Theorem Proving: Deductive Approach via Inference Rules

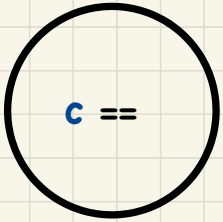
Model Checking: Algorithmic Approach via Exhaustive Search

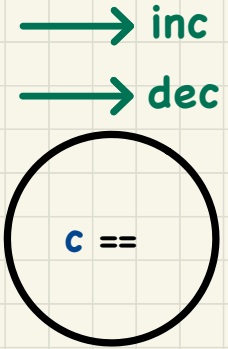
Invariant:

MIN_VALUE <= c <= MAX_VALUE

Definition: A **reachability graph** includes **all** states reachable, via occurrences of **enabled** events, from the **initial** state.

Q: Given variables, the initial state, and the set of possible events, how can a RG be **automatically** generated?





TLA+ Toolbox

*TLA+ (**Temporal Logic of Actions**) is a **high-level language** for modeling programs and systems–especially concurrent and distributed ones. It's based on the idea that the best way to describe things precisely is with **simple mathematics**. TLA+ and its tools are useful for eliminating fundamental **design errors**, which are hard to find and expensive to correct in code.*

TLA+ is a language for modeling ***software*** above the code level and ***hardware*** above the circuit level. It has an ***IDE*** (Integrated Development Environment) for writing models and running tools to check them. The tool most commonly used by engineers is the ***TLC model checker***, but there is also a proof checker. TLA+ is based on mathematics and does not resemble any programming language. Most engineers will find *PlusCal*, described below, to be the easiest way to start using TLA+.

Logical Operator vs. Programming Operator

p	q	$p \wedge q$	$p \vee q$
true	true	true	true
true	false	false	true
false	true	false	true
false	false	false	false

Q. Are the $\wedge$ and $\vee$ operators equivalent to, respectively, && and || in Java?