# L11: Algebraic Path Problems with applications to Internet Routing Lectures 02, 03

Timothy G. Griffin

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

Michaelmas Term, 2014

< ロ > < 同 > < 回 > < 回 >

# Semigroups

## Definition (Semigroup)

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

ASSOCIATIVE :  $a \oplus (b \oplus c) = (a \oplus b) \oplus c$ 

S	$\oplus$	where
$\mathbb{N}^{\infty}$	min	
$\mathbb{N}^{\infty}$	max	
$\mathbb{N}^{\infty}$	+	
2 <sup><i>W</i></sup>	U	
2 <sup><i>W</i></sup>	$\cap$	
$S^*$	0	$(abc \circ de = abcde)$
S	left	(a  left  b = a)
S	right	(a right b = b)

< ロ > < 同 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ >

# **Special Elements**

#### Definition

 α ∈ S is an identity if for all a ∈ S

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

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

 $\omega = \omega \oplus \mathbf{a} = \mathbf{a} \oplus \omega$ 

S	$\oplus$	$\alpha$	ω
$\mathbb{N}^{\infty}$	min	$\infty$	0
$\mathbb{N}^{\infty}$	max	0	$\infty$
$\mathbb{N}^{\infty}$	+	0	$\infty$
2 <sup><i>W</i></sup>	U	{}	W
2 <sup><i>W</i></sup>	$\cap$	Ŵ	{}
$S^*$	0	$\epsilon$	
S	left		
S	right		

**A** 

4 3 5 4 3

## **Important Properties**

### Definition (Some Important Semigroup Properties)

COMMUTATIVE	:	$\pmb{a} \oplus \pmb{b}$	=	$b \oplus a$
SELECTIVE	:	$\pmb{a} \oplus \pmb{b}$	$\in$	{ <i>a</i> , <i>b</i> }
IDEMPOTENT	:	<i>a</i> ⊕ <i>a</i>	=	а

S	$\oplus$	COMMUTATIVE	SELECTIVE	IDEMPOTENT
$\mathbb{N}^{\infty}$	min	*	*	*
$\mathbb{N}^{\infty}$	max	*	*	*
$\mathbb{N}^{\infty}$	+	*		
2 <sup>W</sup>	U	*		*
2 <sup>W</sup>	$\cap$	*		*
<b>S</b> *	0			
S	left		*	*
S	right		*	*

э

(a)

# **Order Relations**

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

Definition (Important Order Properties)

- REFLEXIVE :  $a \le a$
- TRANSITIVE :  $a \leq b \land b \leq c \rightarrow a \leq c$
- ANTISYMMETRIC :  $a \leq b \land b \leq a 
  ightarrow a = b$

#### TOTAL : $a \le b \lor b \le a$

	pre-order	partial order	preference order	total order
REFLEXIVE	*	*	*	*
TRANSITIVE	*	*	*	*
ANTISYMMETRIC		*		*
TOTAL			*	*

< ロ > < 同 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ >

# Canonical Pre-order of a Commutative Semigroup

Suppose  $\oplus$  is commutative.

Definition (Canonical pre-orders)

$$a \trianglelefteq_{\oplus}^{R} b \equiv \exists c \in S : b = a \oplus c$$
  
 $a \trianglelefteq_{\oplus}^{L} b \equiv \exists c \in S : a = b \oplus c$ 

#### Lemma (Sanity check)

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

### Proof.

Note that  $a \trianglelefteq_{\oplus}^{R} b$  means  $\exists c_{1} \in S : b = a \oplus c_{1}$ , and  $b \trianglelefteq_{\oplus}^{R} c$  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  $a \trianglelefteq_{\oplus}^{R} c$ . The proof for  $\trianglelefteq_{\oplus}^{L}$  is similar.

・ ロ ト ・ 同 ト ・ 回 ト ・ 回 ト

# 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  $a \oplus a^{-1} = a^{-1} \oplus a = \alpha$ .

4 **A** N A **B** N A **B** N

# 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  $a \leq_{\oplus}^{L} b$ . In a similar way,  $b \leq_{\oplus}^{R} a$ . Therefore a = b.

4 3 5 4 3

< 🗇 🕨

## Natural Orders

### Definition (Natural orders)

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

$$a \leq_{\oplus}^{L} b \equiv a = a \oplus b$$
  
 $a \leq_{\oplus}^{R} b \equiv b = a \oplus b$ 

#### Lemma

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

#### Proof.

$$\begin{array}{rcl} a \leq^R_{\oplus} b & \Longleftrightarrow & b = a \oplus c = (a \oplus a) \oplus c = a \oplus (a \oplus c) \\ & = & a \oplus b \iff a \leq^R_{\oplus} b \\ a \leq^L_{\oplus} b & \iff a = b \oplus c = (b \oplus b) \oplus c = b \oplus (b \oplus c) \\ & = & b \oplus a = a \oplus b \iff a \leq^L_{\oplus} b \end{array}$$

## Special elements and natural orders

### Lemma (Natural Bounds)

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

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

#### Remark (Thanks to Iljitsch van Beijnum)

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

$$egin{array}{rcl} 0 & \leq^L_{\min} & a & \leq^L_{\min} & \infty \ \infty & \leq^R_{\min} & a & \leq^R_{\min} & 0 \end{array}$$

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

## Examples of special elements

S	$\oplus$	$\alpha$	ω	$\leq^{\mathrm{L}}_{\oplus}$	$\leq^{\mathbb{R}}_{\oplus}$
$\mathbb{N}\cup\{\infty\}$	min	$\infty$	0	$\leq$	$\geq$
$\mathbb{N}\cup\{\infty\}$	max	0	$\infty$	$\geq$	$\leq$
$\mathcal{P}(W)$	U	{}	W	$\subseteq$	⊇
$\mathcal{P}(W)$	$\cap$	W	{}	$\supseteq$	$\subseteq$

T.G.Griffin © 2014 11 / 37

2

# **Property Management**

#### Lemma

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

● IDEMPOTENT $((S, \oplus)) \iff$  REFLEXIVE $((S, \leq_{\oplus}^{D}))$ 

- ② COMMUTATIVE $((S, \oplus)) \implies$  ANTISYMMETRIC $((S, ≤_{\oplus}^{D}))$
- $\begin{array}{l} \textcircled{\begin{subarray}{l} \hline $0$ COMMUTATIVE}(($S$, $\oplus$)) \implies ({\tt SELECTIVE}(($S$, $\oplus$)) \iff {\tt TOTAL}(($S$, $\leq^{D}_{\oplus}))) \end{array} } \end{array}$

#### Proof.

• 
$$a \leq_{\oplus}^{D} a \iff a = a \oplus a,$$
  
•  $a \leq_{\oplus}^{L} b \land b \leq_{\oplus}^{L} a \iff a = a \oplus b \land b = b \oplus a \implies a = b$   
•  $a = a \oplus b \lor b = a \oplus b \iff a \leq_{\oplus}^{L} b \lor b \leq_{\oplus}^{L} a$ 

A (10) A (10)

## Bounds

Suppose  $(S, \leq)$  is a partially ordered set.

#### greatest lower bound

For  $a, b \in S$ , the element  $c \in S$  is the greatest lower bound of a and b, written c = a glb b, if it is a lower bound ( $c \le a$  and  $c \le b$ ), and for every  $d \in S$  with  $d \le a$  and  $d \le b$ , we have  $d \le c$ .

#### least upper bound

For  $a, b \in S$ , the element  $c \in S$  is the least upper bound of a and b, written c = a lub b, if it is an upper bound ( $a \le c$  and  $b \le c$ ), and for every  $d \in S$  with  $a \le d$  and  $b \le d$ , we have  $c \le d$ .

## Semi-lattices

Suppose  $(S, \leq)$  is a partially ordered set.

meet-semilattice

S is a <u>meet-semilattice</u> if a glb b exists for each  $a, b \in S$ .

#### join-semilattice

S is a join-semilattice if a lub b exists for each  $a, b \in S$ .

3

# **Fun Facts**

### Fact 1

Suppose  $(S, \oplus)$  is a commutative and idempotent semigroup.

- $(S, \leq_{\oplus}^{L})$  is a meet-semilattice with a glb  $b = a \oplus b$ .
- $(S, \leq_{\oplus}^{R})$  is a join-semilattice with *a* lub  $b = a \oplus b$ .

## Fact 2

Suppose  $(S, \leq)$  is a partially ordered set.

- If (S, ≤) is a meet-semilattice, then (S, glb) is a commutative and idempotent semigroup.
- If (S, ≤) is a join-semilattice, then (S, lub) is a commutative and idempotent semigroup.

That is, semi-lattices represent the same class of structures as commutative and idempotent semigroups.

**Bi-semigroups and Pre-Semirings** 

## $(\mathcal{S}, \oplus, \otimes)$ is a bi-semigroup when

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

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

- ( $\mathcal{S}, \oplus, \otimes$ ) is a bi-semigroup
- ⊕ is commutative

and left- and right-distributivity hold,

LD : 
$$a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$$
  
RD :  $(a \oplus b) \otimes c = (a \otimes c) \oplus (b \otimes c)$ 

< ロ > < 同 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ >

# Semirings

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

- ( $\mathcal{S}, \oplus, \otimes$ ) 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  $\otimes$

4 3 5 4 3 5

# Examples

Pre-ser	niri	ng	S			
name	)	S	$\oplus$ ,	$\otimes$	$\overline{0}$	1
min_pl	us	$\mathbb{N}$	min	+		0
max_m	in	$\mathbb{N}$	max	min	0	
· · ·						
Semirir	igs					
name	S	5	$\oplus$ ,	$\otimes$	$\overline{0}$	1
sn	Nc	$\infty$	min	+	$\infty$	0
sp						

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

How about (max, +)?

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

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

Semiring (max_plus <sup><math>-\infty</math></sup> = add_zero( $-\infty$ , max_min))							
name	S	$\oplus$ ,	$\otimes$	$\overline{0}$	ī		
$\max_{\text{plus}}^{-\infty}$	$\mathbb{N}\cup\{-\infty\}$	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  $\otimes$ 

$$(\mathbf{A} \oplus \mathbf{B})(i, j) = \mathbf{A}(i, j) \oplus \mathbf{B}(i, j)$$
  
 $(\mathbf{A} \otimes \mathbf{B})(i, j) = \bigoplus \mathbf{A}(i, q) \otimes \mathbf{B}(q, j)$ 

 $\underbrace{\bigcup_{1 \leq q \leq n}}_{1 \leq q \leq n}$ 

J and I

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

tgg22 (cl.cam.ac.uk)

L11: Algebraic Path Problems with applica

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

## For example, here is left distribution

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

$$= \bigoplus_{\substack{1 \le q \le n}}^{(\mathbf{A} \otimes (\mathbf{B} \oplus \mathbf{C}))(i, j)} \\ = \bigoplus_{\substack{1 \le q \le n}}^{(\mathbf{A} \otimes (\mathbf{B} \oplus \mathbf{C}))(i, j)} \\ = \bigoplus_{\substack{1 \le q \le n}}^{(\mathbf{A} \otimes (i, q) \otimes (\mathbf{B} \oplus \mathbf{C}))(q, j))} \\ = \bigoplus_{\substack{1 \le q \le n}}^{(\mathbf{A} \otimes (i, q) \otimes (\mathbf{B} \otimes \mathbf{C}))(q, j))} \\ = (\bigoplus_{\substack{1 \le q \le n}}^{(\mathbf{A} \otimes (i, q) \otimes \mathbf{B})(q, j)) \oplus ((\bigoplus_{\substack{1 \le q \le n}}^{(\mathbf{A} \otimes (i, q) \otimes \mathbf{C})} \mathbf{A}(i, q) \otimes \mathbf{C})(q, j))$$

$$= ((\mathbf{\bar{A}} \otimes \mathbf{B}) \oplus (\mathbf{A} \otimes \mathbf{C}))(i, j)$$

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
- $w \in E \rightarrow S$  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

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

L11: Algebraic Path Problems with applica

# 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?

4 3 5 4 3 5

< 6 k

## Matrix methods

Matrix powers,  $\mathbf{A}^k$   $\mathbf{A}^0 = \mathbf{I}$  $\mathbf{A}^{k+1} = \mathbf{A} \otimes \mathbf{A}^k$ 

## Closure, **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: A\* might not exist. Why?

<ロト < 回 > < 回 > < 三 > < 三 > 三 三

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

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

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

tgg22 (cl.cam.ac.uk)

L11: Algebraic Path Problems with applica

T.G.Griffin © 2014 26 / 37

< ロ > < 同 > < 回 > < 回 >

# Proof of (1)

Induction step.

$$\mathbf{A}^{k+1}(i,j) = (\mathbf{A} \otimes \mathbf{A}^k)(i, j)$$

$$= \bigoplus_{\substack{1 \le q \le n}} \mathbf{A}(i, q) \otimes \mathbf{A}^k(q, j)$$

$$= \bigoplus_{\substack{1 \le q \le n}} \mathbf{A}(i, q) \otimes (\bigoplus_{\substack{p \in P^k(q, j)}} w(p))$$

$$= \bigoplus_{\substack{1 \le q \le n}} \bigoplus_{\substack{p \in P^k(q, j)}} \mathbf{A}(i, q) \otimes w(p)$$

$$= \bigoplus_{\substack{(i, q) \in E}} \bigoplus_{\substack{p \in P^k(q, j)}} w(i, q) \otimes w(p)$$

$$= \bigoplus_{\substack{p \in P^{k+1}(i, j)}} w(p)$$

2

イロト イヨト イヨト イヨト

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

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



#### 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.

## More Fun Facts

### Fact 3

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

#### Fact 4

If *S* is 0-stable, then  $M_n(S)$  is (n-1)-stable. That is,

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

3

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



The adjacency matrix

А

T.G.Griffin © 2014 30 / 37

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



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

The routing matrix



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

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

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

A D b 4 A b

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



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

The routing matrix



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.

4 A N

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



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

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

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.

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



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



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

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

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



< 6 b

## Homework number 1

- Prove that matrix multiplication (slide 20) is associative.
- Prove Fun Facts 1 and 2 (see slide 15)
- Prove Fun Facts 3 and 4 (see slide 29)

A B F A B F

< 6 k