An Algebraic Approach to Internet Routing Lectures 05 and 06

Timothy G. Griffin

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

Michaelmas Term
2010

Outline

Revisit Lexicographic Semiring

[Lex Product Theorem] Assume $\oplus_S$ is commutative and idempotent. Then

$$\text{LD}(S \vec{\times} T) \iff \text{LD}(S) \wedge \text{LD}(T) \wedge (\text{LC}(S) \vee \text{LK}(T))$$

But wait! How could any semiring satisfy either of these properties?

Property	Definition
LC	$\forall a, b, c : c \otimes a = c \otimes b \implies a = b$
LK	$\forall a, b, c : c \otimes a = c \otimes b$

- For LC, note that we always have $\overline{0} \otimes a = \overline{0} \otimes b$, so LC could only hold when $S = \{\overline{0}\}$.
- For LK, let $a = \overline{1}$ and $b = \overline{0}$ and LK leads to the conclusion that every c is equal to $\overline{0}$ (again!). Thanks to Ramana Kumar for pointing this out!

My mistake! The theorem above was formulated in the context of a much more liberal algebraic setting [Sai70, GG07, Gur08] and I should not have introduced it in the context of semirings.

Bisemigroups – a more liberal setting

$(S, \oplus, \otimes)$ is a bisemigroup when

- $\oplus$ is a associative
- $\otimes$ is a associative

Each semiring properties may, or may not, hold

Property	Definition
COMM$\oplus$	$\forall a, b : a \oplus b = b \oplus a$
$\exists\overline{0}$	$\exists\overline{0} : \forall a : a \oplus \overline{0} = \overline{0} \oplus a = a$
$\exists\overline{1}$	$\exists\overline{1} : \forall a : a \otimes \overline{1} = \overline{1} \otimes a = a$
ANN$\overline{0}$	$\forall a : a \otimes \overline{0} = \overline{0} \otimes \overline{0} = \overline{0}$
LD	$\forall a, b, c : c \otimes (a \oplus b) = (c \otimes a) \oplus (c \otimes b)$
RD	$\forall a, b, c : (a \oplus b) \otimes c = (a \otimes c) \oplus (b \otimes c)$

Some bisemigroups (that are not semirings)

name	S	$\oplus$,	$\otimes$	$\overline{0}$	$\overline{1}$	possible routing use
min_plus	$\mathbb{N}$	min	$+$		0	minimum-weight routing
left(W)	2^W	$\cup$	left	$\{\}$		compute next-hop(s)
right(W)	2^W	$\cup$	right	$\{\}$		compute origin(s)

Operation for inserting a zero

Suppose $\overline{0} \notin S$

$$\text{add\_zero}(\overline{0},\ (S,\ \oplus,\ \otimes)) = (S \cup \{\overline{0}\}, \hat{\oplus},\ \hat{\otimes})$$

where

$$a \hat{\oplus} b \quad = \quad \begin{cases} a & (\text{if } b = \overline{0}) \\ b & (\text{if } a = \overline{0}) \\ a \oplus b & (\text{otherwise}) \end{cases}$$

$$a \hat{\otimes} b \quad = \quad \begin{cases} \overline{0} & (\text{if } b = \overline{0}) \\ \overline{0} & (\text{if } a = \overline{0}) \\ a \otimes b & (\text{otherwise}) \end{cases}$$

$$\text{sp} = \text{add\_zero}(\infty,\ \text{min\_plus}).$$

In previous lecture, when I wrote $\text{sp} \vec{\times} \text{bw}$ it should have been $\text{add\_zero}(\infty,\ \text{min\_plus} \vec{\times} \text{bw})$

Operation for inserting a one

Suppose $\overline{1} \notin S$

$$\mathrm{add\_one}(\overline{1},\ (S,\ \oplus,\ \otimes)) = (S \cup \{\overline{1}\}, \hat{\oplus},\ \hat{\otimes})$$

where

$$a \hat{\oplus} b \quad = \quad \begin{cases} \overline{1} & \text{(if } b = \overline{1}\text{)} \\ \overline{1} & \text{(if } a = \overline{1}\text{)} \\ a \oplus b & \text{(otherwise)} \end{cases}$$

$$a \hat{\otimes} b \quad = \quad \begin{cases} a & \text{(if } b = \overline{1}\text{)} \\ b & \text{(if } a = \overline{1}\text{)} \\ a \otimes b & \text{(otherwise)} \end{cases}$$

next hop semiring

For graph $G = (V,\ E)$, let $\mathrm{nh} = \mathrm{add\_one}(\mathrm{self},\ \mathrm{left}(V))$. To use, label earch arc $(u, v) \in E$ as $w(u, v) = \{v\}$.

Prove $\mathrm{LD}(S) \wedge \mathrm{LD}(T) \wedge (\mathrm{LC}(S) \vee \mathrm{LK}(T)) \implies \mathrm{LD}(S \vec{\times} T)$

Assume S and T are bisemigroups, $\mathrm{LD}(S) \wedge \mathrm{LD}(T) \wedge (\mathrm{LC}(S) \vee \mathrm{LK}(T))$, and

$$(s_1, t_1), (s_2, t_2), (s_3, t_3) \in S \times T.$$

Then (dropping operator subscripts for clarity) we have

$$\begin{array}{rcl} \mathrm{lhs} & = & (s_1, t_1) \otimes ((s_2, t_2) \vec{\oplus} (s_3, t_3)) \\ & = & (s_1, t_1) \otimes (s_2 \oplus s_3, t_{\mathrm{lhs}}) \\ & = & (s_1 \otimes (s_2 \oplus s_3), t_1 \otimes t_{\mathrm{lhs}}) \end{array}$$

$$\begin{array}{rcl} \mathrm{rhs} & = & ((s_1, t_1) \otimes (s_2, t_2)) \vec{\oplus} ((s_1, t_1) \otimes (s_3, t_3)) \\ & = & (s_1 \otimes s_2, t_1 \otimes t_2) \vec{\oplus} (s_1 \otimes s_3, t_1 \otimes t_3) \\ & = & ((s_1 \otimes s_2) \oplus_S (s_1 \otimes s_3), t_{\mathrm{rhs}}) \\ & = & (s_1 \otimes (s_2 \oplus s_3), t_{\mathrm{rhs}}) \end{array}$$

where t_{lhs} and t_{rhs} are determined by the definition of $\vec{\oplus}$.
We need to show that *lhs* $=$ *rhs*, that is $t_{\mathrm{rhs}} = t_1 \otimes t_{\mathrm{lhs}}$.

Case 1 : $\text{LC}(S)$

Note that from $\text{LCNZ}(S)$ we have

$$(\star) \quad \forall a, b, c : a \neq b \implies c \otimes a \neq c \otimes b$$

There are four sub-cases to consider.
Case 1.1 : $s_2 = s_2 \oplus s_3 = s_3$. Then $t_{\text{lhs}} = t_2 \oplus t_3$ and $t_1 \otimes t_{\text{lhs}} = t_1 \otimes (t_2 \oplus t_3) = (t_1 \otimes t_2) \oplus (t_1 \otimes t_3)$, by $\text{LD}(S)$. Also, $s_1 \otimes_S s_2 = s_1 \otimes_S s_3$ and $s_1 \otimes s_2 = s_1 \otimes (s_2 \oplus s_3) = (s_1 \otimes s_2) \oplus (s_1 \otimes s_3)$, again by $\text{LD}(S)$. Therefore $t_{\text{rhs}} = (t_1 \otimes t_2) \oplus (t_1 \otimes t_3) = t_1 \otimes t_{\text{lhs}}$.

Case 1.2 : $s_2 = s_2 \oplus s_3 \neq s_3$. Then $t_1 \otimes t_{\text{lhs}} = t_1 \otimes t_2$ Also
$s_2 = s_2 \oplus s_3 \implies s_1 \otimes s_2 = s_1 \otimes (s_2 \oplus s_3)$ and by $\star$
$s_2 \oplus s_3 \neq s_3 \implies s_1 \otimes (s_2 \oplus s_3) \neq s_1 \otimes s_3$. Thus, by $\text{LD}(S)$,
$(s_1 \otimes s_2) \oplus (s_1 \otimes s_3) \neq s_1 \otimes s_3$ and we get $t_{\text{rhs}} = t_1 \otimes t_2 = t_1 \otimes t_{\text{lhs}}$.

Case 1 : $\textsc{lc}(S)$ (continued)

Case 1.3 : $s_2 \neq s_2 \oplus_S s_3 = s_3$. Similar to case 1.2.

Case 1.4 : $s_2 \neq s_2 \oplus_S s_3 \neq s_3$. Then $t_{\text{lhs}} = \overline{0}$ and $t_1 \otimes t_{\text{lhs}} = \overline{0}$. Using $\star$ (twice), we have $s_1 \otimes s_2 \neq (s_1 \otimes s_2) \oplus_S (s_1 \otimes s_3) \neq s_1 \otimes s_3$, so $t_{\text{rhs}} = \overline{0}$.

Case 2 : $\text{LK}(T)$

Proving this case is problem 1 for problem set 2.

Necessary condition for left distributivity?

How about this?

$$\textsc{ld}(S \vec{\times} T) \implies \textsc{ld}(S) \wedge \textsc{ld}(T) \wedge (\textsc{lc}(S) \vee \textsc{lk}(T))$$

Problem : does not (directly) give a “bottom up” method of constructing counter examples.

Alternative

Theorem

$$\textsc{nld}(S) \vee \textsc{nld}(T) \vee (\textsc{nlc}(S) \wedge \textsc{nlk}(T)) \implies \textsc{nld}(S \vec{\times} T)$$

Property	Definition
NLD	$\exists a, b, c : c \otimes (a \oplus b) \neq (c \otimes a) \oplus (c \otimes b)$
NLC	$\exists a, b, c : c \otimes a = c \otimes b \wedge a \neq b$
NLK	$\exists a, b, c : c \otimes a \neq c \otimes b$

Proving this is problem 2 for problem set 2. For additional credit, show clearly how counter examples to $\textsc{ld}(S \vec{\times} T)$ can be constructed.

Outline

The plan

Define a little language (syntax!) $\mathcal{L}$ for bisemigroups,

$$E ::= \cdots$$

with semantics

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

- Let $\mathcal{P}$ be the set of properties that we need or care about (yes, this is vague). We assume that for each property $\text{Q} \in \mathcal{P}$ there is a property $\text{NQ} \in \mathcal{P}$ where $\neg(\text{Q} \wedge \text{NQ})$ holds.
- We may need a *well-formedness* predicate on language expressions, $\text{WF}(E)$.

Now for the hard part ...

Closure

The language $\mathcal{L}$ is closed w.r.t $\mathcal{P}$ if

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

holds constructively.

The Research Challange

Define $\mathcal{L}$, $\mathcal{P}$, and $\textsc{wf}(E)$ is such a way that

- $\mathcal{L}$ is expressive enough to model Internet protocols and more ...
- $\mathcal{L}$ is closed with respect to $\mathcal{P}$

The approach — bottom up construction of $\text{Q}([\![A]\!]) \vee \text{NQ}([\![A]\!])$

For example, with $S \vec{\times} T$ we have

$$\begin{aligned} \text{LD}(S) \vee \text{LD}(T) \vee (\text{LC}(S) \wedge \text{LK}(T)) &\implies \text{LD}(S \vec{\times} T) \\ \text{NLD}(S) \vee \text{NLD}(T) \vee (\text{NLC}(S) \wedge \text{NLK}(T)) &\implies \text{NLD}(S \vec{\times} T) \end{aligned}$$

The ability to do this cleanly may hinge on the details!!

Example : suppose we make the mistake of defining Lexicographic Product of Semigroups this way....

Definition ($\vec{\times}_{\overline{0}}$)

Suppose $(S,\ \oplus_S,\ \overline{0}_S)$ is commutative idempotent monoid and $(T,\ \oplus_T,\ \overline{0}_T)$ is a monoid. The lexicographic product with zero is defined as the monoid

$$(S, \oplus_S)\ \vec{\times}_{\overline{0}}\ (T, \oplus_T) \equiv (((S - \{\overline{0}_S\}) \times T) \cup \{\overline{0}\},\ \vec{\oplus}_{\overline{0}},\ \overline{0})$$

where $\overline{0}$ is the identity for $\vec{\oplus}_{\overline{0}}$ and

$$(s_1, t_1)\vec{\oplus}_{\overline{0}}(s_2, t_2) = \begin{cases} (s_1 \oplus_S s_2, t_1 \oplus_T t_2) & s_1 = s_1 \oplus_S s_2 = s_2 \\ (s_1 \oplus_S s_2, t_1) & s_1 = s_1 \oplus_S s_2 \neq s_2 \\ (s_1 \oplus_S s_2, t_2) & s_1 \neq s_1 \oplus_S s_2 = s_2 \\ (s_1 \oplus_S s_2, \overline{0}_T) & \text{otherwise.} \end{cases}$$

The problem ...

If we restrict ourselves to Semirings, then our new lexicographic product requires rules such as

Property	Definition
LD	$\forall a, b, c : c \otimes (a \oplus b) = (c \otimes a) \oplus (c \otimes b)$
LCNZ	$\forall a, b, c : (c \neq \overline{0} \wedge c \otimes a = c \otimes b) \implies a = b$
LKNZ	$\forall a, b, c : (a \neq \overline{0} \wedge b \neq \overline{0}) \implies c \otimes a = c \otimes b$

These are very hard to work with!

Outline

Bibliography I

[GG07] A. J. T. Gurney and T. G. Griffin.
Lexicographic products in metarouting.
In *Proc. Inter. Conf. on Network Protocols*, October 2007.

[Gur08] Alexander Gurney.
Designing routing algebras with meta-languages.
Thesis in progress, 2008.

[Sai70] Tôru Saitô.
Note on the lexicographic product of ordered semigroups.
Proceedings of the Japan Academy, 46(5):413–416, 1970.