An Algebraic Approach to Internet Routing
Lecture 10
Algebras of Monoid Endomorphisms

Timothy G. Griffin

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

Michaelmas Term
2010

Path Weight with functions on arcs?

For graph $G = (V,\ E)$, and path $p = i_1, i_2, i_3, \cdots, i_k$.

Semiring Path Weight

Weight function $w : E \rightarrow S$

$$w(p) = w(i_1,\ i_2) \otimes w(i_2,\ i_3) \otimes \cdots \otimes w(i_{k-1},\ i_k).$$

How about functions on arcs?

Weight function $w : E \rightarrow (S \rightarrow S)$

$$w(p) = w(i_1,\ i_2)(w(i_2,\ i_3)(\cdots w(i_{k-1},\ i_k)(a) \cdots)),$$

where a is some value originated by node i_k

How can we make this work?

Algebra of Monoid Endomorphisms ([GM08])

A homomorphism is a function that preserves structure. An endomprhism is a homomorphism mapping a structure to itself.

Let $(S, \oplus, \overline{0})$ be a commutative monoid.

$(S, \oplus, F \subseteq S \rightarrow S, \overline{0}, i, \omega)$ is a algebra of monoid endomorphisms (AME) if

- $\forall f \in F \; \forall b, c \in S : f(b \oplus c) = f(b) \oplus f(c)$
- $\forall f \in F : f(\overline{0}) = \overline{0}$
- $\exists i \in F \; \forall a \in S : i(a) = a$
- $\exists \omega \in F \; \forall a \in S : \omega(a) = \overline{0}$

Solving (some) equations over a AMEs

We will be interested in solving for x equations of the form

$$x = f(x) \oplus b$$

Let

$$\begin{array}{rcl} f^0 & = & i \\ f^{k+1} & = & f \circ f^k \end{array}$$

and

$$\begin{array}{rcl} f^{(k)}(b) & = & f^0(b) \oplus f^1(b) \oplus f^2(b) \oplus \cdots \oplus f^k(b) \\ f^{(*)}(b) & = & f^0(b) \oplus f^1(b) \oplus f^2(b) \oplus \cdots \oplus f^k(b) \oplus \cdots \end{array}$$

Definition (q stability)

If there exists a q such that for all b $f^{(q)}(b) = f^{(q+1)}(b)$, then f is *q-stable*. Therefore, $f^{(*)}(b) = f^{(q)}(b)$.

Key result (again)

Lemma

If f is q-stable, then $x = f^{(*)}(b)$ solves the AME equation

$$x = f(x) \oplus b.$$

Proof: Substitute $f^{(*)}(b)$ for x to obtain

$$\begin{array}{rl}
 & f(f^{(*)}(b)) \oplus b \\
= & f(f^{(q)}(b)) \oplus b \\
= & f(f^0(b) \oplus f^1(b) \oplus f^2(b) \oplus \cdots \oplus f^q(b)) \oplus b \\
= & f^1(b) \oplus f^1(b) \oplus f^2(b) \oplus \cdots \oplus f^{q+1}(b) \oplus b \\
= & f^0(b) \oplus f^1(b) \oplus f^1(b) \oplus f^2(b) \oplus \cdots \oplus f^{q+1}(b) \\
= & f^{(q+1)}(b) \\
= & f^{(q)}(b) \\
= & f^{(*)}(b)
\end{array}$$

AME of Matrices

Given an AME $S = (S, \oplus, F)$, define the semiring of $n \times n$-matrices over S,

$$\mathbb{M}_n(S) = (\mathbb{M}_n(S), \oplus, G),$$

where for $\mathbf{A}, \mathbf{B} \in \mathbb{M}_n(S)$ we have

$$(\mathbf{A} \oplus \mathbf{B})(i, j) = \mathbf{A}(i, j) \oplus \mathbf{B}(i, j).$$

Elements of the set G are represented by $n \times n$ matrices of functions in F. That is, each function in G is represented by a matrix $\mathbf{A}$ with $\mathbf{A}(i, j) \in F$. If $\mathbf{B} \in \mathbb{M}_n(S)$ then define $\mathbf{A}(\mathbf{B})$ so that

$$(\mathbf{A}(\mathbf{B}))(i, j) = \sum_{1 \leq q \leq n}^{\oplus} \mathbf{A}(i, q)(\mathbf{B}(q, j)).$$

Here we go again...

Path Weight

For graph $G = (V,\ E)$ with $w : E \rightarrow F$
The *weight* of a path $p = i_1, i_2, i_3, \cdots, i_k$ is then calculated as

$$w(p) = w(i_1,\ i_2)(w(i_2,\ i_3)(\cdots w(i_{k-1},\ i_k)(\omega_{\oplus})\cdots)).$$

adjacency matrix

$$\mathbf{A}(i,\ j) = \begin{cases} w(i,\ j) & \text{if } (i,\ j) \in E, \\ \omega & \text{otherwise} \end{cases}$$

We want to solve equations like these

$$\mathbf{X} = \mathbf{A}(\mathbf{X}) \oplus \mathbf{B}$$

So why do we need Monoid Endomorphisms??

Monoid Endomorphisms can be viewed as semirings

Suppose $(S, \oplus, F)$ is a monoid of endomorphisms. We can turn it into a semiring

$$(F, \hat{\oplus}, \circ)$$

where $(f \hat{\oplus} g)(a) = f(a) \oplus g(a)$

Functions are hard to work with....

- All algorithms need to check equality over elements of semiring,
- $f = g$ means $\forall a \in S : f(a) = g(a)$,
- S can be very large, or infinite.

Lexicographic product of AMEs

$$(S,\ \oplus_S,\ F)\ \vec{\times}\ (T,\ \oplus_T,\ G) = (S \times T,\ \oplus_S\ \vec{\times}\ \oplus_T,\ F \times G)$$

Theorem ([Sai70, GG07, Gur08])

$$\mathrm{D}(S\ \vec{\times}\ T) \iff \mathrm{D}(S) \wedge \mathrm{D}(T) \wedge (\mathrm{C}(S) \vee \mathrm{K}(T))$$

Where

Property	Definition
D	$\forall a, b, f : f(a \oplus b) = f(a) \oplus f(b)$
C	$\forall a, b, f : f(a) = f(b) \implies a = b$
K	$\forall a, b, f : f(a) = f(b)$

Functional Union of AMEs

$$(S,\ \oplus,\ F) +_{\mathrm{m}} (S,\ \oplus,\ G) = (S,\ \oplus,\ F + G)$$

Fact

$$\mathrm{D}(S +_{\mathrm{m}} T) \iff \mathrm{D}(S) \wedge \mathrm{D}(T)$$

Where

Property	Definition
D	$\forall a, b, f : f(a \oplus b) = f(a) \oplus f(b)$

Left and Right

right

$$\textbf{right}(S, \oplus, F) = (S, \oplus, \{i\})$$

left

$$\textbf{left}(S, \oplus, F) = (S, \oplus, K(S))$$

where $K(S)$ represents all constant functions over S. For $a \in S$, define the function $\kappa_a(b) = a$. Then $K(S) = \{\kappa_a \mid a \in S\}$.

Facts

The following are always true.

$$\begin{array}{ll} \text{D}(\textbf{right}(S)) & \\ \text{D}(\textbf{left}(S)) & \text{(assuming } \oplus \text{ is idempotent)} \\ \text{C}(\textbf{right}(S)) & \\ \text{K}(\textbf{left}(S)) & \end{array}$$

Scoped Product

$$S \Theta T = (S \vec{\times} \mathbf{left}(T)) +_{\mathrm{m}} (\mathbf{right}(S) \vec{\times} T)$$

Theorem

$$\mathrm{D}(S \Theta T) \iff \mathrm{D}(S) \wedge \mathrm{D}(T).$$

Proof.

$$\begin{aligned}
& \mathrm{D}(S \Theta T) \\
& \mathrm{D}((S \vec{\times} \mathbf{left}(T)) +_{\mathrm{m}} (\mathbf{right}(S) \vec{\times} T)) \\
\iff & \mathrm{D}(S \vec{\times} \mathbf{left}(T)) \wedge \mathrm{D}(\mathbf{right}(S) \vec{\times} T) \\
\iff & \mathrm{D}(S) \wedge \mathrm{D}(\mathbf{left}(T)) \wedge (\mathrm{C}(S) \vee \mathrm{K}(\mathbf{left}(T))) \\
& \quad \wedge \mathrm{D}(\mathbf{right}(S)) \wedge \mathrm{D}(T) \wedge (\mathrm{C}(\mathbf{right}(S)) \vee \mathrm{K}(T)) \\
\iff & \mathrm{D}(S) \wedge \mathrm{D}(T)
\end{aligned}$$

Delta Product (OSPF-like?)

$$S \Delta T = (S \vec{\times} T) +_{\mathrm{m}} (\mathbf{right}(S) \vec{\times} T)$$

Theorem

$$\mathrm{D}(S \Delta T) \iff \mathrm{D}(S) \wedge \mathrm{D}(T) \wedge (\mathrm{C}(S) \vee \mathrm{K}(T)).$$

Proof.

$$\begin{aligned}
& \mathrm{D}(S \Theta T) \\
& \mathrm{D}((S \vec{\times} T) +_{\mathrm{m}} (\mathbf{right}(S) \vec{\times} T)) \\
\iff & \mathrm{D}(S \vec{\times} T) \wedge \mathrm{D}(\mathbf{right}(S) \vec{\times} T) \\
\iff & \mathrm{D}(S) \wedge \mathrm{D}(\mathbf{left}(T)) \wedge (\mathrm{C}(S) \vee \mathrm{K}(T)) \\
& \quad \wedge \mathrm{D}(\mathbf{right}(S)) \wedge \mathrm{D}(T) \wedge (\mathrm{C}(\mathbf{right}(S)) \vee \mathrm{K}(T)) \\
\iff & \mathrm{D}(S) \wedge \mathrm{D}(T) \wedge (\mathrm{C}(S) \vee \mathrm{K}(T))
\end{aligned}$$

How do we represent functions?

Definition (transforms (indexed functions))

A set of transforms $(S,\ L,\ \rhd)$ is made up of non-empty sets S and L, and a function

$$\rhd \in L \rightarrow (S \rightarrow S).$$

We normally write $l \rhd s$ rather than $\rhd(l)(s)$. We can think of $l \in L$ as the index for a function $f_l(s) = l \rhd s$, so $(S,\ L,\ \rhd)$ represents the set of function $F = \{f_l \mid l \in L\}$.

Examples

Example 1: Trivial

Let $(S, \otimes)$ be a semigroup.

$$\mathrm{transform}(S, \oplus) = (S, S, \rhd_{\otimes}),$$

where $a \rhd_{\otimes} b = a \otimes b$

Example 2: Restriction

For $T \subset S$,

$$\mathrm{Restrict}(T, (S, \oplus)) = (S, T, \rhd_{\otimes}),$$

where $a \rhd_{\otimes} b = a \otimes b$

Example 3 : mildly abstract description of BGP's ASPATHs

Let $\mathrm{apaths}(X) = (\mathcal{E}(\Sigma^*) \cup \{\infty\},\ \Sigma \times \Sigma,\ \triangleright)$ where

$$\begin{array}{rcl}
\mathcal{E}(\Sigma^*) & = & \text{finite, elementary sequences over } \Sigma \text{ (no repeats)} \\
(m,\ n)\ \triangleright\ \infty & = & \infty \\
(m,\ n)\ \triangleright\ l & = & \left\{ \begin{array}{ll} n \cdot l & (\text{if } m \notin n \cdot l) \\ \infty & (\text{otherwise}) \end{array} \right.
\end{array}$$

Bibliography I

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

[GM08] M. Gondran and M. Minoux.
Graphs, Dioids, and Semirings : New Models and Algorithms.
Springer, 2008.

[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.