Databases and Database Security

Abraham J. Reines

March 22, 2024

5.4.1 - Typesetting and Model-Checking HourClock

Replacing Author and Date

Module Replacement:

```
---------------------- MODULE HourClock3 ----------------------
EXTENDS Naturals
(* Abraham J. Reines, 03/20/2024 *)
VARIABLE hr
HCini  ==  hr ∈ (1 .. 11)
HCnxt  ==  hr' = IF hr ≠ 12 THEN hr + 1 ELSE 1
HC  ==  HCini / □[HCnxt]_hr
-------------------------------------------------------------
THEOREM  HC => □HCini
=============================================================
```

System Specification Explanation

The system specification of the `HourClock.tla` is explained as follows:

- The module, named `HourClock3`, employs natural numbers from the extended module `Naturals`.
- Authored by Abraham J. Reines on March 20, 2024, it defines a variable `hr` representing the clock's hour.
- `HCini` sets the initial condition, constraining `hr` to be within 1 to 11, indicating the starting range for the clock.
- The transition function `HCnxt` describes the clock's behavior for the subsequent state. Should `hr` not equal 12, it increments by 1; otherwise, it cycles back to 1.
- The clock's behavior is encapsulated in `HC`, which asserts that the clock starts with `HCini` and consistently adheres to `HCnxt` for all following states.
- Lastly, a theorem `HC ⇒ []HCini` is posited, claiming that if `HC` is valid, then `HCini` invariably remains true, suggesting that the clock should perpetually stay within the 1 to 11 range, which contradicts the inclusive nature of a 12-hour cycle.

It should be noted that the specification appears to improperly represent the 12-hour mark, as the initial condition excludes 12 and the theorem implies the clock should never indicate 12, which is inconsistent with standard 12-hour clock behavior.

Typeset Specification

The typeset specification of `HourClock.tla` can be found in Figure 1.

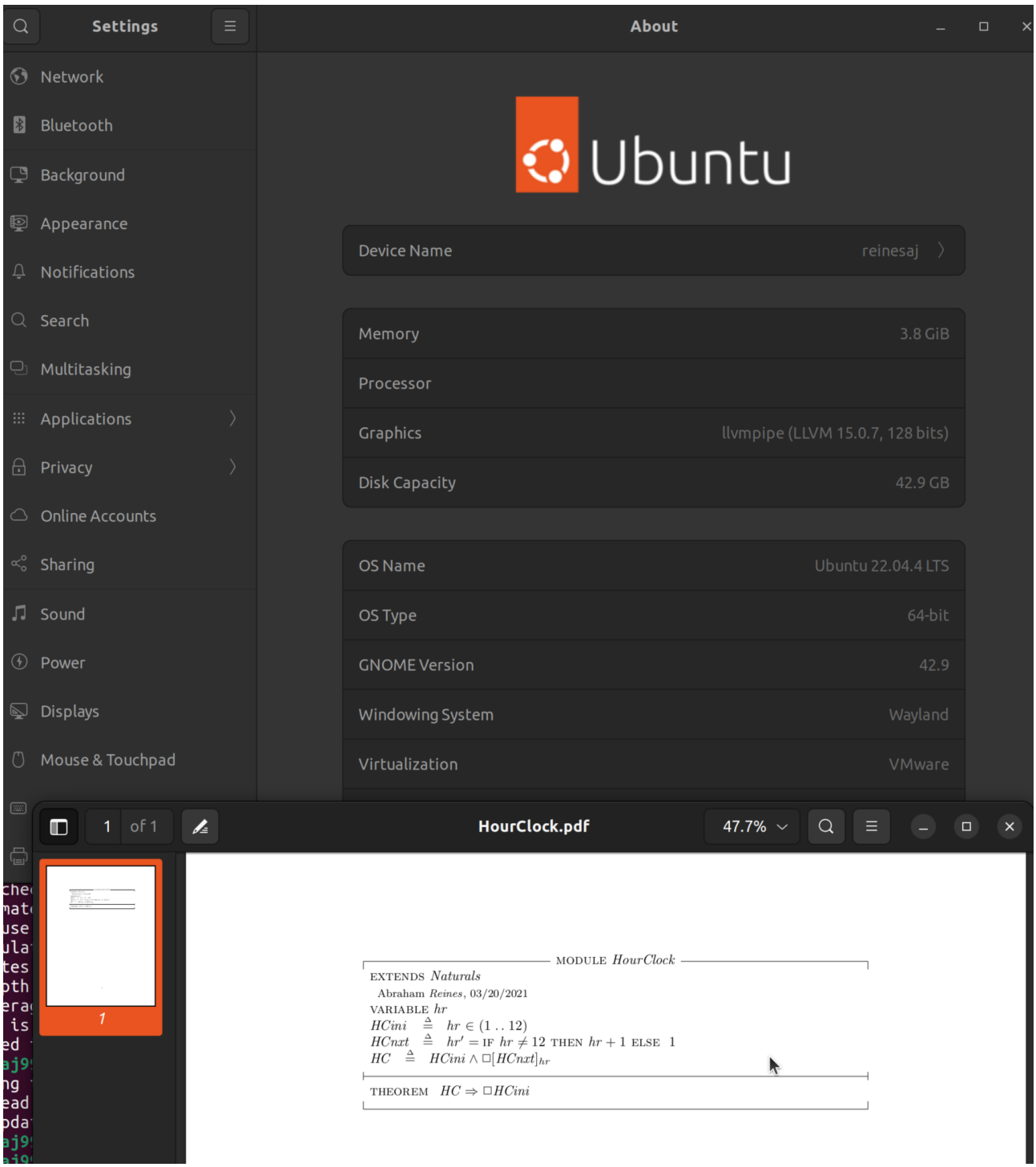

Figure 1: Typeset `HourClock.tla` specification.

Model-Checking Results

The results of the model-checking on `HourClock.tla` are presented in Figure 2.

```
reinesaj99@reinesaj:~/Desktop$ java -classpath tla2tools.jar tlc2.TLC HourClock.tla
TLC2 Version 2.16 of 31 December 2020 (rev: cdddf55)
Warning: Please run the Java VM which executes TLC with a throughput optimized garbage collector by p
assing the "-XX:+UseParallelGC" property.
(Use the -nowarning option to disable this warning.)
Running breadth-first search Model-Checking with fp 99 and seed 6344607557002230172 with 1 worker on
4 cores with 978MB heap and 64MB offheap memory [pid: 466327] (Linux 5.15.0-101-generic aarch64, Ubun
tu 11.0.22 x86_64, MSBDiskFPSet, DiskStateQueue).
Parsing file /home/reinesaj99/Desktop/HourClock.tla
Parsing file /tmp/Naturals.tla
Semantic processing of module Naturals
Semantic processing of module HourClock
Starting... (2024-03-20 14:51:18)
Computing initial states...
Computed 2 initial states...
Computed 4 initial states...
Computed 8 initial states...
Finished computing initial states: 12 distinct states generated at 2024-03-20 14:51:18.
Model checking completed. No error has been found.
  Estimates of the probability that TLC did not check all reachable states
  because two distinct states had the same fingerprint:
  calculated (optimistic):  val = 7.8E-18
24 states generated, 12 distinct states found, 0 states left on queue.
The depth of the complete state graph search is 1.
The average outdegree of the complete state graph is 0 (minimum is 0, the maximum 0 and the 95th perc
entile is 0).
Finished in 00s at (2024-03-20 14:51:18)
```

Figure 2: Model-checking results of `HourClock.tla`.

Academic Integrity Pledge

"This work complies with the JMU honor code. I did not give or receive unauthorized help on this assignment."

References

1. blah