An Algebraic Approach to Internet Routing
Part I

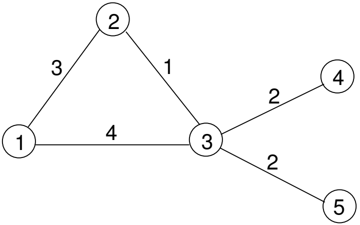
Timothy G. Griffin

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

Shortest paths example

A weighted graph :



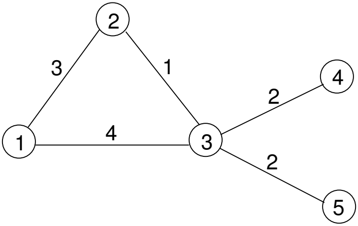
The Adjacency matrix :

$$\mathbf{A} = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{array} \begin{array}{c} \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array} \\ \left(\begin{array}{ccccc} \infty & 3 & 4 & \infty & \infty \\ 3 & \infty & 1 & \infty & \infty \\ 4 & 1 & \infty & 2 & 2 \\ \infty & \infty & 2 & \infty & \infty \\ \infty & \infty & 2 & \infty & \infty \end{array} \right) \end{array}$$

- The algebraic structure is $\mathrm{sp} = (\mathbb{N} \cup \{\infty\},\ \min,\ +)$.
- Path weights are computed from arc weights using $+$.
- Best path weights are selected using min.

Solution to the example

The example graph:



The solution:

$$\mathbf{X} = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{array} \begin{array}{c} \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array} \\ \begin{pmatrix} 0 & 3 & 4 & 6 & 6 \\ 3 & 0 & 1 & 3 & 3 \\ 4 & 1 & 0 & 2 & 2 \\ 6 & 3 & 2 & 0 & 4 \\ 6 & 3 & 2 & 4 & 0 \end{pmatrix} \end{array}$$

How do we find solutions?

- We will mostly look at matrix methods.
- Other familiar methods (Dijktra's algorithm, Bellman-Ford) can be used in special cases to compute a selected row of the solution.

Equational specification of problem being solved

1. Extend $(\min, +)$ to $(\boxplus, \boxtimes)$ on 5×5 matrices in the natural way :

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

$$(\mathbf{A} \boxtimes \mathbf{B})(i, j) = \min_{1 \le q \le 5} \mathbf{A}(i, q) + \mathbf{B}(q, j)$$

2. Solve this matrix equation for **X**:

$$\mathbf{X} = (\mathbf{A} \boxtimes \mathbf{X}) \boxplus \mathbf{I}$$

where **I** is the identity matrix:

$$\mathbf{I} = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{array} \begin{array}{c} \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array} \\ \left(\begin{array}{ccccc} 0 & \infty & \infty & \infty & \infty \\ \infty & 0 & \infty & \infty & \infty \\ \infty & \infty & 0 & \infty & \infty \\ \infty & \infty & \infty & 0 & \infty \\ \infty & \infty & \infty & \infty & 0 \end{array}\right) \end{array}$$

Does it make sense?

Suppose $\mathbf{X}$ satisfies

$$\mathbf{X} = (\mathbf{A} \boxtimes \mathbf{X}) \boxplus \mathbf{I}$$

then

$$\mathbf{X}(i,\ i) = 0$$

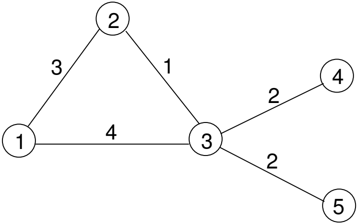
and for $i \neq j$,

$$\mathbf{X}(i,\ j) = \min_{1 \leq q \leq 5} \mathbf{A}(i,\ q)\ +\ \mathbf{X}(q,\ j)$$

Example: Widest paths (max, min)

- The algebraic structure is $\mathrm{bw} = (\mathbb{N} \cup \{\infty\}, \ \max, \ \min)$.
- Path weights are computed from arc weights using min.
- Best path weights are selected using max.

A weighted graph :



The solution: FIX

$$\mathbf{X} = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{array} \begin{array}{c} \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array} \\ \begin{pmatrix} \infty & 3 & 4 & 2 & 2 \\ 3 & \infty & 3 & 3 & 3 \\ 4 & 3 & \infty & 2 & 2 \\ 2 & 2 & 2 & \infty & 2 \\ 2 & 2 & 2 & 2 & \infty \end{pmatrix} \end{array}$$

But $(\max, +)$ does not work. Why?

(Classical) Algebraic Routing

- Generalize to semi-rings

$$(\mathbb{N} \cup \{\infty\},\ \min,\ +) \longrightarrow (S,\ \oplus,\ \otimes)$$

- Use S to assign weights to arcs in a graph with n nodes.
- Extend S to $n \times n$ matrices over S.
- Study properties of S (or of the weighted graph) that imply that we can find solutions to

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

- For example, distribution plays a key role in the classical theory.

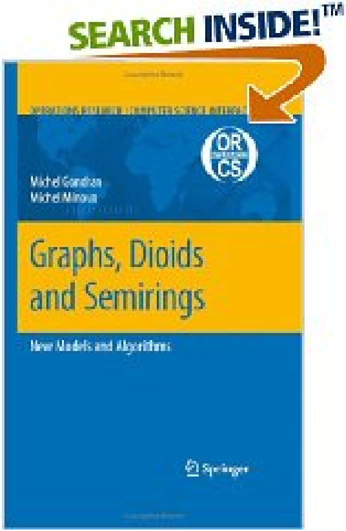
$$\begin{array}{lrcl} (\text{L.DIST}) & a \otimes (b \oplus c) & = & (a \otimes b) \oplus (a \otimes c) \\ (\text{R.DIST}) & (a \oplus b) \otimes c & = & (a \otimes c) \oplus (b \otimes c) \end{array}$$

Semiring Examples

See [Car79, GM84, GM08]

name	S	$\oplus$,	$\otimes$	identity for $\oplus$	identity for $\otimes$	possible use in routing
sp	$\mathbb{N} \cup \{\infty\}$	min	$+$	∞	0	minimum-weight rou
bw	$\mathbb{N} \cup \{\infty\}$	max	min	0	∞	greatest-capacity rou
rel	$[0,\ 1]$	max	$\times$	0	1	most-reliable routing
use	$\{0,\ 1\}$	max	min	0	1	usable-path routing
	$\mathcal{P}(W)$	$\cup$	$\cap$	$\{\}$	W	shared link attributes
	$\mathcal{P}(W)$	$\cap$	$\cup$	W	$\{\}$	shared path attribute

La Santa Biblia



Building new semi-rings from old ...

name	S	$\oplus$,	$\otimes$	$\oplus$ id	$\otimes$ id	desc
sp	$\mathbb{N} \cup \{\infty\}$	min	$+$	∞	0	mini
bw	$\mathbb{N} \cup \{\infty\}$	max	min	0	∞	grea
$\mathrm{sp} \vec{\times} \mathrm{bw}$	$(\mathbb{N} \cup \{\infty\}) \times (\mathbb{N} \cup \{\infty\})$	$\oplus$	$\otimes$	$(\infty, 0)$	$(0, \infty)$	wide

- Where $\oplus$ is a lexicographic addition,

$$(d_1, b_1) \oplus (d_2, b_2) = \begin{cases} (d_1, b_1) & (\text{if } d_1 = \min(d_1, d_2)) \\ (d_2, b_2) & (\text{if } d_2 = \min(d_1, d_2)) \\ (d_1, b_1 \max b_2) & (\text{if } d_1 = d_2) \end{cases}$$

- and $\otimes$ is a direct product

$$(d_1, b_1) \otimes (d_2, b_2) = (d_1 + d_2, b_1 \min b_2)$$

This makes a nice semi-ring!

... but you must be careful!

What if we want shortest, widest-paths (see [Sob02])? Then combine this (lexicographically) in the other order:

- Let

$$(b_1, d_1) \oplus (b_2, d_2) = \begin{cases} (b_1, d_1) & (\text{if } b_1 = \max(b_1, b_2)) \\ (b_2, d_2) & (\text{if } b_2 = \max(b_1, b_2)) \\ (b_1, d_1 \min d_2) & (\text{if } b_1 = b_2) \end{cases}$$

- let $(b_1, d_1) \otimes (b_2, d_2) = (b_1 \min b_2, d_1 + d_2)$

We will see that this does not produce a semi-ring (distribution rules do not hold)!!

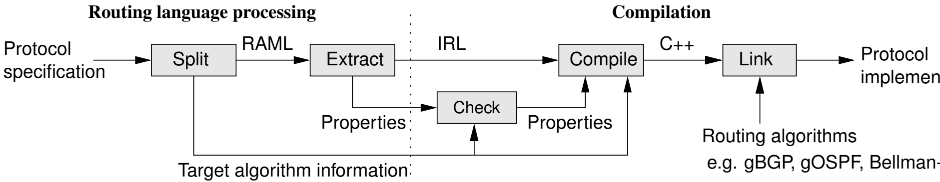
- Why? (A big question, which will be answered!)
- Might it still be useful for routing? (We will see that the answer is MAYBE!)

Defining and implementing a new routing protocol is difficult!

- The space is large
- The proofs are difficult
- Correctness conditions hard to get right

Could the design process be partially automated?

(Prototype) Metarouting System



- Specification : Algorithms are currently picked from a menu, while the routing language is specified in terms of the Routing Algebra Meta-Language (RAML).
- Errors: Each algorithm is associated with properties it requires of a routing language (Example : Dijkstra requires a total order on metrics). Properties are automatically derived from RAML expressions. An error is reported when there is a mis-match.

Outline

- Part I (today)
  - Review of classical theory
- Part II (tomorrow)
  - Present a constructive approach
- Part III (Wednesday)
  - Live dangerously — drop distribution!
  - Model BGP-like protocols
  - Metarouting

Goals these lectures

Goals

- Understand the equation

$$\text{routing protocol} = \text{routing algebra} + \text{routing algorithm}$$

- Understand how to construct new and interesting routing algebras
- Ignore implementation details
- Ignore the pressures of hot-topicism
- Go beyond Gondran and Minoux

Caveats

- This is work in progress.
- We will not explore the important topic of efficient implementation of distributive algorithms.
- We will not explore the relationship between routing and forwarding, or routing and signaling (say PNNI).

Let's start with a bit of notation!

Symbol	Interpretation
$\mathbb{N}$	Natural numbers (starting with zero)
$\mathbb{N}^{\infty}$	Natural numbers, plus infinity
$\mathbb{Z}$	Integers
$\mathbb{R}$	Real numbers
$\mathbb{R}_{\geq 0}$	Positive real numbers (including zero)
$\mathbb{R}_{\geq 0}^{\infty}$	Positive real numbers, plus infinity

Semigroups

Definition (Semigroup)

A semigroup $(S, \oplus)$ is a non-empty set S with a binary operation such that

$$\text{ASSOCIATIVE} \quad : \quad a \oplus (b \oplus c) = (a \oplus b) \oplus c$$

S	$\oplus$	where
$\mathbb{N} \cup \{\infty\}$	min	
$\mathbb{N} \cup \{\infty\}$	max	
$\mathbb{N} \cup \{\infty\}$	$+$	
$\mathcal{P}(W)$	$\cup$	
$\mathcal{P}(W)$	$\cap$	
S^*	$\circ$	$(abc \circ de = abcde)$
S	left	$(a \text{ left } b = a)$
S	right	$(a \text{ right } b = b)$

Special Elements

Definition

- $\alpha \in S$ is an identity if for all $a \in S$

$$a = \alpha \oplus a = a \oplus \alpha$$

- A semigroup is a monoid if it has an identity.
- ω is an annihilator if for all $a \in S$

$$\omega = \omega \oplus a = a \oplus \omega$$

S	$\oplus$	α	ω
$\mathbb{N} \cup \{\infty\}$	min	∞	0
$\mathbb{N} \cup \{\infty\}$	max	0	∞
$\mathbb{N} \cup \{\infty\}$	$+$	0	∞
$\mathcal{P}(W)$	$\cup$	$\{\}$	W
$\mathcal{P}(W)$	$\cap$	W	$\{\}$
S^*	$\circ$	ϵ	
S	left		
S	right		

Important Properties

Definition (Some Important Semigroup Properties)

$$\begin{array}{rcrcl} \text{COMMUTATIVE} & : & a \oplus b & = & b \oplus a \\ \text{SELECTIVE} & : & a \oplus b & \in & \{a,\ b\} \\ \text{IDEMPOTENT} & : & a \oplus a & = & a \end{array}$$

S	$\oplus$	COMMUTATIVE	SELECTIVE	IDEMPOTENT
$\mathbb{N} \cup \{\infty\}$	min	$\star$	$\star$	$\star$
$\mathbb{N} \cup \{\infty\}$	max	$\star$	$\star$	$\star$
$\mathbb{N} \cup \{\infty\}$	$+$	$\star$		
$\mathcal{P}(W)$	$\cup$	$\star$		$\star$
$\mathcal{P}(W)$	$\cap$	$\star$		$\star$
S^*	$\circ$			
S	left		$\star$	$\star$
S	right		$\star$	$\star$

Order Relations

We are interested in order relations $\lesssim \subseteq S \times S$

Definition (Important Order Properties)

$$
\begin{array}{rcl}
\text{REFLEXIVE} & : & a \lesssim a \\
\text{TRANSITIVE} & : & a \lesssim b \wedge b \lesssim c \rightarrow a \lesssim c \\
\text{ANTISYMMETRIC} & : & a \lesssim b \wedge b \lesssim a \rightarrow a = b \\
\text{TOTAL} & : & a \lesssim b \vee b \lesssim a
\end{array}
$$

	pre-order	partial order	preference order	total order
REFLEXIVE	$\star$	$\star$	$\star$	$\star$
TRANSITIVE	$\star$	$\star$	$\star$	$\star$
ANTISYMMETRIC		$\star$		$\star$
TOTAL			$\star$	$\star$

Canonical Pre-order of a Commutative Semigroup

Suppose $\oplus$ is commutative.

Definition (Canonical pre-orders)

$$
\begin{array}{rcl}
a \trianglelefteq^{R}_{\oplus} b & \equiv & \exists c \in S : b = a \oplus c \\
a \trianglelefteq^{L}_{\oplus} b & \equiv & \exists c \in S : a = b \oplus c
\end{array}
$$

Lemma (Sanity check)

Associativity of $\oplus$ implies that these relations are transitive.

Proof.

Note that $a \trianglelefteq^{R}_{\oplus} b$ means $\exists c_1 \in S : b = a \oplus c_1$, and $b \trianglelefteq^{R}_{\oplus} c$ means $\exists c_2 \in S : c = b \oplus c_2$. Letting $c_3 =$ we have $c = b \oplus c_2 = (a \oplus c_1) \oplus c_2 = a \oplus (c_1 \oplus c_2) = a \oplus c_3$. That is, $\exists c_3 / inS : c = a \oplus c_3$, so $a \trianglelefteq^{R}_{\oplus} c$. The proof for $\trianglelefteq^{L}_{\oplus}$ is similar. □

Canonically Ordered Semigroup

Definition (Canonically Ordered Semigroup)

A commutative semigroup $(S, \oplus)$ is canonically ordered when $a \trianglelefteq^R_\oplus c$ and $a \trianglelefteq^L_\oplus c$ are partial orders.

Definition (Groups)

A monoid is a group if for every $a \in S$ there exists a $a^{-1} \in S$ such that $a \oplus a^{-1} = a^{-1} \oplus a = \alpha$.

Canonically Ordered Semigroups vs. Groups

Lemma (THE BIG DIVIDE)

Only a trivial group is canonically ordered.

Proof.

If $a, \ b \in S$, then $a = \alpha_{\oplus} \oplus a = (b \oplus b^{-1}) \oplus a = b \oplus (b^{-1} \oplus a) = b \oplus c$, for $c = b^{-1} \oplus a$, so $a \trianglelefteq^{L}_{\oplus} b$. In a similar way, $b \trianglelefteq^{R}_{\oplus} a$. Therefore $a = b$. □

Natural Orders

Definition (Natural orders)

Let $(S, \oplus)$ be a simigroup.

$$
\begin{aligned}
a \lesssim^{L}_{\oplus} b &\equiv a = a \oplus b \\
a \lesssim^{R}_{\oplus} b &\equiv b = a \oplus b
\end{aligned}
$$

Lemma

If $\oplus$ is commutative and idempotent, then $a \trianglelefteq^{D}_{\oplus} b \iff a \lesssim^{D}_{\oplus} b$, for $D \in \{R, L\}$.

Proof.

$$
\begin{aligned}
a \trianglelefteq^{R}_{\oplus} b &\iff b = a \oplus c = (a \oplus a) \oplus c = a \oplus (a \oplus c) \\
&= a \oplus b \iff a \lesssim^{R}_{\oplus} b \\
a \trianglelefteq^{L}_{\oplus} b &\iff a = b \oplus c = (b \oplus b) \oplus c = b \oplus (b \oplus c) \\
&= b \oplus a = a \oplus b \iff a \lesssim^{L}_{\oplus} b
\end{aligned}
$$

□

Special elements and natural orders

Lemma (Natural Bounds)

- *If α exists, then for all a, $a \preceq^{L}_{\oplus} \alpha$ and $\alpha \preceq^{R}_{\oplus}$*
- *If ω exists, then for all a, $\omega \preceq^{L}_{\oplus} a$ and $a \preceq^{R}_{\oplus} \omega$*
- *If α and ω exist, then S is bounded.*

$$\begin{array}{ccccc} \omega & \preceq^{L}_{\oplus} & a & \preceq^{L}_{\oplus} & \alpha \\ \alpha & \preceq^{R}_{\oplus} & a & \preceq^{R}_{\oplus} & \omega \end{array}$$

Examples of special elements

S	$\oplus$	α	ω	$\preceq_{\oplus}^{L}$	$\preceq_{\oplus}^{L}$
$\mathbb{N} \cup \{\infty\}$	min	∞	0	$\leq$	$\geq$
$\mathbb{N} \cup \{\infty\}$	max	0	∞	$\geq$	$\leq$
$\mathcal{P}(W)$	$\cup$	$\{\}$	W	$\supseteq$	$\subseteq$
$\mathcal{P}(W)$	$\cap$	W	$\{\}$	$\subseteq$	$\supseteq$

Property Management

Lemma

Let $D \in \{R, L\}$.

1. $\text{IDEMPOTENT}((S, \oplus)) \iff \text{REFLEXIVE}((S, \preceq^D_\oplus))$
2. $\text{COMMUTATIVE}((S, \oplus)) \implies \text{ANTISYMMETRIC}((S, \preceq^D_\oplus))$
3. $\text{SELECTIVE}((S, \oplus)) \iff \text{TOTAL}((S, \preceq^D_\oplus))$

Proof.

1. $a \preceq^D_\oplus a \iff a = a \oplus a,$
2. $a \preceq^L_\oplus b \wedge a \preceq^L_\oplus b \iff a = a \oplus b \wedge b = b \oplus a \implies a = b$
3. $a = a \oplus b \vee b = a \oplus b \iff a \preceq^L_\oplus b \vee b \preceq^R_\oplus a$

□

Bi-semigroups and Pre-semirings

Definition

The structure $(S, \oplus, \otimes)$ is a bi-semigroup when

$$\begin{array}{lrcl} \text{ADD.ASSOC} : & (a \oplus b) \oplus c & = & a \oplus (b \oplus c) \\ \text{MULT.ASSOC} : & (a \otimes b) \otimes c & = & a \otimes (b \otimes c), \end{array}$$

that is, when both the additive component $(S, \oplus)$ and the multiplicitive component $(S, \otimes)$ are semigroups.

Definition

A bi-semigroup $(S, \oplus, \otimes)$ is a pre-semiring when

$$\begin{array}{lrcl} \text{ADD.COMMUTATIVE} : & a \oplus b & = & b \oplus a \\ \text{LEFT.DISTRIBUTIVE} : & a \otimes (b \oplus c) & = & (a \otimes b) \oplus (a \otimes c) \\ \text{RIGHT.DISTIBUTIVE} : & (a \oplus b) \otimes c & = & (a \otimes c) \oplus (b \otimes c) \end{array}$$

Semirings

Definition

A pre-semiring $(S, \oplus, \otimes)$ is a semiring when there exists $\alpha_{\oplus} \in S$ and $\alpha_{\otimes} \in S$ such that

$$\begin{array}{rrcl}
(\text{ADD.L.ALPHA}) & \alpha_{\oplus} \oplus a & = & a \\
(\text{ADD.R.ALPHA}) & a \oplus \alpha_{\oplus} & = & a \\
(\text{MULT.L.ALPHA}) & \alpha_{\otimes} \otimes a & = & a \\
(\text{MULT.R.ALPHA}) & a \otimes \alpha_{\otimes} & = & a \\
(\text{MULT.L.OMEGA}) & \alpha_{\oplus} \otimes a & = & \alpha_{\oplus} \\
(\text{MULT.R.OMEGA}) & a \otimes \alpha_{\oplus} & = & \alpha_{\oplus}
\end{array}$$

That is, when both $(S, \oplus, \alpha_{\oplus})$ and $(S, \otimes, \alpha_{\otimes})$ are monoids, and $\omega_{\otimes} = \alpha_{\oplus}$.

Semiring Examples

See [Car79, GM84, GM08]

name	S	$\oplus$,	$\otimes$	identity for $\oplus$	identity for $\otimes$	possible use in routing
sp	$\mathbb{N} \cup \{\infty\}$	min	$+$	∞	0	minimum-weight rou
bw	$\mathbb{N} \cup \{\infty\}$	max	min	0	∞	greatest-capacity rou
rel	$[0, 1]$	max	$\times$	0	1	most-reliable routing
use	$\{0, 1\}$	max	min	0	1	usable-path routing
	$\mathcal{P}(W)$	$\cup$	$\cap$	$\{\}$	W	shared link attributes
	$\mathcal{P}(W)$	$\cap$	$\cup$	W	$\{\}$	shared path attribute

Solving (some) equations over a semiring

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

$$x = (a \otimes x) \oplus b$$

Let

$$\begin{array}{rcl} a^0 & = & \alpha_{\oplus} \\ a^{k+1} & = & a \oplus a^k \end{array}$$

and

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

Definition (q stability)

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

If $\alpha_{\otimes} = \omega_{\oplus}$, then every a is 0-stable!

Key result

Lemma ([GM84, Car79])

If a is q-stable, then $x = a^{(*)} \otimes b$ *solves the semiring equation*

$$x = (a \otimes x) \oplus b.$$

Proof: Substitute $a^{(*)} \otimes b$ for x to obtain

$$\begin{array}{ll}
 & (a \otimes (a^{(*)} \otimes b)) \oplus b \\
= & ((a \otimes a^{(*)}) \otimes b) \oplus b \\
= & ((a \otimes a^{(*)}) \oplus \alpha_{\otimes}) \otimes b \quad \text{(RIGHT.DISTIBU} \\
= & ((a \otimes (a^0 \oplus a^1 \oplus a^2 \oplus \cdots \oplus a^q)) \oplus \alpha_{\otimes}) \otimes b \\
= & (a^1 \oplus a^2 \oplus \cdots \oplus a^{q+1}) \oplus \alpha_{\otimes}) \otimes b \quad \text{(LEFT.DISTIBU} \\
= & a^{(q+1)} \otimes b \\
= & a^{(*)} \otimes b
\end{array}$$

Semiring of Matrices

Given a semiring $S = (S, \oplus \otimes)$, define the semiring of $n \times n$-matrices over S,

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

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

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

and

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

- $\alpha_{\boxplus}(i, j) = \omega_{\boxtimes}(i, j) = \alpha_{\oplus}$.
- $\alpha_{\boxtimes}(i, i) = \alpha_{\otimes}$, $\alpha_{\boxtimes}(i, j) = \alpha_{\oplus}$. The matrix $\alpha_{\boxtimes}$ is often denoted as $\mathbf{I}$.

Check (left) distribution

$$\mathbf{A} \boxtimes (\mathbf{B} \boxplus \mathbf{C}) = (\mathbf{A} \boxtimes \mathbf{B}) \boxplus (\mathbf{A} \boxtimes \mathbf{C})$$

$$\begin{aligned}
& (\mathbf{A} \boxtimes (\mathbf{B} \boxplus \mathbf{C}))(i,\ j) \\
= & \sum_{1 \le q \le n}^{\oplus} \mathbf{A}(i,\ q) \otimes (\mathbf{B} \boxplus \mathbf{C})(q,\ j) \\
= & \sum_{1 \le q \le n}^{\oplus} \mathbf{A}(i,\ q) \otimes (\mathbf{B}(q,\ j) \oplus \mathbf{C}(q,\ j)) \\
= & \sum_{1 \le q \le n}^{\oplus} (\mathbf{A}(i,\ q) \otimes \mathbf{B}(q,\ j)) \oplus (\mathbf{A}(i,\ q) \otimes \mathbf{C}(q,\ j)) \\
= & (\sum_{1 \le q \le n}^{\oplus} \mathbf{A}(i,\ q) \otimes \mathbf{B}(q,\ j)) \oplus (\sum_{1 \le q \le n}^{\oplus} \mathbf{A}(i,\ q) \otimes \mathbf{C}(q,\ j)) \\
= & ((\mathbf{A} \boxtimes \mathbf{B}) \boxplus (\mathbf{A} \boxtimes \mathbf{C}))(i,\ j)
\end{aligned}$$

Adjacency Matrix

$$\alpha_{\boxtimes}(i,\ j) = \mathbf{I}(i,\ j) = \begin{cases} \alpha_{\otimes} & \text{if } i = j, \\ \alpha_{\oplus} & \text{otherwise} \end{cases}$$

adjacency matrix **A** :

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

Note: if **A** is q-stable, then $\mathbf{X} = \mathbf{A}^{(*)} \boxtimes \mathbf{B}$ solves the matrix equation

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

Path Weight

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

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

The empty path ϵ is usually give the weight $\alpha_{\otimes}$.

Ur-algorithms

We now consider two methods of finding solutions to the matrix equation. Denote by $\mathbf{A}^k$ the kth power of $\mathbf{A}$ and by $\mathbf{A}^{(k)}$ the sum

$$\mathbf{A}^{(k)} = \mathbf{I} \boxplus \mathbf{A} \boxplus \cdots \boxplus \mathbf{A}^k.$$

Matrix Iteration

$$\begin{aligned} \mathbf{A}^{[0]}(\mathbf{B}) &= \mathbf{B} \\ \mathbf{A}^{[k+1]}(\mathbf{B}) &= (\mathbf{A} \boxtimes \mathbf{A}^{[k]}(\mathbf{B})) \boxplus \mathbf{B} \end{aligned}$$

When distribution holds we have $A^{(k)} = A^{[k]}$.

Optimality

- Let $P(i, j)$ be the set of paths from i to j.
- Let $P^k(i, j)$ be the set of paths from i to j with exactly k arcs.
- Let $P^{(k)}(i, j)$ be the set of paths from i to j with at most k arcs.

Theorem

$$\begin{array}{llcl} (1) & \mathbf{A}^k(i,j) & = & \sum\limits^{\oplus}_{p \in P^k(i,j)} w(p) \\ (2) & \mathbf{A}^{(k+1)}(i,j) & = & \sum\limits^{\oplus}_{p \in P^k(i,j)} w(p) \\ (3) & \mathbf{A}^{(*)}(i,j) & = & \sum\limits^{\oplus}_{p \in P(i,j)} w(p) \end{array}$$

Proof of (1)

By induction on k. Base Case: $k = 0$. $P^k(i, i) = \{\epsilon\}$, so $\mathbf{A}^0(i, i) = \mathbf{I}(i, i) = \alpha_{\otimes} = w(\epsilon)$. And $i \neq j$ implies $P^k(i, j) = \{\}$. By convention $\sum^{\oplus}_{p \in \{\}} w(p) = \alpha_{\oplus} = \mathbf{I}(i, j)$.

Proof of (1)

Induction step.

$$
\begin{aligned}
\mathbf{A}^{k+1}(i,j) &= (\mathbf{A} \boxtimes \mathbf{A}^k)(i,\ j) \\
&= \sum_{1 \le q \le n}^{\oplus} \mathbf{A}(i,\ q) \otimes \mathbf{A}^k(q,\ j) \\
&= \sum_{1 \le q \le n}^{\oplus} \mathbf{A}(i,\ q) \otimes \Big(\sum_{p \in P^k(q,j)}^{\oplus} w(p) \Big) \\
&= \sum_{1 \le q \le n}^{\oplus} \sum_{p \in P^k(q,j)}^{\oplus} \mathbf{A}(i,\ q) \otimes w(p) \\
&= \sum_{(i,\ q) \in E}^{\oplus} \sum_{p \in P^k(q,j)}^{\oplus} w(i,\ q) \otimes w(p) \\
&= \sum_{p \in P^{k+1}(i,j)}^{\oplus} w(p)
\end{aligned}
$$

Matrix Stability?

- $n \times n$-matrix semirings are not 0-stable (well, unless perhaps $n = 1$).
- Stability depends on stability of underlying semiring S.
- If S is bounded, then $n \times n$-matrix semiring is $n - 1$-stable!

Direct Product of Semigroups

Let $(S, \oplus_S)$ and $(T, \oplus_T)$ be semigroups.

Definition (Direct product semigroup)

The direct product is denoted $(S, \oplus_S) \times (T, \oplus_T) = (S \times T, \oplus)$, where $\oplus = \oplus_S \times \oplus_T$ is defined as

$$(s_1, t_1) \oplus (s_2, t_2) = (s_1 \oplus_S s_2,\ t_1 \oplus_T t_2).$$

Lexicographic Product of Semigroups

Definition (Lexicographic product semigroup (from [Gur08]))

Suppose S is commutative idempotent semigroup and T be a monoid. The lexicographic product is denoted $(S, \oplus_S) \vec{\times} (T, \oplus_T) = (S \times T, \oplus)$, where $\oplus = \oplus_S \vec{\times} \oplus_T$ is defined as

$$(s_1, t_1) \oplus (s_2, t_2) = \begin{cases} (s_1 \oplus_S s_2, t_1 \oplus_T t_2) & s_1 = s_1 \oplus_S s_2 = s_2 \\ (s_1 \oplus_S s_2, t_1) & s_1 = s_1 \oplus_S s_2 \neq s_2 \\ (s_1 \oplus_S s_2, t_2) & s_1 \neq s_1 \oplus_S s_2 = s_2 \\ (s_1 \oplus_S s_2, \alpha_T) & \text{otherwise.} \end{cases}$$

Exercise: prove that this is associative!

Lexicographic Semiring

$$(S,\ \oplus_S,\ \otimes_S)\ \vec{\times}\ (T,\ \oplus_T,\ \otimes_T) = (S \times T,\ \oplus_S\ \vec{\times}\ \oplus_T,\ \otimes_S \times \otimes_T)$$

Theorem ([Sai70, GG07, Gur08])

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

Where

Property	Definition
M	$\forall a, b, c : c \otimes (a \oplus b) = (c \otimes a) \oplus (c \otimes b)$
C	$\forall a, b, c : c \otimes a = c \otimes b \implies a = b$
K	$\forall a, b, c : c \otimes a = c \otimes b$

Return to examples

name	M	C	K
sp	Yes	Yes	No
bw	Yes	No	No

So we have

$$\mathrm{M}(\mathrm{sp} \vec{\times} \mathrm{bw})$$

and

$$\neg(\mathrm{M}(\mathrm{bw} \vec{\times} \mathrm{sp}))$$

Martelli's semiring ([Mar76])

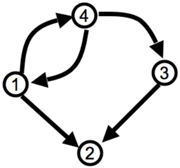
- A cut set $C \subseteq E$ for nodes i and j is a set of edges such there is no path from i to j in the graph $(V,\ E - C)$.
- C is minimal if no proper subset of C is a cut set.
- Martelli's semiring is such that $\mathbf{A}^{(*)}(i,\ j)$ is the set of all minimal cut sets for i and j.
- The arc $(i,\ j)$ is has weight $w(i,\ j) = \{\{(i,\ j)\}\}$.
- S is the set of all subsets of the power set of E.
- $X \oplus Y$ is $\{x \cup y \mid x \in X,\ y \in Y\}$ with any non-minimal sets removed.
- $X \otimes Y$ is $X \cup Y$ with any non-minimal sets removed.

Example

$$
\begin{aligned}
X &= \{\{(2,\ 3\},\ \{(1,\ 3),\ (2,\ 4)\}\} \\
Y &= \{\{(1,\ 3),\ (2,\ 3\},\ \{(1,\ 3),\ (2,\ 4)\}\} \\
X \oplus Y &= \{\{(1,\ 3),\ (2,\ 3\},\ \{(1,\ 3),\ (2,\ 4)\}\} \\
X \otimes Y &= \{\{(2,\ 3\},\ \{(1,\ 3),\ (2,\ 4)\}\}
\end{aligned}
$$

Martelli

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

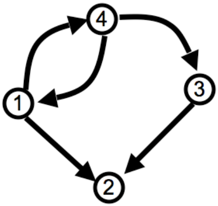


$$A = \begin{bmatrix} \{\phi\} & \{\{(1,2)\}\} & \{\phi\} & \{\{(1,4)\}\} \\ \{\phi\} & \{\phi\} & \{\phi\} & \{\phi\} \\ \{\phi\} & \{\{(3,2)\}\} & \{\phi\} & \{\phi\} \\ \{\{(4,1)\}\} & \{\phi\} & \{\{(4,3)\}\} & \{\phi\} \end{bmatrix}$$

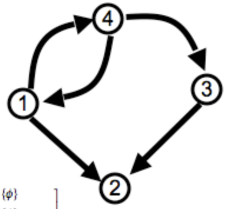
Martelli

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

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



Martelli



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

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

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

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

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

Bibliography I

[Car79] Bernard Carré.
Graphs and Networks.
Oxford University Press, 1979.

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

[GM84] M. Gondran and M. Minoux.
Graphs and Algorithms.
Wiley, 1984.

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

Bibliography II

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

[Mar76] Alberto Martelli.
A gaussian elimination algorithm for the enumeration of cut sets in a graph.
Journal of the ACM, 23(1):58–73, 1976.

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

Bibliography III

[Sob02] Joao Luis Sobrinho.
Algebra and algorithms for QoS path computation and hop-by-hop.
IEEE/ACM Transactions on Networking, 10(4):541–550, August 2002.