2021-03-02 Meeting with Shashank Nuthakki

* Could you walk us through the designs you ran SQED + SSS on? (Vscale, Ridecore, anything else?)
  + Did Eshan run this for OpenSPARC V2?
  + Focused on speed, used small cores
* Were there any notable modifications you had to apply to these designs?
  + CSR Register File, Memory Load Store, Etc
  + Processor bit-width
  + Modifications
    - Most modifications were to existing bugs
    - Actual
    - Found in the folder structure
    - Mostly cosmetic changes
  + Why couldn’t catch all Extremal bugs?
    - If the tool could increase depth, could have found it
  + There is a restriction on the symbolic state, and from the subset that we can start from, we bound the number of unrolled cycles.
  + CSR Register File
    - Supporting these instructions
* Max run time?
  + 24 hours, just marked as unfound if bug did not get detected before then
* What was your thought process when developing your constraints and axioms for SSS?
  + We started with small designs, wanted QED style tests
  + Would add in constraints specific for some designs - but how to generalize this? Came up with those 3 generic constraints for general designs.
* In particular, did you discover Constraint-3/Axiom-2 (RAW dependencies) empirically by running experiments and analyzing the counterexamples? We are interested in developing a general methodology that allows us to identify sufficient constraints related to design features other than pipelines.
  + Started with constrains from previous QED papers (2-3 things from previous work)
    - What were these initial constraints?
      * Did not remember exactly…
      * Final things are in the draft
  + Did not have formal proof before all constraints - had to iterate on those constraints. Had to see what was “generic” across the examples.
* It seems that the 3rd constraint and the 2nd axiom say the same thing - could you elaborate on why they are stated twice?
  + Axioms are not QED specific, we have to assume these are true
  + Constraints are specific to QED
  + Experimentally need to tease out difference between C3 and A2
  + A2 may not hold out of the box for an arbitrary starting state
    - If you remove C3, A2 may not hold.
    - Are axioms not something we want to hold for all states? Even if not reachable.
    - Need to add this into our new proof?
* Are there any notable exceptions to these constraints that we should address?
  + Apparently not on Vscale/Ridecore
* Are there any other resources / directories we should be looking at?
  + We currently have a hardware trojan example on vscale and a folder full of different results on ridecore
  + Python scripts at top level will generate these extremal bugs
* Could you think of other designs that could potentially be interesting to analyze? (BOOM, …?)
  + Both of the current designs are RISC-V ISA and have small ISA subset
  + Go for larger ISA designs, see how the technique applies there