Today’s critical software is still often vulnerable
System software is where vulnerability has the worst effects
Goal: Verify Google pKVM an hypervisor for Android (≈10kLoC)
Verify: Mathematical proof – not just testing.
Need mathematical models of the interface hardware provides
Such a model doesn’t exist
My PhD: Help build such a model and figure out how to reason about it.
In particular: Arm concurrent behavior for virtual memory systems