An Algebraic Approach to Internet Routing
Part II

Timothy G. Griffin

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

Departamento de Ingeniería Telemática
Escuela Politécnica Superior
Universidad Carlos III de Madrid
16, 17, 18 March, 2009

(Modified) Outline

- Part I (Monday)
  - Review of classical theory
- Part II (Tuesday)
  - Functions as arc weights
  - Live dangerously — drop distribution!
    - Model BGP-like protocols
- Part III (Wednesday)
  - Present a constructive approach
  - Metarouting

Path Weight with functions on arcs?

Semiring Path Weight

Path $p = i_1, i_2, i_3, \cdots, i_k$,

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

How about functions on arcs?

For graph $G = (V,\ E)$ with $w : E \rightarrow (S \rightarrow S)$

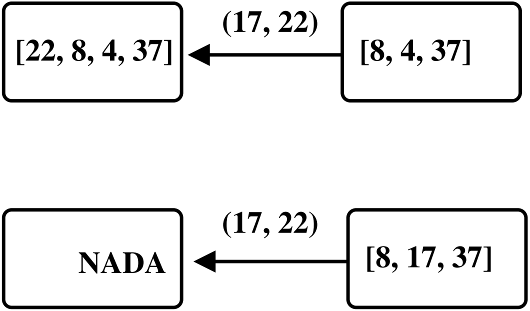
$$w(p) = w(i_1,\ i_2)(w(i_2,\ i_3)(\cdots w(i_{k-1},\ i_k)(a) \cdots)),$$

where a is some value originated by node i_k

How can we make this work?

ASPATHs from BGP

- Think of ASPATHs in BGP.
- the type of “arc labels” and the path values are different.
- So binary operators don’t quite work.



We could model this as some kind of function on the arc.

(left) Cayley transformation

Let's turn the multiplicative semigroup into a set of functions in order to get some inspiration!

- $(S, \otimes)$ a semigroup
- For $a \in S$, define the function f_a so that for all $b \in S$, $f_a(b) = a \otimes b$
- Let $F_\otimes = \{f_a \mid a \in S\}$

The notation $h = f \circ g$ means that for all a, $h(a) = f(g(a))$.

Lemma

If $f, g \in F_\otimes$, then $f \circ g \in F_\otimes$.

Proof :

$$(f_a \circ f_b)(c) = f_a(f_b(c)) = a \otimes (b \otimes c) = (a \otimes b) \otimes c = f_{a \otimes b}(c)$$

How do properties translate?

$(S, \oplus, \otimes)$	$(S, \oplus, F_{\otimes})$
$a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$	$f(b \oplus c) = f(b) \oplus f(c)$
$\alpha_{\oplus} = \omega_{\otimes}$	$f(\alpha_{\oplus}) = \alpha_{\oplus}$
$\alpha_{\oplus} = \omega_{\otimes}$	$\exists \omega \in F \ \forall a \in S : \omega(a) = \alpha_{\oplus}$
$\exists \alpha_{\otimes}$	$\exists i \in F \ \forall a \in S : i(a) = a$

Can we generalize this to a new kind of algebraic structure?

Algebra of Monoid Endomorphisms ([GM08])

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

Let $(S, \oplus, \alpha)$ be a commutative monoid.

$(S, \oplus, F \subseteq S \rightarrow S)$ is a algebra of monoid endomorphisms (AME) if

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

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

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

AME of Matrices

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

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

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

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

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

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

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

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

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])

$$\text{M}(S\ \vec{\times}\ T) \iff \text{M}(S) \wedge \text{M}(T) \wedge (\text{C}(S) \vee \text{K}(T))$$

Where

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

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

Fact

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

Where

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

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.

$\textsc{m}(\textbf{right}(S))$

$\textsc{m}(\textbf{left}(S))$ (assuming $\oplus$ is idempotent)

$\textsc{c}(\textbf{right}(S))$

$\textsc{k}(\textbf{left}(S))$

Motivate Scoped product

Scoped Product

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

Theorem

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

Proof.

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

Delta Product (OSPF-like?)

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

Theorem

$$\textsc{m}(S\Delta T) \iff \textsc{m}(S) \wedge \textsc{m}(T) \wedge (\textsc{c}(S) \vee \textsc{k}(T)).$$

Proof.

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

How do we represent functions?

Definition (Action)

An action $(S, L, \Diamond)$ is made up of non-empty sets S and L, and a function

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

We often write $l \Diamond s$ rather than $\Diamond(l)(s)$.

Think of L as an index set for a set of functions, $f_l(s) = l \Diamond s$.

Example : mildly abstract description of ASPATHs

Let $\mathrm{apaths}(X) = (S, L, \Diamond)$ where

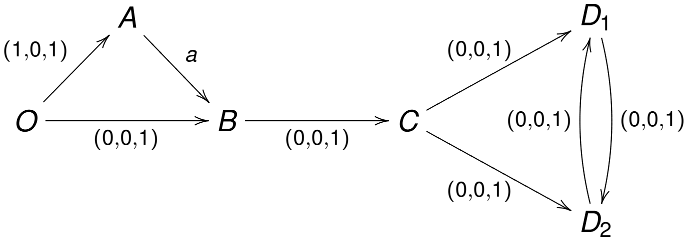
$$\begin{array}{rcl} S & = & X^* \cup \{\infty\} \\ L & = & X \times X \\ (m, n) \Diamond \infty & = & \infty \\ (m, n) \Diamond l & = & \begin{cases} \mathrm{cons}(n, l) & \text{(if } m \notin l) \\ \infty & \text{(otherwise)} \end{cases} \end{array}$$

Could BGP be distributive?

- Suppose **bgp** $=$ **ebgp**$\ominus$**ibgp**
- For $\textsc{M}$(**bgp**) to hold, we need at least $\textsc{M}$(**ebgp**)
- Suppose **ebgp** $=$ **economics** $\vec{\times}$ **aspaths** $\vec{\times}$ **te**
- This means we must have $\textsc{M}$(**economics**) and $\textsc{C}$(**economics**) since we will never have $\textsc{K}$(**aspaths** $\vec{\times}$ **te**).

What if we drop the distribution requirement?

$$R = (\{0,1\}, \max, \min) \vec{\times} (\{0,1\}, \min, \max) \vec{\times} (\mathbb{N} \cup \{\infty\}, \min, +).$$



Progress of the iteration when $a = (1, 0, n)$

step	A	B	C	D_1	D_2
1	$(1, 0, 1)$	$(0, 0, 1)$	—	—	—
2	$(1, 0, 1)$	$(1, 0, n+1)$	$(0, 0, 2)$	—	—
3	$(1, 0, 1)$	$(1, 0, n+1)$	$(0, 0, n+2)$	$(0, 0, 3)$	$(0, 0, 3)$
4	$(1, 0, 1)$	$(1, 0, n+1)$	$(0, 0, n+2)$	$(0, 0, 4)$	$(0, 0, 4)$
5	$(1, 0, 1)$	$(1, 0, n+1)$	$(0, 0, n+2)$	$(0, 0, 5)$	$(0, 0, 5)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$n+3$	$(1, 0, 1)$	$(1, 0, n+1)$	$(0, 0, n+2)$	$(0, 0, n+3)$	$(0, 0, n+3)$

Progress of the iteration when $a = (1, 1, 1)$

step	A	B	C	D_1	D_2
1	$(1, 0, 1)$	$(0, 0, 1)$	—	—	—
2	$(1, 0, 1)$	$(1, 1, 2)$	$(0, 0, 2)$	—	—
3	$(1, 0, 1)$	$(1, 1, 2)$	$(0, 1, 3)$	$(0, 0, 3)$	$(0, 0, 3)$
4	$(1, 0, 1)$	$(1, 1, 2)$	$(0, 1, 3)$	$(0, 0, 4)$	$(0, 0, 4)$
5	$(1, 0, 1)$	$(1, 1, 2)$	$(0, 1, 3)$	$(0, 0, 5)$	$(0, 0, 5)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
k	$(1, 0, 1)$	$(1, 1, 2)$	$(0, 1, 3)$	$(0, 0, k)$	$(0, 0, k)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

What are the conditions needed if distribution is dropped?

For a non-distributed structure $S = (S, \oplus, F)$, can be used to find local optima when the following property holds.

Increasing

$$\text{I} : \forall a \in S : a \neq \alpha \implies a <^{\mathrm{L}}_{\oplus} f(a)$$

In order to derive I we often need the non-decreasing property:

$$\text{ND} : \forall a \in S : a \leq^{\mathrm{L}}_{\oplus} f(a)$$

Some Rules

$$
\begin{aligned}
\mathrm{I}(S \vec{\times} T) &\iff \mathrm{I}(S) \vee (\mathrm{ND}(S) \wedge \mathrm{I}(T)) \\
\mathrm{ND}(S \vec{\times} T) &\iff \mathrm{I}(S) \vee (\mathrm{ND}(S) \wedge \mathrm{ND}(T)) \\
\mathrm{I}(S +_{\mathrm{m}} T) &\iff \mathrm{I}(S) \wedge \mathrm{I}(T) \\
\mathrm{ND}(S +_{\mathrm{m}} T) &\iff \mathrm{ND}(S) \wedge \mathrm{ND}(T) \\
\mathrm{I}(S \ominus T) &\iff \mathrm{I}(S) \wedge \mathrm{I}(T)
\end{aligned}
$$

Could BGP be fixed?

- Suppose **bgp** $=$ **ebgp**Θ**ibgp**
- For I(**bgp**) to hold, we need at least ND(**ebgp**)
- Suppose **ebgp** $=$ **economics** $\vec{\times}$ **aspaths** $\vec{\times}$ **te**
- Since we can probably get I(**aspaths** $\vec{\times}$ **te**), all we need is ND(**economics**).

One Modest Proposal

The Customer/Provider/Peer Algebra ([Sob05])

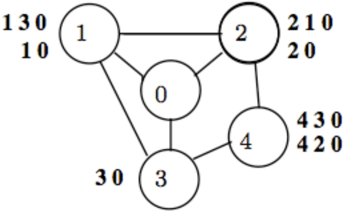
$\Diamond$	C	R	P	∞
c	C	∞	∞	∞
r	R	R	∞	∞
p	P	P	P	∞

Improve to model backup routes ([GS05])

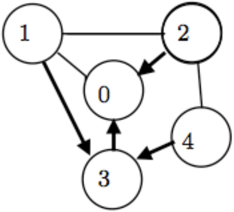
$\Diamond$	$(1, C)$	$(1, R)$	$(1, P)$	$(2, C)$	$(2, R)$	$(2, P)$	$(3, C)$	$(3, R$
c	$(1, C)$	$(2, C)$	$(2, C)$	$(2, C)$	$(3, C)$	$(3, C)$	$(3, C)$	∞
r	$(1, R)$	$(1, R)$	$(2, R)$	$(2, R)$	$(2, R)$	$(3, R)$	$(3, R)$	$(3, R$
p	$(1, P)$	$(1, P)$	$(1, P)$	$(2, P)$	$(2, P)$	$(2, P)$	$(3, P)$	$(3, P$

This is an algebraic presentation of an idea that appeared earlier in [GGR01].

Prehistory : The Stable Paths Problem (SPP) [GSW02]

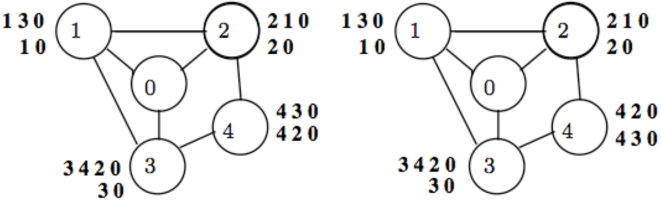


GOOD GADGET
(a)



A routing tree
(b)

More SPP examples



NAUGHTY GADGET
(c)

BAD GADGET
(d)

Proof from [GG08]

Assumptions

- Let $S = (S, \oplus, \otimes)$ be a bisemigroup where
  - $\oplus$ is idempotent ($a = a \oplus a$)
  - $\oplus$ is commutative ($a \oplus b = b \oplus a$)
  - $\oplus$ is selective ($a \oplus b = a \vee a \oplus b = b$)
- Note that this means that $\leq = \leq_{\oplus}^{L}$ is a total order.
- $\alpha_{\oplus}$ and $\alpha_{\otimes}$ exist
- $\alpha_{\oplus} = \omega_{\otimes}$

Assume that S is increasing

$$\text{I} : \forall a, b \in S : a \neq \alpha_{\oplus} \implies a <_{\oplus}^{L} b \otimes a$$

$s^k_{(i,j)}$

Let A be an adjacency matrix over S. Since $\oplus$ is selective, for each $i \neq j$ there exists $s^k_{(i,j)} \in N(i) \equiv \{s \mid (i, s) \in E\}$ such that

$$A^{[k+1]}(i,\ j) = \sum_{s \in N(i)} w(i, s) \otimes B(s,\ j) = w(i, s^k_{(i,j)}) \otimes A^{[k]}(s^k_{(i,j)},\ j)$$

We assume that we have a deterministic method of selecting a unique $s^k_{(i,j)}$.

Histories

Histories

- Inspired by constructs of the same name in [GW00] that record causal chains of events in an asynchronous protocol.
- The history of $A^{[k]}(i,\ j)$, denoted $H^{[k]}(i,\ j)$, will in some sense explain how the value $A^{[k]}(i,\ j)$ came to be adopted at step k of the iteration.

$$
\begin{array}{rcl}
H^{[0]}(i,\ j) & = & (\alpha_{\otimes}) \\
H^{[k+1]}(i,\ j) & = & \begin{cases} H^{[k]}(i,\ j) & \text{if } A^{[k]}(i,\ j) = A^{[k+1]}(i,\ j), \\ H^{[k]}(s^{k}_{(i,j)},\ j),\ A^{[k+1]}(i,\ j) & \text{if } A^{[k+1]}(i,\ j) <^{\oplus}_{L} A^{[k]}(i,\ j) \\ H^{[k]}(s^{k-1}_{(i,j)},\ j),\ A^{[k]}(i,\ j) & \text{if } A^{[k]}(i,\ j) <^{\oplus}_{L} A^{[k+1]}(i,\ j) \end{cases}
\end{array}
$$

Observations

- If $A^{[k+1]}(i,\ j) <_L^{\oplus} A^{[k]}(i,\ j)$, then node i obtained a more preferred value at step $k+1$.
  - In this case the history $H^{[k+1]}(i,\ j)$ is the sequence $H^{[k]}(s^k_{(i,j)},\ j),\ A^{[k+1]}(i,\ j)$, where $H^{[k]}(s^k_{(i,j)},\ j)$ is a history explaining how value $A^{[k]}(s^k_{(i,j)},\ j)$ was adopted at state k.
  - Since $A^{[k+1]}(i,\ j) = w(i, s^k_{(i,j)}) \otimes A^{[k]}(s^k_{(i,j)},\ j)$, the complete history explains how $A^{[k+1]}(i,\ j)$ was adopted at step $k+1$.

Further observations

- On the other hand, when $A^{[k]}(i,\ j) <_L^{\oplus} A^{[k+1]}(i,\ j)$, then node i lost a more preferred value at step $k+1$.
  - In this case the history $H^{[k+1]}(i,\ j)$ is the sequence $H^{[k]}(s_{(i,j)}^{k-1},\ j),\ A^{[k]}(i,\ j)$, which ends in the value lost at step $k+1$.
  - Since this lost value is $A^{[k]}(i,\ j) = w(i, s_{(i,j)}^{k-1}) \otimes A^{[k-1]}(s_{(i,j)}^{k-1},\ j)$, the sequence $H^{[k]}(s_{(i,j)}^{k-1},\ j)$ explains how node $s_{(i,j)}^{k-1}$ came to adopt $A^{[k]}(s_{(i,j)}^{k-1},\ j)$ at step k, thus forcing node i to abandon $A^{[k]}(i,\ j)$ at step $k+1$.

Violations of Monotonicity

(left) Monotonicity

$$\forall a, b, c \in S : a \leq b \rightarrow c \otimes a \leq c \otimes b.$$

Define the dispute relation D_S to record violations of montonicity:

$$D_S \equiv \{(a,\ c \otimes b) \mid a, b, c \in S,\ a \leq b \wedge c \otimes b < c \otimes a\}$$

In addition, define a relation

$$T_S \equiv \{(a,\ b \otimes a) \mid a,\ b \in S,\ b \neq \alpha_{\otimes}\}.$$

Generalized dispute digraph

The generalized dispute digraph is then defined as the relation

$$\mathfrak{D}_S = (T_S \cup D_S)^{tc},$$

where *tc* denotes the transitive closure.

Increasing

Lemma

If S is increasing, then $\mathfrak{D}_S \subseteq <$.

Proof: If $(a,\ b \otimes a) \in T_S$, then if S is increasing we have $a < b \otimes a$. If $(a,\ c \otimes b) \in D_S$, then $a \leq b$, and if S is increasing then $b < c \otimes b$, so $a < c \otimes b$.

Two Lemmas ...

A $\mathfrak{D}_S$ sequence σ is

- any non-empty sequence of values over S
- such that if $\sigma = a_1, a_2, \ldots, a_k$, for $2 \leq k$, then for each $1 \leq i < k$ we have $(a_i,\ a_{i+1}) \in \mathfrak{D}_S$.

Lemma

For each k, i, and j, $H^{[k]}(i,\ j)$ is a $\mathfrak{D}_S$ sequence.

Lemma

Suppose that $A^{[k]}(i,\ j) \neq A^{[k+1]}(i, j)$, then $\mid H^{[k+1]}(i,\ j) \mid = k + 1$.

... and a Theorem

Theorem

If S is an increasing bisemigroup and only simple paths are allowed, then there must exist a k such that $A^{[k]} = A^{[k+1]}$. Thus $B = A^{[k]}$ is a solution to the equation $B = I \oplus (A \otimes B)$.

Proof : Suppose that k does not exist. Since only simple paths are allowed, the set of values $w(p)$ for all paths p is finite. Since histories must grow without bound there must at some point be an a such that $(a,\ a) \in \mathfrak{D}_S$, which contradicts Lemma 7.

Remark

SPP theory also used the concept of *dispute wheels* while Sobrinho's theory [Sob05] used the related concept of *non-free cycles*. These concepts are related to generalized dispute digraphs.

A few lemmas

Lemma

Suppose that $a_1 \, \mathfrak{R}_S \, a_2 \, \mathfrak{R}_S \, a_3$*. That is, there exists* b_1 *and* b_2 *such that*

$$a_1 \leq_R^{\otimes} b_1 \otimes a_1 <_L^{\oplus} a_2 \leq_R^{\otimes} b_2 \otimes a_2 <_L^{\oplus} a_3.$$

Then either $a_1 \leq_R^{\otimes} a_3$ *or* $(b_1 \otimes a_1, \; b_2 \otimes a_2) \in \mathfrak{D}_S$*.*

Corollary

If $(a, \; a) \in \mathfrak{R}_S$*, then* $(a, \; a) \in \mathfrak{D}_S$*.*

In particular, if S is an increasing bisemigroup, then we know that all cycles are free and that dispute wheels cannot exist.

Proof of Lemma 8

The proof is by induction on k. The base case is clear. Suppose every entry of $H^{[k]}$ is a $\mathfrak{D}_S$ sequence. The analysis of $H^{[k+1]}(i,\ j)$ is in three cases.

Case 1 : $A^{[k]}(i,\ j) = A^{[k+1]}(i,\ j)$. Then $H^{[k+1]}(i,\ j) = H^{[k]}(i,\ j)$ and the claim holds.

Proof of Lemma 8

bf Case 2: $A^{[k+1]}(i,\ j) < A^{[k]}(i,\ j)$, so we have

$$\begin{aligned} w(i, s^k_{(i,j)}) \otimes A^{[k]}(s^k_{(i,j)},\ j) &< w(i, s^{k-1}_{(i,j)}) \otimes A^{[k-1]}(s^{k-1}_{(i,j)},\ j) \\ &\leq w(i, s^k_{(i,j)}) \otimes A^{[k-1]}(s^k_{(i,j)},\ j). \end{aligned}$$

So $H^{[k+1]}(i,\ j) = H^{[k]}(s^k_{(i,j)},\ j),\ A^{[k+1]}(i,\ j)$, and there are three sub-cases to consider:

Case 2.1: $A^{[k-1]}(s^k_{(i,j)},\ j) = A^{[k]}(s^k_{(i,j)},\ j)$. This is not possible.

Case 2.2: $A^{[k]}(s^k_{(i,j)},\ j) < A^{[k-1]}(s^k_{(i,j)},\ j)$. Then $(A^{[k]}(s^k_{(i,j)},\ j),\ w(i, s^k_{(i,j)}) \otimes A^{[k]}(s^k_{(i,j)},\ j))$ is in T_S, and since $H^{[k]}(s^k_{(i,j)},\ j)$ ends in $A^{[k]}(s^k_{(i,j)},\ j)$, it follows that $H^{[k+1]}(i,\ j)$ is a $\mathfrak{D}_S$ sequence.

Case 2.3: $A^{[k-1]}(s^k_{(i,j)},\ j) < A^{[k]}(s^k_{(i,j)},\ j)$. Then $(A^{[k-1]}(s^k_{(i,j)},\ j),\ A^{[k+1]}(i,\ j))$ is in D_S, and since $H^{[k]}(s^k_{(i,j)},\ j)$ ends in the value $A^{[k-1]}(s^k_{(i,j)},\ j)$, it follows that $H^{[k+1]}(i,\ j)$ is a $\mathfrak{D}_S$ sequence.

Proof of Lemma 8

Case 3: $A^{[k]}(i,\ j) < A^{[k+1]}(i,\ j)$, so we have

$$\begin{array}{rcl} w(i,\ s^{k-1}_{(i,j)}) \otimes A^{[k-1]}(s^{k-1}_{(i,j)},\ j) & < & w(i,\ s^{k}_{(i,j)}) \otimes A^{[k]}(s^{k}_{(i,j)},\ j) \\ & \leq & w(i,\ s^{k-1}_{(i,j)}) \otimes A^{[k]}(s^{k-1}_{(i,j)},\ j). \end{array}$$

In this case $H^{[k+1]}(i,\ j) = H^{[k]}(s^{k-1}_{(i,j)},\ j),\ A^{[k]}(i,\ j)$. There are three sub-cases to consider:

Case 3.1: $A^{[k-1]}(s^{k-1}_{(i,j)},\ j) = A^{[k]}(s^{k-1}_{(i,j)},\ j)$. This is not possible.

Case 3.2: $A^{[k]}(s^{k-1}_{(i,j)},\ j) < A^{[k-1]}(s^{k-1}_{(i,j)},\ j)$. Then

$$(A^{[k]}(s^{k-1}_{(i,j)},\ j),\ w(i,\ s^{k-1}_{(i,j)}) \otimes A^{[k-1]}(s^{k-1}_{(i,j)},\ j)) \in D_S,$$

and since $H^{[k]}(s^{k-1}_{(i,j)},\ j)$ ends in $A^{[k]}(s^{k-1}_{(i,j)},\ j)$, $H^{[k+1]}(i,\ j)$ is a $\mathfrak{D}_S$ sequence.

Case 3.3: $A^{[k-1]}(s^{k-1}_{(i,j)},\ j) < A^{[k]}(s^{k-1}_{(i,j)},\ j)$. Then $H^{[k]}(s^{k-1}_{(i,j)},\ j)$ ends in the value $A^{[k-1]}(s^{k-1}_{(i,j)},\ j)$, and

$$(A^{[k-1]}(s^{k-1}_{(i,j)},\ j),\ w(i,\ s^{k-1}_{(i,j)}) \otimes A^{[k-1]}(s^{k-1}_{(i,j)},\ j)) \in T_S,$$

Bibliography I

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

[GG08] T. G. Griffin and A. Gurney.
Increasing bisemigroups and algebraic routing.
In *10th International Conference on Relational Methods in Computer Science (RelMiCS10)*, April 2008.

[GGR01] Timothy G. Griffin, Lixin Gao, and Jennifer Rexford.
Inherently safe backup routing with BGP.
In *Proc. IEEE INFOCOM*, April 2001.

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

Bibliography II

[GS05] Timothy G. Griffin and João Luís Sobrinho.
Metarouting.
In *Proc. ACM SIGCOMM*, August 2005.

[GSW02] Timothy G. Griffin, F. Bruce Shepherd, and Gordon Wilfong.
The stable paths problem and interdomain routing.
IEEE/ACM Transactions on Networking, 10(2):232–243, April 2002.

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

[GW00] Timothy Griffin and Gordon Wilfong.
A safe path vector protocol.
In *Proc. IEEE INFOCOM*, March 2000.

Bibliography III

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

[Sob05] Joao Luis Sobrinho.
An algebraic theory of dynamic network routing.
IEEE/ACM Transactions on Networking, 13(5):1160–1173, October 2005.