L11 : Algebraic Path Problems with Applications to Internet Routing
Lecture 16

Timothy G. Griffin

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

Michaelmas Term
2012

How can we fit all the bits together?

Many types of structures ...

Semirings, Closed semirings, semimodules, AMEs, non-distributive structures ...

Many Algorithms ...

Dijkstra, Link-State (distributed), Bellman-Ford, Distributed Bellman-ford, ...

Many metrics ..

$\min -+$, $\max - \min$, products, lexicgraphic combination, semi-direct products ...

Properties needed by some algorithms ...

description	P	**meaning**
Associativity	ass	$\forall x\ y\ z \in S, x \circ (y \circ z) = (x \circ y) \circ z$
Commutativity	com	$\forall x\ y \in S, x \circ y = y \circ x$
Idempotence	idm	$\forall x \in S, x \circ x = x$
Selectivity	sel	$\forall x\ y \in S, x \circ y \in \{x, y\}$
Identity	ide	$\exists i \in S, \forall x \in S, i \circ x = x = x \circ i$
Annihilator	ann	$\exists w \in S, \forall x \in S, w \circ x = w = x \circ w$
L Consistency	l.con	$\mathcal{W}(\text{ide}(S, \oplus)) = \mathcal{W}(\text{ann}(S, \otimes))$
R Consistency	r.con	$\mathcal{W}(\text{ide}(S, \otimes)) = \mathcal{W}(\text{ann}(S, \oplus))$
L absorbing	abs	$\forall x\ y \in S, x \oplus (y \otimes x) = x$
L strict absorbing	str	$\forall x\ y \in S, x \oplus (y \otimes x) = x \wedge x \neq y \otimes x$
L distributivity	l.d	$\forall x\ y\ z \in S, z \otimes (x \oplus y) = (z \otimes x) \oplus (z \otimes y)$
R distributivity	r.d	$\forall x\ y\ z \in S, (x \oplus y) \otimes z = (x \otimes z) \oplus (y \otimes z)$

$\mathcal{W}(\exists x \in S, P(x))$ represents an element $s \in S$ such that $P(s)$ holds.

Metarouting : a domain-specific language for algebraic structures

Starting with an initial set of properties $\mathcal{P}_0$ ...

- Define a language $\mathcal{L}$,
- a well-formedness condition $\textsc{wf}(E)$, for $E \in \mathcal{L}$,
- and a set of properties $\mathcal{P}$, with $\mathcal{P}_0 \subseteq \mathcal{P}$

so that properties are decidable for well-formed expressions:

$$\forall \textsc{q} \in P : \forall E \in \mathcal{L} : \textsc{wf}(E) \implies (\textsc{q}([\![E]\!]) \vee \neg\textsc{q}([\![E]\!]))$$

The logic is constructive!

The challange: increase expressive power while preserving decidability ...

Let's start with a small language fragement for "bisemigroups" ...

$$
\begin{array}{rcl}
E & ::= & \texttt{bNatMinPlus} \\
 & | & \texttt{bNatMaxMin} \\
 & | & \texttt{bAddOne}\ c\ E \\
 & | & \texttt{bAddZero}\ c\ E \\
 & | & \texttt{bLex}\ E\ E \\
 & | & \vdots
\end{array}
$$

where c represents constants supplied by the user.

... and an "untyped" semantics

$$[\![E]\!] = (S,\ \oplus,\ \otimes),$$

Combinators for binary operations ...

- $\circ \in S \times S \to S$
- $\mathrm{id}\ c \circ \in (S \uplus \{c\}) \times (S \uplus \{c\}) \to (S \uplus \{c\})$

where

$$S \uplus T = \{\mathrm{inl}(s) \mid s \in S\} \cup \{\mathrm{inr}(t) \mid t \in T\}$$

$$\begin{aligned} \mathrm{inr}(c) \bullet x &= x, \\ x \bullet \mathrm{inr}(c) &= x, \\ \mathrm{inl}(s_1) \bullet \mathrm{inl}(s_2) &= \mathrm{inl}(s_1 \circ s_2). \end{aligned}$$

where $\bullet = \mathrm{id}\ c \circ$

… in a similar way …

- $\circ \in S \times S \to S$
- $\mathrm{ann}\ c\ \circ \in (S \uplus \{c\}) \times (S \uplus \{c\}) \to (S \uplus \{c\})$

$$\begin{array}{rcl} \mathrm{inr}(c) \star x & = & \mathrm{inr}(c), \\ x \star \mathrm{inr}(c) & = & \mathrm{inr}(c), \\ \mathrm{inl}(s_1) \star \mathrm{inl}(s_2) & = & \mathrm{inl}(s_1 \circ s_2). \end{array}$$

where $\star = \mathrm{ann}\ c\ \circ$.

Direct product

- $\circ \in S \times S \rightarrow S$
- $\diamond \in T \times T \rightarrow T$
- $\circ \times \diamond \in (S \times T) \times (S \times T) \rightarrow (S \times T)$

$$(s_1, t_1) \bullet (s_2, t_2) = (s_1 \circ s_2, t_1 \diamond t_2).$$

where $\bullet = \circ \times \diamond$.

lexicographic product

- $\circ \in S \times S \rightarrow S$
- $\diamond \in T \times T \rightarrow T$
- $\circ \vec{\times} \diamond \in (S \times T) \times (S \times T) \rightarrow (S \times T)$

$$(s_1, t_1) \bullet (s_2, t_2) = \begin{cases} (s_1, t_1 \diamond t_2), & \text{if } s_1 = s_2 \\ (s_1, t_1), & \text{if } s_1 = (s_1 \circ s_2) \neq s_2 \\ (s_2, t_2), & \text{if } s_1 \neq (s_1 \circ s_2) = s_2 \end{cases}$$

where $\bullet = \circ \vec{\times} \diamond$.

$[\![E]\!] = (S,\ \oplus,\ \otimes)$

$$
\begin{array}{rcl}
\overline{1}_c\ (S,\ \oplus,\ \otimes) & = & (S \uplus \{c\},\ \mathrm{ann}\ c\ \oplus,\ \mathrm{id}\ c\ \otimes) \\
\overline{0}_c\ (S,\ \oplus,\ \otimes) & = & (S \uplus \{c\},\ \mathrm{id}\ c\ \oplus,\ \mathrm{ann}\ c\ \otimes) \\
(S,\ \oplus_S,\ \otimes_S)\ \vec{\times}\ (T,\ \oplus_T,\ \otimes_T) & = & (S \times T,\ \oplus_S\ \vec{\times}\ \oplus_T,\ \otimes_S \times \otimes_T)
\end{array}
$$

$[\![E]\!] = (S,\ \oplus,\ \otimes)$

$$
\begin{array}{rcl}
[\![\texttt{bNatMinPlus}]\!] & = & (\mathbb{N},\ \mathsf{min},\ +) \\
[\![\texttt{bNatMaxMin}]\!] & = & (\mathbb{N},\ \mathsf{max},\ \mathsf{min}) \\
[\![\texttt{bAddOne}\ c\ E]\!] & = & \overline{1}_c[\![E]\!] \\
[\![\texttt{bAddZero}\ c\ E]\!] & = & \overline{0}_c[\![E]\!] \\
[\![\texttt{bLex}\ E\ E']\!] & = & [\![E]\!]\ \vec{\times}\ [\![E']\!] \\
\vdots & \vdots & \vdots
\end{array}
$$

"Typed" Semantics

Either

$$[\![E]\!] = \mathrm{ERROR}$$

or

$$[\![E]\!] = ((S,\ \oplus,\ \otimes),\ \vec{\rho},\ \vec{\pi})$$

$\vec{\rho}$	proofs of required properties
$\vec{\pi}$	proofs or refutations of optional properties

Where to draw the line is a *design decision*!

For bisemigroups we only require $\oplus$ and $\otimes$ to be associative.

Our method

For every combinator C and every property P

find $\mathrm{wf}_{P,C}$ and $\beta_{P,C}$ such that

$$\mathrm{wf}_{P,C}(\vec{a}) \Rightarrow (P(C(\vec{a})) \Leftrightarrow \beta_{P,C}(\vec{a}))$$

Example needed to guarantee associativity of lexicographic operator

$$\mathrm{wf}_{\mathrm{l.dist},\vec{\times}} = \mathrm{COM}(S, \oplus_S) \wedge \mathrm{SEL}(S, \oplus_S)$$

Rewrite above as two "bottom-up rules" ...

$$\begin{array}{rcl} \mathrm{wf}_{P,C}(\vec{a}) \wedge \beta_{P,C}(\vec{a}) & \Rightarrow & P(C(\vec{a})) \\ \mathrm{wf}_{P,C}(\vec{a}) \wedge \neg\beta_{P,C}(\vec{a}) & \Rightarrow & \neg P(C(\vec{a})), \end{array}$$

When does $\text{L.D}(S \vec{\times} T)$ hold?

$$\text{COM}(S, \oplus_S) \wedge \text{SEL}(S, \oplus_S) \Rightarrow$$
$$\text{L.D}(S \vec{\times} T) \iff \text{L.D}(S) \wedge \text{L.D}(T) \quad \wedge \quad (\text{L.C}(S_\otimes) \vee \text{L.K}(T_\otimes))$$

This forces us to add these to $\mathcal{P}$

Property	Definition
L.C	$\forall xyz \in S, z \otimes y = z \otimes y \implies x = y$
L.K	$\forall xyz \in T, z \otimes x = z \otimes y$

Now need to "close" set of theorems under these new properties. Rinse, wash, repeat....

Current prototype being developed using the Coq theorem prover

name	signature	prefix	(positive) properties	constructors
Sets	(S)	d	3	9
Semigroups	$(S, \oplus)$	s	14	17
Preorders	$(S, \leq)$	p	4	5
Bisemigroups	$(S, \oplus, \otimes)$	b	22	20
Order semigroups	$(S, \leq, \oplus)$	o	17	6
Transforms	$(S, L, \triangleright)$	t	2	8
Order transforms	$(S, L, \leq, \triangleright)$	ot	3	2
Semigroup transforms	$(S, L, \oplus, \triangleright)$	st	4	10

where $\triangleright \in L \to S \to S$.

This represents over 1700 bottom-up rules ...

HW3 : A few definitions

Definition: min-sets

Suppose that $(S, \lesssim)$ is a pre-ordered set (reflexive, transitive pre-order). Let $A \subseteq S$ be finite. Define

$$\begin{aligned} \min_{\lesssim}(A) &\equiv \{a \in A \mid \forall b \in A : \neg(b < a)\} \\ \mathcal{P}(S, \lesssim) &\equiv \{A \subseteq S \mid A \text{ is finite and } \min_{\lesssim}(A) = A\} \end{aligned}$$

HW3 : Problems 1 and 2

Problem 1

Prove that $(\mathcal{P}(S, \lesssim), \oplus^{\lesssim}_{\min})$ where

$$A \oplus^{\lesssim}_{\min} B = \min_{\lesssim}(A \cup B)$$

is a semiroup. It is clear that $\{\}$ is the identity. Is there always an annihilator?

Problem 2

Given a semigroup $(S, \otimes)$, prove that $(\mathcal{P}(S, \lesssim), \otimes^{\lesssim}_{\min})$ where

$$A \otimes^{\lesssim}_{\min} B = \min_{\lesssim}(\{a \otimes b \mid a \in A, b \in B\})$$

is a semiroup. It is clear that $\{\}$ is the annihilator. Is there always an identity?

HW3 : Problem 3

Define

$$F(S,\ \oplus,\ \otimes) \quad = \quad (\mathcal{P}(S,\ \lesssim),\ \otimes^{\lesssim}_{\text{min}},\ \oplus^{\lesssim}_{\text{min}})$$

$$[\![\texttt{bMinSetsRight}\ E]\!] \quad = \quad F([\![E]\!])$$

where $a \lesssim b \iff a \oplus b = b$ (the right natural order).

Problem 3

Derive an "iff-rule" for this constructor for the property of left-distributivity.

Problem 4 (rather difficult)

Definition

- A cut set $C \subseteq E$ for nodes i and j is a set of edges such there is no path from i to j in the graph $(V,\ E - C)$.
- C is minimal if no proper subset of C is a cut set.

Let $G = (V,\ E)$ be a graph and define

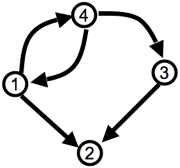
$$M = F(2^E,\ \cup,\ \cup).$$

Problem 4

- Show that M is a semiring.
- Show that if every arc $(i,\ j)$ is has weight $w(i,\ j) = \{\{(i,\ j)\}\}$, then $\mathbf{A}^{(*)}(i,\ j)$ is the set of all minimal cut sets for i and j.

Example for M

$$(i,j) \in E \rightarrow w(i,j) = \{\{(i,j)\}\}$$

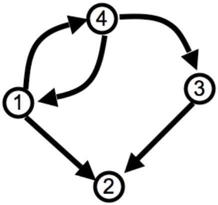


$$A = \begin{bmatrix} \{\phi\} & \{\{(1,2)\}\} & \{\phi\} & \{\{(1,4)\}\} \\ \{\phi\} & \{\phi\} & \{\phi\} & \{\phi\} \\ \{\phi\} & \{\{(3,2)\}\} & \{\phi\} & \{\phi\} \\ \{\{(4,1)\}\} & \{\phi\} & \{\{(4,3)\}\} & \{\phi\} \end{bmatrix}$$

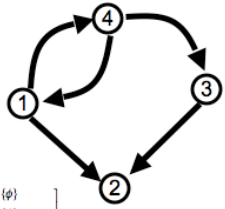
Example for M

$$A^2 = A \otimes A = \begin{bmatrix} \{\phi\} & \{\{(1,2)\}\} & \{\phi\} & \{\{(1,4)\}\} \\ \{\phi\} & \{\phi\} & \{\phi\} & \{\phi\} \\ \{\phi\} & \{\{(3,2)\}\} & \{\phi\} & \{\phi\} \\ \{\{(4,1)\}\} & \{\phi\} & \{\{(4,3)\}\} & \{\phi\} \end{bmatrix} \otimes \begin{bmatrix} \{\phi\} & \{\{(1,2)\}\} & \{\phi\} & \{\{(1,4)\}\} \\ \{\phi\} & \{\phi\} & \{\phi\} & \{\phi\} \\ \{\phi\} & \{\{(3,2)\}\} & \{\phi\} & \{\phi\} \\ \{\{(4,1)\}\} & \{\phi\} & \{\{(4,3)\}\} & \{\phi\} \end{bmatrix}$$

$$= \begin{bmatrix} \{\{(1,4)\},\{(4,1)\}\} & \{\phi\} & \{\{(1,4)\},\{(4,3)\}\} & \{\phi\} \\ \{\phi\} & \{\phi\} & \{\phi\} & \{\phi\} \\ \{\phi\} & \{\phi\} & \{\phi\} & \{\phi\} \\ \{\phi\} & \{\{(1,2),(3,2)\},\{(1,2),(4,3)\},\{(4,1),(3,2)\},\{(4,1),(4,3)\}\} & \{\phi\} & \{\{(1,4)\},\{(4,1)\}\} \end{bmatrix}$$



Example for M



$$A = \begin{bmatrix} \{\phi\} & \{\{(1,2)\}\} & \{\phi\} & \{\{(1,4)\}\} \\ \{\phi\} & \{\phi\} & \{\phi\} & \{\phi\} \\ \{\phi\} & \{\{(3,2)\}\} & \{\phi\} & \{\phi\} \\ \{\{(4,1)\}\} & \{\phi\} & \{\{(4,3)\}\} & \{\phi\} \end{bmatrix}$$

$$A^2 = \begin{bmatrix} \{\{(1,4)\},\{(4,1)\}\} & \{\phi\} & \{\{(1,4)\},\{(4,3)\}\} & \{\phi\} \\ \{\phi\} & \{\phi\} & \{\phi\} & \{\phi\} \\ \{\phi\} & \{\phi\} & \{\phi\} & \{\phi\} \\ \{\phi\} & \{\{(1,2),(3,2)\},\{(1,2),(4,3)\},\{(4,1),(3,2)\},\{(4,1),(4,3)\}\} & \{\phi\} & \{\{(1,4)\},\{(4,1)\}\} \end{bmatrix}$$

$$A^3 = A^5 = \begin{bmatrix} \{\phi\} & \{\{(1,4)\},\{(1,2),(3,2)\},\{(1,2),(4,3)\},\{(4,1),(3,2)\},\{(4,1),(4,3)\}\} & \{\phi\} & \{\{(1,4)\},\{(4,1)\}\} \\ \{\phi\} & \{\phi\} & \{\phi\} & \{\phi\} \\ \{\phi\} & \{\phi\} & \{\phi\} & \{\phi\} \\ \{\{(1,4)\},\{(4,1)\}\} & \{\phi\} & \{\{(4,1)\},\{(1,4)\},\{(4,3)\}\} & \{\phi\} \end{bmatrix}$$

$$A^4 = \begin{bmatrix} \{\{(1,4)\},\{(4,1)\}\} & \{\phi\} & \{\{(1,4)\},\{(1,4),(4,3)\}\} & \{\phi\} \\ \{\phi\} & \{\phi\} & \{\phi\} & \{\phi\} \\ \{\phi\} & \{\phi\} & \{\phi\} & \{\phi\} \\ \{\phi\} & \{\{(4,1)\},\{(1,4)\},\{(1,2),(3,2)\},\{(1,2),(4,3)\}\} & \{\phi\} & \{\{(1,4)\},\{(1,4)\}\} \end{bmatrix}$$

$$A^{(4)} = \begin{bmatrix} \phi & \{\{(1,2),(1,4)\},\{\{(1,2),(3,2)\},\{(1,2),(4,3)\}\} & \{\{(1,4)\},\{(4,3)\}\} & \{\{(1,4)\}\} \\ \{\phi\} & \phi & \{\phi\} & \{\phi\} \\ \{\phi\} & \{(3,2)\} & \phi & \{\phi\} \\ \{\{(4,1)\}\} & \{\{(1,2),(3,2)\},\{(1,2),(4,3)\},\{(4,1),(3,2)\},\{(4,1),(4,3)\}\} & \{\{(4,3)\}\} & \phi \end{bmatrix}$$