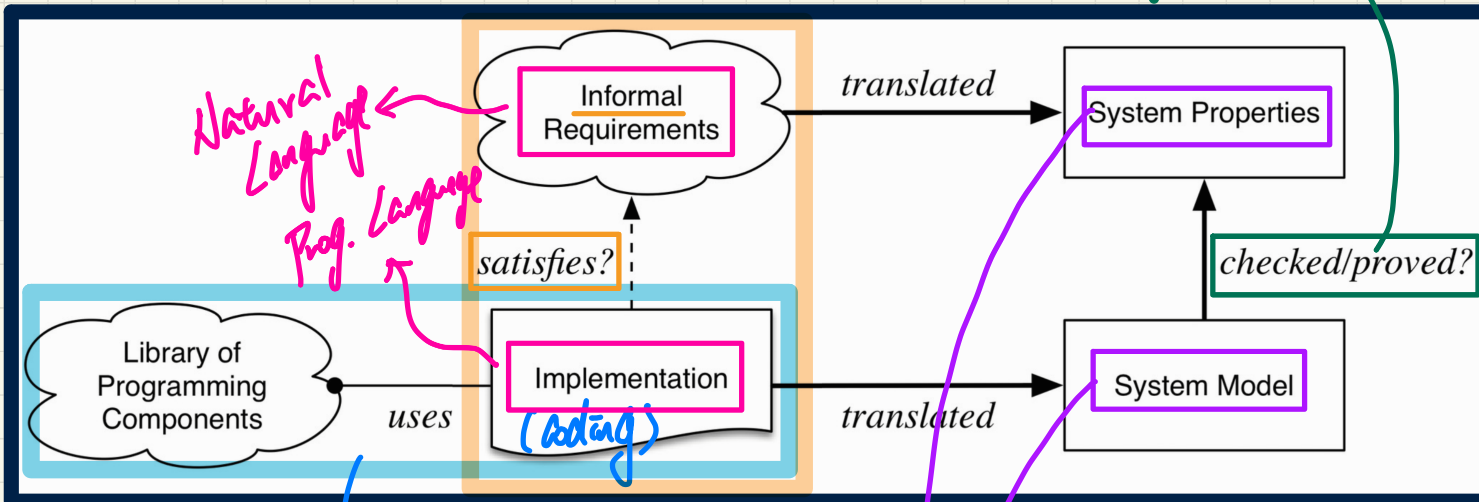
Lecture 1a

Introduction

Building the product right?

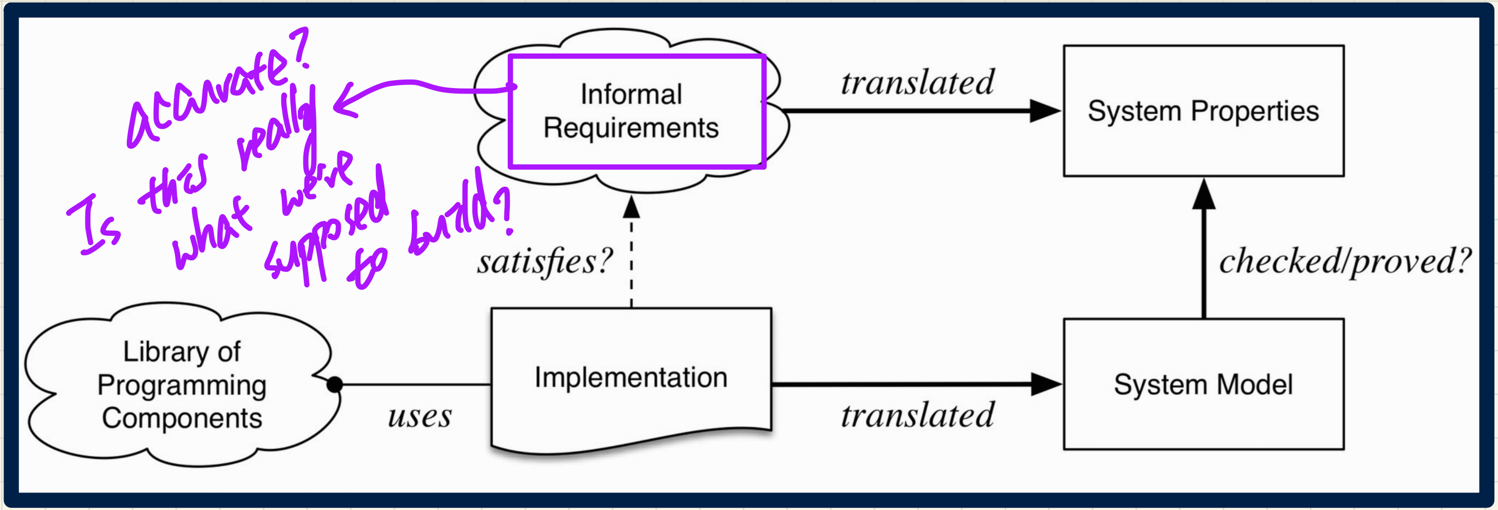
Success means the right product to build? Not necessarily.



e.g. using Java API

specified using the same formal language.

Building the right product?



Model-Based Development

(Scenario I)

$m_0 \xrightarrow{\text{refined by}} m_1 \longrightarrow \cdots\cdots m_n$

a refinement of m_0

$(n+1)$ models for same system.

m_0: most abstract (contains the least amount of details)

easiest to prove some properties

refined by: to be a valid refinements, some proofs need to be done

m_1: more concrete than m_0 (contains more details)

m_n: basis for coding

most concrete (closest to actual code)

(Scenario 2) → infeasible to prove directly these classes

Java classes

Lecture 1b

Review on Math

p	q	$p \Rightarrow q$
true	true	true
true	false	false
false	true	true
false	false	true

p only if q

↳ p holds, then the only way for ⇒ to hold is if q holds

q is necessary for p

↳ p holds, then it's necessary for q to hold s.t. ⇒ holds.

p	q	$p \Rightarrow q$
true	true	true
true	false	false
false	true	true
false	false	true

When is $p \Rightarrow q$ true?

1. both P and q hold

2. p does not hold

q unless $\neg p$

$p \Rightarrow q \equiv \neg p \vee q$

$\forall$ universal quantification ("for all")

$\exists$ existential quantification ("there exists")

$$\exists i, j \bullet (i \in \mathbb{Z} \wedge j \in \mathbb{Z} \wedge i < j) \vee i > j$$

how the predicate is evaluated ∵ $\wedge$ binds more tightly than $\vee$

Precedence of Logical Ops.

$\neg$

$\wedge$

$\vee$

$\Leftrightarrow$ $\equiv$

$$\exists i, j \bullet \underbrace{i \in \mathbb{Z} \wedge j \in \mathbb{Z}}_{R} \wedge \underbrace{(i < j \vee i > j)}_{P}$$

Conversions between $\forall$ and $\exists$

1. $(\forall i \cdot i \in S \Rightarrow i > 0) \Leftrightarrow \neg(\exists i \cdot i \in S \land \neg(i > 0))$

2. $(\exists \underline{\underline{i}} \cdot i \in S \land i > 0) \Leftrightarrow \neg(\forall i \cdot i \in S \Rightarrow \neg(i > 0))$

$\in$ membership

$e \notin S \equiv \neg(e \in S)$

$S = \{1, 2, 3\}$

$T = \{2, 3, 1\}$

$U = \{3, 2\}$

$(i \le j \wedge j \le i) \Leftrightarrow i = j$

$(S \subseteq T \wedge T \subseteq S) \Leftrightarrow S = T$

$S \subseteq T$ ✓ $\quad S \subset S$ ✗

$T \subseteq S$ ✓ $\quad S \subset T$ ✗

$U \subseteq S$ ✓ $\quad S \subset U$ ✗

$U \subseteq T$ ✓

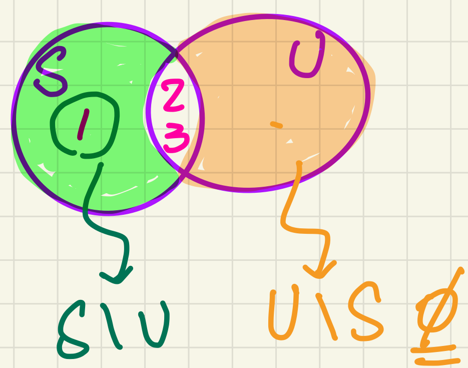
$U \subset S$ ✓

$U \subset T$ ✓

not commutative

$S \boxed{\setminus} U = \{1\}$

$U \setminus S = \emptyset$



Power Set

$$\binom{3}{1} = \underline{\underline{3}}$$

$$\mathbb{P}(\underline{\{1, 2, 3\}})$$

$$\binom{3}{2} = \binom{3}{1} = 3$$

$$= \{ S \mid S \subseteq \{1, 2, 3\} \}$$

$$= \left\{ \begin{array}{l} \underline{\emptyset} \; 0, \\ \boxed{\{1\}, \quad \{2\}, \quad \{3\}}, \\ \boxed{\{1, 2\}, \; \{2, 3\}, \; \{1, 3\}}, \\ \underline{\{1, 2, 3\}} \; 3 \end{array} \right\}$$

subsets of card. 1

subsets of card. 2

int i ; → i stores a single integer

type: set of 2^{32} values

:

$\boxed{i \in int}$

$r : \mathbb{P}(\boxed{S \times T})$

$\in$

declared to store the value of a single relation, which is a subset of $S \times T$

each member is a subset of $S \times T$ (which will be a relation smaller than or equal to $S \times T$)

max relation on S and T

$r : \mathbb{P}(S \times T)$

$\equiv$

$r : S \leftrightarrow T$

$\boxed{\text{Enumerate : } \{a, b\} \leftrightarrow \{1, 2, 3\}}$

$$\mathbb{P}(\{a, b\} \times \{1, 2, 3\})$$

relations of card. 2

$$\binom{6}{2} = \frac{6 * 5}{2!} = 15.$$

card. of max relation

relation of card. 0

$\emptyset$,

relations of card. 1 $\binom{6}{1} = 6$

$\{(a,1)\}$, $\{(a,2)\}$, $\{(a,3)\}$, $\{(b,1)\}$, $\{(b,2)\}$, $\{(b,3)\}$

relations of card. 2 15

$\{(a,1), (a,2)\}$, $\{(a,2), (a,3)\}$, ...

card 3.

4.

5.

max relation of card. 6

$\{(a,1), (a,2), (a,3), (b,1), (b,2), (b,3)\}$

$r = \{(a, 1), (b, 2), (c, 3), (a, 4), (b, 5), (c, 6), (d, 1), (e, 2), (f, 3)\}$

$dom(r) = \{a, b, c, d, e, f\}$

$r = \{(a, 1), (b, 2), (c, 3), (a, 4), (b, 5), (c, 6), (d, 1), (e, 2), (f, 3)\}$

$ran(r) = \{1, 2, 3, 4, 5, 6\}$

$r = \{(a, 1), (b, 2), (c, 3), (a, 4), (b, 5), (c, 6), (d, 1), (e, 2), (f, 3)\}$

① $dom(r^{-1}) = ran(r)$ ② $ran(r^{-1}) = dom(r)$

$r^{-1} = \{(1, a), (2, b), (3, c), (4, a), (5, b), (6, c), (1, d), (2, e), (3, f)\}$

$r: S \leftrightarrow T$

$r = \{(a, 1), (b, 2), (c, 3), (a, 4), (b, 5), (c, 6), (d, 1), (e, 2), (f, 3)\}$

$r[\underbrace{\{a, b\}}_{\subseteq S}] = \{1, 2, 4, 5\}$

$r = \{(a, 1), (b, 2), (c, 3), (a, 4), (b, 5), (c, 6), (d, 1), (e, 2), (f, 3)\}$

$$\{a, b\} \lhd r = \underbrace{\{(a, 1), (b, 2), (a, 4), (b, 5)\}}_{r \text{ domain-restricted to } \{a, b\}}$$

$r = \{(a, 1), (b, 2), (c, 3), (a, 4), (b, 5), (c, 6), (d, 1), (e, 2), (f, 3)\}$

$$r \rhd \{1, 2\} = \underbrace{\{(a, 1), (b, 2), (d, 1), (e, 2)\}}_{r \text{ range-restricted to } \{1, 2\}}$$

$r = \{(a, 1), (b, 2), (c, 3), (a, 4), (b, 5), (c, 6), (d, 1), (e, 2), (f, 3)\}$

$$\{a, b\} ⩤ r = \underbrace{\{(c, 3), (c, 6), (d, 1), (e, 2), (f, 3)\}}_{r \text{ domain-subtracted by } \{a, b\}}$$

$r = \{(a, 1), (b, 2), (c, 3), (a, 4), (b, 5), (c, 6), (d, 1), (e, 2), (f, 3)\}$

$$r ⩥ \{1, 2\} = \underbrace{\{(c, 3), (a, 4), (b, 5), (c, 6), (f, 3)\}}_{r \text{ range-subtracted by } \{1, 2\}}$$