Week-6

L1 Logic Coverage eg. 2

- detecting type of Δ. 1 → scalene, 2 → isoceles, 3 → eqε. 4 → not a Δ.
- If there is an int. variable, solve it in terms of inputs.

L2 Logic Coverage Specificaⁿ

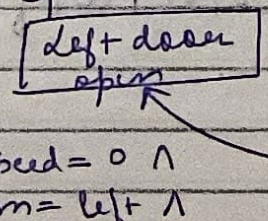
- Specifications can be in formal lang. or Eng. They have several logical conditions. If given in Eng., we need to derive logical predicates from the specificaⁿ & then apply logic criteria as relevant.

Eg. name must't be empty, state must be valid, pin 6 digits
name != "" ∧ state in list ∧ (pin >= 000000 ∧ pin <= 999999)

- A CNF (conjunctive normal form) if it consists of clauses or disjuncts connected by conjuncⁿ operator (and). For a predicate of a ∧ b ∧ c, a major clause is made active by making all other clauses True.
- A DNF → consists of clauses of conjuncts connected by disjuncⁿ op. Eg a ∨ b ∨ c. A major clause is made active by making all other clauses false.

L3 FSMs

- Transitions in FSMs have gaurds which are logical expressions.
- Train eg.



trainSpeed = 0 ∧
platform = left ∧
(locaⁿ = insta ∨
(emergStop ∧ doorsOpen ∧ locaⁿ = inTunnel))

- predicate has 6 clauses
- FSM model has 2 locaⁿ – inStaⁿ & inTunnel. They both are false in ITR, which is not possible ⇒ error

L4 Logic Coverage Summary

- Predicate transformaⁿ deals with re-writing the predicates in the prog. so that they have only 1 clause each. It is mandatory for security testing where multiple clauses can lead to issues.
- ACC criteria is expensive for testers and can be overcome by re-writing the predicate.
- PT involves Δing the control structure of the prog. using nested decision statements that represent how the various clauses in the predicate are connected to each other. The resulting prog. is difficult to read & maintain & hence not recommended.
- ACC criteria on the re-written prog. are not always eqv to the criteria on original prog.

eg. `if (a && b):` ⟹

```
if (a)
{
  if (b)
    S1
  else S2
}
else:
  S2
```

tr: {(t,t), (t,f), (f,t)}

tr: {(t,t), (t,f), (f,f)}

L5 SMT Solvers

- The SAT problem determines if there exists an assignment of T/F values that satisfies a given propositional logic formula. It is NP-complete.
- But we deal with predicate logic, the SAT problem is undecidable. But some instances are decidable.
- Satisfiability modulo theories (SMT) is the problem of determining whether a given predicate is satisfiable.
- SMT solver uses SAT solver as underlying engine. They are used extensively in formal verification & program analysis, for proving the correctness of prog.