CS4211: Formal Methods for Software Engineering

Lecture Notes

Kevin Toh

Table of Contents

1. Introduction and Latex Setup
2. Z Specification
3. Communicating Sequential Processes (CSP)
4. Process Analysis Toolkit (PAT)

Introduction to Formal Methods

- Requirements are difficult to define because its written in **Natural Language** which can be imprecise and ambiguous at times.
- As we cannot anticipate the ways a system may be used, written test cases only covers a small subset of use cases.
- We want to verify if a system always satisify a certain property, in possible all cases.
- In Formal Methods, we use **Mathematics** to define the **structure** and **behaviour** of our software because it is **precise** and **unambiguous**
- Eventually, we can use a model checker to automatically verify the software by checking if a certain property holds in all cases.

Latex Setup

- The Latex package that we will be using is zed-csp
- **Setup Code:**

```
% For latex document
\documentstyle[12pt,zed]{article}

% For beamer slides
\usepackage{zed-csp}

\begin{document}
\end{document}

```

- Reference: https://sg.mirrors.cicku.me/ctan/macros/latex/contrib/zed-csp/zed2e.pdf

Table of Contents

1 Introduction and Latex Setup

2 Z Specification

3 Communicating Sequential Processes (CSP)

4 Process Analysis Toolkit (PAT)

The Z Specification Language

- Based on set theory and mathematical logic
  - We will be doing a recap on predicates, set theory, functions and relations next.
- Uses schemas to declare object properties
  - Schemas are similar to defining the structure of a class and its properties in an Object-Oriented Programming Language.
- Uses operations to describe state transitions
  - Each object has a state representing the values it's properties hold at a certain moment in time.
  - Operations are similar to methods of a class.
  - Operations modify the state of an object.
  - We use predicates to describe state transitions in an operation.
- We can then proof that a certain property holds manually

Recap on Predicates and Logic

Predicate

A statement that is either true or false.

1. There are 365 days in 2024. (**false**)
2. Let $P(x, y)$ be $x + y = 9$
   - $P(4, 5)$ is **true**.
   - $P(3, 7)$ is **false**.

Logic Operators

1. Not ($\neg$) Eg:
2. And ($\wedge$)
3. Or ($\vee$)
4. Implies ($\Rightarrow$)
5. Equivalence ($\Leftrightarrow$)

Recap on Quantifiers

1. Universal Quantifier ($\forall$)
   - Example: All natural numbers are greater than -1.
   - Mathematically, we would write $\forall n \in \mathbb{N}, n > -1$
   - In Z Specification, we would write $\forall n : \mathbb{N} \bullet n > -1$
   - $\forall n : \mathbb{N} \bullet n > 0$
   - In general, $\exists x : X \bullet P(x)$ abbreviates $P(a) \land P(b) \land P(c) \land \ldots$
2. Existential Quantifier ($\exists$)
   - Example: There exists a natural number more than 0.
   - In Z Specification, we would write $\exists n : \mathbb{N} \bullet n > 0$
   - In general, $\exists x : X \bullet P(x)$ abbreviates $P(a) \lor P(b) \lor P(c) \lor \ldots$

Differences between Mathematical Notations and Z Specification

- In Mathemical Notation, : or | means "such that" when used in Set Expressions.
- In Z Specification, : means "belongs to".
  - The difference between : and $\in$ will be explained later.
- In Z Specification, $\bullet$ means "such as" when writing predicates.

Recap on Set Theory

- A set is a collection of elements (or members)
  - Elements are not ordered: $\{a, b, c\} = \{b, a, c\}$
  - Elements are not repeated" $\{a, a, b\} = \{a, b\}$
  - Given Sets
    - $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ (The set of all natural numbers)
    - $\mathbb{N}_1 = \{1, 2, 3, \ldots\}$
    - $\mathbb{Z} = \{0, 1, -1, 2, -2, \ldots\}$ (The set of all integers)
    - $\mathbb{R}$ (The set of all real numbers)
    - $\emptyset$ (Empty Set: The set with no elements)
- Membership: $x \in \mathbb{X}$ is a predicate which is
  - true if x is in the set $\mathbb{X}$. Eg: $a \in \{a, b, c\}$
  - false if x is not in the set $\mathbb{X}$. Eg: $d \in \{a, b, c\}$

Difference between ':' and '$\in$'

Example: $\forall x : \mathbb{Z} \bullet x > 5 \Rightarrow x \in \mathbb{N}$

- $x : \mathbb{Z}$ declares a new variable x of type $\mathbb{Z}$
- $x \in \mathbb{N}$ is a predicate which is either true or false depending on the value of the declared x.

Recap on Set Theory

- Set Expressions
  - We can express a set by listing its elements if the set is finite and small.
    - $\{a, b, c, d\}$ is a finite set.
  - If a set is large or infinite, we can definite a set by giving a predicate which specifies precisely those elements in a set.
    - $\mathbb{N}$ is an infinite set.
    - The set of natural numbers less than 99 is $\{n : \mathbb{N} \mid n < 99\}$
    - In general the set $\{x : \mathbb{X} \mid P(x)\}$ is the set of elements of $\mathbb{X}$ for which predicate P is true.
- Set Examples
  - The set of even integers is $\{z : \mathbb{Z} \mid \exists\, k : \mathbb{Z} \bullet z = 2k\}$
  - The set of natural numbers which when divided by 7 leave a remaineder of 4 is $\{n : \mathbb{N} \mid \exists\, m : \mathbb{N} \bullet n = 7m + 4\}$
  - $\mathbb{N}$ is the set $\{z : \mathbb{Z} \mid z \geq 0\}$
  - $\mathbb{N}_1$ is the set $\{n : \mathbb{N} \mid n \geq 1\}$
  - If a, b are any natural numbers, then $a \,..\, b$ is defined as the set of all natural numbers between a and b inclusive.
    - $a \,..\, b$ is the set $\{n : \mathbb{N} \mid a \leq n \leq b\}$

Recap on Set Theory

- Subset ($\subseteq$): If S and T are sets, $S \subset T$ is a predicate equivalent to $\forall s : S \bullet s \in T$.
  - The following predicates are true:
    - $\{0, 1, 2\} \subseteq \mathbb{N}$
    - $2 \mathinner{..} 3 \subseteq 1 \mathinner{..} 5$
    - $\{a, b\} \subseteq \{a, b, c\}$
    - $\emptyset \subseteq X$ for any set X
    - $\{x\} \subseteq X \Leftrightarrow x \in X$
- Proper Subset ($\subset$): If S and T are sets, $S \subset T$ is a predicate equivalent to $S \subseteq T \land S \neq T$.
- Power Set ($\mathbb{P}$): If X is a set, $\mathbb{P}\ X$ (the power set of X) is the set of all subsets of X.
  - $A \in \mathbb{P}\ B = A \subseteq B$
  - The following predicates are true:
    - $\mathbb{P}\{a, b\} = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$
    - $\mathbb{P}\ \emptyset = \{\emptyset\} \neq \emptyset$
    - $1..5 \in \mathbb{P}\ \mathbb{N}$
    - $2..5 \in \mathbb{P}(1..5)$
  - If X has k elements, then $\mathbb{P}\ X$ has 2^k elements.

Recap on Set Theory

- Set Operations
  - Set Union: Suppose $S, T : \mathbb{P}\, X$ or $S \subseteq X, T \subseteq X$, then $S \cup T = \{x : X \mid x \in S \vee x \in T\}$
    - $\{a, b, c\} \cup \{b, g, h\} = \{a, b, c, g, h\}$
    - $A \cup \emptyset = A$ (for any set A)
  - Set Intersection: Suppose $S, T : \mathbb{P}\, X$, then $S \cap T = \{x : X \mid x \in S \wedge x \in T\}$
    - $\{a, b\} \cap \{b, c\} = \{b\}$
    - $\{a, b, c\} \cap \{d, g\} = \emptyset$ (disjoint sets)
    - $A \cap \emptyset = \emptyset$ (for any set A)
  - Set Difference: Suppose $S, T : \mathbb{P}\, X$, then $S - T = \{x : X \mid x \in S \wedge x \notin T\}$
    - $\{a, b, c\} - \{b, g, h\} = \{a, c\}$
    - $\mathbb{N}_1 = \mathbb{N} = \{0\}$
  - Cartesian Product: If A and B are sets, then $A \times B$ is the set of all ordered pairs (a, b) with $a \in A$ and $b \in B$.
    - $\{a, b\} \times \{a, c\} = \{(a, a), (a, c), (b, a), (b, c)\}$
  - Cardinality: $\#X$ is a natural number denoting the cardinality of (number of elements in) a finite set X.
    - $\#\{a, b, c\} = 3$

Tuples and Cartesian Product

- An n-tuple $(x_1, \ldots, x_n)$ is present in the Cartesian Product $\mathbf{a_1} \times \ldots \times \mathbf{a_n}$ if and only if each element x_i is an element of the corresponding set $\mathbf{a_i}$.
- To refer to a particular component of a tuple t, we use the projection notation $(.)$
- Suppose we have $t = (x_1, x_2, \ldots, x_n)$
  - The first component of the tuple t is written as $t.1$ which is the value $\mathbf{x_1}$.
  - The second component of the tuple t is written as $t.2$ which is the value $\mathbf{x_2}$.
  - The n-th component of the tuple t is written as $t.n$ which is the value $\mathbf{x_n}$

Recap on Relations

- A relation R from sets A to B, is declared as $R : A \leftrightarrow B$ is a subset of $A \times B$
- Example: $R = \{(c, x), (c, z), (d, x), (d, y), (d, z)\}$
  - The following predicates are equivalent
    1. $(c, z) \in R$
    2. $c \rightarrow z \in R$
    3. cRz
- **Domain:** $\mathrm{dom}\, R$ is the set $\{a : A \mid \exists\, b : B \bullet aRb\}$
- **Range:** $\mathrm{ran}\, R$ is the set $\{b : B \mid \exists\, a : A \bullet aRb\}$

Types in Z Specification

- Z specification language is **strongly typed**.
- Every expression is given a type.
- Any set can be used as a type.
- The following are equivalent declarations of variables x and y of types A and B respectively.
  - $(x, y) : A \times B$
  - $x : A, y : B$
  - $x, y : A$ (only when $B = A$)

Modelling using Z Specification

- When we write a program, we can write code procedurally, functionally or in an object oriented manner.
- Z Specification can help us model our code using two distinct sections.
  1. Declaration: To define variables.
  2. Predicate: Often used to define behaviours or invariants.
- **Example #1:** We can define the relation **divides** between two natural numbers.

  | `divides:` $\mathbb{N}_1 \leftrightarrow \mathbb{N}$

  | ----------

  | $\forall x : \mathbb{N}_1;\ y : \mathbb{N} \bullet x \ \underline{\text{divides}}\ y \Leftrightarrow \exists k : \mathbb{N} \bullet x \cdot k = y$

  Usage: 3 $\underline{\text{divides}}$ 6, $\neg$ (3 $\underline{\text{divides}}$ 7)
- **Example #2:** We can define the relation $\leq$ between two natural numbers.

  | $\_ <= \_$: $\mathbb{N} \leftrightarrow \mathbb{N}$

  | ----------

  | $\forall x, y : \mathbb{N} \bullet x <= y \Leftrightarrow \exists k : \mathbb{N} \bullet x + k = y$

  The relation $<=$ is the infinite subset of ordered pairs in $\mathbb{N} \times \mathbb{N}$.

  $\{(0,0), (0,1), (1,1), (0,2)(1,2), (2,2), \ldots\}$

Domain and Range Restriction

- Let A, B, R, S, T be sets.
- A is the domain set, B is the range set and R is the relation set.
- Note that S is a subset of the domain set and T is the subset of the range set.
- Suppose $R : A \leftrightarrow B, S \subseteq A$ and $T \subseteq B$.
  - **Domain Restriction:** $S \lhd R$ is the set $\{(a, b) : R \mid a \in S\}$
  - **Range Restriction:** $R \rhd T$ is the set $\{(a, b) : R \mid b \in T\}$
- Notice that both $S \lhd R \in A \leftrightarrow B$ and $R \rhd T \in A \leftrightarrow B$, meaning that both domain restriction and range restrictions are relations from sets A to B.
- If has_sibling: People $\leftrightarrow$ People then
  - female $\lhd$ has_sibling is the relationship is_sister_of.
  - has_sibling $\rhd$ female is the relationship has_sister.

Domain and Range Subtraction

- Let A, B, R, S, T be sets.
- A is the domain set, B is the range set and R is the relation set.
- Note that S is a subset of the domain set and T is the subset of the range set.
- Suppose $R : A \leftrightarrow B, S \subseteq A$ and $T \subseteq B$.
  - **Domain Subtraction:** $S \lhd R$ is the set $\{(a, b) : R \mid a \notin S\}$
  - **Range Subtraction:** $R \rhd T$ is the set $\{(a, b) : R \mid b \notin T\}$
- The following predicates are true.
  - $S \lhd R = (A - S) \lhd R$
  - $R \rhd T = R \rhd (B - T)$
  - $S \lhd R \in A \leftrightarrow B$
  - $R \rhd T \in A \leftrightarrow B$
- If has_sibling: People $\leftrightarrow$ People then
  - female $\lhd$ has_sibling is the relationship is_brother_of.
  - has_sibling $\rhd$ female is the relationship has_brother.

Relational Image

- Suppose the relation $R : A \leftrightarrow B$ and $S \leftrightarrow A$
- $R(\!| S |\!) = \{b : B \mid \exists a : S \bullet aRb\}$
- $R(\!| S |\!) \leftrightarrow B$
- Example
  - $divides(\!| \{8, 9\} |\!) = \{x : \mathbb{N} \mid \exists k : \mathbb{N} \bullet x = 8 \cdot k \lor 9 \cdot k\} = \{0, 8, 9, 16, 18, \ldots\}$
  - $<= (\!| 3, 7, 21 |\!) = \{x : \mathbb{N} \mid x >= 3\}$
- In summary, the relational image returns the set of all elements $b \in B$ such that there exists an $a \in S$ with $(a, b) \in R$.
- The difference between relational image and range restriction is that range restriction returns the subset of R which are ordered pairs of (a, b) where $a \in A$ and $b \in B$ and the first element a of the ordered pair is in S. The relational image simply just returns the set of all second elements b.

Inverse and Relational Composition

- **Inverse:** R^{-1} is the set $\{(b, a) : B \times A \mid aRb\}$ or $R^{-1} \in B \leftrightarrow A$
  - $has\_sibling^{-1} = has\_sibling$
  - $divisor^{-1} = has\_divisor$
- Example: $succ^{-1} = \text{pred}$

  | succ : $\mathbb{N} \leftrightarrow \mathbb{N}$

  |----------

  | $\forall x, y : \mathbb{N} \bullet x \ \underline{\texttt{succ}} \ y \leftrightarrow x + 1 = y$
- **Relational Composition ($\fatsemi$)**
  - Suppose $R : A \leftrightarrow B$ and $S : B \leftrightarrow C$ are two relations.
  - $R \fatsemi S = \{(a, c) : A \times C \mid \exists\, b : B \mid aRb \land bSc\}$
  - $R \fatsemi S \in A \leftrightarrow C$
- Examples
  - $is\_parent\_of \fatsemi is\_parent\_of = is\_grandparent\_of$
  - $R^0 = id[A]$
  - $R^1 = R$
  - $R^2 = R \fatsemi R$
  - $R^3 = R \fatsemi R \fatsemi R$

Recap on Functions

- A (partial) function from a set A to a set B, denoted by $f : A \pfun B$ is a subset f of $A \times B$ with the property that for each $a \in A$, there is **at most one** $b \in B$ with $(a, b) \in f$.
- $\dom f$ is the set $\{a : A \mid \exists\, b : B \bullet (a, b) \in f\}$
- $\ran f$ is the set $\{b : B \mid \exists\, a : A \bullet (a, b) \in f\}$
- Suppose $f : A \pfun B$ and $a \in \dom f$, then $f(a)$ denotes the unique image $b \in B$ that a is mapped to by f.
- $(a, b) \in f$ is equivalent to $f(a) = b$
- **Total Function:** If the function $f : A \pfun B$ is a total function, then $f : A \fun B$ if and only if $\dom f = A$

Function Overriding

- Suppose $f, g : A \pfun B$, then $f \oplus g$ is the function $(\dom g \domsub f) \cup g$.
- The following predicates are true:
  1. $\dom f \oplus g = \dom f \cup \dom g$
  2. $a : \dom g \bullet (f \oplus g)(a) = g(a)$
  3. $\forall a : \dom f - \dom g \bullet (f \oplus g)(a) = f(a)$
  4. $\mathrm{f} \oplus \mathrm{g} \in a \pfun b$
- Examples
  1. $\{a \mapsto x, b \mapsto y, c \mapsto x\} \oplus \{a \mapsto y\} = \{a \mapsto y, b \mapsto y, c \mapsto x\}$
  2. double $\oplus$ root $= \{(0,0), (1,1), (2,4), (3,6), (4,2), \ldots\}$ (Note: $(4,8)$ was replaced with $(4,2)$ as the domain 4 is both in f and g, so the range was replaced with 2 that was in g)

Specifying Functions

1. Using a look-up table
   - If a function $f : A \pfun B$ is finite (and not too large), we can specify the function explicity by listing all pairs (a, b) in the subset $A \times B$.
   - Example: PassportNo $\to$ Address

PassportNo	Address
A001017	77 Sunset Strip
...	...
G707165	19 Mail Street

2. Declaring Axioms: A function can be specified by giving a **predicate** determining which pairs (a, b) are in the function.
   - **Example: The root function that calculates the square root of a natural number**

`root` $\mathbb{N} \pfun \mathbb{N}$
$\dom root = \{n : \mathbb{N} \mid \exists m : \mathbb{N} \bullet m^2 = n\}$
$\forall n : \dom root \bullet (root(n))^2 = n$

Specifying Functions

3. Using Recursion: For functions defined recursively in terms of itself.

   | fact $\mathbb{N}_1 \pfun \mathbb{N}$
   |---
   | fact(1) = 1
   | $\forall n : \mathbb{N}_1 - \{1\} \bullet fact(n) = n * fact(n-1)$

4. Giving an Algorithm: A function $f : A \pfun B$ is specified by an algorithm such that given any element a in the domain of f, the element $f(a)$ can be computed using the algorithm.

```
1  input n : N
2  var x, y: integer;
3  begin
4      x := n; y:= 0;
5      while x != 0 do
6      begin
7          x := x - 1; y:= y + 2
8      end;
9  write(y)
10 end
```

| double: $\mathbb{N} \to \mathbb{N}$
| ---
| $\forall n : \mathbb{N} \bullet double(n) = 2n$

Sequences

- A sequence s of elements of a set A, denoted $s : \mathrm{seq}\, A$, is a function $s : \mathbb{N} \pfun A$ where $\mathrm{dom}\, s = 1 \,..\, n$ for some natural number n.
- **Example**
  - $< b, c, a, b >$ denotes the sequence (function) $\{1 \mapsto b, 2 \mapsto c, 3 \mapsto a, 4 \mapsto b\}$
  - The empty sequence is denoted by $<>$
- The set of all sequences of elements from A is denoted as $\mathrm{seq}\, A$ and is defined to be $\mathrm{seq}\, A = \{s : \mathbb{N} \pfun A \mid \exists\, n : \mathbb{N} \bullet \mathrm{dom}\, s = 1 \,..\, n\}$
- $\mathrm{seq}_1\, A = \mathrm{seq}\, A - \{<>\}$ is defined as the set of non-empty sequences.
- Since sequences are ordered mapping, $< a, b, a > \neq < a, a, b > \neq < a, b >$

Special Functions for Sequence

1. Concatenation
   - $< a, b > \frown < b, a, c > = < a, b, b, a, c >$
2. Head
   - $| \texttt{ head: } \quad \mathrm{seq}_1 A \rightarrow A$
     $|\texttt{----------}$
     $| \forall s : \mathrm{seq}_1 A \bullet head(s) = s(1)$
   - $head < c, b, b > = c$
3. Tail
   - $| \texttt{ tail: } \quad \mathrm{seq}_1 A \rightarrow \mathrm{seq}\, A$
     $|\texttt{----------}$
     $| \forall s : \mathrm{seq}_1 A \bullet < head(s) > \frown tail(s) = s$
   - $tail < c, b, b > = < b, b >$
4. Filter
   - $< a, b, c, d, e, d, c, b, a > \upharpoonright \{a, d\} = < a, d, d, a >$
   - Filter only keeps the element in the specified set, preserves order in the original sequence and outputs a new sequence.

Z Specification

- As explained in an earlier slide, we can write Z Specification to formally specify requirements in **two distinct sections**
  1. Declaration: To define variables.
  2. Predicate: Often used to restrain the possible values of the declared variables to define behaviours or invariants.
- Formal Specification can be done in the form of both **axioms** and **schemas**.
- When we were specifying functions earlier, we were formally specifying them in the form of **axioms** in the **axiom environment**.
- Later we will introduce how to formally specify **schemas** which are used to specify relationships between variable values.
- There are two main type of schemas in the **schema environment**
  - State Schema
  - Operation Schema

The zed-csp Package

- We can use the zed-csp package to formally specify requirements in Z Specification and render axioms and schemas them in TeX.
- There are **two types of environment** in the zed-csp package.

1. Axiom Environment

$$limit : \mathbb{N}$$

$$limit \leq 65535$$

```
\begin{axdef}
    limit: \nat
    \where
    limit \leq 65535
\end{axdef}
```

2. Schema Environment

PhoneDB

$$known : \mathbb{P}\, NAME$$
$$phone : NAME \pfun PHONE$$

$$known = \mathrm{dom}\, phone$$

```
\begin{schema}{PhoneDB}
known: \power NAME \\ phone: NAME \pfun PHONE
\where
known = \dom phone
\end{schema}
```

State Schema

- A **state schema** specifies a relationship between variable values
- It specifies a snapshot of a system
- **Variables** are declared and typed in the **top part of the schema**.
- A **predicate (axiom)** restraining the possible values of the declared variables are given in the **bottom part of the schema.**
- An instance of a schema is an assignment of values to variables consistent with their type declaration and satisfying the predicate.

Operation Schema

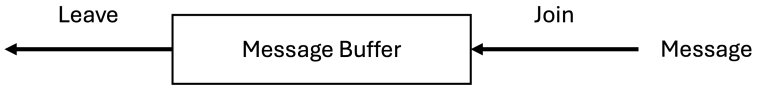
- The state schema provides a static view of the system.
- To specify how the system can change, we need to specify the operation schema.
- An operation can be thought as taking an instance of the state schema and producing a new instance.
- To specify such an operation, we express as a predicate the relationship between the **instance of the state before the operation** and the **instance after the operation.**

Convention

- The value of the state variables before the operation are denoted by **unprimed identifiers**.
  - Example: `items : seq MSG`
- Values after the operation are denoted by **primed identifiers**.
  - Example: `items' : seq MSG`
- Note: Let `MSG` be the set of all possible messages that can be transmitted.

Case Study: A Message Buffer

- We are going to model a message buffer to learn about **schema specification**.
- A message buffer stores messages within a queue data structure and operates on a first in / first out (FIFO) principle.
- Suppose we have a line which might be occupied by traffic, many messages join the buffer and but only the first message in the queue leaves the buffer when the line is free.
- The buffer may contain several messages at any time, but there is a fixed upper limit on the number of messages the buffer may contain.
- To model a message buffer, we minimally need the following:
  1. States: Buffer (to store messages)
  2. Operations: Join (new message joins the buffer), Leave (message leaves the buffer)



Formal Specification: Message Buffer

State Schema: Buffer

- Let MSG be the set of all possible messages that can be transmitted.
- Let max : $\mathbb{N}$ be the constant maximum number of messages that can be held in the buffer at any one time.
- Example: Let $MSG = \{m1, m2, m3\}$ and $max = 4$
  1. $items =< m1, m2 >$ is a valid instance.
  2. $items =< m3, m1, m1, m2, m2 >$ is an invalid instance.

Operation Schema: Join

- The decoration ? denotes an input
- There is an implicit $\wedge$ between each line in the predicate section.

Buffer

$items : \mathrm{seq}\, MSG$

$\#items \leq max$

Join

$items, items' : \mathrm{seq}\, MSG$
$msg? : MSG$

$\#items \leq max$
$\#items' \leq max$
$\#items < max$
$items' = items^\frown < msg? >$

Explanation: Predicate of the Join Operation

$$
\begin{array}{|l}
\hline
\textit{Join} \\
\textit{items}, \textit{items}' : \operatorname{seq} \textit{MSG} \\
\textit{msg}? : \textit{MSG} \\
\hline
\#\textit{items} \leq \textit{max} \\
\#\textit{items}' \leq \textit{max} \\
\#\textit{items} < \textit{max} \\
\textit{items}' = \textit{items}^\frown < \textit{msg}? > \\
\hline
\end{array}
$$

- The first two lines of the predicate indicate that we have a valid instance of the state schema **Buffer** both before and after the operation.
- The third line of the predicate is a pre-condition for the operation. It indicates that for the **Join** operation to be possible, the buffer must not be completely full.
- The last line of the predicate specifies the relationship between the buffer contents before and after the operation which is that the input message is already appended to the sequence of messages already in the buffer.

Formal Specification: Message Buffer (Continued)

Operation Schema: Leave

- The decoration ! denotes an output
- There is an implicit $\wedge$ between each line in the predicate section.
- Explanation for Leave Operation Predicate
  1. The first two lines of the predicate indicate that we have a valid instance of the state schema **Buffer** both before and after the operation.
  2. The third line of the predicate is a **pre-condition** for the operation. It indicates that for the **Leave** operation to be possible, the buffer must not be empty.
  3. The last line of the predicate specifies the relationship between the buffer contents before and after the operation. The output message is taken from the head of the sequence of messages in the buffer, leaving just the tail of the sequence of buffers.

Leave

$items, items' : \mathrm{seq}\, MSG$

$msg! : MSG$

$\#items \leq max$

$\#items' \leq max$

$\#items \neq \emptyset$

$items = < msg! > \frown items'$

Special States: Delta (Δ) and Initial State ($_{INIT}$)

1. Delta (Δ): To specify a **before** and **after** instance of the state schema for any operation.

$$\Delta Buffer$$
$$items, items' : \operatorname{seq} MSG$$
$$\#items \leq max$$
$$\#items' \leq max$$

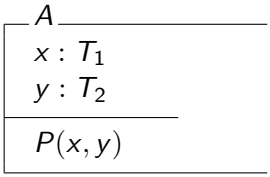
2. Initial State ($_{INIT}$): To specify a state when an instance of a state is first initialized.

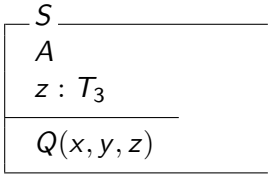
$$Buffer_{INIT}$$
$$Buffer$$
$$items = <>$$

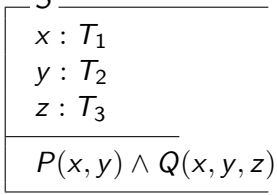
- Initially the buffer would be empty.
- Then, the operations of **Join** and **Leave** can occur whenever they are enabled.
- Operations are assumed to be atomic.
- At all times, an observer will notice that the state schema is satisfied.

Schema Inclusion

- Schema Inclusion is the act of including a schema in the declaration of another schema.
- It means the included schema has its declaration added to the new schema, and its predicate cojoined to the predicate of the new schema.
- The first "S" Schema is the **short form**, while the second "S" Schema is the **long form**.







Example: Schema Inclusion

Join

$\Delta Buffer$

$msg? : MSG$

$\#items < max$

$items' = items^\frown < msg? >$

Leave

$\Delta Buffer$

$msg! : MSG$

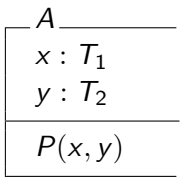
$items \neq \emptyset$

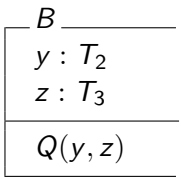
$items =< msg! > ^\frown items'$

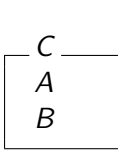
- We can include the $\Delta Buffer$ schema to both the Join and Leave operations.
- Explanation for Leave Operation Predicate
  1. The first line of the predicate is a **pre-condition** for the operation. It indicates that for the **Leave** operation to be possible, the buffer must not be empty.
  2. The last line of the predicate specifies the relationship between the buffer contents before and after the operation. The output message is taken from the head of the sequence of messages in the buffer, leaving just the tail of the sequence of buffers.

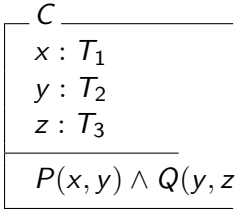
Merging Schemas

- **Type Compatability** is needed to merge schemas.
- In this case, the variable y is common between states A and B.
- We can simply merge the two types into a new state C without further specifying any new predicates.
- The full form of state C is also provided.









Extending Specifications: Slow Buffer and Slow Operations

- Applying concepts such as **Schema Inclusion** and **Merging Schemas**, we can extend specifications similar to inheritance or creating specialized classes in Object-Oriented Programming.
- To demonstrate this, we will attempt to model a **Slow Buffer** which has a constant $delay : \mathbb{N}$ to simulate that each new message can only join the buffer after $delay$ seconds.

SlowBuffer

$Buffer$

$idle : \mathbb{N}$

Tick

$\Delta SlowBuffer$

$idle' = idle + 1$

$items' = items$

$SlowBuffer_{INIT}$

$SlowBuffer$

$Buffer_{INIT}$

$idle = 0$

SlowJoin

$\Delta SlowBuffer$

$Join$

$idle \geq delay$

$idle' = 0$

SlowLeave

$\Delta SlowBuffer$

$Leave$

$idle \geq delay$

$idle' = 0$

Extending Specifications: Slow Buffer and Slow Operations (Full Form)

SlowBuffer

$$items : \operatorname{seq} MSG$$
$$idle : \mathbb{N}$$
$$\#items \leq max$$

SlowBuffer$_{INIT}$

$$items : \operatorname{seq} MSG$$
$$idle : \mathbb{N}$$
$$\#items \leq max$$
$$items = <>$$
$$idle = 0$$

SlowJoin

$$items, items' : \operatorname{seq} MSG$$
$$idle, idle' : \mathbb{N} \quad msg? : MSG$$
$$\#items \leq max \land \#items' \leq max$$
$$\#items < max \land items' = items^\frown < msg? >$$
$$idle \geq delay \land idle' = 0$$

SlowLeave

$$items, items' : \operatorname{seq} MSG$$
$$idle, idle' : \mathbb{N}$$
$$msg! : MSG$$
$$\#items \leq max \land \#items' \leq max$$
$$items \neq \emptyset \land items = items'^\frown < msg? >$$
$$idle \geq delay \land idle' = 0$$

Tick

$$items : \operatorname{seq} MSG$$
$$idle : \mathbb{N}$$
$$\#items \leq max \land \#items' \leq max$$
$$idle' = idle + 1 \land items' = item$$

Reasoning About The Specification

- Suppose, we want to verify that message buffer specified has the **FIFO property**.
- We want to show that the messages leave the buffer in the same order they arrive.
- In this case, we introduce **auxillary sequences** `inhist` and `outhist` to record the history of the flow of messages into and out of the buffer.
- Create a new schema which includes the original Buffer and Operation schemas and extra information about the auxillary variables.
- When a message **joins** the buffer, it is also added to the `inhist` sequence.
- When a message **leaves** the buffer, it is added to the `outhist` sequence.

Recorded Buffer and Operations

RecordedBuffer

$Buffer$

$inhist : \mathrm{seq}\ MSG$

$outhist : \mathrm{seq}\ MSG$

RecordedJoin

$\Delta RecordedBuffer$

$Join$

$inhist' = inhist^\frown < msg? >$

$outhist' = outhist$

RecordedBuffer$_{INIT}$

$RecordedBuffer$

$Buffer_{INIT}$

$inhist = <>$

$outhist = <>$

RecordedLeave

$\Delta RecordedBuffer$

$Join$

$inhist' = inhist$

$outhist' = outhist^\frown < msg! >$

RecordedJoin: Expanded Schema

RecordedJoin

$items, items' : \operatorname{seq} MSG$

$inhist, inhist' : \operatorname{seq} MSG$

$outhist, outhist' : \operatorname{seq} MSG$

$msg? : MSG$

$\#items \leq max \land \#items' \leq max$

$\#items < max \land items' = items^\frown < msg? >$

$inhist' = inhist^\frown < msg? > outhist' = outhist$

Proving the FIFO Property

- How can we use the auxillary variables `inhist` and `outhist` to prove that the buffer satisifies the **FIFO property**?
- We can prove that the predicate $\forall\, RecordedBuffer \bullet inhist = outhist \frown items$ is true.
- Prove using structural induction.
  1. Initially `inhist = outhist = items = <>`, so the predicate is true for the initial state.
  2. Suppose the predicate is true, and RecordedJoin occurs. After the operation, $inhist' = inhist \frown < msg? > \land outhist' = outhist \land items' = items \frown < msg? >$
  3. Hence, $inhist \frown < msg? > = (outhist \frown items) \frown < msg? >$ $= outhist \frown (items \frown < msg? >) = outhist' \frown items'$
  4. Therefore, the predicate remains true.
- We can construct a similar argument that the operation **RecordedLeave** also preserves the predicate.

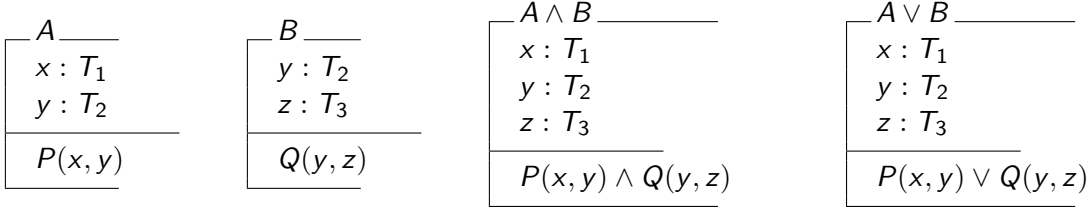
Conjunction of Schemas

- When using the conjunction ($\wedge$) operator on two schemas, it is equivalent to merging the two schemas.
- Suppose A and B are schemas
  - The declaration of $A \wedge B$ is the **union** of the declarations of A and B
  - The predicate of $A \wedge B$ is the **conjunction** of the predicates of A and B
- Examples
  1. $SlowRecordedBuffer \mathrel{\widehat=} SlowBuffer \wedge RecordedBuffer$
  2. $SlowRecordedBuffer_{INIT} \mathrel{\widehat=} SlowBuffer_{INIT} \wedge RecordedBuffer_{INIT}$
  3. $SlowRecordedJoin \mathrel{\widehat=} SlowJoin \wedge RecordedJoin$
- SlowRecordedBuffer Schema

$$\begin{array}{|l} \hline SlowRecordedBuffer \\ \hline SlowBuffer \\ RecordedBuffer \\ \hline \end{array}$$

Disjunction of Schemas

- Using the conjunction ($\wedge$) operator on two schemas yields a different result.
- Suppose A and B are schemas
  - The declaration of $A \vee B$ is the **union** of the declarations of A and B
  - The predicate of $A \vee B$ is the **disjunction** of the predicates of A and B



Disjunction of Schemas: Example

- Let $Flag ::= ok \mid error$ (The Flag type can be either 'ok' or 'error')
- Ξ State is another special state that is used for operations that access information in the state **without changing the state at all**.
- Example: $CompleteJoin \mathrel{\widehat=} JoinOk \lor JoinError$

JoinOk

$Join$

$flag! : Flag$

$flag! = ok$

JoinError

$\Xi Buffer$

$flag! : Flag$

$\#items = max \land flag! = error$

CompleteJoin

$\Delta Buffer$

$msg? : MSG;\ flag! : Flag$

$\#items < max \land items' = item^\frown < msg? > \land flag! = ok$

$\lor$

$\#items = max \land items' = items \land flag! = error$

Composition of Schemas

- Using the composition operator ($\fatsemi$) on two schemas is typically used to combine the effects of two operations.
- Example: $JoinLeave = Join \fatsemi Leave$
  - The pre-state of *Join* is the pre-state of $Join \fatsemi Leave$.
  - The post-state of *Join* is identified with the pre-state of *Leave* hidden within $Join \fatsemi Leave$.
  - The consequent post-state of *Leave* is the post-state of $Join \fatsemi Leave$.
- Convention: Hidden state is denoted with double prime (″).

JoinLeave

$\Delta Buffer$

$msg?, msg! : MSG$

$\#items < max$

$\exists items'' : \mathrm{seq}\, MSG \bullet items'' = items^\frown < msg? > \wedge items'' = < msg! > ^\frown items'$

Composition of Schemas in general

A

$x : T_1$
$y : T_2$

$P(x, y)$

AOP_1

δA
$t_3? : T_3;\ t_4! : T_4$

$Q_1(x, x', y, y', t_3?, t_4!)$

AOP_2

δA
$t_5? : T_5;\ t_6! : T_6$

$Q_2(x, x', y, y', t_5?, t_6!)$

$AOP_1 \fatsemi AOP_2$

δA
$t_3? : T_3;\ t_4! : T_4;\ t_5? : T_5;\ t_6! : T_6$

$\exists x'' : T_1;\ y'' : T_2 \bullet Q_1(x, x', y, y', t_3?, t_4!) \land Q_2(x, x', y, y', t_5?, t_6!)$

Table of Contents

1 Introduction and Latex Setup

2 Z Specification

3 Communicating Sequential Processes (CSP)

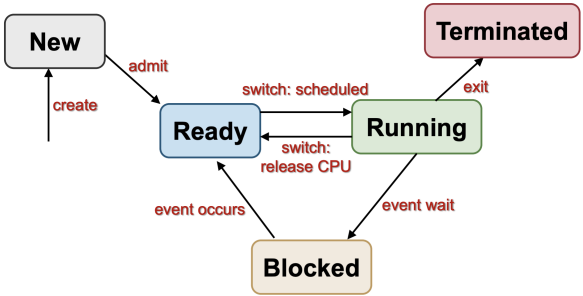
4 Process Analysis Toolkit (PAT)

Introduction to CSP

- **Communicating Sequential Processes (CSP)** is a formal language to describe patterns interaction between concurrent processes in computer systems.
- CSP was created by **Tony Hoare** to reason about the behaviour of concurrent systems.
- CSP provides **event based** notation primarily aimed at describing the sequencing of behaviour within a process and the synchronisation of behaviour (or communication) between processes.
- In CSP, there are two main fundamental concepts
  1. Process
  2. Event
- Events represent a co-operative synchronisation between process and environment.
- Both process and environment may control the behaviour of each other by enabling or refusing certain events or sequences of events.

Recap: Process State Model

- To gain a better understanding of **Communicating Sequential Processes**, revisit the first half of **CS2106: Operating Systems** where Processes, Concurrency, Synchronisation and Semaphores were covered.
- The Process State Model is shown here to help you visualize potential process behaviour that can be modelled using CSP.



Specifying a Process

- A process is determined or specified by what it can do.
- In other words, a process is defined by its behaviour, which are the events that we can observe.
- The perceived behaviour of a process will depend on the observer.
- In this course, we are mainly concerned with specifying the interaction between a system and its environment which is also the **external or visible behaviour**.

Concepts in CSP: Events

- A process engages in **events**.
- Each event is an atomic action.

Alphabet

The **set of events** a process can possibly engage in is the **alphabet** of the process.

- Example: Chocolate Vending Machine
- Events for a chocolate vending machine
  1. coin - insert a coin
  2. choc - extract a chocolate
- The alphabet of a chocolate vending machine is $\{coin, choc\}$

Concepts in CSP: Trace

Trace

A finite sequence of events

- A deterministic process is specified by the set of processes denoting its possible behaviour.
- Any execution of the process will be one of these sequences.
- Example: The traces of the chocolate vending machine are:
  - $\langle\rangle$
  - $\langle coin \rangle$
  - $\langle coin, choc \rangle$
  - $\langle coin, choc, coin \rangle$
  - ...
- Any execution of the process will be one of the above sequences or traces.
- If $s \frown t$ is a trace of a process, then s is also a trace of a process. This means that set of traces is prefixed closed.
  - Example: Let $s = \langle coin, choc \rangle, t = \langle coin \rangle$, then $s \frown t = \langle coin, choc, coin \rangle$.

Notations and Conventions

- **Events** are denoted in **lower case**
  - Example: x, y, z are variables that denote events.
- **Processes** are denoted in **upper case**
  - Example: X, Y, Z are variables that denote processes.
- The **alphabet** of a process P is denoted by αP
- The set of traces of P is denoted by `traces(P)`
- **Trace Notation**
  - If A is a set of events, then $\mathrm{seq}\, A$ denotes the set of all finite sequences of events from A.
  - In this scenario, α `P = A` and `trace(P) =` $\mathrm{seq}\, A$
  - Let $s, t : \mathrm{seq}\, A$, $s \frown t$ be the concatenation of s with t.
  - We define the relation $<=$ to be the **sequence prefix** of two sequences.

$$\frac{<= : \mathrm{seq}\, A \leftrightarrow \mathrm{seq}\, A}{s <= t \Leftrightarrow \exists u : \mathrm{seq}\, A \bullet s \frown u = t}$$

  - $s^n = s \frown s \frown s \frown \ldots \frown s$ denotes the event s concatenated with itself n times.

Examples of Process Specification using CSP

1. Let $STOP_A$ be the process with alphabet A that can do nothing.
   - $traces(STOP_A) = \{\langle\rangle\}$
2. Let CLOCK be the process with $\alpha CLOCK = tick$ which can 'tick' at any time.
   - $traces(Clock) = tick^*$ where $* \geq 0$
3. Let VM be the process with $\alpha VM = \{coin, choc\}$ which repeatedly supplies a chocolate after a coin has been inserted.
   - $traces(VM) = \{s : \mathrm{seq}\{coin, choc\} \mid \exists\, n : \mathbb{N} \bullet s <= \langle coin, choc\rangle^n\}$
   - Note: $<=$ is the sequence prefix relation from the previous slide.
4. Let WALK be a one-dimensional random walk process with $\alpha WALK = \{left, right\}$.
   - $traces(WALK) = (left \vee right)^*$ where $* \geq 0$
5. Let LIFE be the process with $\alpha LIFE = \{beat\}$ which can stop (die) at any time.
   - $traces(LIFE) = beat^*$ where $* \geq 0$

CSP Syntax

1. Prefix: $a \rightarrow P$
2. Sequential Composition: $P;\ Q$
3. Parallel Composition (Synchronous): $P \,|[\, X \,]|\, Q$
4. Interleaving (Asynchronous): $P \,|||\, Q$
5. Choice: $a \rightarrow P \,\Box\, b \rightarrow Q$
6. Interrupt Process: $P \,\nabla\, e \rightarrow Q$

[0] Note that in the `zed-csp` package, the interrupt symbol is $\triangle$.

Prefix

- A process which may participate in **event a** then act according to **process description P** is written as: `a -> P`.
- **a** is the event prefix to **P**.
- The **event a** is initially enabled by the process and occurs as soon as it is requested by its environment. All other events are refused initially.
- The **event a** is sometimes referred to as the guard of the process.
- Examples
  1. $VMU = coin \rightarrow STOP$
  2. $SHORTLIFE = (beat \rightarrow (beat \rightarrow STOP)) = beat \rightarrow beat \rightarrow STOP$
  3. $VMS = coin \rightarrow choc \rightarrow STOP$

Sequential Composition (P; Q)

- Let ✓ be the Termination event.
- The process which may only terminate is written as $SKIP$.
- Let $SKIP = ✓ \rightarrow STOP$.
- The sequential composition of processes P and Q, written as P; Q, acts as P until P terminates by communicating ✓ and then proceeds to act as Q.

Parallel Composition

- The parallel composition of **processes P and Q** synchronised on the **event set X** is written as $P \,|[\, X \,]|\, Q$.
- No event from X may occur in $P \,|[\, X \,]|\, Q$ unless **jointly enabled** by both P and Q.
- When events from X occur, they occur in both P and Q simultaneously, and are referred to as **synchronisations**.
- Events **not from X** may occur in either P or Q seperately **but not jointly**.
- Example: $(a \rightarrow P) \,|[\, a \,]|\, (c \rightarrow a \rightarrow Q)$
  - All **a** events must be Synchronous between the two processes.
- Often, it is simply written as $P \parallel Q$ where the common event set $X = \alpha P \cap \alpha Q$ is omitted.
  - When $P \parallel Q$ is given, we still know that all common events in $X = \alpha P \cap \alpha Q$ must be synchronous between P and Q.

Interleaving

- $P \mid\mid\mid Q$ denotes an asynchronous parallel composition between two processes **P** and **Q**.
- Both components **P** and **Q execute concurrently** without any synchronisation.
- Example: $((a \rightarrow P) \mid\mid\mid (c \rightarrow a \rightarrow Q))$
  - One possible trace is $\langle c, a, a \rangle$, after which the process acts as $P \mid\mid\mid Q$
    1. c from $c \rightarrow a \rightarrow Q$ is engaged, leaving us with $((a \rightarrow P) \mid\mid\mid (a \rightarrow Q))$
    2. a from $a \rightarrow P$ is engaged, leaving us with $(P \mid\mid\mid (a \rightarrow Q))$
    3. a from $a \rightarrow Q$ is engaged, leaving us with $P \mid\mid\mid Q$
  - Another possible trace is $\langle a, c, a \rangle$, after which the process acts as $P \mid\mid\mid Q$
    1. a from $a \rightarrow P$ is engaged, leaving us with $(P \mid\mid\mid (c \rightarrow a \rightarrow Q))$
    2. c from $c \rightarrow a \rightarrow Q$ is engaged, leaving us with $(P \mid\mid\mid (a \rightarrow Q))$
    3. a from $a \rightarrow Q$ is engaged, leaving us with $P \mid\mid\mid Q$

Choice

- In a general choice, $(a \rightarrow P) \,\square\, (b \rightarrow Q)$, the process begins with both events **a** and **b** enabled.
- The subsequent behaviour depends on the event which occured.
  - If the event which occured is **a**, the process will act as **P** afterwards.
  - If the event which occured is **b**, the process will act as **Q** afterwards.
- There are other types of choices, namely external or internal choice in the CSP syntax.
- For most cases, general choice is sufficient, hence in this module, we focus on general choice only.
- Example: $(a \rightarrow P) \,\square\, (c \rightarrow a \rightarrow Q)$
  - If the first event is **a**, after which the process acts as P.
  - If the first event is **c**, after which the process acts as $a \rightarrow Q$.

Interrupt

- The interrupt process $P \bigtriangledown e \rightarrow Q$ behaves as **process P** until the first occurrence of **event e** which then the control passes to **process Q**.
- When coding the specification, the keyword **interrupt** is used instead of the symbol $\bigtriangledown$.
- For the System process, the first event can be a routine or an exception.
- After that, it still behaves as a System process.

```
1 Err() = exception -> Err();
2 Routine() = routine -> Routine();
3 ExceptionHandling() = Routine() interrupt exception -> ExceptionHandling();
4 System = Err() || ExceptionHandling();
```

[0]Note that in the zed-csp package, the interrupt symbol is $\bigtriangleup$.

Concurrency Example #1

We are given the following system specification in CSP

```
1 VMC = coin -> ((choc -> VMC)[](bisc -> VMC));
2 CHOCLOV = choc -> CHOCLOV [] coin -> choc -> CHOCLOV;
3 #alphabet VMC{coin, choc, bisc};
4 #alphabet VMC{coin, choc, bisc};
5 System = VMC || CHOCLOV;
```

- Semi-colon marks the end of each statement.
- When coding process specifications in CSP, we use the keyword **#alphabet**, instead of the symbol α.
- The only possible trace for this example is $\langle coin, choc \rangle^n$ for $n : \mathbb{N}_1$ after which the system acts as $VMC \parallel CHOCLOV$.
  - As defined in lines 3 and 4 of the specification, the common events are the alphabets of VMC and CHOCLOV which are **coin**, **choc** and **bisc**.
  - However, the process **CHOCLOV** does not have the event **bisc**.
  - In VMC, the **coin** event has to be engaged first before we can engage $choc \rightarrow VMC$
  - Hence, both VMC and CHOCLOV engages in the **coin** event first then the **choc** event before acting as $VMC \parallel CHOCLOV$ again.

Concurrency Example #2

We are given the same specification as the previous slide in CSP except that we now do not define the alphabet for the **VMC** and **CHOCLOV** processes.

```
1 VMC = coin -> ((choc -> VMC)[](bisc -> VMC));
2 CHOCLOV = choc -> CHOCLOV [] coin -> choc -> CHOCLOV;
3 System = VMC || CHOCLOV;
```

- If we did not explicity define the alphabet for each process, it can be **auto inferred**.
  - $\alpha VMC = \{coin, choc, bisc\}$
  - $\alpha CHOCLOV = \{coin, choc\}$
- In this specification the system may deadlock with the following trace $\langle coin, bisc \rangle$.
  - After $\langle coin, bisc \rangle$, no event is possible.
  - This is because now the **bisc** event is not common to both **VMC** and **CHOCLOV** processes.
  - Hence, the **bisc** event can occur seperately.
  - After $\langle coin, bisc \rangle$ has occurred, the system would be stuck at $VMC \parallel choc \rightarrow CHOCLOV$.
  - Since **coin** and **choc** are common events, neither events can be engaged synchronously as **coin** is a prefix for **choc**.

Concurrency Example #3

We are given the following system specification in CSP

```
1 VMH = on -> coin -> choc -> off -> VMH;
2 CUST = on -> ((coin -> bisc -> CUST) [] (curse -> coin -> choc -> CUST));
3 System = VMH || CUST;
```

- The common events between **VMH** and **CUST** are **on**, **coin** and **choc** and they must occur synchronously in the two processes.
- $\langle on, curse, coin, choc, off \rangle$ is a possible trace.
  - After the trace, the process will still behave as a System process.
- Deadlocks can occur with the following trace $\langle on, coin, bisc \rangle$
  - The system will be stuck at $choc \rightarrow off \rightarrow VMH \parallel CUST$ and no event can be engaged.

Concurrency Example #4

We are given the following system specification in CSP

```
SLOWALK = left -> rest -> SLOWALK [] right -> rest -> SLOWALK;
SLOCLIMB = up -> rest -> SLOCLIMB [] down -> SLOCLIMB;
System = SLOWALK || SLOCLIMB;
```

Are the following traces possible?

1. $\langle up, rest \rangle$
   - No. The common event between **SLOWALK** and **SLOCLIMB** is **rest**.
   - $\langle up, left, rest \rangle$ and $\langle up, right, rest \rangle$ are possible traces.
2. $\langle \ldots, up, rest \rangle$ where up may not the first event.
   - Yes. For example $\langle left, up, rest \rangle$ and $\langle right, up, rest \rangle$.

Laws for Concurrency

- Law 1: $P \parallel Q = Q \parallel P$
- Law 2: $P \parallel (Q \parallel R) = (P \parallel Q) \parallel R$
- Law 3: $P \parallel STOP_{\alpha P} = STOP_{\alpha P}$

Let...

1. $a \in (\alpha P - \alpha Q)$
2. $b \in (\alpha Q - \alpha P)$
3. $\{c, d\} \subseteq (\alpha P \cap \alpha Q)$

- Law 4A: $(c \rightarrow P) \parallel (c \rightarrow Q) = c \rightarrow (P \parallel Q)$
- Law 4B: $(c \rightarrow P) \parallel (d \rightarrow Q) = STOP$ if $c \neq d$
- Law 5A: $(a \rightarrow P) \parallel (c \rightarrow Q) = a \rightarrow (P \parallel (c \rightarrow Q))$
- Law 5A: $(c \rightarrow P) \parallel (b \rightarrow Q) = b \rightarrow ((c \rightarrow P) \parallel Q)$
- Law 6: $(a \rightarrow P) \parallel (b \rightarrow Q) = a \rightarrow (P \parallel (b \rightarrow Q)) \ \square \ b \rightarrow ((a \rightarrow P) \parallel Q)$

Channel

- Processes may communicate through channels.
- A channel is like a message buffer for one process to send a value to another process.
- A channel event is written as one of the following forms:

Form	Description
$c!n$	Channel Output. This event occurs when a process writes n (a value) to the tail of channel c's buffer
$c?n$	Channel Input. This event occurs when a process reads a value from the head of channel c's buffer to a local variable n
$c.n$	Channel output and its matching channel input are engaged together by two processes.

Channel Example

Suppose we are given the following specification in CSP.

```
channel c 1; // Channel with buffer size = 1
Sender(i) = c!i -> Sender(i);
Receiver() = c?x -> a.x -> Receiver();
System() = Sender(5) ||| Receiver();
```

- Note: A process can have optional parameters, eg: Sender(i)
- The first event must be c!5 since c's buffer is empty.
- The second event must be c?5 since c's buffer size is 1.
- The third event can either be c!5 or a.5

Channel Example: Synchronous Buffer

Suppose we are given the following specification in CSP.

```
1 channel c 0; // Synchronous Buffer
2 Sender(i) = c!i -> Sender(i);
3 Receiver() = c?x -> a.x -> Receiver();
4 System() = Sender(5) ||| Receiver();
```

- Note: A synchronous buffer is defined by setting the buffer size to 0.
- The first event must be c.5, since the sender must write to the c's buffer and the reciever must read from c's buffer simultaneously.
- The second event must be a.5

CSP Model Checkers: Automatic Reasoning

- A CSP Model Checker can check if a property is always satisfied.
- In the next part, we will explore how we can verify certain properties of our process model using PAT (CSP#).
- Suppose we are given the specification of the **Dining Philosophers Problem**.

```
1 #define N 2;
2 Phil(i) = get.i.(i+1)%N -> get.i.i -> eat.i -> put.i.(i+1)%N -> put.i.i ->
      Phil(i);
3 Fork(x) = get.x.x -> put.x.x -> Fork(x) [] get.(x-1)%N.x -> put.(x-1)%N.x ->
       Fork(x);
4 College() = ||x:{0..N-1}@(Phil(x)||Fork(x));
5 #assert College() deadlockfree; // Check if a property is satisifed.
```

- $\| \, x : \{1 \ldots n\} @ P(x)$ is equivalent to $P(1) \parallel \ldots \parallel P(n)$
- `#assert College() deadlockfree` is the property we want to verify.
- If the property isn't always True, the Model Checker gives a counter example: $\langle get.1.0, get.0.1 \rangle$

Table of Contents

1 Introduction and Latex Setup

2 Z Specification

3 Communicating Sequential Processes (CSP)

4 Process Analysis Toolkit (PAT)

Introduction to Process Analysis Toolkit (PAT)

- The Process Analysis Toolkit is a self-contained framework to support composing, simulating and reasoning of concurrent, real-time systems and other possible domains.
- In PAT 3.5, there are 11 developed modules provided to model a variety of different systems ranging from **Communicating Sequential Processes (CSP) Module**, **Real-Time System Module** to the **Web Service Module**.
- In this module, we will be focusing on the **Communicating Sequential Programs (CSP#) module**

Introduction to PAT's CSP#

- PAT's CSP# module supports a rich modeling language named CSP#(pronounced 'CSP sharp', short for Communicating Sequential Programs)
- CSP# combines high-level modeling operators like (conditional or non-deterministic) choices, interrupt, (alphabetized) parallel composition, interleaving, hiding, asynchronous message passing channel, etc., with programmer-favored low-level constructs like variables, arrays, if-then-else, while, etc ...
- CSP# offers great flexibility on how to model systems. For instance, communication among processes can be either based on shared memory (using global variables) or message passing (using asynchronous message passing or CSP-style multi-party barrier synchronization).
- The high-level operators are based on the classic process algebra Communicating Sequential Processes (CSP).
- The design principle for CSP# is to maximally keep the original CSP as a sub-language of CSP#, whilst offering a connection to the data states and executable data operations.

Operational Semantics

- Earlier, we want a way to automatically reason if a model satisfies a certain property.
- Hence, we will need to study **Operational Semantics** to understand how a process transitions from one state to another during the execution of CSP Specification.
- **Operational Semantics** tell us at given a system state, what are the possible actions the system can perform and what are the outcomes (next state)?
  - Example: $P \xrightarrow{a} Q$
  - The above is read as: If process P engages event a, it will become process Q.
  - In most cases the states are the process and actions are the events.
  - We will see in later examples what are states and actions.
- Operational Semantics can be presented using a set of inference rules in the following form similar to the philosophy of logic.

$$\frac{\textit{Premises}}{\textit{Conclusion}}$$

Operational Semantics: Primitives

- STOP (A process that does nothing)
- SKIP

$$\frac{}{SKIP \xrightarrow{\checkmark} STOP}$$

SKIP can only engage the **termination event**, afterwards it becomes STOP.

- Prefixing

$$\frac{}{(a \rightarrow P) \xrightarrow{a} P}$$

$a \rightarrow P$ can only engage event **a**, afterwards it becomes process **P**.

Operational Semantics

General Choice

- If P is choosen

$$\frac{P \xrightarrow{a} P'}{(P \,\square\, Q) \xrightarrow{a} P'}$$

- If Q is chosen

$$\frac{Q \xrightarrow{a} Q'}{(P \,\square\, Q) \xrightarrow{a} Q'}$$

Sequential Composition

- In process P;Q, P takes control first and Q starts only when P has finished.
- Let ✓ be the termination event.

$$\frac{P \xrightarrow{a} P'}{(P;\ Q) \xrightarrow{a} (P';\ Q)}$$

$$\frac{P \xrightarrow{\checkmark} P'}{(P \,\square\, Q) \xrightarrow{\checkmark} Q}$$

Interrupt

- In process P ∇ Q, whenever an event is engaged by Q, P is interrupted and the control is transferred to Q.

$$\frac{P \xrightarrow{a} P'}{(P \nabla Q) \xrightarrow{a} (P' \nabla Q)}$$

$$\frac{Q \xrightarrow{a} Q'}{(P \nabla Q) \xrightarrow{a} Q}$$

Operational Semantics: Example #1

- Let $VMS = coin \rightarrow (choc \rightarrow VMS \ \Box \ bisc \rightarrow VMS)$

Operation Semantics

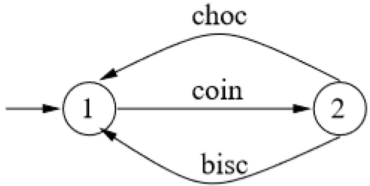
Step 1. $VMS \xrightarrow{coin} (choc \rightarrow VMS \ \Box \ bisc \rightarrow VMS)$

Step 2. $(choc \rightarrow VMS \ \Box \ bisc \rightarrow VMS) \xrightarrow{choc} VMS$

Step 2. $(choc \rightarrow VMS \ \Box \ bisc \rightarrow VMS) \xrightarrow{bisc} VMS$

Labelled Transition System (LTS)

- A **Labelled Transition System** contains a set of states, an initial state (where the system starts from) and a labelled transition relation.



- Let $VMS = coin \rightarrow (choc \rightarrow VMS \ \square \ bisc \rightarrow VMS)$
- State 1 represents the process VMS.
- State 2 represents the process $(choc \rightarrow VMS \ \square \ bisc \rightarrow VMS)$

[1] The Labelled Transition System is a directed graph

Operational Semantics

Interleaving

- In process $P \,|||\, Q$, P and Q behaves independently.
- The exception is the termination, hence assume a is not $\checkmark$.

$$\frac{P \xrightarrow{a} P'}{(P \,|||\, Q) \xrightarrow{a} (P' \,|||\, Q)}$$

$$\frac{Q \xrightarrow{a} Q'}{(P \,|||\, Q) \xrightarrow{a} (P \,|||\, Q')}$$

Synchronization

- In process $P \,|[\, X \,]|\, Q$, no event from X may occur unless jointly by both P and Q.
- When events from X do occur, they occur in P and Q simultaneously.

$$\frac{P \xrightarrow{a} P', a \notin X}{(P \,|[\, X \,]|\, Q) \xrightarrow{a} (P' \,|[\, X \,]|\, Q)}$$

$$\frac{Q \xrightarrow{a} Q', a \notin X}{(P \,|[\, X \,]|\, Q) \xrightarrow{a} (P \,|[\, X \,]|\, Q')}$$

$$\frac{P \xrightarrow{a} P', Q \xrightarrow{a} Q', a \in X}{(P \,|[\, X \,]|\, Q) \xrightarrow{a} (P' \,|[\, X \,]|\, Q')}$$

Operational Semantics: Example #2

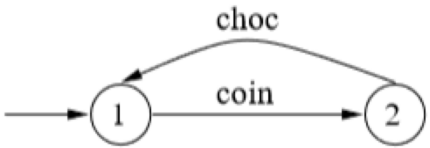
Given the process $a \rightarrow P \,|[\, a \,]|\, (c \rightarrow a \rightarrow Q)$

1. $(a \rightarrow P \,|[\, a \,]|\, (c \rightarrow a \rightarrow Q)) \xrightarrow{c} (a \rightarrow P \,|[\, a \,]|\, (a \rightarrow Q))$
   Only event **c** can be engaged at first as **a** is a common event in both $a \rightarrow P$ and $c \rightarrow a \rightarrow Q$.
2. $(a \rightarrow P \,|[\, a \,]|\, (a \rightarrow Q)) \xrightarrow{a} (P \,|[\, a \,]|\, Q)$
   Engage the common event **a** on both $a \rightarrow P$ and $a \rightarrow Q$.

Operational Semantics: Example #3

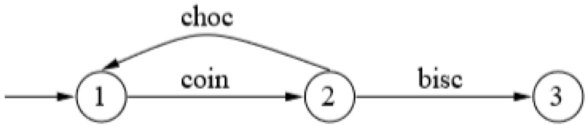
- $VMC = coin \rightarrow (choc \rightarrow VMC \ \square \ bisc \rightarrow VMC)$
- $CHOCLOV = choc \rightarrow CHOCLOV \ \square \ coin \rightarrow choc \rightarrow CHOCLOV$

1. How would the process $VMC \,||[\,A\,]||\, CHOCLOV$ behave when $A = \{coin, choc, bisc\}$
   - Step 1:
     $VMC \,||[\,A\,]||\, CHOCLOV \xrightarrow{coin} (choc \rightarrow VMC \ \square \ bisc \rightarrow VMC) \,||[\,A\,]||\, (choc \rightarrow CHOCLOV)$
   - Step 2:
     $(choc \rightarrow VMC \ \square \ bisc \rightarrow VMC) \,||[\,A\,]||\, (choc \rightarrow CHOCLOV) \xrightarrow{choc} VMC \,||[\,A\,]||\, CHOCLOV$



Operational Semantics Example: #4

- $VMC = coin \rightarrow (choc \rightarrow VMC \ \square \ bisc \rightarrow VMC)$
- $CHOCLOV = choc \rightarrow CHOCLOV \ \square \ coin \rightarrow choc \rightarrow CHOCLOV$
2. How would the process $VMC \ |[\{coin, choc\}]| \ CHOCLOV$ or equivalently $VMC \parallel CHOCLOV$ behave?
   - Step 1: $VMC \parallel CHOCLOV \xrightarrow{coin} (choc \rightarrow VMC \ \square \ bisc \rightarrow VMC) \parallel (choc \rightarrow CHOCLOV)$
   - Step 2:
     $(choc \rightarrow VMC \ \square \ bisc \rightarrow VMC) \ |[A]| \ (choc \rightarrow CHOCLOV) \xrightarrow{choc} VMC \ |[A]| \ CHOCLOV$
   - Step 2: $(choc \rightarrow VMC \ \square \ bisc \rightarrow VMC) \ |[A]| \ (choc \rightarrow CHOCLOV) \xrightarrow{choc}$
     $VMC \ |[A]| \ (choc \rightarrow CHOCLOV)$



Case Study: Dining Philosophers

1. Specify the dining philosophers

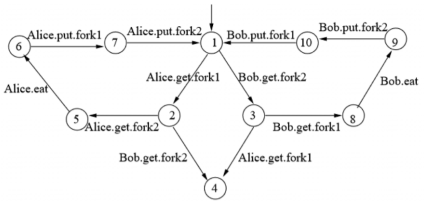
```
1 Alice = Alice.get.fork1 -> Alice.get.fork2 -> Alice.eat -> Alice.put.
      fork1 -> Alice.put.fork2 -> Alice
2 Bob = Bob.get.fork1 -> Bob.get.fork2 -> Bob.eat -> Bob.put.fork1 -> Bob.
      put.fork2 -> Bob
3 Fork1 = (Alice.get.fork1 -> Alice.put.fork1 -> Fork1) [] (Bob.get.fork1
      -> Bob.put.fork1 -> Fork1)
4 Fork2 = (Alice.get.fork2 -> Alice.put.fork2 -> Fork2) [] (Bob.get.fork2
      -> Bob.put.fork2 -> Fork2)
5 College = Alice || Bob || Fork1 || Fork2
```

2. Get the alphabets of each process
   - $\alpha Alice = \{Alice.get.fork1, Alice.get.fork2, Alice.eat, Alice.put.fork1, Alice.put.fork2\}$
   - $\alpha Bob = \{Bob.get.fork1, Bob.get.fork2, Bob.eat, Bob.put.fork1, Bob.put.fork2\}$
   - $\alpha Fork1 = \{Alice.get.fork1, Alice.put.fork1, Bob.get.fork1, Bob.put.fork1\}$
   - $\alpha Fork2 = \{Alice.get.fork2, Alice.put.fork2, Bob.get.fork2, Bob.put.fork2\}$

Case Study: Dining Philosophers

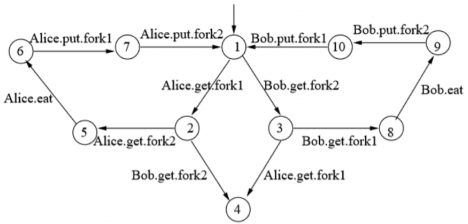
3. Apply the operational semantics rule (one at a time) to build the Labelled Transition System.
   - Alice can perform Alice.get.fork1
   - Bob can perform Bob.get.Fork2
   - Fork1 can perform Alice.get.fork1 or Bob.get.fork1
   - Fork2 can perform Alice.get.fork2 or Bob.get.Fork2
   - By rule syn3, College can perform either Alice.get.fork1 or Bob.get.fork2, and then a state of the form.

$$\cdots \parallel \cdots \parallel \cdots \parallel \cdots$$



Case Study: Dining Philosophers

4. Analyze the Labelled Transition system
   - Is the system deadlock-free?
   - Will Alice or Bob starve to death?



Safety

- Safety means **something bad never happens**.
- Examples
  1. deadlock-freeness

     ```
     #assert College() deadlockfree;
     ```

     The system never deadlocks
  2. invariant

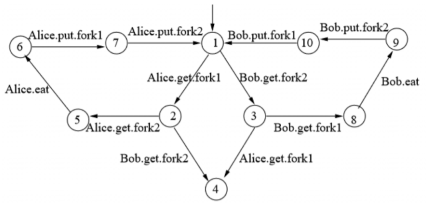
     ```
     #assert Bank() |= [] Value >= Debit;
     ```

     The savings of a bank account must always be non-negative.

[1] '[]' signifies 'always' in Linear Temporal Logic.
[2] '|=' represents 'satisfisfaction' in Linear Temporal Logic.

Verifying Safety

- To verify safety, perform **reachability analysis** on the **Labelled Transition System**.
- A counterexample to the safety property is a finite execution which leads to a bad state.
- Perform either **Depth First Search (DFS)** or **Breadth First Search (BFS)** to search all reachable states for a 'bad' one.
- Example:



1. Depth First Search: $1 \rightarrow 2 \rightarrow 5 \rightarrow 7 \rightarrow 1 \rightarrow$ backtrack $\rightarrow 4 \rightarrow$ FOUND!
2. Breadth First Search: $1 \rightarrow 2 \rightarrow 3 \rightarrow 5 \rightarrow 4 \rightarrow$ FOUND!

[1] State 4 is the bad state as there is no outgoing edges.

Applications of Safety Verification

Many properties can be formulated as a safety property and solved using **reachability analysis**.

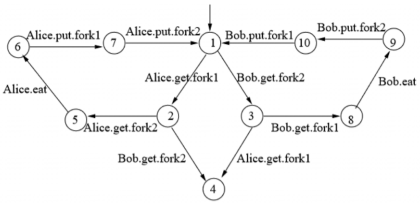
1. Mutual Exclusion: []!(more than one process accessing the critical section)
   - There will never be more than one process accessing the critical section.
2. Security: [](only the authorized user can access the information)
   - It is always the case that only the authorized user can access the information.
3. Program Analysis
   - Arrays are always bounded.
   - Pointers are always non-null
   - etc...

Liveness

- Liveness means **something good eventually happens**.
- Examples
  1. A program is eventually terminating.
  2. A file writer is eventually closed.
  3. Both Alice and Bob eventually get to eat.

Verifying Liveness

- To verify liveness, perform **loop searching** on the **Labelled Transition System**.
- A counterexample to a liveness property is an infinite system execution during which the 'good' thing never happens.
  - Example: An infinite loop fails the property that the program is eventually terminating.
- We can search through the Labelled Transition System for a bad loop using **Nested Depth First Search** or **Strongly Connected Component based Search**
- Example



Assertion: Alice will always eventually eat. (**False**)

```
1 #assert College() |= Alice.eat
```

Counterexamples

- $\langle Alice.get.fork1, Bob.get.fork2 \rangle$
- $< Bob.get.fork2 \rightarrow Bob.get.fork1 \rightarrow Bob.eat \rightarrow Bob.put.fork2, \rightarrow Bob.put.fork1 >^*$