Model-Checking

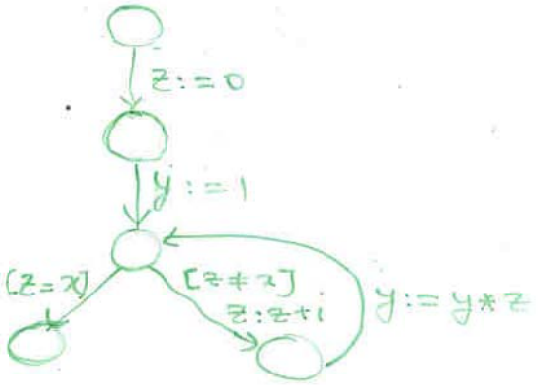
- In many applications, we have model of system we want to verify

  Examples: Protocols, hardware systems, logic control software, etc.

- For programs models can be extracted as control flow graphs.

Example:

```
z := 0
y := 1
while (z ≠ x) do {
z := z+1
y := y * z }
```



A control flow graph is a state-transition system with states representing program control state and transitions have two lables:

(i) enabling guard (1^{st}-order predicate), and (missing ⇒ guard = True)

(ii) assignment that assigns variables a new expression (missing ⇒ identity assignment)

Model-checking: Given a model and a specification (the property model should satisfy) verify whether model satisfies property.

Model ≡ Typically a state-transition system
Specification ≡ Typically a temporal-logic formula.

- Temporal Logic is used to specify property of a seq/tree of states
  Propositional/predicate logic can only specify property of a given state.