Meeting 18: Axiomatic

C'MON, CALVIN. WE'RE GOING TO THE STORE.
CAN HOBBES COME?
NO, JUST LEAVE HIM HERE.
BUT I WANT HIM TO COME WITH US!!
IF YOU CAN'T WIN BY REASON, GO FOR VOLUME.
WATTERSON

Announcements

- Homework 4
    - Part 3 (finalized project proposals) due next Friday at 6:00pm. Push to your GitHub repos.
    - Rest of homework extended to after spring break, Friday, April 6. **As a project-based class, remember to continue to make steady progress.** Homework 4 is shorter but just the week after spring break is not enough.
- Talk (with me, with the class in office hours, on Piazza) about your course project ideas. Brainstorm "moonshot" ideas.

Questions

– 1. OCaml implementation: steps_pap, lam
2. Hoare logic on IMP

– 3. Δ in HW3 ?

Assignment #4: Program Verification and Implementation

CSCI 5535 / ECEN 5533: Fundamentals of Programming Languages

Spring 2018: Due Friday, March 23, 2018

This homework has two parts. The first considers a deductive system for thinking about program correctness. The second considers a semantics that is closer a machine implementation.

1 Axiomatic Semantics: IMP

We continue to consider the same language **IMP** with the syntax chart:

Typ	τ	::=	`num`	`num`	numbers
			`bool`	`bool`	booleans
Exp	e	::=	`addr`[a]	a	addresses (or "assignables")
			`num`[n]	n	numeral
			`bool`[b]	b	boolean
			`plus`(e_1; e_2)	$e_1 + e_2$	addition
			`times`(e_1; e_2)	$e_1 * e_2$	multiplication
			`eq`(e_1; e_2)	$e_1 == e_2$	equal
			`le`(e_1; e_2)	$e_1 <= e_2$	less-than-or-equal
			`not`(e_1)	$!e_1$	negation
			`and`(e_1; e_2)	$e_1 \&\& e_2$	conjunction
			`or`(e_1; e_2)	$e_1 \mid\mid e_2$	disjunction
Cmd	c	::=	`set`[a](e)	$a := e$	assignment
			`skip`	`skip`	skip
			`seq`(c_1; c_2)	c_1; c_2	sequencing
			`if`(e; c_1; c_2)	`if` e `then` c_1 `else` c_2	conditional
			`while`(e; c_1)	`while` e `do` c_1	looping
Addr	a				

As before, addresses a represent static memory store locations and are drawn from some unbounded set Addr and all memory locations only store numbers. A store σ is thus a mapping from addresses to numbers, written as follows:

$$\text{Store} \quad \sigma \quad ::= \quad \cdot \mid \sigma, a \hookrightarrow n$$

The semantics of **IMP** is as a formalized as before operationally, and we consider the Hoare rules for partial correctness as in Chapter 6 of *FSPL*.

1.1. **Program Correctness**. Prove using Hoare rules the following property: if we start the command $\texttt{while}\, e\, \texttt{do}\; a := a + 2$ in a state that satisfies the assertion $\mathrm{even}(a)$, then it terminates in a state satisfying $\mathrm{even}(a)$. That is, prove the the following judgment:

$$\{\mathrm{even}(a)\}\ \texttt{while}\, e\, \texttt{do}\; a := a + 2\ \{\mathrm{even}(a)\}$$

Hint: your proof should *not* use induction.

1.2. **Hoare Rules**. Consider an extension to IMP

$$c \quad ::= \quad \texttt{do}(c_1; e) \quad \texttt{do}\; c_1\; \texttt{while}\; e \quad \text{at-least-once looping}$$

with a command for at-least-once looping. Extend the Hoare judgment form $\{A\}\, c\, \{B\}$ for this command.

2 Abstract Machines and Control Flow

In this section, we will consider a new implementation of language PCF based on abstract machines (i.e., K from Chapter 28 of *PFPL*).

One aspect of a structural small-step operational semantics (as we used in previous assignments) that seems wasteful from an implementation perspective is that we “forget” where we are reducing at each step. An abstract machine semantics makes explicit the “program counter” in its state.

2.1. Give a specification for K as a call-by-value language. That is, modify the definition of the judgments $f\ \mathsf{frame}$ and $s \longmapsto s'$ from Section 28.1 of *PFPL*. You will also need to update the auxiliary frame-typing judgment $f : \tau \rightsquigarrow \tau'$ from Section 28.2 in order to state safety.

2.2. **Safety**.

(a) Prove preservation: if $s\ \mathsf{ok}$ and $s \longmapsto s'$, then $s'\ \mathsf{ok}$.

(b) Prove progress: if $s\ \mathsf{ok}$, then either $s\ \mathsf{final}$ or $s \longmapsto s'$ for some state s'.

2.3. **Implementation**.

(a) Implement call-by-value K. You need not include previously implemented language features (though you may include some of them if you want).

First, we have some new syntactic forms:

frames	f	**type** `frame`
stacks	k	**type** `stack = frame list`
states	s	**type** `state = Eval` **of** `stack * exp	Ret` **of** `stack * exp`

Then, we will implement functions that define both the static and dynamic semantics of the language.

$[e'/x]e$	**val** `subst : exp -> var -> exp -> exp`
$e\,\mathsf{val}$	**val** `is_val : exp -> bool`
$\Gamma \vdash e : \tau$	**val** `exp_typ : typctx -> exp -> typ option`
$s \longmapsto s'$	**val** `step : state -> state`
$s\,\mathsf{final}$	**val** `is_final : state -> bool`
$k \rhd : \tau$	**val** `stack_type : stack -> typ option`
$f : \tau \leadsto \tau'$	**val** `frame_type : frame -> typ -> typ option`
$s\,\mathsf{ok}$	**val** `is_ok : state -> bool`
$s \hookrightarrow_{\mathsf{ok}} s'$	**val** `steps_pap : state -> state`

The $s \hookrightarrow_{\mathsf{ok}} s'$ is the analogous iterate-step-with-preservation-and-progress for states.

$$\frac{s\,\mathsf{ok} \qquad s\,\mathsf{final}}{s \hookrightarrow_{\mathsf{ok}} s} \qquad\qquad \frac{s\,\mathsf{ok} \qquad s \longmapsto s' \qquad s' \hookrightarrow_{\mathsf{ok}} s''}{s \hookrightarrow_{\mathsf{ok}} s''}$$

(b) **Extra credit: Exceptions**. Extend your K machine with exceptions as in Section 29.2. You may choose `nat` for the type of the value carried by the exception.

(c) **Extra credit: Continuations**. Extend your K machine with continuations as in Section 30.2. Implementing continuations is independent of implementing exceptions, so you may choose to do either or both. (Technically, you can encode exceptions with continuations.)

3 Final Project Preparation: Proposal Revision

3.1. **Reading Papers**. Follow some citations based on the papers you chose in Homework 2 and read in Homework 3. List at least three cited papers that seems relevant to follow up on. Include a citation along with a URL for each paper. For each of the additional papers, and for each question below, write two concise sentences:

(a) Why did *you* select this cited paper?

(b) What is the relation between the "main idea" of this cited paper and the "main idea" of the paper that cites it? You may want to skim the introductory and concluding bits of the cited paper along with the related work in the citing paper.

3.2. **Proposal**. Finalize your class project plan. Write an updated explanation of your plan (expanding and revising as necessary), and what you hope to accomplish with your project by the end of the semester. That is, on what artifact do you want to be graded?

Here are questions that you should address in your project proposal.

(a) Define the problem that you will solve as concretely as possible. Provide a scope of expected and potential results. Give a few example programs that exhibit the problem that you are trying to solve.

(b) What is the general approach that you intend to use to solve the problem?

(c) Why do you think that approach will solve the problem? What resources (papers, book chapters, etc.) do you plan to base your solution on? Is there one in particular that you plan to follow? What about your solution will be similar? What will be different?

(d) How do you plan to demonstrate your idea?

(e) How will you evaluate your idea? What will be the measurement for success?

4 Feedback and Discussion

4.1. **Assignment Feedback**. Complete the survey on the linked from the moodle after completing this assignment. Any non-empty answer will receive full credit for this part.

4.2. **Assignment Discussion**. Remember to sign up for a discussion session with your grader once you have received written feedback on your assignment. Engaging in a discussion session will receive full credit for this part.

Assignment #3: Compilation and Interpretation

CSCI 5535 / ECEN 5533: Fundamentals of Programming Languages

Spring 2018: Due Friday, March 9, 2018

This homework has two parts. The first asks you to consider the relationship between a denotational formalization and an operational one. The second asks you to extend your language implementation in OCaml to further gain experience translating formalization to implementation.

1 Denotational Semantics: IMP

Recall the syntax chart for IMP:

Typ	τ	::=	`num`	`num`	numbers
			`bool`	`bool`	booleans
Exp	e	::=	`addr`$[a]$	a	addresses (or "assignables")
			`num`$[n]$	n	numeral
			`bool`$[b]$	b	boolean
			`plus`$(e_1;e_2)$	$e_1 + e_2$	addition
			`times`$(e_1;e_2)$	$e_1 * e_2$	multiplication
			`eq`$(e_1;e_2)$	$e_1 == e_2$	equal
			`le`$(e_1;e_2)$	$e_1 <= e_2$	less-than-or-equal
			`not`(e_1)	$!e_1$	negation
			`and`$(e_1;e_2)$	$e_1 \mathbin{\&\&} e_2$	conjunction
			`or`$(e_1;e_2)$	$e_1 \mathbin{\|\|} e_2$	disjunction
Cmd	c	::=	`set`$[a](e)$	$a := e$	assignment
			`skip`	`skip`	skip
			`seq`$(c_1;c_2)$	$c_1;c_2$	sequencing
			`if`$(e;c_1;c_2)$	`if` e `then` c_1 `else` c_2	conditional
			`while`$(e;c_1)$	`while` e `do` c_1	looping
Addr	a				

As before, addresses a represent static memory store locations and are drawn from some unbounded set Addr and all memory locations only store numbers. A store σ is thus a mapping from addresses to numbers, written as follows:

$$\text{Store} \quad \sigma \quad ::= \quad \cdot \mid \sigma, a \hookrightarrow n$$

The semantics of IMP is as a formalized in the previous assignment operationally. In this section, we will consider a denotational formalization.

The set of values Val are the disjoint union of numbers and booleans:

$$\mathsf{Val} \quad v ::= \texttt{num}[n] \mid \texttt{bool}[b]\,.$$

1.1. (a) Formalize the dynamics of IMP as two denotational functions.

$$\begin{array}{lcl} [\![\cdot]\!] & : & \mathsf{Exp} \to (\mathsf{Store} \rightharpoonup \mathsf{Val}) \\ [\![\cdot]\!] & : & \mathsf{Cmd} \to (\mathsf{Store} \rightharpoonup \mathsf{Store}) \end{array}$$

(b) Prove that your denotational definitions coincide with your operational ones.

i. State the lemma that your definitions for expressions coincide.

ii. Prove the equivalence of your definitions for commands, that is,
$(\sigma,\sigma') \in [\![c]\!]$ if and only if $\langle c,\sigma\rangle \Downarrow \sigma'$.
Begin by copying your definition of $\langle c,\sigma\rangle \Downarrow \sigma'$ from your previous homework submission.

1.2. **Manual Program Verification**. Prove the following statement about the denotational semantics of IMP.

$$\text{If } [\![\texttt{while}\ e\ \texttt{do}\ a := a+2]\!]\,\sigma \;=\; \sigma' \text{ such that } \mathrm{even}(\sigma(a)),\text{ then } \mathrm{even}(\sigma'(a))$$

Unlike in the previous assignment, this time you should use your denotational semantics for the proof. *Hint*: your proof should proceed by mathematical induction.

2 Comparing Operational and Denotational Semantics

Regular expressions are commonly used as abstractions for string matching. Here is an abstract syntax for regular expressions:

r	$::=$	‘c’	singleton – matches the character c	
	$\mid$	empty	skip – matches the empty string	
	$\mid$	$r_1\ r_2$	concatenation – matches r_1 followed by r_2	;
	$\mid$	$r_1 \mid r_2$	or – matches r_1 or r_2	if ---.
	$\mid$	$r*$	Kleene star – matches 0 or more occurrences of r	while ---
	$\mid$	.	matches any single character	
	$\mid$	[‘c_1’–‘c_2’]	matches any character between c_1 and c_2 inclusive	
	$\mid$	$r+$	matches 1 or more occurrences of r	
	$\mid$	$r?$	matches 0 or 1 occurrence of r	

We will call the first five cases the *primary* forms of regular expressions. The last four cases can be defined in terms of the first five. We also give an abstract grammar for strings (modeled as lists of characters):

s	$::=$	$\cdot$	empty string
	$\mid$	cs	string with first character c and other characters s

We write "bye" as shorthand for bye·.

We introduce the following big-step operational semantics judgment for regular expression matching:

$$r \text{ matches } s \text{ leaving } s'$$

The interpretation of the judgment is that the regular expression r matches some prefix of the string s, leaving the suffix s' unmatched. If $s' = \cdot$, then r matched s exactly. For example,

$$\text{'h'('e'+) matches "hello" leaving "llo"}$$

Note that this operational semantics may be considered *non-deterministic* because we expect to be able to derive all three of the following:

$$\text{('h' | 'e')* matches "hello" leaving "hello"}$$
$$\text{('h' | 'e')* matches "hello" leaving "ello"}$$
$$\text{('h' | 'e')* matches "hello" leaving "llo"}$$

We leave the rules of inference defining this judgment unspecified. You may consider giving this set of inference rules an optional exercise.

Instead, we will use *denotational semantics* to model the fact that a regular expression can match a string leaving many possible suffixes. Let Str be the set of all strings, let $\wp(\text{Str})$ be the powerset of Str, and let RE range over regular expressions. We introduce a semantic function:

complete

$$[\![\cdot]\!] : \underline{\text{RE}} \to \underbrace{(\text{Str} \to \wp(\text{Str}))}$$

The interpretation is that $[\![r]\!]$ is a function that takes in a string-to-be-matched and returns a set of suffixes. We might intuitively define $[\![\cdot]\!]$ as follows:

$$[\![r]\!] = \lambda s. \left\{ s' \mid r \text{ matches } s \text{ leaving } s' \right\}$$

$r ::=$ nomatch

$[\![\text{nomatch}]\!] \overset{\text{def}}{=} \lambda s. \{\}$

In general, however, one should not define the denotational semantics in terms of the operational semantics. Here are two correct semantic functions:

$$[\![\underline{\text{'}c\text{'}}]\!] \overset{\text{def}}{=} \lambda s. \left\{ s' \mid s = \text{'}c\text{'} :: \boxed{s'} \right\}$$
$$[\![\underline{\text{empty}}]\!] \overset{\text{def}}{=} \lambda s. \{\underline{s}\}$$

← set of suffixes of any matches

2.1. Give the denotational semantics functions for the other three primal regular expressions. Your semantics functions *may not* reference the operational semantics. ✓

2.2. We want to update our operational semantics for regular expressions to capture multiple suffixes. We want our new operational semantics to be deterministic—it should give the same answer as the denotational semantics above. We introduce a new judgment as follows:

$$r \text{ matches } s \text{ leaving } S$$

where S is a meta-variable for a set of strings. And use rules of inference like the following:

$$\frac{}{\text{'}c\text{'} \text{ matches } s \text{ leaving } \left\{ s' \mid s = \text{'}c\text{'} :: s' \right\}} \qquad \frac{}{\text{empty matches } s \text{ leaving } \{s\}}$$

$$\frac{r_1 \text{ matches } s \text{ leaving } S_1 \qquad r_2 \text{ matches } s \text{ leaving } S_2}{r_1 \mid r_2 \text{ matches } s \text{ leaving } S_1 \cup S_2}$$

Do one of the following:

$$[\![r_1 \, r_2]\!] \overset{\text{def}}{=} \lambda s. \bigcup_{s' \in [\![r_1]\!](s)} [\![r_2]\!] s'$$

$$[\![r_1 \mid r_2]\!] \overset{\text{def}}{=} \lambda s. \quad [\![r_1]\!] s \cup [\![r_2]\!] s$$

$[\![r^*]\!]$? $\quad r^* \text{ `` = '' } \text{empty} \,\underline{|}\, r\, r^*$

$$\mathbb{K} : RE \to \overset{k \in}{Nat} \to (Str \to \mathcal{P}(Str))$$

$$\mathbb{K}_r \; 0 \overset{\text{def}}{=} \lambda s. \{\}$$

$$\mathbb{K}_r \; k{+}1 \overset{\text{def}}{=} \lambda s. \{s\} \cup \bigcup_{s' \in [\![r]\!] s} (\mathbb{K}_r(k)(s'))$$

$$[\![r^*]\!] \overset{\text{def}}{=} \lambda s. \bigcup_{k \in Nat} \mathbb{K}_r(k)(s)$$

- *Either* give operational semantics rules of inference for $r*$ and $r_1\ r_2$. Your operational semantics rules may *not* reference the denotational semantics. You may *not* place a derivation inside a set constructor, as in: $\{s \mid \exists S.\ r \text{ matches } s \text{ leaving } S\}$. Each inference rule must have a finite and fixed set of hypotheses.
- *Or* argue in one or two sentences that it cannot be done correctly in the given framework. Back up your argument by presenting two attempted but "wrong" rules of inference and show that each one is either unsound or incomplete with respect to our intuitive notion of regular expression matching.

Part of doing research in any area is getting stuck. When you get stuck, you must be able to recognize whether "you are just missing something" or "the problem is actually impossible."

3 Implementation: General Recursion and Polymorphism

In this section, we will reformulate language **ETPS** so that it admits general recursion (and thus non-terminating programs) and parametric polymorphism.

Follow the "Translating a Language to OCaml" guidance from the previous homework assignment. That is, we will implement functions that define both the static and dynamic semantics of the language.

$[e'/x]e$	**val** `subst : exp -> var -> exp -> exp`
$e\ \mathsf{val}$	**val** `is_val : exp -> bool`
$\Gamma \vdash e : \tau$	**val** `exp_typ : typctx -> exp -> typ option`
$e \longmapsto e'$	**val** `step : exp -> exp`
$e \hookrightarrow_{:\tau} e'$	**val** `steps_pap : typ -> exp -> exp`

To avoid redundancy in the assignment, you may skip implementing the big-step evaluator $e \Downarrow e'$ in this assignment.

3.1. Adapt your language **ETPS** with general recursion. That is, replace the language **T** portion (primitive recursion with natural numbers) with language **PCF** from Chapter 19 of *PFPL* (general recursion with natural numbers).

3.2. Add recursive types (i.e., language **FPC** from Chapter 20 of *PFPL*). While type `nat` of natural numbers is definable in **FPC**, leave the primitive `nat` in for convenience in testing.

3.3. Add parametric polymorphism (i.e., System **F** from Chapter 16 of *PFPL*). Note that System **F** extends the typing judgment with an additional context for type variables:

$$\begin{array}{lcll} \Delta & ::= & \cdot \mid \Delta, t\ \mathsf{type} & \text{kind contexts} \\ t & & & \text{type variables} \end{array}$$

$$\frac{r_1 \text{ matches } s \text{ leaving } S \qquad \bigcup_{s' \in S} \{ S' \mid r_2 \text{ matches } s' \text{ leaving } S' \}}{r_1\, r_2 \text{ matches } s \text{ leaving}}$$

$\Delta ::= \cdot \mid t \text{ type}$

$\Gamma ::= \cdot \mid x : \tau$

type variables

$\tau ::= t \mid \ldots$ $\forall(t).\, t \to t$ $\mid$ num $\mid$ str $\mid$ arr$(\tau_1; \tau_2)$

and a well-formedness judgment for types $\Delta \vdash \tau$ type. We thus have to update our implementation accordingly:

t type $\vdash t \to t$ type

t	**type** `typvar = string`
Δ	**type** `kindctx` = typvar list
$\Delta\,\Gamma \vdash e : \tau$	**val** `exp_typ : kindctx -> typctx -> exp -> typ option`
$\Delta \vdash \tau$ type	**val** `typ_form : kindctx -> typ -> bool`

Explain your testing strategy and justify that your test cases attempt to cover your code as thoroughly as possible (e.g., they attempt to cover different execution paths of your implementation with each test). Write this explanation as comments alongside your test code.

4 Final Project: Proposal

4.1. **Reading Papers**. Continue reading the papers that you chose in Homework 2. For each of the five papers, and for each question below, write two concise sentences:

(a) Why did *you* select this paper?

(b) What is the "main idea" of the paper?

(c) How well is this main idea communicated to you when you read the *first two sections and conclusion* of paper, and skimmed the rest? In particular, explain what aspects seem important, are which are clear versus unclear. You may want to read deeper into the details of the paper body if these beginning and ending sections do not make the main ideas clear; make a note if this is required.

Take a look at Keshav's "How to Read a Paper"[1] for further advice on reading papers.

4.2. **Proposal**. Continue thinking about your class project. Write an updated explanation of your plan (expanding and revising as necessary), and what you hope to accomplish with your project by the end of the semester. That is, on what artifact do you want to be graded? By writing your plan now, you are also generating a draft of part of your final report.

Here are questions that you should address in your project proposal. You will have the opportunity to revise your proposal in the next assignment, but the more concrete your proposal is early on, the better the feedback you are likely to receive.

(a) Define the problem that you will solve as concretely as possible. Provide a scope of expected and potential results. Give a few example programs that exhibit the problem that you are trying to solve.

(b) What is the general approach that you intend to use to solve the problem?

(c) Why do you think that approach will solve the problem? What resources (papers, book chapters, etc.) do you plan to base your solution on? Is there one in particular that you plan to follow? What about your solution will be similar? What will be different?

(d) How do you plan to demonstrate your idea?

(e) How will you evaluate your idea? What will be the measurement for success?

[1] S. Keshav. 2007. How to read a paper. SIGCOMM Comput. Commun. Rev. 37, 3 (July 2007), 83-84. `http://ccr.sigcomm.org/online/files/p83-keshavA.pdf`

$\boxed{\tau \text{ type}}$ When a type τ (obj lang) is well formed "is a valid type"

$\boxed{\tau \text{ wf}}$

$$\dfrac{\dfrac{\overline{t \text{ type} \vdash t \text{ type}} \qquad \overline{t \text{ type} \vdash t \text{ type}}}{t \text{ type} \vdash t \to t \text{ type}}}{\cdot \vdash \Lambda(t)\, t \to t \text{ type}}$$

$\cdot \vdash \Lambda(t)\, t \to s \text{ type}$ ✗