Kleene Algebra — Lecture 1

ESSLLI 2023

Housekeeping

- Best way to reach me is by email.
- Website: `https://kap.pe/esslli`.
- 5 lectures, two 40-minute parts, 10-ish minute break.
- Extensive lecture notes, including exercises.
- It is *always* OK to ask me for clarification.
- It is *always* OK to discuss the exercises with other people.

Motivation

```
while a and b do
  e;
while a do
  f;
  while a and b do
    e;
```

```
while a do
  if b then
    e;
  else
    f;
```

These programs are the same... but how do you prove that?

Overview

- We can reason *equationally*, using properties of programs.
- We can reason *operationally*, by comparing abstract machines.
- These are *two sides of the same coin*.

Equational reasoning

- Speaks to our intuition — you have all done this before.
- Helps to relate *programs* to *specifications*.
- Allows us to prove validity of refactoring operations.
- Solve equations to find program satisfying a specification.

Operational reasoning

- Corresponds much more closely to what computers do.
- Long tradition of powerful automated reasoning.
- Will cover this in more detail from lecture 3 onwards.

Syntax

Primitive actions $\Sigma = \{\mathtt{a}, \mathtt{b}, \mathtt{c}, \dots\}$.

Compound expressions:

$$\mathbb{E} \ni e, f ::= 0 \mid 1 \mid \mathtt{a} \in \Sigma \mid e + f \mid e \cdot f \mid e^*$$

Think of $e \in \mathbb{E}$ as a *pattern of behavior* for a program.

Example: Integer Square Root

In a traditional language:

$$
\begin{array}{l}
i \leftarrow 0; \\
\texttt{while } (i+1)^2 \leq n \texttt{ do} \\
\quad i \leftarrow i + 1;
\end{array}
$$

In our language (for now):

$$\texttt{init} \cdot (\texttt{guard} \cdot \texttt{incr})^* \cdot \texttt{validate}$$

Semantics

Definition (Interpretation)

An *interpretation* is a pair $\langle S, \sigma \rangle$ where S is a set, and $\sigma : \Sigma \to 2^{S \times S}$.

Definition (Relational semantics)

Let σ be an interpretation. $[\![e]\!]_\sigma$ is a relation on S, defined inductively by

$$[\![0]\!]_\sigma = \emptyset \qquad [\![1]\!]_\sigma = \mathrm{id}_S \qquad [\![\mathtt{a}]\!]_\sigma = \sigma(\mathtt{a})$$

$$[\![e + f]\!]_\sigma = [\![e]\!]_\sigma \cup [\![f]\!]_\sigma \qquad [\![e \cdot f]\!]_\sigma = [\![e]\!]_\sigma \circ [\![f]\!]_\sigma \qquad [\![e^*]\!]_\sigma = [\![e]\!]_\sigma^*$$

Example: Integer Square Root

$$\texttt{init} \cdot (\texttt{guard} \cdot \texttt{incr})^* \cdot \texttt{validate}$$

$$S = \{f : \{i, n\} \to \mathbb{N}\}$$

$$\sigma(\texttt{init}) = \{\langle s, s[0/i]\rangle : s \in S\}$$

$$\sigma(\texttt{guard}) = \{\langle s, s\rangle : (s(i) + 1)^2 \leq s(n)\}$$

$$\sigma(\texttt{incr}) = \{\langle s, s[s(i) + 1/i]\rangle : s \in S\}$$

$$\sigma(\texttt{validate}) = \{\langle s, s\rangle : (s(i) + 1)^2 > s(n)\}$$

Reasoning

Which things are true regardless of σ?

For instance, $+$ is commutative:

$$[\![e + f]\!]_\sigma = [\![e]\!]_\sigma \cup [\![f]\!]_\sigma = [\![f]\!]_\sigma \cup [\![e]\!]_\sigma = [\![f + e]\!]_\sigma$$

Can you think of any other laws?

Axioms

Definition (Kleene Algebra)

We define $\equiv$ as the smallest congruence on $\mathbb{E}$ satisfying the following:

$$e + 0 \equiv e \qquad e + e \equiv e \qquad e + f \equiv f + e \qquad e + (f + g) \equiv (e + f) + g$$

$$e \cdot (f \cdot g) \equiv (e \cdot f) \cdot g \qquad e \cdot (f + g) \equiv e \cdot f + e \cdot g \qquad (e + f) \cdot g \equiv e \cdot g + f \cdot g$$

$$e \cdot 1 \equiv e \equiv 1 \cdot e \qquad e \cdot 0 \equiv 0 \equiv 0 \cdot e \qquad 1 + e \cdot e^* \equiv e^* \equiv 1 + e^* \cdot e$$

$$e + f \cdot g \leqq g \implies f^* \cdot e \leqq g \qquad e + f \cdot g \leqq f \implies e \cdot g^* \leqq f$$

Here $e \leqq f$ is shorthand for $e + f \leqq f$.

Axioms

Lemma (Soundness)

If $e \equiv f$, then $[\![e]\!]_\sigma = [\![f]\!]_\sigma$ for all interpretations σ.

Proof sketch.

By induction on the construction of $\equiv$; for instance, if $e = g_1 \cdot (g_2 \cdot g_3)$ and $f = (g_1 \cdot g_2) \cdot g_3$, then we can derive as follows:

$$[\![e]\!]_\sigma = [\![g_1]\!]_\sigma \circ ([\![g_2]\!]_\sigma \circ [\![g_3]\!]_\sigma) = ([\![g_1]\!]_\sigma \circ [\![g_2]\!]_\sigma) \circ [\![g_3]\!]_\sigma = [\![f]\!]_\sigma \qquad \square$$

Homework exercise: show that if $[\![e + f \cdot g]\!]_\sigma \subseteq [\![g]\!]_\sigma$, then $[\![f^* \cdot e]\!]_\sigma \subseteq [\![g]\!]_\sigma$.

Reasoning

Lemma

If $e \leqq f$ and $f \leqq e$, then $e \equiv f$.

Proof.

Recall that $e \leqq f$ and $f \leqq e$ means that $e + f \equiv f$ and $f + e \equiv e$, so

$$e \equiv f + e \equiv e + f \equiv f \qquad \square$$

Reasoning

Lemma

$e \cdot (f \cdot e)^* \leqq (e \cdot f)^* \cdot e$.

Proof.

We can first show that

$$e + ((e \cdot f)^* \cdot e) \cdot (f \cdot e) \leqq (e \cdot f)^* \cdot e$$

To see this, we derive that

$$\begin{aligned} e + ((e \cdot f)^* \cdot e) \cdot (f \cdot e) &\equiv e + ((e \cdot f)^* \cdot (e \cdot f)) \cdot e \\ &\equiv (1 + (e \cdot f)^* \cdot (e \cdot f)) \cdot e \\ &\equiv (e \cdot f)^* \cdot e \end{aligned}$$

$\square$

Completeness

Suppose showing that $e \equiv f$, is not working out.

- Maybe $[\![e]\!]_\sigma \neq [\![f]\!]_\sigma$ for a certain (cleverly constructed) σ.
- Maybe $[\![e]\!]_\sigma = [\![f]\!]_\sigma$ for all σ, but $e \equiv f$ is simply not provable.

How can you tell the difference?

By the end of this course, you will be able to exclude these possibilities.

A language model — motivation

The interpretation σ is cumbersome to carry around!

We need a model that is agnostic of the interpretation.

Solution: collect possible sequences of primitive actions.

A language model — ground terms

Definition (Words)

A *word* over Σ is a sequence $\mathrm{a}_1 \cdots \mathrm{a}_n$ where $\mathrm{a}_i \in \Sigma$.

We write ϵ for the *empty word*.

When $w, x \in \Sigma^*$, we write wx for the concatenation of w and x.

Definition (Languages)

A set of words is called a *language*. Let L and K be languages.

We write $L \cdot K$ for the language $\{wx : w \in L, x \in K\}$.

We also write L^* for the language $\{w_1 w_2 \cdots w_n : w_i \in L\}$.

Note: this makes Σ^* the set of all words.

A language model — definition

Idea: collect all sequences of actions denoted by $e \in \mathbb{E}$ in a language.

Definition (Language model)

We define $[\![-]\!]_{\mathbb{E}} : \mathbb{E} \to 2^{\Sigma^*}$ inductively, as follows:

$$[\![0]\!]_{\mathbb{E}} = \emptyset \qquad [\![1]\!]_{\mathbb{E}} = \{\epsilon\} \qquad [\![\mathtt{a}]\!]_{\mathbb{E}} = \{\mathtt{a}\}$$

$$[\![e + f]\!]_{\mathbb{E}} = [\![e]\!]_{\mathbb{E}} \cup [\![f]\!]_{\mathbb{E}} \qquad [\![e \cdot f]\!]_{\mathbb{E}} = [\![e]\!]_{\mathbb{E}} \cdot [\![f]\!]_{\mathbb{E}} \qquad [\![e^*]\!]_{\mathbb{E}} = [\![e]\!]_{\mathbb{E}}^*$$

Connecting the models

How do these models interrelate?

Theorem (Equivalence of models)

Let $e, f \in \mathbb{E}$. The following are equivalent:

(i) $[\![e]\!]_{\mathbb{E}} = [\![f]\!]_{\mathbb{E}}$

(ii) *for all* σ, $[\![e]\!]_{\sigma} = [\![f]\!]_{\sigma}$.

Corollary

Let $e, f \in \mathbb{E}$. If $e \equiv f$, then $[\![e]\!]_{\mathbb{E}} = [\![f]\!]_{\mathbb{E}}$.

Connecting the models — languages to relations

Lemma

Let $e, f \in \mathbb{E}$. If $[\![e]\!]_{\mathbb{E}} = [\![f]\!]_{\mathbb{E}}$, then for all σ, we have $[\![e]\!]_\sigma = [\![f]\!]_\sigma$.

Proof sketch.

First, define the action of σ on a language as follows:

$$\hat{\sigma}(L) = \bigcup_{\mathtt{a}_1 \cdots \mathtt{a}_n \in L} \sigma(\mathtt{a}_1) \circ \cdots \circ \sigma(\mathtt{a}_n)$$

Then, show that if $g \in \mathbb{E}$, then $\hat{\sigma}([\![g]\!]_{\mathbb{E}}) = [\![g]\!]_\sigma$, by induction on g.

Finally, derive $[\![e]\!]_\sigma = \hat{\sigma}([\![e]\!]_{\mathbb{E}}) = \hat{\sigma}([\![f]\!]_{\mathbb{E}}) = [\![f]\!]_\sigma$ $\square$

Connecting the models — relations to languages

Lemma

Let $e, f \in \mathbb{E}$. If $[\![e]\!]_\sigma = [\![f]\!]_\sigma$ for all σ, then $[\![e]\!]_\mathbb{E} = [\![f]\!]_\mathbb{E}$.

Proof sketch.

Consider the map $\sharp : 2^{\Sigma^*} \to 2^{\Sigma^* \times \Sigma^*}$, given by

$$\sharp(L) = \{\langle w, wx\rangle : w \in \Sigma^*, x \in L\}$$

One can show that $\sharp$ is injective. So, it suffices to show that $\sharp([\![e]\!]_\mathbb{E}) = \sharp([\![f]\!]_\mathbb{E})$.

Let's choose $S = 2^{\Sigma^* \times \Sigma^*}$, and set $\sigma(\mathtt{a}) = \sharp(\{\mathtt{a}\})$.

Now for $g \in \mathbb{E}$, we have $[\![g]\!]_\sigma = \sharp([\![g]\!]_\mathbb{E})$.

Finally, derive $\sharp([\![e]\!]_\mathbb{E}) = [\![e]\!]_\sigma = [\![f]\!]_\sigma = \sharp([\![f]\!]_\mathbb{E})$. $\square$

Looking ahead

Tomorrow: incorporate reasoning about control flow.