CS 430/530
Formal Semantics

Zhong Shao
Yale University
Department of Computer Science

Course Overview
August 28, 2013
Today’s Lecture

• Why study formal semantics?
• How I teach this course?
• Math background and predicate logic
What Is Formal Semantics?

**formal** --- “mathematically rigorous”

**semantics** --- “study of meanings”

Obviously:

- What is a programming language? What is a program?
- What are the meanings of specific language features and how they interact?
- How to make sure that a program behaves according to its “specification”?

But also:

- How do we explain these “meanings”? in which “language”?
- What is a meta logic? What is a mechanized meta logic?
- What is a specification language? What is its “semantics”? 
Why Take CS-430?

• Software reliability and security are the biggest problems faced by the IT industry today! You are likely to worry about them in your future jobs.

• It will give you an edge over your competitors: industry and most other schools don’t teach this.

• It will improve your programming skills – because you will have a better appreciation of what your programs actually mean.

• You will be better able to compare and contrast programming languages, or even design your own.

• It is an important and exciting area of research, with many new ideas and perspectives frequently emerging.
Arianne 5

40 seconds into its flight it veered off course and exploded.

It was later found to be an error in reuse of a software component.

On June 4, 1996, the Arianne 5 took off on its maiden flight.

(This picture became quite popular in talks on software reliability and related topics.)
“Better, Faster, Cheaper”

In 1999, NASA lost both the Mars Polar Lander and the Climate Orbiter.

Later investigations determined software errors were to blame.

- Orbiter: Component reuse error.
- Lander: Precondition violation.
USS Yorktown

“After a crew member mistakenly entered a zero into the data field of an application, the computer system proceeded to divide another quantity by that zero. The operation caused a buffer overflow, in which data leaked from a temporary storage space in memory, and the error eventually brought down the ship's propulsion system. The result: the Yorktown was dead in the water for more than two hours.”
Therac-25

From 1985-1987, several cancer patients were killed or seriously injured as a result of being over-radiated by Therac-25, a radiation treatment facility.

The problem was due to a subtle race condition between concurrent processes.
Computer Viruses

Need we say more?

For more “software horror stories”, see http://www.cs.tau.ac.il/~nachumd/horror.html
Observations

• Failure often due to simple problems “in the details”.

• Small theorems about large programs would be useful.

• Need clearly specified interfaces and checking of interface compliance.

• Better languages would help!
Challenges

The impact and cost of software failures will increase, as will the demand for extensibility.

The distinction between “safety-critical” and “consumer electronics” software will fade away.

*Who will provide the technology for “safe” software systems?*
10 Emerging Technologies 2011,
In: Technology Review, 2011(6), MIT Press
http://www.technologyreview.com/tr10/

- Social Indexing
  Facebook remaps the Web to personalize online services

- Homomorphic Encryption
  Making cloud computing more secure

- Smart Transformers
  Controlling the flow of electricity to stabilize the grid

- Cloud Streaming
  Bringing high-performance software to mobile devices

- Gestural Interfaces
  Controlling computers with our bodies

- Crash-Proof Code
  Making critical software safer

- Cancer Genomics
  Deciphering the genetics behind the disease

- Separating Chromosomes
  A more precise way to read DNA will change how we treat disease

- Solid-State Batteries
  High-energy cells for cheaper electric cars

- Synthetic Cells
  Designing new genomes could speed the creation of vaccines and biofuel-producing bacteria
Opportunities

High assurance / reliability depends fundamentally on our ability to reason about programs.

The opportunities for new languages as well as formal semantics, type theory, computational logic, and so on, are great.
Certifying a computing host?

Need to reason about:

- human behaviors
- cosmic rays + natural disasters
- hardware failure
- software

VIEW #1: bug-free host impossible. Treat it as a biological system.
Certifying a computing host?

Need to reason about:
- human behaviors
- cosmic rays + natural disasters
- hardware failure
- software

VIEW #2: focus on software since it is a rigorous mathematical entity!
Certified software

Find a mathematical *proof* showing that

*if the HW/Env follows its model, the software will run according to its specification*
Certified OS kernel

Research tasks & key innovations:

• new **OS kernel** that can “crash-proof” the entire system & application SW

• new **PLs** for writing certified kernel plug-ins (new OCAP + DSPLs)

• new **formal methods** for automating proofs & specs (VeriML)
Certified “hypervisor” kernel

- Problems w. existing platforms
  - Attacks: Zero-Day Kernel Vulnerabilities (ZDKVs) & rogue driver certificates
  - leads to rogue kernels
  - leads to rogue WinCC/Step7 apps
  - leads to rogue PLC firmware

- New CRASH technologies
  - A small certified “hypervisor” kernel provides a reliable ZDKV-free core to fall back on, even under attacks
  - Information-Flow-Control to enforce security
  - Mechanized proof certificates are unforgeable
CertikOS architecture
Compositional specification & verification

- **abs-layer-x spec**
  - kmodx.c
  - kmodx.s
- **abs-layer-1 spec**
  - kmod1.c
  - kmod1.s
- **abs-layer-2 spec**
  - kmod2.c
  - kmod2.s
- **abs-layer-k spec**
  - kmodk.s
- **abs-layer-z spec**
  - kmodz.c
  - kmodz.s

- **high-level kernel spec**
  - kinit.c
  - kmody.c
  - kmody.s

- **Raw Machine / HW Spec**

- **Safety**
  (never crash)
- **Correctness**
- **Secure**
  (no info leak)
- **Liveness**
  (resource usage)
Compositional specification & verification

current target: single-core CertiKOS

User-space
- User-space Virtual Machine Manager
- Virtual Device 1
- Virtual Device 2
- ... Virtual Device N
- Virtual Machine
- Certified App
- Uncertified App

Trap
- Trap Handlers
  (interrupts, exceptions, system call handlers)

Virtualization
- AMD SVM Abstraction
  (primitives for VMCB & NPT)

Process & Thread
- Process & Thread Management

MM
- Memory Management
  (Physical Memory & Virtual Memory Management)

Driver
- CPU Driver
- ACPI Driver
- Interrupt Controller Driver
- Console Driver
- Timer Driver
- IDE Driver
- SVM Driver

HW
- CPU
- Local APIC
- IOAPIC
- Memory
- Timer (8254)
- KBD (8042)
- IDE Controller
- VGA
Decomposing CertiKOS

Initialization of paging mechanism

Providing address space

Physical Memory and Virtual Memory Management

Based on the abstract machine provided by boot leader
Decomposing CertiKOS (cont’d)

Thread and Process Management
Course Overview
My Goals

I have two goals:

• To teach the most common methods for specifying formal semantics. In particular, the denotational, operational, axiomatic and type-theoretic methods.

  This will give you the necessary tools to understand semantic specifications and to develop new ones.

• To survey existing language features to provide a deep understanding of what these features really mean, what they do, and how they compare.

  This will enable you to better evaluate existing languages and new ones as they are developed.
Prerequisites

• CS-201, CS-202, CS-223, CS-323 (or equivalents)

• Mathematical background: logic, sets, relations, functions, products, and unions. (See Appendix in Reynolds textbook.)

• A desire to learn!
Course Requirements

Class attendance is recommended
  • Outside material will be introduced.

Problem sets
  • Problems from textbooks.
  • Programming assignments; We will *prototype* some of our semantics specifications in Coq (or ML/Haskell).

Readings
  • Selected chapters in the main textbooks (Harper and Reynolds).
  • A couple of research papers.
  • Coq (or ML/Haskell) tutorials if you don’t know them.

Grading
  • About 70% problem sets, 30% final project/exam (no midterm).
Syllabus

1. Introduction; Predicate Logic
2. Inductive Definitions
3. Abstract Syntax and Binding
4. Imp; Denotational Semantics
5. Failure, Input-Output, and Continuations
6. Static and Dynamic Semantics
7. Program Specifications and Proofs
8. Function Types
9. Plotkin's PCF
10. Finite Data Types
11. Infinite Data Types
12. Untyped Lambda Calculus
13. Dynamic Typing
Syllabus (cont’d)

14. Polymorphic Types
15. Existential Types
16. Control Stacks and Exceptions
17. Continuations
18. Types and Propositions
19. Subtyping; Semantics of Types
20. Storage Effects
21. Monads and Comonads
22. Lazy Evaluation
23. Parallelism
24. Process Calculus
25. Monadic Concurrency
Course Webpage

http://flint.cs.yale.edu/cs430
Predicate Logic

&

Math Background
Predicate Logic

Predicate logic over integer expressions:

   a language of logical assertions, for example

\[ \forall x. \ x + 0 = x \]

Why discuss predicate logic?

- It is an example of a simple language
- It has simple denotational semantics
- We will use it later in program specifications
Abstract Syntax

Describes the structure of a phrase ignoring the details of its representation.

An abstract grammar for predicate logic over integer expressions:

\[
\text{intexp ::= } 0 \mid 1 \mid \ldots \\
\quad \mid \text{var} \\
\quad \mid \neg \text{intexp} \mid \text{intexp} + \text{intexp} \mid \text{intexp} - \text{intexp} \mid \ldots
\]

\[
\text{assert ::= } \text{true} \mid \text{false} \\
\quad \mid \text{intexp} = \text{intexp} \mid \text{intexp} < \text{intexp} \mid \text{intexp} \leq \text{intexp} \mid \ldots \\
\quad \mid \neg \text{assert} \mid \text{assert} \land \text{assert} \mid \text{assert} \lor \text{assert} \\
\quad \mid \text{assert} \Rightarrow \text{assert} \mid \text{assert} \Leftrightarrow \text{assert} \\
\quad \mid \forall \text{var. assert} \mid \exists \text{var. assert}
\]
Resolving Notational Ambiguity

- Using parentheses: \( (\forall x. (((((x) + (0)) + 0) + 0) = (x))) \)

- Using precedence and parentheses: \( \forall x. (x + 0) + 0 = x \)
  arithmetic operators \( (\ast / \text{rem} \ldots) \) with the usual precedence
  relational operators \( (= \neq < \leq \ldots) \)

- The body of a quantified term extends to a delimiter.
Carriers and Constructors

- **Carriers:** sets of abstract phrases (e.g. `intexp`, `assert`)
- **Constructors:** specify abstract grammar productions

\[
\begin{align*}
\text{intexp} &::= 0 \quad \rightarrow \quad c_0 \in \{\langle \rangle \} \rightarrow \text{intexp} \\
\text{intexp} &::= \text{intexp} + \text{intexp} \quad \rightarrow \quad c_+ \in \text{intexp} \times \text{intexp} \rightarrow \text{intexp}
\end{align*}
\]

Note: Independent of the concrete pattern of the production:

\[
\begin{align*}
\text{intexp} &::= \text{plus} \ \text{intexp} \ \text{intexp} \quad \rightarrow \quad c_+ \in \text{intexp} \times \text{intexp} \rightarrow \text{intexp}
\end{align*}
\]

- Constructors must be injective and have disjoint ranges
- Carriers must be either predefined or their elements must be constructible in finitely many constructor applications
Inductive Structure of Carrier Sets

With these properties of constructors and carriers, carriers can be defined inductively:

\[
\begin{align*}
\text{intexp}^{(0)} &= \{\} \\
\text{intexp}^{(j+1)} &= \{c_0\langle\rangle, \ldots\} \cup \{c_+(x_0, x_1) \mid x_0, x_1 \in \text{intexp}^{(j)}\} \cup \ldots \\
\text{assert}^{(0)} &= \{\} \\
\text{assert}^{(j+1)} &= \{c_{\text{true}}\langle\rangle, c_{\text{false}}\langle\rangle\} \\
&\quad \cup \{c=(x_0, x_1) \mid x_0, x_1 \in \text{intexp}^{(j)}\} \cup \ldots \\
&\quad \cup \{c_-(x_0) \mid x_0 \in \text{assert}^{(j)}\} \cup \ldots
\end{align*}
\]

\[
\begin{align*}
\text{intexp} &= \bigcup_{j=0}^{\infty} \text{intexp}^{(j)} \\
\text{assert} &= \bigcup_{j=0}^{\infty} \text{assert}^{(j)}
\end{align*}
\]
Denotational Semantics of Predicate Logic

The meaning of a term \( e \in intexp \) is \( \llbracket e \rrbracket_{intexp} \)
i.e. the function \( \llbracket - \rrbracket_{intexp} \) maps \( intexp \) objects to their meanings.

What is the set of meanings?

The meaning \( \llbracket 5 + 37 \rrbracket_{intexp} \) of the term \( 5 + 37 \) could be the integer 42.
(that is, \( c_{+}(c_{5}\langle \rangle, c_{37}\langle \rangle) \))

However the term \( x + 5 \) contains the free variable \( x \),
so the meaning of an \( intexp \) in general cannot be an integer…
Mathematical Background

- Sets
- Relations
- Functions
- Sequences
- Products and Sums
## Sets

\[
x \in S \quad \text{membership}
\]

\[
x \notin S \quad S = \{x\}
\]

\[
S \subseteq T \quad \text{inclusion}
\]

\[
S \subseteq^\text{fin} T \quad \text{finite subset}
\]

\[
\{E \mid P\} \quad \text{set comprehension}
\]

\[
S \cap T \quad \text{intersection} \quad = \{x \mid x \in S \text{ and } x \in T\}
\]

\[
S \cup T \quad \text{union} \quad = \{x \mid x \in S \text{ or } x \in T\}
\]

\[
S - T \quad \text{difference} \quad = \{x \mid x \in S \text{ and not } x \in T\}
\]

\[
\mathcal{P} S \quad \text{powerset} \quad = \{T \mid T \subseteq S\}
\]

\[
m \text{ to } n \quad \text{integer range} \quad = \{x \mid m \leq x \text{ and } x \leq n\}
\]

- \(\emptyset\) the empty set
- \(\mathbb{N}\) natural numbers
- \(\mathbb{Z}\) integers
- \(\mathbb{B} = \{\text{true, false}\}\)
Generalized Set Operations

\[ \bigcup S \overset{\text{def}}{=} \{ x \mid \exists T \in S. x \in T \} \quad \bigcap S \overset{\text{def}}{=} \{ x \mid \forall T \in S. x \in T \} \]

\[ \bigcup_{i \in I} S \overset{\text{def}}{=} \bigcup \{ S' \mid i \in I \} \quad \bigcap_{i \in I} S \overset{\text{def}}{=} \bigcap \{ S' \mid i \in I \} \ldots \]

\[ \bigcup_{i=m}^{n} S \overset{\text{def}}{=} \bigcup_{i \in m \text{ to } n} S \quad \bigcap_{i=m}^{n} S \overset{\text{def}}{=} \bigcap_{i \in m \text{ to } n} S \]

\[ \bigcup \{ \} = \{ \} \]

\[ \bigcap \{ \} \quad \text{meaningless} \]

Examples:

\[ A \cup B = \bigcup \{ A, B \} \]

\[ \bigcup \{ i \text{ to } (i + 1) \mid i \in \{ j^2 \mid j \in 1 \text{ to } 3 \} \} = \{1, 2, 4, 5, 9, 10\} \]
Relations

A relation $\rho$ is a set of primitive pairs $[x, y]$.

\[
\rho \text{ relates } x \text{ and } y \iff x \rho y \iff [x, y] \in \rho
\]

$\rho$ is an identity relation $\iff (\forall x, y. x \rho y \Rightarrow x = y)$

the identity on $S$ $I_S \overset{\text{def}}{=} \{[x, x] | x \in S\}$

the domain of $\rho$ $\text{dom} \ \rho \overset{\text{def}}{=} \{x | \exists y. x \rho y\}$

the range of $\rho$ $\text{ran} \ \rho \overset{\text{def}}{=} \{x | \exists y. y \rho x\}$

composition of $\rho$ with $\rho'$ $\rho' \cdot \rho \overset{\text{def}}{=} \{[x, z] | \exists y. x \rho y \text{ and } y \rho' z\}$

reflection of $\rho$ $\rho^\dagger \overset{\text{def}}{=} \{[y, x] | [x, y] \in \rho\}$
Relations: Properties and Examples

$$(\rho_3 \cdot \rho_2) \cdot \rho_1 = \rho_3 \cdot (\rho_2 \cdot \rho_1)$$

$$\rho \cdot I_S \subseteq \rho \supseteq I_T \cdot \rho$$

$$\text{dom } I_S = S = \text{ran } I_S$$

$$I_T \cdot I_S = I_{T \cap S}$$

$$I_S^\dagger = I_S$$

$$(\rho^\dagger)^\dagger = \rho$$

$$(\rho_2 \cdot \rho_1)^\dagger = \rho_1^\dagger \cdot \rho_2^\dagger$$

$$\rho \cdot \{\} = \{\} = \{\} \cdot \rho$$

$$I_\{\} = \{\} = \{\}^\dagger$$

$$\text{dom } \rho = \{\} \Rightarrow \rho = \{\}$$

$${\mathbf{I}}_N = \{[0, 0], [1, 1], [2, 2], \ldots\}$$

$$\lt = \{[0, 1], [0, 2], [1, 2], \ldots\}$$

$$\leq = \{[0, 0], [0, 1], [1, 1], [0, 2], \ldots\}$$

$$\geq = \{[0, 0], [1, 0], [1, 1], [2, 0], \ldots\}$$

$$\lt \subseteq \leq$$

$$\lt \cup {\mathbf{I}}_N = \leq$$

$$\leq \cap \geq = {\mathbf{I}}_N$$

$$\lt \cap \geq = \{\}$$

$$\lt \cdot \leq = \lt$$

$$\leq \cdot \leq = \leq$$

$$\geq = \leq^\dagger$$
Functions

A relation $f$ is a function if
\[ \forall x, x', x''. ([x, x'] \in f \text{ and } [x, x''] \in f) \Rightarrow x' = x'' \]

If $f$ is a function,
\[ f x = y \iff f x = y \iff f \text{ maps } x \text{ to } y \iff [x, y] \in f \]

$I_S$ and $\{\}$ are functions.
If $f$ and $g$ are functions, then $g \cdot f$ is a function: $(g \cdot f) x = g(f x)$

$f^\dagger$ is not necessarily a function:
consider $f = \{[[\text{true}, \{\}]], [[\text{false}, \{\}]]\}$

$f$ is an injection if both $f$ and $f^\dagger$ are functions.
Notation for Functions

Typed abstraction: \( \lambda x \in S. \, E \overset{\text{def}}{=} \{ [x, E] \mid x \in S \} \)

Defined only when \( E \) is defined for all \( x \in S \)

(consider \( \lambda g \in \mathbb{N}. \, g \, 3 \))

\( I_S = \lambda x \in S. \, x \)

\( g \cdot f = \lambda x \in \text{dom } f. \, g(f \, x), \text{ if ran } f \subseteq \text{dom } g. \)

Placeholder: \( E \) with a dash (\( - \)) standing for the bound variable

\( g \, (-) \, h = \lambda x \in S. \, (g \, (x)) \, h \)

\(- + 42 = \lambda x \in \mathbb{N}. \, x + 42 \)

Variation of a function \( f \): \([f \mid x : y] \, z = \begin{cases} y, & \text{if } z = x \\ f \, z, & \text{otherwise} \end{cases} \)

\( \text{dom } [f \mid x : y] = (\text{dom } f) \cup \{x\} \)

\( \text{ran } [f \mid x : y] = ((\text{ran } f) - \{z \mid [x, z] \in f\}) \cup \{y\} \)
Sequences

\[[f \mid x_1 : y_1 | \ldots | x_n : y_n] \overset{\text{def}}{=} \ldots [f \mid x_1 : y_1] \ldots | x_n : y_n\]

\[[x_1 : y_1 | \ldots | x_n : y_n] \overset{\text{def}}{=} [\{\} | x_1 : y_1 | \ldots | x_n : y_n]\]

\[\langle x_0, \ldots x_{n-1} \rangle \overset{\text{def}}{=} [0 : x_0 | \ldots n-1 : x_{n-1}]\]

\[
\begin{align*}
\emptyset &= \{\}\quad — \text{the empty function} \\
\langle \rangle &= [\emptyset] = \{\}\quad — \text{the empty sequence} \\
\langle x_0, \ldots x_{n-1} \rangle &= \text{an } n\text{-tuple} \\
\langle x, y \rangle &= \text{a (non-primitive) pair} \\
\text{dom } \langle x_0, \ldots x_{n-1} \rangle &= 0 \text{ to } (n-1) \\
\langle x_0, \ldots x_{n-1} \rangle_i &= x_i \quad \text{when } i \in 0 \text{ to } (n-1)
\end{align*}
\]
Products

Let $\theta$ be an indexed family of sets (a function with sets in its range). The **Cartesian product** of $\theta$ is

$$
\prod \theta \equiv \{ f \mid \text{dom } f = \text{dom } \theta \text{ and } \forall i \in \text{dom } \theta. f i \in \theta i \}
$$

$$
\prod \langle B, B \rangle \\
= \prod (\lambda x \in 0 \text{ to } 1. B) \\
= \{ [0 : \text{true}, 1 : \text{true}], [0 : \text{true}, 1 : \text{false}], \\
[0 : \text{false}, 1 : \text{true}], [0 : \text{false}, 1 : \text{false}] \} \\
= \{ \langle \text{true}, \text{true} \rangle, \langle \text{true}, \text{false} \rangle, \langle \text{false}, \text{true} \rangle, \langle \text{false}, \text{false} \rangle \}
$$
More Products

\[
\prod_{x \in T} S \overset{\text{def}}{=} \prod \lambda x \in T. S
\]

\[
\prod_{i=m}^{n} S \overset{\text{def}}{=} \prod_{i \in (m \text{ to } n)} S
\]

\[
S_1 \times \ldots \times S_n \overset{\text{def}}{=} \prod_{i=1}^{n} \text{"}S_i\text{"}
\]

\[
S^T \overset{\text{def}}{=} \prod_{x \in T} S
\]

\[
S^n \overset{\text{def}}{=} S^0 \text{ to } (n-1) = S \times \ldots \times S \overset{n \text{ times}}{=}
\]

\[
\prod \langle B, B \rangle = B \times B = B^2
\]

\[
S^0 = S^\{\} = \{\langle \rangle\} = \{\{\}\}
\]
## Sets of Sequences

<table>
<thead>
<tr>
<th>Expression</th>
<th>Definition</th>
<th>Set Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$S^+$</td>
<td>$\bigcup_{i=1}^{\infty} S^i$</td>
<td>Let $U = {\langle \rangle}$</td>
</tr>
<tr>
<td>$S^*$</td>
<td>$S^0 \cup S^+$</td>
<td>$U^+ = {\langle \rangle, \langle \rangle, \langle \rangle, \langle \rangle, \langle \rangle, \langle \rangle, \ldots \text{(finite)}}$</td>
</tr>
<tr>
<td>$S^\infty$</td>
<td>$S^* \cup S^\mathbb{N}$</td>
<td>$U^\infty = {\langle \rangle, \langle \rangle, \langle \rangle, \langle \rangle, \langle \rangle, \langle \rangle, \langle \rangle, \langle \rangle, \ldots \text{(infinite)}}$</td>
</tr>
</tbody>
</table>
Sums

Let $\theta$ be an indexed family of sets (a function with sets in its range). The **disjoint union** (sum) of $\theta$ is

$$\sum \theta \overset{\text{def}}{=} \{ \langle i, x \rangle \mid i \in \text{dom} \theta \text{ and } x \in \theta i \}$$

$$\sum_{x \in T} S \overset{\text{def}}{=} \sum \lambda x \in T. S \quad S_1 + \ldots + S_n \overset{\text{def}}{=} \sum_{i=1}^n \langle \text{"S}_i\rangle$$

$$\sum_{i=m}^n S \overset{\text{def}}{=} \sum_{i \in (m \text{ to } n)} S \quad T \times S = \sum_{x \in T} S$$

$$n \times S = (0 \text{ to } (n - 1)) \times S = \underbrace{S + \ldots + S}_{n \text{ times}}$$

$$B + B = \sum \langle B, B \rangle = \{ \langle 0, \text{true} \rangle, \langle 0, \text{false} \rangle, \langle 1, \text{true} \rangle, \langle 1, \text{false} \rangle \}$$

$$= 2 \times B$$
 Functions of Multiple Arguments

- Use **tuples** instead of multiple arguments:

\[
\begin{align*}
  f(a_0, \ldots a_{n-1}) & \longrightarrow f\langle a_0, \ldots a_{n-1}\rangle \\
\end{align*}
\]

Syntactic sugar:

\[
\begin{align*}
  \lambda\langle x_0 \in S_0, \ldots, x_{n-1} \in S_{n-1}\rangle. E \\
  \overset{\text{def}}{=} \lambda x \in S_0 \times \ldots \times S_{n-1}. (\lambda x_0 \in S_0. \ldots \lambda x_{n-1} \in S_{n-1}. E) \\
  (x_0) \ldots (x(n-1))
\end{align*}
\]

- Use **Currying**:

\[
\begin{align*}
  f(a_0, \ldots a_{n-1}) & \longrightarrow f\ a_0 \ldots a_{n-1} \\
  = (\ldots (f\ a_0) \ldots)\ a_{n-1}
\end{align*}
\]

where \( f \) is a Curried function \( \lambda x_0 \in S_0. \ldots \lambda x_{n-1} \in S_{n-1}. E \).
Relations Between Sets

\( \rho \) is a relation from \( S \) to \( T \)

\[ \iff \quad \rho \in S \xrightarrow{\text{REL}} T \]

\[ \iff \quad \text{dom } \rho \subseteq S \text{ and } \text{ran } \rho \subseteq T. \]

Relation on \( S \) \( \overset{\text{def}}{=} \) relation from \( S \) to \( S \).

\( I_S \in S \xrightarrow{\text{REL}} S \)

\( \rho \in S \xrightarrow{\text{REL}} T \implies \rho \uparrow \in T \xrightarrow{\text{REL}} S \)

For all \( S \) and \( T \), \( \{\} \in S \xrightarrow{\text{REL}} T \)

\( \{\} \in! S \xrightarrow{\text{REL}} \{\} \)

\( \{\} \in! \{\} \xrightarrow{\text{REL}} T \)
Total Relations

\( \rho \in S_{\text{REL}} T \) is a total relation from \( S \) to \( T \)

\[ \iff \quad \rho \in S_{\text{TREL}} T \]

\[ \iff \quad \forall x \in S. \exists y \in T. x \, \rho \, y \]

\[ \iff \quad \text{dom } \rho = S \]

\[ \iff \quad I_S \subseteq \rho^\dagger \cdot \rho \]

\[ \rho \in (\text{dom } \rho)_{\text{TREL}} T \iff T \supseteq \text{ran } \rho \]
Functions Between Sets

\[ f \text{ is a partial function from } S \text{ to } T \]

\[ \iff f \in S \xrightarrow{\text{PFUN}} T \]

\[ \iff f \in S \xrightarrow{\text{REL}} T \text{ and } f \text{ is a function.} \]

“Partial”: \( f \in S \xrightarrow{\text{REL}} T \Rightarrow \text{dom } f \subseteq S \)

\[ f \in S \xrightarrow{\text{PFUN}} T \text{ is a (total) function from } S \text{ to } T \]

\[ \iff f \in S \rightarrow T \]

\[ \iff \text{dom } f = S. \]

- \( S \rightarrow T = T^S = \prod_{x \in S} T \)
- \( S \rightarrow T \rightarrow U = S \rightarrow (T \rightarrow U) \)
Surjections, Injections, Bijections

\( f \) is a surjection from \( S \) to \( T \) \iff \( \text{ran } f = T \)

\( f \) is a injection from \( S \) to \( T \) \iff \( f^\dagger \in T \xrightarrow{\text{PFUN}} S \)

\( f \) is a bijection from \( S \) to \( T \) \iff \( f^\dagger \in T \rightarrow S \)

\[ \iff f \text{ is an isomorphism from } S \text{ to } T \]
Back to Predicate Logic

\[\text{intexp} ::= 0 | 1 | \ldots\]
\[\phantom{\text{intexp}} | \text{var} \]
\[\phantom{\text{intexp}} | \neg\text{intexp} | \text{intexp} + \text{intexp} | \text{intexp} - \text{intexp} | \ldots\]

\[\text{assert} ::= \text{true} | \text{false} \]
\[\phantom{\text{assert}} | \text{intexp} = \text{intexp} | \text{intexp} < \text{intexp} | \text{intexp} \leq \text{intexp} | \ldots\]
\[\phantom{\text{assert}} | \neg\text{assert} | \text{assert} \land \text{assert} | \text{assert} \lor \text{assert} \]
\[\phantom{\text{assert}} | \text{assert} \Rightarrow \text{assert} | \text{assert} \Leftrightarrow \text{assert} \]
\[\phantom{\text{assert}} | \forall \text{var}. \text{assert} | \exists \text{var}. \text{assert} \]
Denotational Semantics of Predicate Logic

The meaning of term $e \in intexp$ is $\llbracket e \rrbracket_{intexp}$ i.e. the function $\llbracket - \rrbracket_{intexp}$ maps objects from $intexp$ to their meanings.

What is the set of meanings?

The meaning $\llbracket 5 + 37 \rrbracket_{intexp}$ of the term $5 + 37$ could be the integer 42.

But the term $x + 5$ contains the free variable $x$...
Environments

...hence we need an environment (variable assignment, state)

\[ \sigma \in \Sigma \overset{\text{def}}{=} \text{var} \rightarrow \mathbb{Z} \]

to give meaning to free variables.

The meaning of a term is a function from the states to \( \mathbb{Z} \) or \( \mathbb{B} \).

\[
\begin{align*}
\llbracket - \rrbracket_{\text{intexp}} & \in \text{intexp} \rightarrow \Sigma \rightarrow \mathbb{Z} \\
\llbracket - \rrbracket_{\text{assert}} & \in \text{assert} \rightarrow \Sigma \rightarrow \mathbb{B}
\end{align*}
\]

if \( \sigma = [x:3, y:4] \), then \( \llbracket x+5 \rrbracket_{\text{intexp}} \sigma = 8 \)

\( \llbracket \exists z. x < z \land z < y \rrbracket \sigma = \text{false} \)
Direct Semantics Equations for Predicate Logic

\[ v \in \text{var} \quad e \in \text{intexp} \quad p \in \text{assert} \]

\[
\begin{align*}
\llbracket 0 \rrbracket \text{intexp}\sigma &= 0 \\
(\text{really } \llbracket c_0 \langle \rangle \rrbracket \text{intexp}\sigma &= 0)
\end{align*}
\]

\[
\begin{align*}
\llbracket v \rrbracket \text{intexp}\sigma &= \sigma v \\
\llbracket e_0 + e_1 \rrbracket \text{intexp}\sigma &= \llbracket e_0 \rrbracket \text{intexp}\sigma + \llbracket e_1 \rrbracket \text{intexp}\sigma \\
\llbracket \text{true} \rrbracket \text{assert}\sigma &= \text{true} \\
\llbracket e_0 = e_1 \rrbracket \text{assert}\sigma &= \llbracket e_0 \rrbracket \text{intexp}\sigma = \llbracket e_1 \rrbracket \text{intexp}\sigma \\
\llbracket \neg p \rrbracket \text{assert}\sigma &= \neg (\llbracket p \rrbracket \text{assert}\sigma) \\
\llbracket p_0 \land p_1 \rrbracket \text{assert}\sigma &= \llbracket p_0 \rrbracket \text{assert}\sigma \land \llbracket p_1 \rrbracket \text{assert}\sigma \\
\llbracket \forall v. \ p \rrbracket \text{assert}\sigma &= \forall n \in \mathbb{Z}. \llbracket p \rrbracket \text{assert}[\sigma | v : n]
\end{align*}
\]
Example: The Meaning of a Term

\[[\forall x. x+0=x]_{assert}\sigma\]

\[= \forall n \in \mathbb{Z}. [[x+0=x]]_{assert} [\sigma|x:n]\]

\[= \forall n \in \mathbb{Z}. [[x+0]]_{intexp} [\sigma|x:n] = [[x]]_{intexp} [\sigma|x:n]\]

\[= \forall n \in \mathbb{Z}. [[x]]_{intexp} [\sigma|x:n] + [[0]]_{intexp} [\sigma|x:n] = [[x]]_{intexp} [\sigma|x:n]\]

\[= \forall n \in \mathbb{Z}. [\sigma|x:n](x) + 0 = [\sigma|x:n](x)\]

\[= \forall n \in \mathbb{Z}. n + 0 = n\]

\[= \text{true}\]
Properties of the Semantic Equations

- They are syntax-directed (homomorphic):
  - exactly one equation for each abstract grammar production (constructor)
  - result expressed using functions (meanings) of subterms only (arguments of constructor)

  $\Rightarrow$ they have exactly one solution $\langle \llbracket \cdot \rrbracket_{\text{intexp}}, \llbracket \cdot \rrbracket_{\text{assert}} \rangle$ (proof by induction on the structure of terms).

- They define compositional semantic functions (depending only on the meaning of the subterms)
  $\Rightarrow$ “equivalent” subterms can be substituted
Validity of Assertions

\( p \) holds / is true in \( \sigma \) \iff \( \sigma \) satisfies \( p \) \iff \([p]_{assert}\sigma = \text{true}\)

\( p \) is valid \iff \( \forall \sigma \in \Sigma. \) \( p \) holds in \( \sigma \)

\( p \) is unsatisfiable \iff \( \forall \sigma \in \Sigma. \) \([p]_{assert}\sigma = \text{false}\)
\iff \neg \( p \) is valid

\( p \) is stronger than \( p' \) \iff \( \forall \sigma \in \Sigma. \) \((p' \) holds if \( p \) holds \)
\iff \( (p \Rightarrow p') \) is valid

\( p \) and \( p' \) are equivalent \iff \( p \) is stronger than \( p' \)
and \( p' \) is stronger than \( p \)
## Inference Rules

<table>
<thead>
<tr>
<th>Class</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="" alt="Inference Rule" /></td>
<td><img src="" alt="Examples" /></td>
</tr>
</tbody>
</table>

- \( \vdash p \) (Axiom)
- \( \vdash p \) (Axiom Schema)
- \( \vdash p_0 \ldots \vdash p_{n-1} \) (Rule)
- \( \vdash x + 0 = x \) (xPlusZero)
- \( \vdash e_1 = e_0 \Rightarrow e_0 = e_1 \) (SymmObjEq)
- \( \vdash p \vdash p \Rightarrow p' \) (ModusPonens)
- \( \vdash p \vdash \forall v. p \) (Generalization)
Formal Proofs

A set of inference rules defines a logical theory $\vdash$.

A formal proof (in a logical theory):

a sequence of instances of the inference rules, where
the premisses of each rule occur as conclusions earlier in the sequence.

1. $\vdash x + 0 = x$  \hspace{1cm} (xPlusZero)
2. $\vdash x + 0 = x \Rightarrow x = x + 0$ \hspace{1cm} (SymmObjEq)
   \hspace{1cm} $[e_0 : x \mid e_1 : x + 0]$
3. $\vdash x = x + 0$  \hspace{1cm} (ModusPonens, 1, 2)
   \hspace{1cm} $[p : x + 0 = x \mid p' : x = x + 0]$
4. $\vdash \forall x. x = x + 0$  \hspace{1cm} (Generalization, 3)
   \hspace{1cm} $[v : x \mid p : x = x + 0]$
Tree Representation of Formal Proofs

\[ \vdash x + 0 = x \quad \vdash x + 0 = x \Rightarrow x = x + 0 \] (SymmObjEq)

\[ \vdash x = x + 0 \] (MP)

\[ \vdash \forall x. x = x + 0 \] (Gen)
Soundness of a Logical Theory

An inference rule is **sound** if in every instance of the rule the conclusion is valid if all the premisses are.

A logical theory $\vdash$ is sound if all inference rules in it are sound.

If $\vdash$ is sound and there is a formal proof of $\vdash p$, then $p$ is valid.

Object vs Meta implication:

$$\vdash p \Rightarrow \forall v. p$$

is not a sound rule, although $\vdash p$ is.
Completeness of a Logical Theory

A logical theory $\vdash$ is **complete** if
for every valid $p$ there is a formal proof of $\vdash p$.

A logical theory $\vdash$ is **axiomatizable** if
there exists a finite set of inference rules
from which can be constructed formal proofs of all assertions in $\vdash$.

No first-order theory of arithmetic is complete and axiomatizable.
Variable Binding

\[ \forall x. \exists y. \ x < y \wedge \exists x. \ x > y \]
\[\forall x. \exists y. x < y \land \exists x. x > y\]
Bound and Free Variables

In $\forall v. p$, $v$ is the binding occurrence (binder) and $p$ is its scope.

If a non-binding occurrence of $v$ is within the scope of a binder for $v$, then it is a bound occurrence; otherwise it’s a free one.

\[
\begin{align*}
FV_{\text{intexp}}(0) &= \emptyset \\
FV(v) &= \{v\} \\
FV(-e) &= FV(e) \\
FV(e_0 + e_1) &= FV(e_0) \cup FV(e_1) \\
FV(e_0 = e_1) &= FV(e_0) \cup FV(e_1) \\
FV(\neg p) &= FV(p) \\
FV(\forall v. p) &= FV(p) - \{v\}
\end{align*}
\]

Example:

\[
FV(\exists y. x < y \land \exists x. x > y) = \{x\}
\]
Only Assignment of Free Variables Matters

Coincidence Theorem:

If \( \sigma v = \sigma' v \) for all \( v \in FV_\theta(p) \), then \( \llbracket p \rrbracket_\theta \sigma = \llbracket p \rrbracket_\theta \sigma' \) (where \( p \) is a phrase of type \( \theta \)).

Proof: By structural induction.

Inductive hypothesis:
The statement of the theorem holds for all phrases of depth less than that of the phrase \( p' \).

Base cases:

\[ p' = 0 \Rightarrow \llbracket 0 \rrbracket_{\text{intexp}} \sigma = 0 = \llbracket 0 \rrbracket_{\text{intexp}} \sigma' \]

\[ p' = v \Rightarrow \llbracket v \rrbracket_{\text{intexp}} \sigma = \sigma v = \sigma' v = \llbracket v \rrbracket_{\text{intexp}} \sigma', \text{since } FV(v) = \{ v \}. \]
Proof of Concidence Theorem, cont’d

Coincidence Theorem:

If \( \sigma v = \sigma' v \) for all \( v \in FV(\theta(p)) \), then \([p]_{\theta} \sigma = [p]_{\theta} \sigma'\).

Inductive cases:

\( p' = e_0 + e_1 \):

by IH \([e_i]_{\text{intexp}} \sigma = [e_i]_{\text{intexp}} \sigma' \), \( i \in \{1, 2\}\).

\([p']_{\text{intexp}} \sigma = [e_0]_{\text{intexp}} \sigma + [e_1]_{\text{intexp}} \sigma' = [e_0]_{\text{intexp}} \sigma' + [e_1]_{\text{intexp}} \sigma' = [p']_{\text{intexp}} \sigma'\)

\( p' = \forall u. q \):

\( \sigma v = \sigma' v \), \( \forall v \in FV(p') = FV(q) - \{u\} \)
then \([\sigma|u : n] v = [\sigma'|u : n] v \), \( \forall v \in FV(q), n \in \mathbb{Z} \)

Then by IH \([q]_{\text{assert}}[\sigma|u : n] = [q]_{\text{assert}}[\sigma'|u : n] \) for all \( n \in \mathbb{Z} \), hence \( \forall n \in \mathbb{Z}. [q]_{\text{assert}}[\sigma|u : n] = \forall n \in \mathbb{Z}. [q]_{\text{assert}}[\sigma'|u : n] \)

\( [\forall u. q]_{\text{assert}} \sigma = [\forall u. q]_{\text{assert}} \sigma' \).
Substitution

\[-/\delta \in \text{intexp} \rightarrow \text{intexp}\]  \(\text{when } \delta \in \text{var} \rightarrow \text{intexp}\)

\[
\begin{align*}
0/\delta &= 0 \\
(-e)/\delta &= -(e/\delta) \\
(e_0 + e_1)/\delta &= (e_0/\delta) + (e_1/\delta) \\
\vdots
\end{align*}
\]

\[
\begin{align*}
v/\delta &= \delta v \\
(p_0 \land p_1)/\delta &= (p_0/\delta) \land (p_1/\delta) \\
(\forall v. p)/\delta &= \forall v'. (p/\{\delta|v : v'\})
\end{align*}
\]

where \(v' \notin \bigcup_{u \in \text{FV}(p) - \{v\}} \text{FV}(\delta u)\)

Examples:

\[
(x < 0 \land \exists x. x \leq y)/[x : y+1] = y+1 < 0 \land \exists x. x \leq y
\]

\[
(x < 0 \land \exists x. x \leq y)/[y : x+1] = x < 0 \land \exists z. z \leq x+1
\]
Preserving Binding Structure

\[(x < 0 \land \exists x. x \leq y)/[x : y+1] = y+1 < 0 \land \exists x. x \leq y\]
Avoiding Variable Capture

\[(x < 0 \land \exists x. x \leq y) / [y : x+1] = x < 0 \land \exists z. z \leq x+1\]
Substitution Theorem:
If $\sigma = \llbracket \cdot \rrbracket_{intexp} \sigma' \cdot \delta$ on $FV(p)$, then $(\llbracket \cdot \rrbracket \sigma)p = (\llbracket \cdot \rrbracket \sigma' \cdot (-/\delta))p$.

Finite Substitution Theorem:
$\llbracket p/v_0 \to e_0, \ldots v_{n-1} \to e_{n-1} \rrbracket \sigma = \llbracket p \rrbracket [\sigma|v_0: \llbracket e_0 \rrbracket \sigma, \ldots]$. where
$p/v_0 \to e_0, \ldots v_{n-1} \to e_{n-1} \overset{\text{def}}{=} p/\llbracket \text{cvar}|v_0: e_0| \ldots |v_{n-1}: e_{n-1} \rrbracket$.

Renaming:
If $u \not\in FV(q) - \{v\}$, then $\llbracket \forall u. (q/v \to u) \rrbracket_{boolexp} = \llbracket \forall v. q \rrbracket_{boolexp}$.