An Algebraic Approach to Internet Routing
Day 2

Timothy G. Griffin

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

School of Mathematical Sciences Colloquium
The University of Adelaide
23 June, 2011
Path Weight with functions on arcs?

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

### 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?
A homomorphism is a function that preserves structure. An endomorphism is a homomorphism mapping a structure to itself.

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

\((S, \oplus, F \subseteq S \to S, \bar{0}, i, \omega)\) is an algebra of monoid endomorphisms (AME) if

- \(\forall f \in F \forall b, c \in S : f(b \oplus c) = f(b) \oplus f(c)\)
- \(\forall f \in F : f(\bar{0}) = \bar{0}\)
- \(\exists i \in F \forall a \in S : i(a) = a\)
- \(\exists \omega \in F \forall a \in S : \omega(a) = \bar{0}\)
Solving (some) equations over a AMEs

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

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

Let

$$f^0 = i$$

$$f^{k+1} = f \circ f^k$$

and

$$f^{(k)}(b) = f^0(b) \oplus f^1(b) \oplus f^2(b) \oplus \cdots \oplus f^k(b)$$

$$f^{(*)}(b) = f^0(b) \oplus f^1(b) \oplus f^2(b) \oplus \cdots \oplus f^k(b) \oplus \cdots$$

**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

\[
\begin{align*}
f(f^{(*)}(b)) & \oplus b \\
& = f(f^{(q)}(b)) \oplus b \\
& = f(f^0(b) \oplus f^1(b) \oplus f^2(b) \oplus \cdots \oplus f^q(b)) \oplus b \\
& = f^1(b) \oplus f^1(b) \oplus f^2(b) \oplus \cdots \oplus f^{q+1}(b) \oplus b \\
& = f^0(b) \oplus f^1(b) \oplus f^1(b) \oplus f^2(b) \oplus \cdots \oplus f^{q+1}(b) \\
& = f(q+1)(b) \\
& = f(q)(b) \\
& = f^{(*)}(b)
\end{align*}
\]
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 $A, B \in \mathbb{M}_n(S)$ we have

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

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 $A$ with $A(i, j) \in F$. If $B \in \mathbb{M}_n(S)$ then define $A(B)$ so that

$$(A(B))(i, j) = \sum_{1 \leq q \leq n} A(i, q)(B(q, j)).$$
Here we go again...

### Path Weight

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

The *weight* of a path $p = i_1, i_2, i_3, \ldots, i_k$ 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

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

### We want to solve equations like these

$$X = A(X) \oplus B$$
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.
Convolution Product [GM08]

\[(S, \oplus, \otimes, 0, 1)\] a semiring

\[(T, \cdot, 1_T)\] a monoid

\[F \subseteq T \rightarrow S\] (suitably closed)

**Construct a semiring** \((F, \hat{\oplus}, \star)\)

\[(f \hat{\oplus} g)(a) = f(a) \oplus g(a)\]

\[(f \star g)(a) = \bigoplus_{a=b\cdot c} f(b) \otimes g(c)\]

Note: when \(S\) is a ring and \(T\) is a commutative semigroup, this construction results in a ring called a commutative semigroup ring (R. Gilmer, 1984). Thanks to Snigdhayan Mahanta for pointing this out.
Lexicographic product of AMEs

\[(S, \oplus_S, F) \times (T, \oplus_T, G) = (S \times T, \oplus_S \times \oplus_T, F \times G)\]

**Theorem ([Sai70, GG07, Gur08])**

\[D(S \times T) \iff D(S) \land D(T) \land (C(S) \lor K(T))\]

Where

<table>
<thead>
<tr>
<th>Property</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>D</td>
<td>(\forall a, b, f : f(a \oplus b) = f(a) \oplus f(b))</td>
</tr>
<tr>
<td>C</td>
<td>(\forall a, b, f : f(a) = f(b) \implies a = b)</td>
</tr>
<tr>
<td>K</td>
<td>(\forall a, b, f : f(a) = f(b))</td>
</tr>
</tbody>
</table>
Functional Union of AMEs

\[(S, \oplus, F) +_m (S, \oplus, G) = (S, \oplus, F + G)\]

**Fact**

\[D(S +_m T) \iff D(S) \land D(T)\]

**Where**

<table>
<thead>
<tr>
<th>Property Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>[\forall a, b, f : f(a \oplus b) = f(a) \oplus f(b)]</td>
</tr>
</tbody>
</table>
Left and Right

**right**

\[
\text{right}(S, \oplus, F) = (S, \oplus, \{i\})
\]

**left**

\[
\text{left}(S, \oplus, F) = (S, \oplus, K(S))
\]

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.

- \(D(\text{right}(S))\)
- \(D(\text{left}(S))\) (assuming \(\oplus\) is idempotent)
- \(C(\text{right}(S))\)
- \(K(\text{left}(S))\)
Scoped Product

\[ S \Theta T = (S \leftarrow \text{left}(T)) +_m (\text{right}(S) \leftarrow T) \]

**Theorem**

\[ D(S \Theta T) \iff D(S) \land D(T). \]

**Proof.**

\[
\begin{align*}
D(S \Theta T) \\
D((S \leftarrow \text{left}(T)) +_m (\text{right}(S) \leftarrow T)) \\
\iff D(S \leftarrow \text{left}(T)) \land D(\text{right}(S) \leftarrow T) \\
\iff D(S) \land D(\text{left}(T)) \land (C(S) \lor K(\text{left}(T))) \\
\hspace{1cm} \land D(\text{right}(S)) \land D(T) \land (C(\text{right}(S)) \lor K(T)) \\
\iff D(S) \land D(T)
\end{align*}
\]
How do we represent functions?

**Definition (transforms (indexed functions))**

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

\[
\triangleright \in L \rightarrow (S \rightarrow S).
\]

We normally write \(l \triangleright s\) rather than \(\triangleright(l)(s)\). We can think of \(l \in L\) as the index for a function \(f_l(s) = l \triangleright s\), so \((S, L, \triangleright)\) represents the set of function \(F = \{f_l \mid l \in L\}\).
Example 3: mildly abstract description of BGP’s ASPATHs

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

\[
\mathcal{E}(\Sigma^*) = \text{finite, elementary sequences over } \Sigma \text{ (no repeats)}
\]

\[
(m, n) \triangleright \infty = \infty
\]

\[
(m, n) \triangleright l = \begin{cases} 
    n \cdot l & \text{(if } m \notin n \cdot l) \\
    \infty & \text{(otherwise)}
\end{cases}
\]
Minimal Sets

Definition (Min-sets)
Suppose that \((S, \preceq)\) is a pre-ordered set. Let \(A \subseteq S\) be finite. Define

\[
\min_{\preceq}(A) \equiv \{a \in A \mid \forall b \in A : \neg (b < a)\}
\]

\[
\mathcal{P}(S, \preceq) \equiv \{A \subseteq S \mid A \text{ is finite and } \min_{\preceq}(A) = A\}
\]

Definition (Min-Set Semigroup)
Suppose that \((S, \preceq)\) is a pre-ordered set. Then

\[
\mathcal{P}_{\min}(S, \preceq) = (\mathcal{P}(S, \preceq), \oplus_{\min})
\]

is the semigroup where

\[
A \oplus_{\min} B \equiv \min_{\preceq}(A \cup B).
\]
Min-Set-Map construction

**Definition**

Suppose that $S = (S, \preceq, F)$ a routing algebra in the style of Sobrinho [Sob03, Sob05]. Then

$$\text{minsetmap}(S) \equiv (\mathcal{P}(S, \preceq), \oplus_{\text{min}}, F_{\text{min}})$$

where $F_{\text{min}} \preceq = \{g_f | f \in F\}$ and

$$g_f(A) \equiv \min_{\preceq}(\{f(a) | a \in A\}).$$
Let's turn to BGP MED’s — First, hot potato
The (4) represents a MED value.
The values (0) and (1) represent MED values sent by AS 4. The other values are IGP link weights.
Best route selection at nodes $A$ and $B$.

- $r_C$, $r_D$ and $r_E$ denote routes received from routers C, D, and E, respectively.
- $A$ receives route $r_E$ through route reflector $B$.
- $B$ receives routes $r_C$ and $r_D$ through route reflector $A$.

<table>
<thead>
<tr>
<th>$u$</th>
<th>$S$</th>
<th>BGP best of $S$ at $u$</th>
<th>due to</th>
</tr>
</thead>
<tbody>
<tr>
<td>$A$</td>
<td>{$r_C, r_D$}</td>
<td>$r_D$</td>
<td>IGP</td>
</tr>
<tr>
<td>$A$</td>
<td>{$r_D, r_E$}</td>
<td>$r_E$</td>
<td>MED</td>
</tr>
<tr>
<td>$A$</td>
<td>{$r_E, r_C$}</td>
<td>$r_C$</td>
<td>IGP MED</td>
</tr>
<tr>
<td>$A$</td>
<td>{$r_C, r_D, r_E$}</td>
<td>$r_C$</td>
<td>MED, IGP</td>
</tr>
<tr>
<td>$B$</td>
<td>{$r_D, r_E$}</td>
<td>$r_E$</td>
<td>MED</td>
</tr>
<tr>
<td>$B$</td>
<td>{$r_E, r_C$}</td>
<td>$r_C$</td>
<td>IGP</td>
</tr>
</tbody>
</table>
There is not stable routing!

Assume $A$ always has routes $r_C$ and $r_D$, so only two cases:

- $A$ knows the routes $\{r_C, r_D, r_E\}$ and so selects $r_C$. This implies that $B$ has chosen $r_E$, and this is a contradiction, since $B$ would have $\{r_E, r_C\}$ and select $r_C$.

- $A$ has only $\{r_C, r_D\}$ and selects $r_D$. Since $A$ does not learn a route from $B$, we know that $B$ must have selected $r_C$. This is a contradiction since $B$ would learn $r_D$ from $A$ and then pick $r_E$. 
What’s going on with MED?

Assume MEDs are represented by pairs of the form \((a, m)\), where \(a\) is an ASN and \(m\) is an integer metric.

The partial order on MEDs is defined as

\[(\alpha_1, m) \preceq_M (\alpha_2, n) \iff \alpha_1 = \alpha_2 \land m \preceq n.\]

We can think abstractly of BGP routes as elements of

\[(P, \preceq_P) \times (M, \preceq_M) \times (S, \preceq_S),\]

where \((P, \preceq_P)\) represents the prefix of attributes considered before MED, and \((S, \preceq_S)\) represents the suffix of attributes considered after MED.
What is going on?

Suppose that we have the lexicographic product,

\[(A, \lesssim_A) \times (B, \lesssim_B) \equiv (A \times B, \preceq),\]

and that \(W\) is a finite subset of \(A \times B\). We would like to explore efficient (and correct) methods for computing the min-set \(\min_{\preceq}(W)\).

Let \(\sim_A\) and \(\sim_B\) be the preorders on \(A\) and \(B\) for which all elements are related.

**Pipeline method**

We say the pipeline method is correct when

\[
\min_{\preceq_{A \times B}} (W) = \min_{\sim_A \times \sim_B} (\min_{\sim_{A \times B}} (W)).
\]
The pipeline method is correct if and only if no two elements of $B$ are strictly ordered, or no two elements of $A$ are incomparable.

Proof: For the interesting direction, suppose that $A$ does contain two elements $a_1$ and $a_2$ with $a_1 \not\leq a_2$, and $B$ does contain two elements $b_1$ and $b_2$ with $b_1 <_B b_2$. Then

$$\min_{\preceq_A \times \preceq_B} \{(a_1, b_1), (a_2, b_2)\} = \{(a_1, b_1), (a_2, b_2)\}$$

but

$$\min_{\omega_A \times \omega_B} \left( \min_{\preceq_A \times \preceq_B} \{(a_1, b_1), (a_2, b_2)\} \right)$$

$$= \min_{\omega_A \times \omega_B} \{(a_1, b_1), (a_2, b_2)\}$$

$$= \{(a_1, b_1)\}.$$
Can we generalize the min-set constructions?

Pathfinding through Congruences
Alexander J. T. Gurney, Timothy G. Griffin
12th International Conference on Relational and Algebraic Methods in Computer Science (RAMiCS 12)
June 2011
Semigroup congruence

An equivalence relation \(\sim\) on semigroup \((S, \oplus)\) is a congruence if

\[
a \sim b \implies (a \oplus c) \sim (b \oplus c) \land (c \oplus a) \sim (c \oplus b)
\]

\((S/\sim, \oplus_\sim)\) is a semigroup

\[
[a] \oplus_\sim [b] = [a \oplus b]
\]
If \((S, \oplus)\) is a semigroup and \(r\) is a function from \(S\) to \(S\), then \(r\) is a reduction if for all \(a\) and \(b\) in \(S\):

1. \(r(a) = r(r(a))\)
2. \(r(a \oplus b) = r(r(a) \oplus b) = r(a \oplus r(b))\)

For monoids the first axiom is not needed since \(r(a \oplus 0) = r(r(a) \oplus 0)\) from the second axiom. Similarly, the second axiom can be simplified to a single equality in the case of a commutative semigroup.
A function on a semiring is called a reduction if it is a reduction with respect to both of the semiring operations. Similarly, a reduction on a semigroup transform \((S, \oplus, F)\) is a function \(r\) from \(S\) to itself, such that \(r\) is a reduction on \((S, \oplus)\) and

\[
r(f(a)) = r(f(r(a)))
\]

for all \(a\) in \(S\) and \(f\) in \(F\).
Lemma

For any reduction $r$ on $(S, \oplus)$, define a relation $\sim_r$ on $S$ by

$$a \sim_r b \iff r(a) = r(b).$$

This $\sim_r$ is a congruence.

Proof.

This is obviously an equivalence relation. To prove that it is a congruence, suppose that $a \sim_r b$, so that $r(a) = r(b)$. Then

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

and likewise for $r(c \oplus a) = r(c \oplus b)$. Hence $\sim_r$ is indeed a congruence.
Lemma

Let \((S, \oplus)\) be a semigroup, \(\sim\) a congruence, and \(\rho^\natural\) the natural map. If \(\theta : S/\sim \longrightarrow S\) is such that \(\rho^\natural \circ \theta = \text{id}\), then \(\theta \circ \rho^\natural\) is a reduction; and \(\sim\) is equal to \(\sim_{\theta \circ \rho^\natural}\).

- We can represent any reduction \(r\) as a pair \((\sim, \theta)\)
Specifically, for a given $(S, \oplus, F)$ and reduction $r : S \rightarrow S$ we can define the quotient $S/r$ as follows.

1. The carrier consists of $r$-equivalence classes of elements of $S$; we can choose the canonical representative of each class to be a fixed point of $r$.

2. The semigroup operation is given by $\rho^{\parallel}(a) \oplus / r \rho^{\parallel}(b) = \rho^{\parallel}(a \oplus b)$.

3. The functions in $F$ are lifted: $f(\rho^{\parallel}(a)) = \rho^{\parallel}(f(a))$.

This can be verified to be a semigroup transform. The minset construction is clearly a special case, where $r$ is min, $S$ is a set of sets, and $\oplus$ is set union.
Modeling Path Errors?

- The same node is visited more than once.
- The path is intended to be filtered out.
- The path violates known economic relationships between networks.
- The path is too long (exceeding a maximum size for routing announcements).
- The origin is unexpected (given neighbours are only anticipated to advertise certain addresses).
- Route data is otherwise malformed.
Only Simple Paths

\[ \overrightarrow{S \times P} \]

- \((S, \leq, F)\) be an order transform for encoding the path weights.
- \(P\) be the algebra of paths \((N^*, \leq, C)\), where \(p \leq q\) if and only if \(|p| \leq |q|\), and \(C\) consists of functions \(c_n\) for all \(n\) in \(N\), which concatenate the node \(n\) onto the given path.

Bad paths \(B \subseteq S \times N^*\)

\[ B \equiv \{(s, p) \in S \times N^* \mid p \text{ is not simple}\}. \]

A reduction over subsets of \(S \times N^*\)

\[ r(A) \overset{\text{def}}{=} \min(A \setminus E); \quad (2) \]

where \(\min\) uses the lexicographic order on \(S \times N^*.\)
The construction...

A semigroup transform can be constructed where

- the elements are those subsets of \( S \times N^* \) which are fixed points of \( r \);
- the operation \( \oplus \) is given by \( A \oplus B \equiv r(A \cup B) \); and
- the functions are pairs \((f, c_n)\) for \( f \) in \( F \), where

\[
(f, c_n)(A) \equiv r(\{(f(s), c_n(p)) \mid (s, p) \in A\}).
\]

It can be seen that this algebra implements the simple paths criterion in the case of multipath routing: if during the course of computation a non-simple path is computed, it and its associated \( S \)-value will be removed from the candidate set.
Lexicographic products in metarouting.

[GM08] M. Gondran and M. Minoux.

Designing routing algebras with meta-languages.


Bibliography III

[Sob05] Joao Luis Sobrinho.
An algebraic theory of dynamic network routing.

Endless BGP convergence problem in Cisco IOS software releases.
*Field Note*, October 10 2001,

Semirings and path spaces.