L11: Algebraic Path Problems with applications to Internet Routing Lecture 13 Reduction Redux

Timothy G. Griffin

timothy.griffin@cl.cam.ac.uk
Computer Laboratory
University of Cambridge, UK

Michaelmas Term, 2018

Recall : Reduced semigroup.

Here I have made equality explicit.

If $(S, =, \bullet)$ is semigroup and $r \in S \to S$, then define

$$\mathrm{reduce}((S, =, \bullet), r) \equiv (S_r, =, \bullet_r)$$

where

$$\begin{array}{rcl} S_r & \equiv & \{s \in S \mid r(s) = s\} \\ x \bullet_r y & \equiv & r(x \bullet y) \end{array}$$

General vs classical reductions

Both require $\mathbb{RIP}(S,\ r)$.

General Reduction (note quantification over S_r)

$$\mathbb{RAS}((S,\ \bullet),\ r) \equiv \forall x, y, z \in S_r,\ r(x \bullet r(y \bullet z)) = r(r(x \bullet y) \bullet z)$$

Classical reduction (all quantification over S)

$$\begin{aligned}\mathbb{RLC}((S,\ \bullet),\ r) &\equiv \forall x, y \in S,\ r(r(x) \bullet y) = r(x \bullet y)\\ \mathbb{RRC}((S,\ \bullet),\ r) &\equiv \forall x, y \in S,\ r(x \bullet r(y)) = r(x \bullet y)\end{aligned}$$

Example of a non-classical reduction?

Recall our "hack" from Lecture 9:

We redefined the multiplication $\otimes$ of

$$\text{AddZero}(\infty,\ (\mathbb{N},\ \text{min},\ +) \vec{\times} \text{epaths}(V))$$

as follows:

$$\begin{aligned}x \otimes' \text{inr}(\infty) &= \text{inr}(\infty)\\ \text{inr}(\infty) \otimes' x &= \text{inr}(\infty)\\ \text{inl}(d_1,\ X) \otimes' \text{inl}(d_1,\ Y) &= \begin{cases}\text{inr}(\infty) & \text{if } X \tilde{\odot} Y = \{\}\\ \text{inl}(d_1 + d_2,\ X \tilde{\odot} Y) & \text{otherwise}\end{cases}\end{aligned}$$

Ah, can we do this as a reduction?

Example of a non-classical reduction?

Define r as

$$
\begin{array}{rcl}
r(\mathrm{inr}(\infty)) & \equiv & \mathrm{inr}(\infty) \\
r(\mathrm{inrl}(d,\ X)) & \equiv & \begin{cases} \mathrm{inr}(\infty) & \text{if } X = \{\} \\ \mathrm{inl}(d,\ X) & \text{otherwise} \end{cases}
\end{array}
$$

Lets look at $\mathrm{reduce}(\mathrm{AddZero}(\infty,\ (\mathbb{N},\ \min,\ +)\ \vec{\times}\ \mathrm{epaths}(V)),\ r)$

The additive component:

$$
\begin{array}{rcl}
S_r & \equiv & ((\mathbb{N} \times \mathcal{P}_{\mathrm{fin}}(\mathrm{elem}(V))) \uplus \{\infty\})_r \\
\oplus_r & \equiv & ((\min \vec{\times} \cup)^{\mathrm{id}}_{\infty})_r
\end{array}
$$

Example of a non-classical reduction?

Let's construct a violation of

$$\mathbb{RLC}((S,\ \oplus),\ r) \equiv \forall x, y \in S,\ r(r(x) \oplus y) = r(x \oplus y)$$

Suppose $d < d'$ and $X \neq \{\}$, then let

$$
\begin{array}{rcl}
x & \equiv & \mathrm{inl}(d,\ \{\}) \\
y & \equiv & \mathrm{inl}(d',\ X) \\
\overline{\infty} & \equiv & \mathrm{inr}(\infty)
\end{array}
$$

then

$$
\begin{array}{rcl}
\mathrm{lhs} & \equiv & r(r(x) \oplus y) = r(\overline{\infty} \oplus y) = r(y) = y \\
\mathrm{rhs} & \equiv & r(x \oplus y) = r(x) = \overline{\infty}
\end{array}
$$

This gives us an example that violates associativity:

$$(x \oplus_r \overline{\infty}) \oplus_r y \neq x \oplus_r (\overline{\infty} \oplus_r y)$$

Example of a non-classical reduction?

But r does satisfy $\mathbb{RAS}$ for $\oplus$ and $\otimes$

$$\mathbb{RAS}((S,\ \oplus),\ r) \equiv \forall x, y, z \in S_r,\ r(x \oplus r(y \oplus z)) = r(r(x \oplus y) \oplus z)$$

$$\mathbb{RAS}((S,\ \otimes),\ r) \equiv \forall x, y, z \in S_r,\ r(x \otimes r(y \otimes z)) = r(r(x \otimes y) \otimes z)$$

where

$$\otimes \equiv ((+ \times \tilde{\odot})^{\text{ann}}_{\infty})$$

However, distributivity is lost!

In general, we want for all $a, b, c \in S_r$

$$a \otimes_r (b \oplus_r c) = (a \otimes_r b) \oplus_r (a \otimes_r c)$$

That is

$$r(a \otimes r(b \oplus c)) = r(r(a \otimes b) \oplus r(a \otimes c))$$

Construct a counterexample:

- lhs : Suppose $b \oplus c = b$, $r(b) = b$ and $r(a \otimes b) = \overline{\infty}$ becaue of a loop.
- rhs : $r(r(a \otimes b) \oplus r(a \otimes c)) = r(\overline{\infty} \oplus r(a \otimes c)) = r(r(a \otimes c)) = r(a \otimes c)$, and suppose $a \otimes c$ is loop-free.
- Then lhs $\neq$ rhs.

Fully reduced semigroup.

If $(S, =, \bullet)$ is semigroup and $r \in S \to S$, then define

$$\text{fullReduce}((S, =, \bullet), r) \equiv (S, =^r, \bullet^r)$$

where we assume $\mathbb{RIP}(S, r)$ and define

$$\begin{array}{rcl} s =^r s' & \equiv & r(s) = r(s') \\ x \bullet^r y & \equiv & r((r(x) \bullet r(y)) \end{array}$$

Remarks

- Easy to show that $(S, =^r)$ is an equivalence relation iff $(S_r, =)$ is an equivalence relation (proof requires $\mathbb{RIP}(S, r)$).
- In standard programming languages (those without dependent types) it is much easier to implement $\text{fullReduce}((S, =, \bullet), r)$ than $\text{reduce}((S, =, \bullet), r)$.

Associativity?

Fact

$$\mathbb{AS}(\text{reduce}((S, =, \bullet), r)) \leftrightarrow \mathbb{AS}(\text{fullReduce}((S, =, \bullet), r))$$

Proof is rather tedious: It relies heavily on $\mathbb{RIP}(S, r)$ and congruences:

$$\begin{array}{rcl} \mathbb{RCONG}(S, =, r) & \equiv & \forall s_1, s_2 \in S, s_1 = s_2 \to r(s_1) = r(s_2) \\ \mathbb{CONG}(S, =, \bullet) & \equiv & \forall s_1, s_2, s_3, s_4 \in S, \\ & & (s_1 = s_2 \wedge s_3 = s_4) \to s_1 \bullet s_3 = s_2 \bullet s_4 \end{array}$$