# COURSE STRUCTURE

**CONSTRAINT SOLVERS**

- Propositional Logic, SAT solving, DPLL
- First-Order Logic, SMT
- First-Order Theories

**DEDUCTIVE VERIFICATION**

- Operational Semantics
- Strongest Post-condition, Weakest Pre-condition
- Hoare Logic

**MODEL CHECKING AND OTHER VERIFICATION TECHNIQUES**

- Abstract Interpretation
- Predicate Abstraction, CEGAR
- Property-directed Reachability

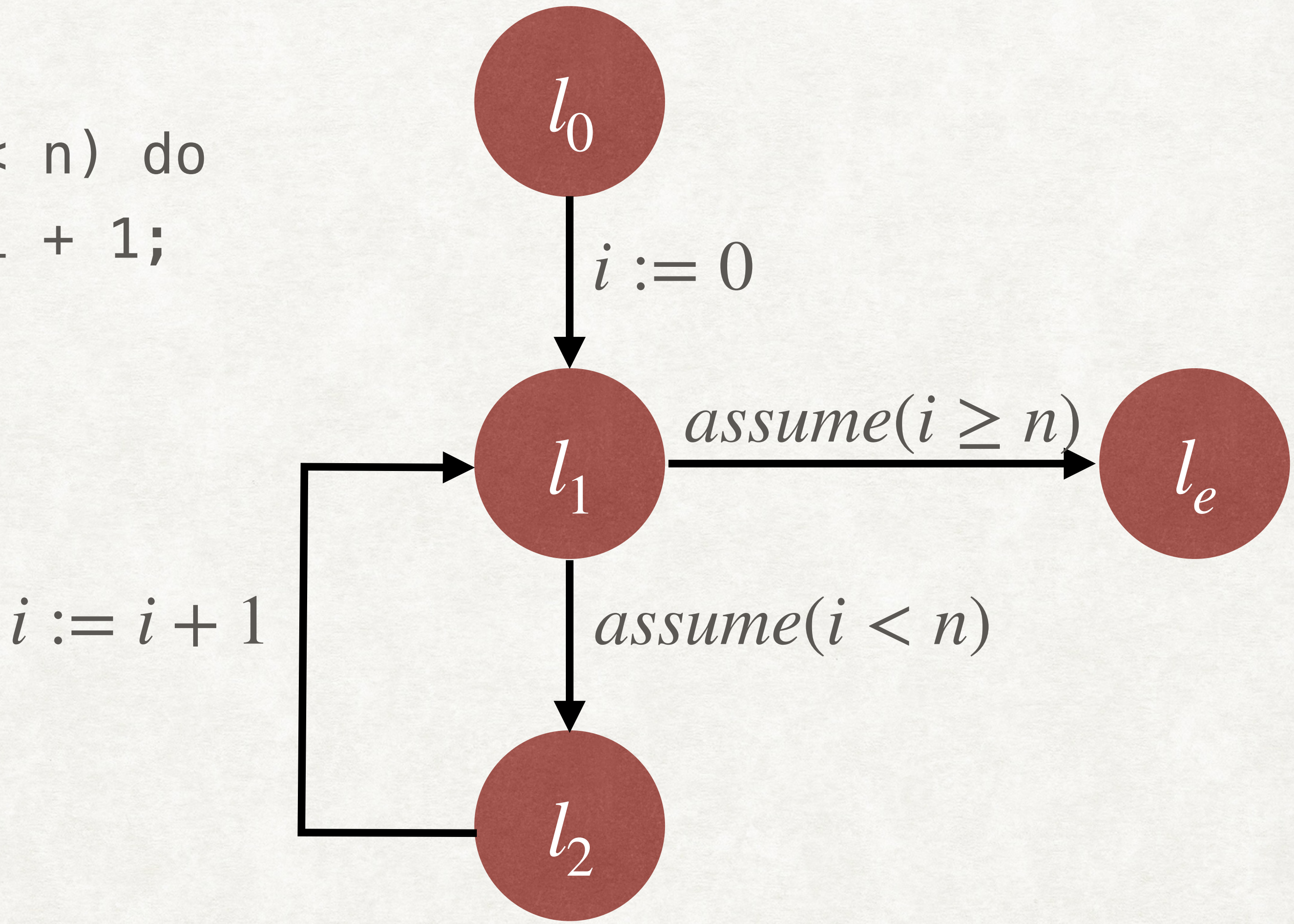
# ABSTRACT INTERPRETATION

# LABELLED TRANSITION SYSTEM

- We express the program $c$ as a labelled transition system $\Gamma_c \equiv (V, L, l_0, l_e, T)$
  - $V$ is the set of program variables
  - $L$ is the set of program locations
  - $l_0$ is the start location
  - $l_e$ is the end location
  - $T \subseteq L \times c \times L$ is the set of labelled transitions between locations.

# EXAMPLE

```
i := 0;
while(i < n) do
    i := i + 1;
```



# PROGRAMS AS LTS

- There are various ways to construct the LTS of a program
  - We can use control flow graph
  - We can use basic paths as defined by the book (BM Chapter 5). A basic path is a sequence of instructions that begins at the start of the program or a loop head, and ends at a loop head or the end of the program.
- Program State $(\sigma, l)$ consists of the values of the variables $(\sigma : V \to \mathbb{R})$ and the location.
- An execution is a sequence of program states, $(\sigma_0, l_0), (\sigma_1, l_1), \ldots, (\sigma_n, l_n)$, such that for all $i$, $0 \leq i \leq n-1$, $(l_i, c, l_{i+1}) \in T$ and $(\sigma_i, c) \hookrightarrow^* (\sigma_{i+1}, skip)$.
- A program satisfies its specification $\{P\}c\{Q\}$ if $\forall \sigma \in P$, for all executions $(\sigma, l_0), (\sigma_1, l_1), \ldots, (\sigma', l_e)$ of $\Gamma_c$, $\sigma' \in Q$.

# INDUCTIVE ASSERTION MAP

- With each location, we associate a set of states which are reachable at that location in any execution.
  - $\mu : L \rightarrow \Sigma(V)$
- To express that such a map is an inductive assertion map, we will use Strongest Post-condition.
  - $\forall (l, c, l') \in T \,.\, sp(\mu(l), c) \rightarrow \mu(l')$
- Then, if $\mu$ is an inductive assertion map on $\Gamma_c$, the Hoare triple $\{P\}c\{Q\}$ is valid if $P \rightarrow \mu(l_0)$ and $\mu(l_e) \rightarrow Q$.

# GENERATING THE INDUCTIVE ASSERTION MAP

- We can express the inductive assertion map as a solution of a system of equations:
  - $X_{l_0} = P$
  - For all other locations $l \in L \setminus \{l_0\},\ X_l = \bigvee_{(l',c,l) \in T} sp(X_{l'}, c)$