1 Introduction

Reliability: continuity of service

Availability: readiness for usage

Security: e.g. preservation of confidentiality

Safety: avoid catastrophic consequences

Fault prevention: system does not contain faults

Fault tolerance: system can recover from a system failure

Fail safety: in case of failure, no fatal consequences can occur

Preventing design bugs in hardware is important, because:

- costs are higher
- bug fixes are usually not possible
- quality expectations are higher
- time a new product gets on the market severely impacts revenue

Validation: Are we building the right thing?

Verification: Are we building the thing right?

Problem with testing: Can uncover faults, but doesn't guarantee their absence.

Formal verification can guarantee fault freeness.

2 Model Checking

Model: formal abstraction of the system of interest

Constraints: system requirements specified with precise logical statements A model checker automaticall checks the model against the constraints. If something violates the constraints, an execution path is returned.

Examples of system properties

- functional correctness: system behaving as expected?
- reachability: can we end up in a deadlock?
- safety: something "bad" never happens
- liveness: something "good" will eventually happen
- fairness: can, under certain conditions, an event occur repeatedly?
- real-time: is the system acting in time?

Must ensure that model is **as simle as possible**: prevent state explosion.

Livelock: a procass is always able to request resource, but always refused.

Unconditional fairness: Every process executes infinitely often. ($\square \diamond p$)

Strong fairness: Every process that can run, will run. $\square \diamond q \Rightarrow \square \diamond p$

Weak fairness: Every process that can continuously run from a certain point onwards, will execute infinitely often. $\diamond \square q \Rightarrow \square \diamond p$

3 PROMELA: Process Meta Language

Spec language used in **Spin**. Used to check **concurrent systems**:

- interleaved processes (stuff behaving independently)
- shared global variables
- synchronous/asynchronous channels

Can label certain parts of the model that are of interest and then assert stuff only about those states.

Can check for desirable end states.

Checking liveness in Spin: annotate program with `progress[a-zA-Z0-9]*:` labels, and it will be checked if we pass through the labels infinitely often.

Trace constraint: can restrain the internal interleaving to only perform certain kinds of transitions (i.e., some channels only send/receive one kind of message, always alternating, etc.)
A trace **synchronises** with the spec

Never claim: define an undesired system behaviour and check if it ever holds, and reports if it does.
It *succeeds* if it terminates of passes through its accept labels infintely often. If no transition is possible in the never claim, the claim automaton will stop search in that branch and backtrack. A never claim is **interleaved** with the model spec. (It always executes before the next transition)

4 LTL: Linear Temporal Logic

All valid LTL formulae may be derived from the grammar

$$\phi ::= \text{true} \,|\, \text{false} \,|\, p \,|\, \neg \,|\, \wedge \,|\, \vee \,|\, (\phi) \,|\, \diamond \phi \,|\, \Box \phi \,|\, \phi \; \mathcal{U} \; \phi$$

where p is an **atomic proposition** (basically just a Boolean variable). They are **simple** known facts about the model at a particular state.

Note: next can be denoted X, $\mathcal{N}$ or $\circ$.

Examples

- Invariant: $\Box p$
- Reply: $p \Rightarrow \diamond q$
- Guaranteed Reply: $\Box(p \Rightarrow \; \mathcal{N} \; (\diamond q))$
- Infinitely often: $\Box \diamond p$
- Eventually always: $\diamond \Box p$
- Exclusion: $\Box(p \Rightarrow \neg q)$

Equivalences

- $\neg \Box p \equiv \diamond \neg p$
- $\neg \diamond p \equiv \Box \diamond \neg p$
- $\Box p \wedge q \equiv \Box p \wedge \Box q$
- $\diamond p \vee q \equiv \diamond p \vee \diamond q$
- $\diamond p \equiv \text{true} \; \mathcal{U} \; p$

Transition System a TS is defined as $TS = (S, Act, T, I, AP, L)$

- S: set of all possible states (nodes of the multigraph)
- Act: set of all possible transitions
- $T \subseteq S \times Act \times S$: transition table (edges of the multigraph)
- $I \subseteq S$: initial states
- AP: set of atomic propositions
- $L : S \to 2^{AP}$: labelling function (state labels)

A TS if **finite** iff S, Act and AP are finite. A state satisfies a formula if its label set satisfies it, i.e.

$$s \vDash \phi \equiv L(s) \vDash \phi$$

Definitions

- **direct α-successors of a state** s: $\text{Post}(s, \alpha) = \{s' \in S \mid (s, \alpha, s') \in T\}$ for $s \in S$ and $\alpha \in Act$. (States that are pointed to by an α arrow from s.)
- **α-predecessors of** s: $\text{Pre}(s, \alpha) = \{s' \in S \mid (s', \alpha, s) \in T\}$ for $s \in S$ and $\alpha \in Act$. (States that point to s with an α arrow from s.)
- **terminal state**: $s \in S$ is terminal iff $\text{Post}(s) = \emptyset$.
- **finite execution fragment (FEF)**: for a TS, a FEF is

  $$\rho = s_0 \xrightarrow{\alpha_1} s_1 \xrightarrow{\alpha_2} \ldots \xrightarrow{\alpha_n} s_n$$

  where $s_i \in S$ and $\alpha_j \in Act$.
- **maximal execution fragment (MEF)**: FEF ending in a terminal state or an infinite EF.
- **initial execution fragment (IEF)**: EF whose first state is an initial state.
- **execution of a TS**: IEF + MEF
- **reachable state**: a state $s \in S$ is reachable iff

  $$\exists \rho. \quad \rho = s_0 \xrightarrow{\alpha_1} \ldots \xrightarrow{\alpha_n} s_n$$

  where $s_0 \in I$ and $s_n = s$ (you can transition into it in a finite amount of time).
- **state satisfying LTL formula**: a state $s \in S$ satisfies an LTL claim ϕ iff all paths starting in s satisfy it.
- **TS satisfying LTL formula**: a TS satisfies and LTL claim iff all of its initial paths satisfy it. **Note:** since one path might satisfy a claim, and another might not, it is possible that a TS satisfies neither a claim nor its negation!

5 Data-Dependent Systems

Want to deal with transitions dependent on some "global state". In a TS: use nondeterminism (this doesn't scale well), or **conditional transitions**.

Conditional transition: $g : \alpha$ where α is an action and g is a boolean condition (guard).

Definitions (bonkers)

- **set of typed variables**: `Var`
- **domain of a variable**: the type of $x \in$ `Var` is (inexplicably) called its domain, denoted $\text{dom}(x)$.
- **evaluations**: The set of **evaluations** over `Var` is the set that contains how we allow variables to evaluate and is denoted Eval(`Var`). e.g. we might say that x can evaluate to $1, 42$ and y can evaluate to "banana", "apple", respectively. Then we can define $\eta_1(x) = 1$, $\eta_1(y) =$ "banana"' $\eta_2(x) = 42$, $\eta_2(y) =$ "apple", and hence Eval(`Var`) $= \{\eta_1, \eta_2\}$.
- **condition set**: the **condition set** over `Var` is a set of boolean conditions involving the elements of `Var`.
- **Effect function**: indicates how variables evolve if we perform some action. Namely, Effect : $Act \times \text{Eval}(Var) \to \text{Eval}($`Var`$)$. e.g. if α represents incrementing x, and $\eta_i(x) = i$, then

  $$\text{Effect}(\alpha, \eta_i) = \eta_{i+1}.$$

  Since this is a function, we can evaluate it:

  $$\text{Effect}(\alpha, \eta_i)(x) = \eta_{i+1}(x) = i + 1.$$

- **Program Graph**: a PG is $PG = (Loc, Act, \text{Effect}, C_\dagger, Loc_0, g_0)$, where
  - Loc: set of locations, because the word state is not good anymore. (the justification being that the some location can be in different "states")
  - Act: Act is still good though, set of actions
  - Effect: see above
  - $C_\dagger$: $C_\dagger \subseteq Loc \times \text{Cond}($`Var`$) \times Act \times Loc$, the conditional transition table. A generic element looks like

    $$l_1 \xrightarrow{g:\alpha} l_2$$

    i.e. if g holds when we perform α in l_1, we transition into l_2.

- Loc_0: $Loc_0 \in Loc$ set of initial locations
- g_0: $g_0 \in \text{Cond}(\texttt{Var})$ is the initial condition (basically ensuring that our variables exist and have some initial value).

A PG can be converted into a TS, by "unfolding" it, i.e. adding a state for every location + evaluation combo, and a transition between them if we the guard of the transition connecting the two locations is true. Formally:

$$\frac{l_1 \xrightarrow{g:\alpha} l_2 \wedge \eta \vDash g}{\langle l_1, \eta \rangle \xrightarrow{\alpha} \langle l_2, \text{Effect}(\alpha, \eta) \rangle}$$

6 Parallelism

TSs are good for **sequential** systems. How do we model **parallel** systems? Depends on how *subsystem*s communticate: no communication, synchronous comm., asynchronous comm.

$$TS = TS_1 \mid\mid TS_2 \mid\mid \ldots \mid\mid TS_n$$

where $||$ is the **parallel composition operator**, meaning that the TS_i execute at the same time.

Interleaving is choosing the order of execution for the TS_i. Two TSs interleaved is the Cartesian product of their states and union of their action sets and atomic props, and is denoted $TS_1 ||| TS_2$, where $|||$ is called the **interleaving operator**. Note: interleaving doesn't reflect the expected behaviour of shared variables.
For programs with shared variables, we interleave PGs, and then unfold them.

Concurrency is nondeterministic interleaving

Independent actions are actions that can be interleaved, and their effect doesn't change

Local variables of PG_1 and PG_2 are $\texttt{Var}_1 \setminus \texttt{Var}_2$ and vice versa.

Global Variables are $\texttt{Var}_1 \cap \texttt{Var}_2$.

Note: Look at Lecture 8 - 10 for the graphs.

6.1 Handshaking

Processes interact at the same time through sychronous communication. handshaking done through shared actions: for TS_1, TS_2 and $H \subseteq Act_1 \cap Act_2$. Then

$$TS_1||_H TS_2 \equiv (S_1 \times S_2, Act_1 \cup Act_2, T, I_1 \times I_2, AP_1 \cup AP_2, L)$$

where if an action is not in H, then we add two arrows for the two separate state tuples, whereas if the action is in H, then the states connected by α are merged. Formally:

$$\forall \alpha \notin H. \quad \frac{s_1 \xrightarrow{\alpha} s_1'}{\langle s_1, s_2 \rangle \xrightarrow{\alpha} \langle s_1', s_2 \rangle} \quad \text{and} \quad \frac{s_2 \xrightarrow{\alpha} s_2'}{\langle s_1, s_2 \rangle \xrightarrow{\alpha} \langle s_1, s_2' \rangle} \quad \text{(interleaving)}$$

and

$$\forall \alpha \in H. \quad \frac{s_1 \xrightarrow{\alpha} s_1' \wedge s_2 \xrightarrow{\alpha} s_2'}{\langle s_1, s_2 \rangle \xrightarrow{\alpha} \langle s_1', s_2' \rangle} \quad \text{(synchronisation)}$$

Note: $TS_1||_\emptyset = TS_1|||TS_2$.

7 Asynchronous communication

Processes communicate via channels. Many critical systems depend on time as well: train crossing, radiation machine, space shuttles etc. How to add time?

Bad Approach: use global "clock variable" and synchronise all transitions on it. Why it's bad: it's confusing, overly complex and error-prone.

Good Approach: Timed Automata

7.1 Timed Automata

Extend a program graph with a finite set of **clock variables**, which can only be **inspected** or **reset**. We can then use impose **clock constraints**: guards and time a PG spends in a state.

definitons

- **Timed Automaton**: $TA = PG + (C, Inv)$, where C is the set of clocks and $Inv : Loc \to CC(C)$ where $CC(C)$ is the set of clock constraints.
- **Clock Reset**: $l_1 \xrightarrow{g:\alpha,D} l_2$ everything as in the PG, but also reset all clocks to 0 in $D \subseteq C$.
- **Timelock**: if we can't leave a state before one of its invariants expire (i.e. one of the clocks violates its time constraint).

- **Interleaving and handshaking**: defined analogously to PGs, but when we synchronise, we union the clocks and the constraints too.

Note: See Lecture 11-13 for graphs.

8 CTL: Computational Tree Logic

want to express constraints about the paths: LTL talks about all executions, no good. Solution: CTL.

Definitions

- **CTL formula** a valid CTL claim can be decomposed into **State formulae** and **Path formulae**. It can be derived from the following and only the following grammar:

$$\Phi ::= \text{true} \mid a \mid \Phi \wedge \Phi \mid \neg\Phi \mid \exists\phi \mid \forall\phi \quad \textbf{(State Formulae)}$$
$$\phi ::= \mathcal{N}\ \Phi \mid \Phi\ \mathcal{U}\ \Phi \quad \textbf{(Path Formulae)}$$

  Other operators may be derived from the above.
  $\exists\phi$ holds in a state s iff there is at least one path from s that satisfies ϕ.
  $\forall\phi$ holds in a state iff all paths from it satisfy ϕ **Note:** if the second argument of $\mathcal{U}$ never holds, it is false.

- **Satisfaction Set**: $\text{Sat}_{TS}(\Phi) = \{s \in S \mid s \vDash \Phi\}$, i.e. the states in the TS that satisfy the state formula. (NOT just the initial states!)

- **TS satisfies CTL claim**: if all the inital states satisfy the claim. Formally: $I \subseteq \text{Sat}_{TS}(\Phi)$.

Model checking a TS against a CTL claim: recursively build all the satisfaction sets starting from the terminal states (including the end-point of loops), then check if $I \subseteq \text{Sat}_{TS}(\Phi)$.

Examples

- $\exists \diamond P$: P potentially holds (there is at least one path where it holds at least for one state). "There will be a day when it will rain for some time"

- $\exists\Box P$: P potentially always hold (there is at least one path where it always holds). "There is a timeline where from now on it rains until the end of time"

- $\forall \diamond P$: P is inevitable (it will hold at some point for all paths). "I will die at some point, no matter what".

- $\forall\Box P$: P is invariantly true (it holds from the point onwards for all paths). "2 + 2 = 4".

- $\neg\exists \diamond \Phi = \forall\Box\neg\Phi$
- $\forall \diamond \Phi = \forall(\text{true } \mathcal{U}\ \Phi)$

9 TCTL: Timed CTL

Just like CTL, but with clocks added from timed automata. Doesn't have $\mathcal{N}$, only have

$$\phi ::= \Phi\ \mathcal{U}^{\ J}\Phi$$

where J is a non-negative interval of time until which the first argument must hold.

Examples

- $\exists\Box^J\Phi$: there is a path where Φ holds during interval J. "There is a timeline where it will continuously rain between 11:00 and 15:00 tomorrow."
- $\forall\Box^J\Phi$: Φ always holds in the interval. "In any case I will sleep between midnight and 8 am"

10 UPPAAL not examined

11 Petri Nets

Graphical descriptions for distributed systems for behavioural analysis.

Definitions

- **Petri Net**: $N = (P, T, G)$, where
  - P set of places (nodes)
  - T set of transitions
  - G directed graph linking places and transitions. Formally: $G \subseteq (P \times T) \cup (T \times P)$
- **pre-transition regions**: $\text{pre}(t) = \{p \in P \,|\, (p,t) \in G\}$, the set of places from which we can transition using t.
- **post-transition regions**: $\text{post}(t) = \{p \in P \,|\, (t,p) \in G\}$, the set of places to which we can transition using t.
- **marking**: $M : P \to \mathbb{N}_0$, the number of tokens at a place.

- **transition firing**: t can fire under M iff there is one token in every element in the pre-transition set of t. Formally, $\forall p \in \text{pre}(t)$, we have $M(p) \geq 1$. If a transition can fire, then we say it is **enabled**. A firing takes a token from each of its pre-set elements and moves one token to each element of its post-set.
- **concurrently enabled transitions**: The set of all transitions that are enabled.
- **reachable markings** let N a Petri Net and M a marking for it, then Reachable$(N, M) = \{M' | M' \text{ is a marking for } N\}$, such that there is a sequence of transitions through which we get to M'.
  Note: a marking for which there is no enabled transition signals a **deadlock**.
- **Reachability Graph**: the Petri Net equivalent of an unfolded Program Graph, i.e.: it models how a Petri net can evolve, where the nodes are the entire state current state (how many tokens are in every place) with the set of enabled transitions being the edges.
  Note: this may be an infinite graph.
- **Overlapping Graph**: generalised Reachability Graph, where if we can have two markings where one marking M has bigger values than some other marking M', then we merge the two markings together.

Note : reachability of a marking from another is **undecidable**.

Note : the reachability of an overlapping marking given a marking M is decidable.