

- Interactive & Hands-on
  - "Write" a TLA+ spec and meet the tools
  - Zoom *meeting*
  - Git repository (each commit represents a concept)
    - If you miss a beat, skip to the next commit
    - Weeks of debugging save hours of TLA+
- 4x 1.25h over 2 days totaling 5h
  - Not exhaustive (breadths over depths)
  - "Specifying Systems" or "TLA+ in Practice and Theory" for depth

http://etc.ch/ziM6

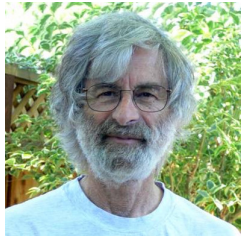
My Background

- Not a mathematician (logician), but software engineer
- Learned TLA+ by working on its tools (~decade)
- Wrote many TLA+ specs related to the tools, examples, ...

http://etc.ch/ziM6

TLA$^+$ 30.000ft above

TLA$^+$ is a specification language to design, document, and verify reactive systems.



Leslie Lamport

Specify Large Systems in TLA+

- DynamoDB: scalable high-performance "no SQL" data store with cross datacenter replication and strong consistency guarantees
- First informal proofs and excessive (fault-injecting) testing

Specify Large Systems in TLA+

- DynamoDB: scalable high-performance "no SQL" data store with cross datacenter replication and strong consistency guarantees
- First informal proofs and excessive (fault-injecting) testing

- TLC found very subtle bug: shortest error trace 35 steps
- "Using TLA+ in place of traditional proof writing would thus likely have improved time to market, in addition to achieving greater confidence in the system's correctness." [Newcombe, 2014, Newcombe et al., 2015]

Your background

- https://directpoll.com/r?XDbzPBd3ixYqg8AIK7KI7E0zwD6RtEdWCc3UvSu

Bibliography

Chris Newcombe. Why Amazon Chose TLA+. In David Hutchison, Takeo Kanade, Josef Kittler, Jon M. Kleinberg, Alfred Kobsa, Friedemann Mattern, John C. Mitchell, Moni Naor, Oscar Nierstrasz, C. Pandu Rangan, Bernhard Steffen, Demetri Terzopoulos, Doug Tygar, Gerhard Weikum, Yamine Ait Ameur, and Klaus-Dieter Schewe, editors, Abstract State Machines, Alloy, B, TLA, VDM, and Z, volume 8477, pages 25–39. Springer Berlin Heidelberg, Berlin, Heidelberg, 2014. ISBN 978-3-662-43651-6 978-3-662-43652-3. URL http://link.springer.com/10.1007/978-3-662-43652-3_3.

Chris Newcombe, Tim Rath, Fan Zhang, Bogdan Munteanu, Marc Brooker, and Michael Deardeuff. How Amazon Web Services Uses Formal Methods. Communications of the ACM, 58(4):66–73, March 2015. ISSN 00010782. doi: 10.1145/2699417. URL http://dl.acm.org/citation.cfm?doid=2749359.2699417.