L11 : Algebraic Path Problems with Applications to Internet Routing
Lectures 2 and 3

Timothy G. Griffin

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

Michaelmas Term
2012

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)

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

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)

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

	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)

$$a \trianglelefteq^R_\oplus b \equiv \exists c \in S : b = a \oplus c$$
$$a \trianglelefteq^L_\oplus b \equiv \exists c \in S : a = b \oplus c$$

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 $a \trianglelefteq^{R}_{\oplus} c$ 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 semigroup.

$$a \leq^{L}_{\oplus} b \quad \equiv \quad a = a \oplus b$$
$$a \leq^{R}_{\oplus} b \quad \equiv \quad b = a \oplus b$$

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.

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

Special elements and natural orders

Lemma (Natural Bounds)

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

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

Remark (Thanks to Iljitsch van Beijnum)

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

$$\begin{array}{cccc} 0 & \leq^{L}_{\min} & a & \leq^{L}_{\min} & \infty \\ \infty & \leq^{R}_{\min} & a & \leq^{R}_{\min} & 0 \end{array}$$

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

Examples of special elements

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

Proof.

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

Bi-semigroups and Pre-Semirings

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

- $(S, \oplus)$ is a semigroup
- $(S, \otimes)$ is a semigroup

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

- $(S, \oplus, \otimes)$ is a bi-semigroup
- $\oplus$ is commutative

and left- and right-distributivity hold,

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

Semirings

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

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

Examples

Pre-semirings

name	S	$\oplus$,	$\otimes$	$\overline{0}$	$\overline{1}$
min_plus	$\mathbb{N}$	min	$+$	∞	0
max_min	$\mathbb{N}$	max	min	0	

Semirings

name	S	$\oplus$,	$\otimes$	$\overline{0}$	$\overline{1}$
sp	$\mathbb{N}^{\infty}$	min	$+$	∞	0
bw	$\mathbb{N}^{\infty}$	max	min	0	∞

Note the sloppiness — the symbols $+$, max, and min in the two tables represent different functions....

Operation for inserting a zero

Suppose $\overline{0} \notin S$

$$\text{add\_zero}(\overline{0},\ (S,\ \oplus,\ \otimes)) = (S \cup \{\overline{0}\}, \hat{\oplus},\ \hat{\otimes})$$

where

$$a \hat{\oplus} b \quad = \quad \begin{cases} a & (\text{if } b = \overline{0}) \\ b & (\text{if } a = \overline{0}) \\ a \oplus b & (\text{otherwise}) \end{cases}$$

$$a \hat{\otimes} b \quad = \quad \begin{cases} \overline{0} & (\text{if } b = \overline{0}) \\ \overline{0} & (\text{if } a = \overline{0}) \\ a \otimes b & (\text{otherwise}) \end{cases}$$

$$\text{sp} = \text{add\_zero}(\infty,\ \text{min\_plus}).$$

Operation for inserting a one

Suppose $\overline{1} \notin S$

$$\text{add\_one}(\overline{1},\ (S,\ \oplus,\ \otimes)) = (S \cup \{\overline{1}\}, \hat{\oplus},\ \hat{\otimes})$$

where

$$a \hat{\oplus} b \quad = \quad \begin{cases} \overline{1} & (\text{if } b = \overline{1}) \\ \overline{1} & (\text{if } a = \overline{1}) \\ a \oplus b & (\text{otherwise}) \end{cases}$$

$$a \hat{\otimes} b \quad = \quad \begin{cases} a & (\text{if } b = \overline{1}) \\ b & (\text{if } a = \overline{1}) \\ a \otimes b & (\text{otherwise}) \end{cases}$$

$$\text{bw} = \text{add\_one}(\infty,\ \text{max\_min}).$$

How about (max, $+$)?

Pre-semiring

name	S	$\oplus$,	$\otimes$	$\overline{0}$	$\overline{1}$
max_plus	$\mathbb{N}$	max	$+$	0	0

- What about "$\overline{0}$ is an annihilator for $\otimes$"? No!

Semiring ($\text{max\_plus}^{-\infty} = \text{add\_zero}(-\infty, \text{max\_min})$)

name	S	$\oplus$,	$\otimes$	$\overline{0}$	$\overline{1}$
$\text{max\_plus}^{-\infty}$	$\mathbb{N} \cup \{-\infty\}$	max	$+$	$-\infty$	0

Matrix Semirings

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

$\oplus$ and $\otimes$

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

$$(\mathbf{A} \otimes \mathbf{B})(i,\ j) \quad = \quad \bigoplus_{1 \leq q \leq n} \mathbf{A}(i,\ q) \otimes \mathbf{B}(q,\ j)$$

J and I

$$\mathbf{J}(i,\ j) \quad = \quad \overline{0}$$

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

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

For example, here is left distribution

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

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

Note : we only needed left-distributivity on S.

Matrix encoding path problems

- $(S,\ \oplus,\ \otimes,\ \overline{0},\ \overline{1})$ a semiring
- $G = (V,\ E)$ a directed graph
- $w \in E \to S$ 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 **A**, find **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?

Matrix methods

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. Why?

Matrix methods can compute optimal path weights

- 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

$$(1) \qquad \mathbf{A}^k(i,\ j) \ = \bigoplus_{p \in P^k(i,\ j)} w(p)$$

$$(2) \qquad \mathbf{A}^{(k+1)}(i,\ j) \ = \bigoplus_{p \in P^{(k)}(i,\ j)} w(p)$$

$$(3) \qquad \mathbf{A}^{(*)}(i,\ j) \ = \bigoplus_{p \in P(i,\ j)} w(p)$$

Warning again: for some semirings the expression $\mathbf{A}^{(*)}(i,\ j)$ might not be well-defeind. Why?

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.

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

When does $\mathbf{A}^{(*)}$ exist? Try a general approach.

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

Powers, a^k

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

Closure, a^*

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

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.

Two facts

Fact 1

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

Fact 2

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

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