An Algebraic Approach to Internet Routing Lectures 01 — 04

Timothy G. Griffin

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

Michaelmas Term
2010

Outline

Background

Current Internet routing protocols exhibit several types of anomalies that can reduce network reliability and increase operational costs.

A very incomplete list of problems:

BGP No convergence guarantees [KRE00, GR01, MGWR02], wedgies [GH05]. Excessive table growth in backbone (see current work on Locator/ID separation in the RRG, for example [FFML09]).

IGPs The lack of options has resulted in some large networks using BGP as an IGP (see Chapter 5 of [ZB03] and Chapter 3 of [WMS05]).

RR and AD Recent work has illustrated some pitfalls of Route Redistribution (RR) and Administrative Distance (AD) [LXZ07, LXP$^+$08, LXZ08].

We will return to these issues later in the term.

How did we get here?

- Internet protocols have evolved in a culture of ‘rough consensus and running code’ — pivotal to the success of the Internet due to the emphasis on interoperability.
- This has worked fairly well for data-transport and application-oriented protocols (IPv4, TCP, FTP, DNS, HTTP, ...)
- Then why are routing protocols so broken?

Why are routing protocols so broken?

- Routing protocols tend not to run on a user's end system, but rather on specialized devices (routers) buried deep within a network's infrastructure.
- The router market has been dominated by a few large companies — an environment that encourages proprietary extensions and the development of *de facto* standards.
- The expedient hack usually wins.
- And finally, let's face it — routing is hard to get right.

What is to be done?

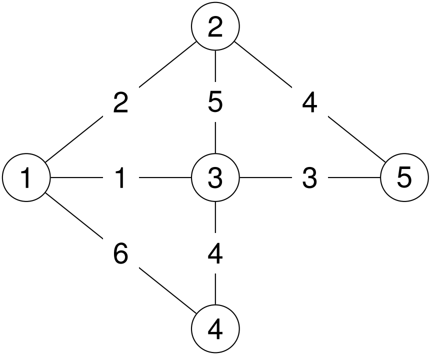
Central Thesis

The culture of the Internet has confounded two things that should be clearly distinguished — what problem is being solved and how it is being solved algorithmically.

Your challenge

- Think of yourself broadly as a Computer Scientist, not narrowly as a "networking person" ...
- Remember that the Internet did not come out of the established networking community! (See John Day's wonderful book [Day08].) Why do we think the next generation network will??
- Routing research should be about more than just understanding the accidental complexity associated with artifacts pooped out by vendors.

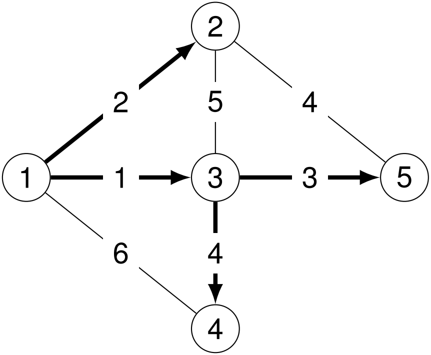
Shortest paths example, $(\mathbb{N}^{\infty}, \min, +)$



The adjacency matrix

$$\mathbf{A} = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{array} \begin{array}{c} \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array} \\ \begin{bmatrix} \infty & 2 & 1 & 6 & \infty \\ 2 & \infty & 5 & \infty & 4 \\ 1 & 5 & \infty & 4 & 3 \\ 6 & \infty & 4 & \infty & \infty \\ \infty & 4 & 3 & \infty & \infty \end{bmatrix} \end{array}$$

Shortest paths example, $(\mathbb{N}^{\infty}, \min, +)$



Bold arrows indicate the shortest-path tree rooted at 1.

The routing matrix

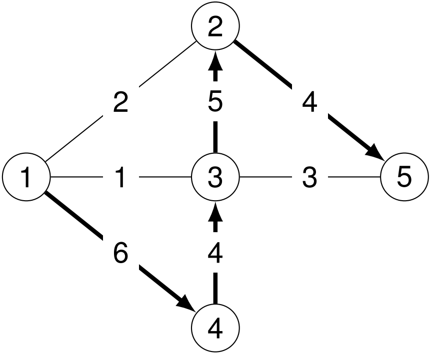
$$\mathbf{R} = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{array} \begin{array}{c} \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array} \\ \begin{bmatrix} 0 & 2 & 1 & 5 & 4 \\ 2 & 0 & 3 & 7 & 4 \\ 1 & 3 & 0 & 4 & 3 \\ 5 & 7 & 4 & 0 & 7 \\ 4 & 4 & 3 & 7 & 0 \end{bmatrix} \end{array}$$

Matrix **R** solves this global optimality problem:

$$\mathbf{R}(i, j) = \min_{p \in P(i, j)} w(p),$$

where $P(i, j)$ is the set of all paths from i to j.

Widest paths example, $(\mathbb{N}^{\infty}, \ \max, \ \min)$



Bold arrows indicate the widest-path tree rooted at 1.

The routing matrix

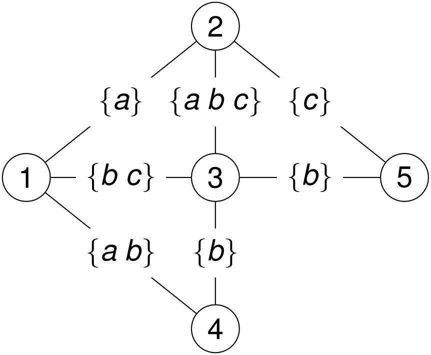
$$
\mathbf{R} \quad = \quad \begin{array}{c|c} & \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array} \\ \begin{array}{c} 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{array} & \begin{bmatrix} \infty & 4 & 4 & 6 & 4 \\ 4 & \infty & 5 & 4 & 4 \\ 4 & 5 & \infty & 4 & 4 \\ 6 & 4 & 4 & \infty & 4 \\ 4 & 4 & 4 & 4 & \infty \end{bmatrix} \end{array}
$$

Matrix **R** solves this global optimality problem:

$$
\mathbf{R}(i, \ j) = \max_{p \in P(i, \ j)} w(p),
$$

where $w(p)$ is now the minimal edge weight in p.

Strange example, $(2^{\{a,\ b,\ c\}},\ \cup,\ \cap)$



We want a Matrix **R** to solve this global optimality problem:

$$\mathbf{R}(i,\ j) = \bigcup_{p \in P(i,\ j)} w(p),$$

where $w(p)$ is now the intersection of all edge weights in p.

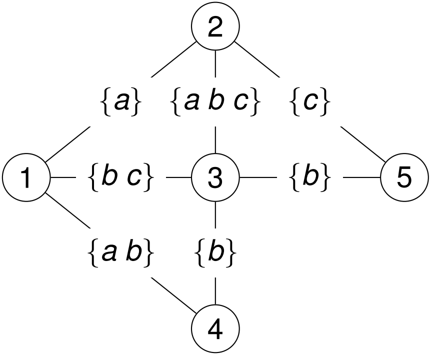
For $x \in \{a,\ b,\ c\}$, interpret $x \in \mathbf{R}(i,\ j)$ to mean that there is at least one path from i to j with x in every arc weight along the path.

Strange example, $(2^{\{a,\ b,\ c\}},\ \cup,\ \cap)$

The matrix **R**

$$
\begin{array}{c}
\\
1\\ 2\\ 3\\ 4\\ 5
\end{array}
\begin{array}{c}
\begin{array}{ccccc} \quad 1 \quad & \quad 2 \quad & \quad 3 \quad & \quad 4 \quad & \quad 5 \quad \end{array} \\
\left[\begin{array}{ccccc}
\{a\ b\ c\} & \{a\ b\ c\} & \{a\ b\ c\} & \{a\ b\} & \{b\ c\} \\
\{a\ b\ c\} & \{a\ b\ c\} & \{a\ b\ c\} & \{a\ b\} & \{b\ c\} \\
\{a\ b\ c\} & \{a\ b\ c\} & \{a\ b\ c\} & \{a\ b\} & \{b\ c\} \\
\{a\ b\} & \{a\ b\} & \{a\ b\} & \{a\ b\ c\} & \{b\} \\
\{b\ c\} & \{b\ c\} & \{b\ c\} & \{b\} & \{a\ b\ c\}
\end{array}\right]
\end{array}
$$

Another strange example, $(2^{\{a,\ b,\ c\}}, \cap, \cup)$



We want matrix **R** to solve this global optimality problem:

$$\mathbf{R}(i,\ j) = \bigcap_{p \in P(i,\ j)} w(p),$$

where $w(p)$ is now the union of all edge weights in p.

For $x \in \{a,\ b,\ c\}$, interpret $x \in \mathbf{R}(i,\ j)$ to mean that every path from i to j has at least one arc with weight containing x.

Another strange example, $(2^{\{a,\ b,\ c\}},\ \cap,\ \cup)$

The matrix **R**

$$
\begin{array}{c|ccccc}
 & 1 & 2 & 3 & 4 & 5 \\
\hline
1 & \{\} & \{\} & \{b\} & \{b\} & \{\} \\
2 & \{\} & \{\} & \{b\} & \{b\} & \{\} \\
3 & \{b\} & \{b\} & \{\} & \{b\} & \{b\} \\
4 & \{b\} & \{b\} & \{b\} & \{\} & \{b\} \\
5 & \{\} & \{\} & \{b\} & \{b\} & \{\}
\end{array}
$$

These structures are examples of Semirings

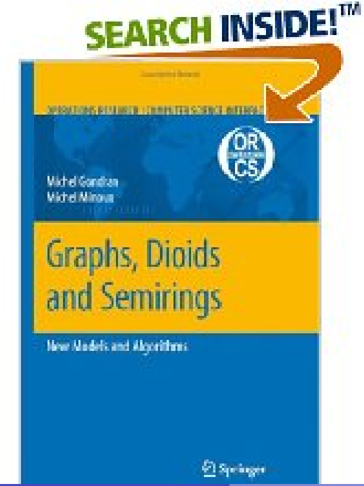
See [Car79, GM84, GM08]

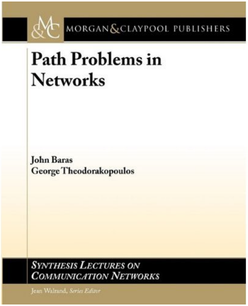
name	S	$\oplus$,	$\otimes$	$\overline{0}$	$\overline{1}$	possible routing use
sp	$\mathbb{N}^{\infty}$	min	$+$	∞	0	minimum-weight routing
bw	$\mathbb{N}^{\infty}$	max	min	0	∞	greatest-capacity routing
rel	$[0,\ 1]$	max	$\times$	0	1	most-reliable routing
use	$\{0,\ 1\}$	max	min	0	1	usable-path routing
	2^W	$\cup$	$\cap$	$\{\}$	W	shared link attributes?
	2^W	$\cap$	$\cup$	W	$\{\}$	shared path attributes?

A wee bit of notation!

Symbol	Interpretation
$\mathbb{N}$	Natural numbers (starting with zero)
$\mathbb{N}^{\infty}$	Natural numbers, plus infinity
$\overline{0}$	Identity for $\oplus$
$\overline{1}$	Identity for $\otimes$

Recomended Reading





What algebraic properties are associated with global optimality?

Distributivity

$$
\begin{array}{lcrcl}
\mathrm{L.D} & : & a \otimes (b \oplus c) & = & (a \otimes b) \oplus (a \otimes c), \\
\mathrm{R.D} & : & (a \oplus b) \otimes c & = & (a \otimes c) \oplus (b \otimes c).
\end{array}
$$

What is this in $\mathrm{sp} = (\mathbb{N}^{\infty},\ \min,\ +)$?

$$
\begin{array}{lcrcl}
\mathrm{L.DIST} & : & a + (b \min c) & = & (a + b) \min (a + c), \\
\mathrm{R.DIST} & : & (a \min b) + c & = & (a + c) \min (b + c).
\end{array}
$$

Local Optimality?

Say that $\mathbf{R}$ is a left-locally optimal solution when

$$\mathbf{R} = (\mathbf{A} \otimes \mathbf{R}) \oplus \mathbf{I}.$$

That is, for $i \neq j$ we have

$$\mathbf{R}(i,\ j) = \bigoplus_{q \in V} \mathbf{A}(i,\ q) \otimes \mathbf{R}(q,\ j)$$

where $N(i) = \{q \mid (i,\ q) \in E\}$ is the set of neighbors of i.

In other words, $\mathbf{R}(i,\ j)$ is the best possible value given the values $\mathbf{R}(q,\ j)$, for all neighbors q of i.

Oh, don't forget Right Local Optimality....

Say that $\mathbf{R}$ is a right-locally optimal solution when

$$\mathbf{R} = (\mathbf{R} \otimes \mathbf{A}) \oplus \mathbf{I}.$$

That is, for $i \neq j$ we have

$$\mathbf{R}(i,\ j) = \bigoplus_{q \in V} \mathbf{R}(i,\ q) \otimes \mathbf{A}(q,\ j)$$

In other words, $\mathbf{R}(i,\ j)$ is the best possible value given the values $\mathbf{R}(q,\ j)$, for all in-neighbors q of destination j.

With Distributivity

A is an adjacency matrix over semiring S.

For Semirings, the following two problems are essentially the same — locally optimal solutions are globally optimal solutions.

Global Optimality	Local Optimality
Find **R** such that	Find **R** such that
$\mathbf{R}(i,\ j) = \sum^{\oplus}_{p \in P(i,\ j)} w(p)$	$\mathbf{R} = (\mathbf{A} \otimes \mathbf{R}) \oplus \mathbf{I}$

Without Distributivity

When $\otimes$ does not distribute over $\oplus$, the following two problems are distinct.

Global Optimality	Local Optimality
Find $\mathbf{R}$ such that $\mathbf{R}(i,\ j) = \sum^{\oplus}_{p \in P(i,\ j)} w(p)$	Find $\mathbf{R}$ such that $\mathbf{R} = (\mathbf{A} \otimes \mathbf{R}) \oplus \mathbf{I}$

Global Optimality

This has been studied, for example [LT91b, LT91a] in the context of circuit layout. See Chapter 5 of [BT10]. This approach does not play well with (loop-free) hop-by-hop forwarding!

Local Optimality

At a very high level, this is the type of problem that BGP attempts to solve!!

Outline

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
$\mathbb{N}^{\infty}$	min	
$\mathbb{N}^{\infty}$	max	
$\mathbb{N}^{\infty}$	$+$	
2^W	$\cup$	
2^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
$\mathbb{N}^{\infty}$	min	∞	0
$\mathbb{N}^{\infty}$	max	0	∞
$\mathbb{N}^{\infty}$	$+$	0	∞
2^W	$\cup$	$\{\}$	W
2^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
$\mathbb{N}^\infty$	min	$\star$	$\star$	$\star$
$\mathbb{N}^\infty$	max	$\star$	$\star$	$\star$
$\mathbb{N}^\infty$	$+$	$\star$		
2^W	$\cup$	$\star$		$\star$
2^W	$\cap$	$\star$		$\star$
S^*	$\circ$			
S	left		$\star$	$\star$
S	right		$\star$	$\star$

Order Relations

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

Definition (Important Order Properties)

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

	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 $c_3 = c_1 \oplus c_2$ 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, $\exists c_3 \in S : c = a \oplus c_3$, 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 $a \trianglelefteq_{\oplus}^{R} c$ and $a \trianglelefteq_{\oplus}^{L} c$ 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 $a = b$. $\square$

Natural Orders

Definition (Natural orders)

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

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

Lemma

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

Proof.

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

$\square$

Special elements and natural orders

Lemma (Natural Bounds)

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

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

Remark (Thanks to Iljitsch van Beijnum)

Note that this means for (min, $+$) we have

$$\begin{array}{ccccc} 0 & \leq_{\min}^{L} & a & \leq_{\min}^{L} & \infty \\ \infty & \leq_{\min}^{R} & a & \leq_{\min}^{R} & 0 \end{array}$$

and still say that this is bounded, even though one might argue with the terminology!

Examples of special elements

S	$\oplus$	α	ω	$\leq_{\oplus}^{\mathrm{L}}$	$\leq_{\oplus}^{\mathrm{R}}$
$\mathbb{N} \cup \{\infty\}$	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. $\text{IDEMPOTENT}((S, \oplus)) \iff \text{REFLEXIVE}((S, \leq_{\oplus}^{D}))$
2. $\text{COMMUTATIVE}((S, \oplus)) \implies \text{ANTISYMMETRIC}((S, \leq_{\oplus}^{D}))$
3. $\text{SELECTIVE}((S, \oplus)) \iff \text{TOTAL}((S, \leq_{\oplus}^{D}))$

Proof.

1. $a \leq_{\oplus}^{D} a \iff a = a \oplus a,$
2. $a \leq_{\oplus}^{L} b \wedge b \leq_{\oplus}^{L} a \iff a = a \oplus b \wedge b = b \oplus a \implies a = b$
3. $a = a \oplus b \vee b = a \oplus b \iff a \leq_{\oplus}^{L} b \vee b \leq_{\oplus}^{L} a$

□

Outline

Semirings

$(S, \oplus, \otimes, \overline{0}, \overline{1})$ is a semiring when

- $(S, \oplus, \overline{0})$ is a commutative monoid
- $(S, \otimes, \overline{1})$ is a monoid
- $\overline{0}$ is an annihilator for $\otimes$

and distributivity holds,

$$\begin{array}{lcrcl} \mathrm{LD} & : & a \otimes (b \oplus c) & = & (a \otimes b) \oplus (a \otimes c) \\ \mathrm{RD} & : & (a \oplus b) \otimes c & = & (a \otimes c) \oplus (b \otimes c) \end{array}$$

Encoding path problems

- $(S, \oplus, \otimes, \overline{0}, \overline{1})$ a semiring
- $G = (V, E)$ a directed graph
- $w \in E \rightarrow S$ a weight function

Path weight

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

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

The empty path is given the weight $\overline{1}$.

Adjacency matrix **A**

$$\mathbf{A}(i, j) = \begin{cases} w(i, j) & \text{if } (i, j) \in E, \\ \overline{0} & \text{otherwise} \end{cases}$$

The general problem of finding globally optimal paths

Given an adjacency matrix $\mathbf{A}$, find $\mathbf{R}$ such that for all $i, j \in V$

$$\mathbf{R}(i, j) = \bigoplus_{p \in P(i, j)} w(p)$$

How can we solve this problem?

Powers and closure

- $(S, \oplus, \otimes, \overline{0}, \overline{1})$ a semiring

Powers, a^k

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

Closure, a^*

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

Definition (q stability)

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

Fact 1

If $\overline{1}$ is an annihiltor for $\oplus$, then every $a \in S$ is 0-stable!

Lift semiring to matrices

- $(S, \oplus, \otimes, \overline{0}, \overline{1})$ a semiring
- Define the semiring of $n \times n$-matrices over S : $(\mathbb{M}_n(S), \oplus, \otimes, \mathbf{J}, \mathbf{I})$

$\oplus$ and $\otimes$

$$
\begin{aligned}
(\mathbf{A} \oplus \mathbf{B})(i, j) &= \mathbf{A}(i, j) \oplus \mathbf{B}(i, j) \\
(\mathbf{A} \otimes \mathbf{B})(i, j) &= \bigoplus_{1 \le q \le n} \mathbf{A}(i, q) \otimes \mathbf{B}(q, j)
\end{aligned}
$$

J and I

$$
\begin{aligned}
\mathbf{J}(i, j) &= \overline{0} \\
\mathbf{I}(i, j) &= \begin{cases} \overline{1} & (\text{if } i = j) \\ \overline{0} & (\text{otherwise}) \end{cases}
\end{aligned}
$$

$\mathbb{M}_n(S)$ is a semiring!

Check (left) distribution

$$\mathbf{A} \otimes (\mathbf{B} \oplus \mathbf{C}) = (\mathbf{A} \otimes \mathbf{B}) \oplus (\mathbf{A} \otimes \mathbf{C})$$

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

On the matrix semiring

Matrix powers, $\mathbf{A}^k$

$$\mathbf{A}^0 = \mathbf{I}$$

$$\mathbf{A}^{k+1} = \mathbf{A} \otimes \mathbf{A}^k$$

Closure, $\mathbf{A}^*$

$$\mathbf{A}^{(k)} = \mathbf{I} \oplus \mathbf{A}^1 \oplus \mathbf{A}^2 \oplus \cdots \oplus \mathbf{A}^k$$

$$\mathbf{A}^* = \mathbf{I} \oplus \mathbf{A}^1 \oplus \mathbf{A}^2 \oplus \cdots \oplus \mathbf{A}^k \oplus \cdots$$

Note: $\mathbf{A}^*$ might not exist (sum may not converge)

Fact 2

If S is 0-stable, then $\mathbb{M}_n(S)$ is $(n-1)$-stable. That is,

$$\mathbf{A}^* = \mathbf{A}^{(n-1)} = \mathbf{I} \oplus \mathbf{A}^1 \oplus \mathbf{A}^2 \oplus \cdots \oplus \mathbf{A}^{n-1}$$

Computing optimal paths

- 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

$$
\begin{array}{lrcl}
(1) & \mathbf{A}^k(i,\ j) & = & \bigoplus_{p \in P^k(i,\ j)} w(p) \\
(2) & \mathbf{A}^{(k+1)}(i,\ j) & = & \bigoplus_{p \in P^{(k)}(i,\ j)} w(p) \\
(3) & \mathbf{A}^{(*)}(i,\ j) & = & \bigoplus_{p \in P(i,\ j)} w(p)
\end{array}
$$

Proof of (1)

By induction on k. Base Case: $k = 0$.

$$P^0(i,\ i) = \{\epsilon\},$$

so $\mathbf{A}^0(i\ , i) = \mathbf{I}(i,\ i) = \overline{1} = w(\epsilon)$.

And $i \neq j$ implies $P^0(i, j) = \{\}$. By convention

$$\bigoplus_{p \in \{\}} w(p) = \overline{0} = \mathbf{I}(i,\ j).$$

Proof of (1)

Induction step.

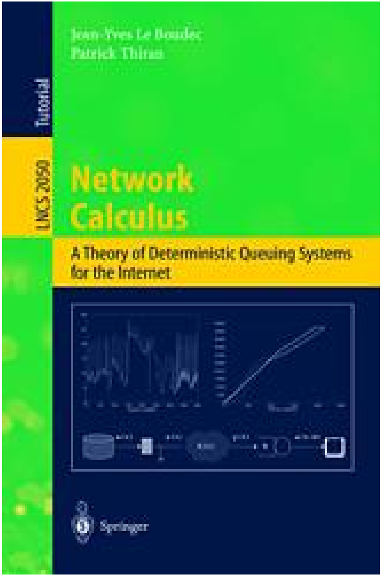
$$
\begin{aligned}
\mathbf{A}^{k+1}(i,j) &= (\mathbf{A} \otimes \mathbf{A}^{k})(i,\ j) \\
&= \bigoplus_{1 \leq q \leq n} \mathbf{A}(i,\ q) \otimes \mathbf{A}^{k}(q,\ j) \\
&= \bigoplus_{1 \leq q \leq n} \mathbf{A}(i,\ q) \otimes \Big(\bigoplus_{p \in P^{k}(q,\ j)} w(p) \Big) \\
&= \bigoplus_{1 \leq q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

Semirings have other applications in Networking

Network calculus [BT01]. For analyzing performance guarantees in networks. Traffic flows are subject to constraints imposed by the system components :

- link capacity
- traffic shapers (leaky buckets)
- congestion control
- background traffic

Algebraic means of expressing and analyzing these constraints starts with the min-plus semiring.



Outline

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 $\vec{\oplus} = \oplus_S \vec{\times} \oplus_T$ is defined as

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

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])

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

Where

Property	Definition
LD	$\forall a, b, c : c \otimes (a \oplus b) = (c \otimes a) \oplus (c \otimes b)$
LC	$\forall a, b, c : c \otimes a = c \otimes b \implies a = b$
LK	$\forall a, b, c : c \otimes a = c \otimes b$

Return to examples

name	LD	LC	LK
sp	Yes	Yes	No
bw	Yes	No	No

So we have

$$\text{LD}(\text{sp} \vec{\times} \text{bw})$$

Is something wrong here? Is it really true that $\text{LC}(\text{sp})$? What about elements such as $(\infty, 17)$ or $(21, 0)$? How can this be fixed?

Note that

$$\neg(\text{LD}(\text{bw} \vec{\times} \text{sp}))$$

$\text{sp} \vec{\times} \text{bw}$

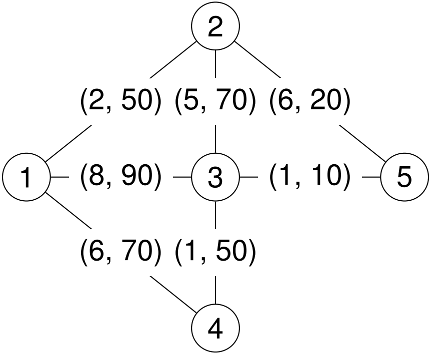
$\text{sp} \vec{\times} \text{bw}$

Let $(S,\ \oplus,\ \otimes,\ \overline{0},\ \overline{1}) = \text{sp} \vec{\times} \text{bw}$.

$$
\begin{array}{rcl}
\text{sp} & = & (\mathbb{N}^{\infty},\ \text{min},\ +,\ \infty,\ 0) \\
\text{bw} & = & (\mathbb{N}^{\infty},\ \text{max},\ \text{min},\ 0,\ \infty) \\
\text{sp} \vec{\times} \text{bw} & = & (\mathbb{N}^{\infty} \times \mathbb{N}^{\infty},\ \text{min} \vec{\times} \text{max},\ + \times \text{min},\ (\infty,\ 0),\ (0,\ \infty))
\end{array}
$$

$$
\begin{array}{rcl}
(17,\ 10) \oplus (21, 100) & = & (17,\ 10) \\
(17,\ 10) \oplus (17, 100) & = & (17,\ 100) \\
(17,\ 10) \otimes (21, 100) & = & (38,\ 10) \\
(17,\ 10) \otimes (17, 100) & = & (34,\ 10)
\end{array}
$$

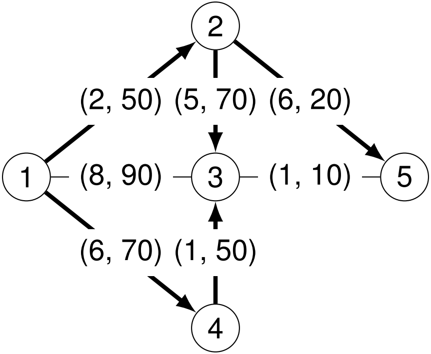
Sample instance for $\text{sp} \vec{\times} \text{bw}$



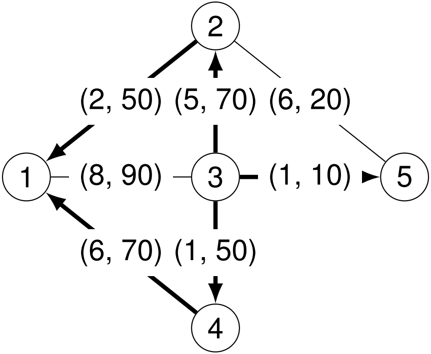
The adjacency matrix

$$
\begin{array}{c c}
 & \begin{array}{ccccc} \quad 1 \quad & \quad 2 \quad & \quad 3 \quad & \quad 4 \quad & \quad 5 \quad \end{array} \\
\begin{array}{c} 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{array} &
\left[\begin{array}{ccccc}
(\infty,\ 0) & (2,\ 50) & (8,\ 90) & (6,\ 70) & (\infty,\ 0) \\
(2,\ 50) & (\infty,\ 0) & (5,\ 70) & (\infty,\ 0) & (6,\ 20) \\
(8,\ 90) & (5,\ 70) & (\infty,\ 0) & (1,\ 50) & (1,\ 10) \\
(6,\ 70) & (\infty,\ 0) & (1,\ 50) & (\infty,\ 0) & (\infty,\ 0) \\
(\infty,\ 0) & (6,\ 20) & (1,\ 10) & (\infty,\ 0) & (\infty,\ 0)
\end{array}\right]
\end{array}
$$

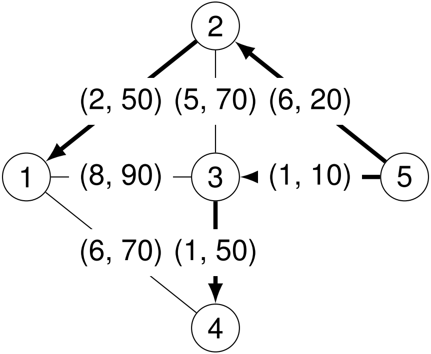
Shortest-path DAG rooted at 1



Shortest-path DAG rooted at 3



Shortest-path DAG rooted at 5



The routing matrix

$$
\begin{array}{c c}
 & \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array} \\
\begin{array}{c} 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{array} &
\left[\begin{array}{ccccc}
(0,\ \infty) & (2,\ 50) & (7,\ 50) & (6,\ 70) & (8,\ 20) \\
(2,\ 50) & (0,\ \infty) & (5,\ 70) & (6,\ 50) & (6,\ 20) \\
(7,\ 50) & (5,\ 70) & (0,\ \infty) & (1,\ 50) & (1,\ 10) \\
(6,\ 70) & (6,\ 50) & (1,\ 50) & (0,\ \infty) & (2,\ 10) \\
(8,\ 20) & (6,\ 20) & (1,\ 10) & (2,\ 10) & (0,\ \infty)
\end{array}\right]
\end{array}
$$

Outline

Bibliography I

[BT01] J.-Y. Le Boudec and P. Thiran.
Network Calculus: A Theory of Deterministic Queuing Systems for the Internet.
Springer, 2001.

[BT10] John S. Baras and George Theodorakopoulos.
Path problems in networks.
Morgan & Claypool, 2010.

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

[Day08] John Day.
Patterns in Network Architectures : A return to fundamentals.
Prentice Hall, 2008.

Bibliography II

[FFML09] D. Farinacci, V. Fuller, D. Meyer, and D. Lewis.
Locator/ID separation protocol (LISP).
draft-ietf-lisp-02.txt, 2009.
Work In Progress.

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

[GH05] Timothy G. Griffin and Geoff Huston.
RFC 4264: BGP Wedgies, November 2005.
IETF.

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

Bibliography III

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

[GR01] Lixin Gao and Jennifer Rexford.
Stable internet routing without global coordination.
IEEE/ACM Transactions on Networking, pages 681–692, December 2001.

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

[KRE00] K.Varadhan, R.Govindan, and D Estrin.
Persistent route oscillations in inter-domain routing.
Computer Networks, 32:1–16, 2000.

Bibliography IV

[LT91a] T. Lengauer and D. Theune.
Efficient algorithms for path problems with general cost criteria.
Lecture Notes in Computer Science, 510:314–326, 1991.

[LT91b] T. Lengauer and D. Theune.
Unstructured path problems and the making of semirings.
Lecture Notes in Computer Science, 519:189–200, 1991.

[LXP+08] Franck Le, Geoffrey Xie, Dan Pei, Jia Wang, and Hui Zhang.
Shedding light on the glue logic of the internet routing architecture.
In *Proc. ACM SIGCOMM*, 2008.

Bibliography V

[LXZ07] Franck Le, Geoffrey Xie, and Hui Zhang.
Understanding route redistribution.
In *Proc. Inter. Conf. on Network Protocols*, 2007.

[LXZ08] Franck Le, Geoffrey Xie, and Hui Zhang.
Instability free routing: Beyond one protocol instance.
In *Proc. ACM CoNext*, December 2008.

[MGWR02] D. McPherson, V. Gill, D. Walton, and A. Retana.
RFC3345: Border gateway protocol (BGP) persistent route oscillation condition, 2002.

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

Bibliography VI

[WMS05] Russ White, Danny McPherson, and Srihari Sangli.
Practical BGP.
Addison Wesley, 2005.

[ZB03] Randy Zhang and Micah Bartell.
BGP Design and Implementation.
Cisco Press, 2003.