L11: Algebraic Path Problems with applications to Internet Routing

Timothy G. Griffin

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

Michaelmas Term, 2019

L11: Algebraic Path Problems with applica

イヨト イモト イモト

Shortest paths example, $sp = (\mathbb{N}^{\infty}, \min, +, \infty, \mathbf{0})$



The adjacency matrix

Α

Shortest paths solution



solves this global optimality problem:

$$\mathbf{A}^*(i, j) = \min_{\boldsymbol{p} \in \pi(i, j)} \boldsymbol{w}(\boldsymbol{p}),$$

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

< 6 k

I

Widest paths example, $\mathbf{bw} = (\mathbb{N}^{\infty}, \text{ max}, \text{ min}, \mathbf{0}, \infty)$



			1	2	3	4	5	
		1	ŝ	4	4	6	4	٦
		2	4	∞	5	4	4	
A *	=	3	4	5	∞	4	4	
		4	6	4	4	∞	4	
		5	4	4	4	4	∞	

solves this global optimality problem:

$$\mathbf{A}^*(i, j) = \max_{\mathbf{p} \in \pi(i, j)} \mathbf{w}(\mathbf{p}),$$

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

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



We want **A*** to solve this global optimality problem:

$$\mathbf{A}^*(i, j) = \bigcup_{\mathbf{p}\in\pi(i, j)} \mathbf{w}(\mathbf{p}),$$

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

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

$$\mathbf{A}^{*}(4, 1) = \{a, b\}$$
 $\mathbf{A}^{*}(4, 5) = \{b\}$

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



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

$$\mathbf{A}^*(i, j) = \bigcap_{\mathbf{p} \in \pi(i, j)} \mathbf{w}(\mathbf{p}),$$

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

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

$$\mathbf{A}^*(4, \ 1) = \{b\} \quad \ \mathbf{A}^*(4, \ 5) = \{b\} \quad \ \mathbf{A}^*(5, \ 1) = \{\}$$

Semirings (generalise $(\mathbb{R}, +, \times, 0, 1)$)

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

A wee bit of notation!

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

Recommended (on reserve in CL library)

Morgan&claypool publishers	
Path Problems in Networks	Michel Gondran
John Baras George Theodorakopoulos	Graphs and Se
	New Models and
Synthesis Lectures on Communication Networks	
Jean Waltand, Serie Estar	

I COMPUTER SCIENCE INTERFACES , Dioids mirings Algorithms

2 Springer

tgg22 (cl.cam.ac.uk)

L11: Algebraic Path Problems with applica

T.G.Griffin@2017 8/107

nan

We will look at all of the axioms of semirings, but the most important are

distributivity

$$\begin{array}{rcl} \mathbb{L}\mathbb{D} & : & a \otimes (b \oplus c) & = & (a \otimes b) \oplus (a \otimes c) \\ \mathbb{R}\mathbb{D} & : & (a \oplus b) \otimes c & = & (a \otimes c) \oplus (b \otimes c) \end{array}$$

(4) (5) (4) (5)

< 6 b

Distributivity, illustrated



 $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$ *j* makes the choice = i makes the choice

tgg22 (cl.cam.ac.uk)

L11: Algebraic Path Problems with applica

T.G.Griffin © 2017 10 / 107

э

< 日 > < 同 > < 回 > < 回 > < 回 > <

Should distributivity hold in Internet Routing?



- *j* prefers long path though one of its customers (not the shorter path through a competitor)
- given two routes from a provider, *i* prefers the one with a shorter path
- More on inter-domain routing in the Internet later in the term ...

< 同 ト < 三 ト < 三 ト

Widest shortest-paths

- Metric of the form (*d*, *b*), where *d* is distance (min, +) and *b* is capacity (max, min).
- Metrics are compared lexicographically, with distance considered first.
- Such things are found in the vast literature on Quality-of-Service (QoS) metrics for Internet routing.



Weights are globally optimal (we have a semiring)

Widest shortest-path weights computed by Dijkstra and Bellman-Ford



A (10) A (10)

But what about the paths themselves?

Four optimal paths of weight (3, 10).

There are standard ways to extend Bellman-Ford and Dijkstra to compute paths (or the associated <u>next hops</u>).

Do these extended algorithms find all optimal paths?

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

Surprise!

Four optimal paths of weight (3, 10)

Paths computed by (extended) Dijkstra

Notice that 0's paths cannot both be implemented with next-hop forwarding since $\mathbf{P}_{\text{Dijkstra}}(1,2) = \{(1,4,2)\}.$

Paths computed by distributed Bellman-Ford

э.

Optimal paths from 0 to 2. Computed by Dijkstra but not by Bellman-Ford



L11: Algebraic Path Problems with applica

Optimal paths from 2 to 1. Computed by Bellman-Ford but not by Dijkstra



How can we understand this (algebaically)?



Preview

- We can add paths explicitly to the widest shortest-path semiring to obtain a new algebra.
- We will see that distributivity does not hold for this algebra.
- Why? We will see that it is because min is not cancellative!
 (amin b = amin c does not imply that b = c)

・ ロ ト ・ 同 ト ・ 回 ト ・ 回 ト

Towards a non-classical theory of algebraic path finding

We need theory that can accept algebras that violate distributivity.

Global optimality

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

Left local optimality (distributed Bellman-Ford)

 $\textbf{L}=(\textbf{A}\otimes\textbf{L})\oplus\textbf{I}.$

Right local optimality (Dijkstra's Algorithm)

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

Embrace the fact that all three notions can be distinct.

tgg22 (cl.cam.ac.uk)

L11: Algebraic Path Problems with applica

T.G.Griffin@2017 20 / 107

3

Lectures 2, 3

- Semigroups
- A few important semigroup properties
- Semigroup and partial orders

3 > 4 3

< 61

Semigroups

Semigroup

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

AS associative
$$\equiv \forall a, b, c \in S, a \bullet (b \bullet c) = (a \bullet b) \bullet c$$

Important Assumption — We will ignore trival semigroups We will impicitly assume that $2 \le |S|$.

Note

Many useful binary operations are not semigroup operations. For example, (\mathbb{R}, \bullet) , where $a \bullet b \equiv (a + b)/2$.

Some Important Semigroup Properties

\mathbb{ID}	identity	\equiv	$\exists \alpha \in \boldsymbol{S}, \ \forall \boldsymbol{a} \in \boldsymbol{S}, \ \boldsymbol{a} = \alpha \bullet \boldsymbol{a} = \boldsymbol{a} \bullet \alpha$
$\mathbb{A}\mathbb{N}$	annihilator	\equiv	$\exists \omega \in S, \ \forall a \in S, \ \omega = \omega \bullet a = a \bullet \omega$
\mathbb{CM}	commutative	\equiv	$\forall a, b \in S, a \bullet b = b \bullet a$
\mathbb{SL}	selective	\equiv	$\forall a, b \in S, a \bullet b \in \{a, b\}$
\mathbb{IP}	idempotent	\equiv	$\forall a \in S, \ a \bullet a = a$

A semigroup with an identity is called a monoid.

Note that

$$\mathbb{SL}(S, \bullet) \implies \mathbb{IP}(S, \bullet)$$

< 口 > < 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 > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ >

A few concrete semigroups

S	•	description	α	ω	\mathbb{CM}	\mathbb{SL}	\mathbb{IP}
S	left	$x \operatorname{left} y = x$				*	*
S	right	x right $y = y$				*	*
S^*		concatenation	ϵ				
\mathcal{S}^+		concatenation					
$\{t, f\}$	~	conjunction	t	f	*	*	*
$\{t, f\}$	\sim	disjunction	f	t	*	*	*
\mathbb{N}	min	minimum		0	*	*	*
\mathbb{N}	max	maximum	0		*	*	*
2 ^{<i>W</i>}	U	union	{}	W	*		*
2 ^{<i>W</i>}	\cap	intersection	W	{}	*		*
fin(2 ^{<i>U</i>})	U	union	{}		*		*
fin(2 ^{<i>U</i>})	\cap	intersection		{}	*		*
\mathbb{N}	+	addition	0		*		
\mathbb{N}	×	multiplication	1	0	*		

W a finite set, *U* an infinite set. For set *Y*, fin(*Y*) $\equiv \{X \in Y \mid X \text{ is finite}\}$

A few abstract semigroups

S	•	description	α	ω	\mathbb{CM}	\mathbb{SL}	\mathbb{IP}
2 ⁰	U	union	{}	U	*		*
2 ^{<i>U</i>}	\cap	intersection	U	{}	*		*
$2^{U \times U}$	\bowtie	relational join	ΊU	{}			
$X \to X$	0	composition	$\lambda \mathbf{x}.\mathbf{x}$				

$\begin{array}{l} U \text{ an infinite set} \\ X \bowtie Y \equiv \{(x,z) \in U \times U \mid \exists y \in U, \ (x,\ y) \in X \land (y,\ z) \in Y \} \\ \mathcal{I}_U \equiv \{(u,\ u) \mid u \in U \} \end{array}$

subsemigroup

Suppose (S, \bullet) is a semigroup and $T \subseteq S$. If T is closed w.r.t \bullet (that is, $\forall x, y \in T, x \bullet y \in T$), then (T, \bullet) is a subsemigroup of S.

Order Relations

We are interested in order relations $\leq \subseteq S \times S$ Definition (Important Order Properties) reflexive $\equiv a \leq a$ $\mathbb{R}\mathbb{X}$ TR transitive $\equiv a \leq b \land b \leq c \rightarrow a \leq c$ antisymmetric $\equiv a \leq b \land b \leq a \rightarrow a = b$ AY total $\equiv a \leq b \lor b \leq a$ TO partial preference total ordor ordor order nro_ordor

	pro oraor	01001	01001	0.001
$\mathbb{R}\mathbb{X}$	*	*	*	*
\mathbb{TR}	*	*	*	*
AY		*		*
\mathbb{TO}			*	*

4 A N

EN 4 EN

Canonical Pre-order of a Commutative Semigroup

Definition (Canonical pre-orders)

$$a \trianglelefteq^{R}_{\bullet} b \equiv \exists c \in S : b = a \bullet c$$
$$a \trianglelefteq^{L}_{\bullet} b \equiv \exists c \in S : a = b \bullet c$$

Lemma (Sanity check)

Associativity of • implies that these relations are transitive.

Proof.

Note that $a \leq_{\bullet}^{R} b$ means $\exists c_{1} \in S : b = a \bullet c_{1}$, and $b \leq_{\bullet}^{R} c$ means $\exists c_{2} \in S : c = b \bullet c_{2}$. Letting $c_{3} = c_{1} \bullet c_{2}$ we have $c = b \bullet c_{2} = (a \bullet c_{1}) \bullet c_{2} = a \bullet (c_{1} \bullet c_{2}) = a \bullet c_{3}$. That is, $\exists c_{3} \in S : c = a \bullet c_{3}$, so $a \leq_{\bullet}^{R} c$. The proof for \leq_{\bullet}^{L} is similar.

Canonically Ordered Semigroup

Definition (Canonically Ordered Semigroup)

A commutative semigroup (S, \bullet) is canonically ordered when $a \trianglelefteq_{\bullet}^{R} c$ and $a \trianglelefteq_{\bullet}^{L} c$ 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 $a \bullet a^{-1} = a^{-1} \bullet a = \alpha$.

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 $a = \alpha_{\bullet} \bullet a = (b \bullet b^{-1}) \bullet a = b \bullet (b^{-1} \bullet a) = b \bullet c$, for $c = b^{-1} \bullet a$, so $a \trianglelefteq_{\bullet}^{L} b$. In a similar way, $b \trianglelefteq_{\bullet}^{R} a$. Therefore $a = b$.

< 回 > < 三 > < 三 >

Natural Orders

Definition (Natural orders)

Let (\mathcal{S}, \bullet) be a semigroup.

$$a \leq {}^{L}_{\bullet} b \equiv a = a \bullet b$$

 $a \leq {}^{R}_{\bullet} b \equiv b = a \bullet b$

Lemma

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

Proof.

$$a \leq^{R}_{\bullet} b \iff b = a \bullet c = (a \bullet a) \bullet c = a \bullet (a \bullet c)$$
$$= a \bullet b \iff a \leq^{R}_{\bullet} b$$
$$a \leq^{L}_{\bullet} b \iff a = b \bullet c = (b \bullet b) \bullet c = b \bullet (b \bullet c)$$
$$= b \bullet a = a \bullet b \iff a \leq^{L}_{\bullet} b$$

Special elements and natural orders

Lemma (Natural Bounds)

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

$$\omega \leq {}^{\mathsf{L}} a \leq {}^{\mathsf{L}} \alpha$$
$$\alpha \leq {}^{\mathsf{R}} a \leq {}^{\mathsf{R}} \omega$$

Remark (Thanks to Iljitsch van Beijnum)

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

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

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

tgg22 (cl.cam.ac.uk)

L11: Algebraic Path Problems with applica

Examples of special elements

S	•	α	ω	$\leq^{\mathrm{L}}_{\bullet}$	\leq^{R}_{\bullet}
\mathbb{N}_{∞}	min	∞	0	\leq	\geqslant
$\mathbb{N}^{-\infty}$	max	0	$-\infty$	≥	\leq
$\mathcal{P}(W)$	U	{}	W	\subseteq	\supseteq
$\mathcal{P}(W)$	\cap	W	{}	⊇	\subseteq

tgg22 (cl.cam.ac.uk)

L11: Algebraic Path Problems with applica

T.G.Griffin ©2017

32 / 107

크

Property Management

Lemma Let $D \in \{R, L\}$. (1) $\mathbb{IP}(S, \bullet) \iff \mathbb{RX}(S, \leq^{D}_{\bullet})$ (2) $\mathbb{CM}(S, \bullet) \implies \mathbb{AY}(S, \leq^{D}_{\bullet})$ (3) $\mathbb{AS}(S, \bullet) \implies \mathbb{TR}(S, \leq^{D}_{\bullet})$ (4) $\mathbb{CM}(S, \bullet) \implies (\mathbb{SL}(S, \bullet) \iff \mathbb{TO}(S, \leq^{D}_{\bullet}))$

Proof.

$$a \leq^{D}_{\bullet} a \iff a = a \bullet a,$$

$$a \leq^{L}_{\bullet} b \land b \leq^{L}_{\bullet} a \iff a = a \bullet b \land b = b \bullet a \implies a = b$$

$$a \leq^{L}_{\bullet} b \land b \leq^{L}_{\bullet} c \iff a = a \bullet b \land b = b \bullet c \implies a = a \bullet (b \bullet c) = (a \bullet b) \bullet c = a \bullet c \implies a \leq^{L}_{\bullet} c$$

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 ($c \leq a$ and $c \leq b$), and for every $d \in S$ with $d \leq a$ and $d \leq b$, we have $d \leq c$.

least upper bound

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

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 $a, b \in S$.

< 回 > < 回 > < 回 > -

Fun Facts

Fact 1

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

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

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.

・ロト ・ 同ト ・ ヨト ・ ヨト … ヨー

Lecture 3

- Semirings
- Matrix semirings
- Shortest paths
- Minimax

크

(4) (5) (4) (5)

< 17 ▶

Bi-semigroups and Pre-Semirings

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

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

$(\textbf{\textit{S}},\,\oplus,\,\otimes)$ is a pre-semiring when

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

and left- and right-distributivity hold,

$$\begin{array}{rcl} \mathbb{L}\mathbb{D} & : & a \otimes (b \oplus c) & = & (a \otimes b) \oplus (a \otimes c) \\ \mathbb{R}\mathbb{D} & : & (a \oplus b) \otimes c & = & (a \otimes c) \oplus (b \otimes c) \end{array}$$

A (10) A (10)

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

The Sec. 74

Examples

Pre-ser	niri	ng	S			
name)	S	⊕,	\otimes	$\overline{0}$	1
min_pl	us	\mathbb{N}	min	+		0
max_m	in	\mathbb{N}	max	min	0	
Semirir	igs					
name	S	;	⊕,	\otimes	0	1
		~			\sim	Δ
sp	\mathbb{N}°	δ	min	+	ω	0

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

< 回 > < 回 > < 回 >

How about (max, +)?

Pre-semir	ing				
name	S	⊕,	\otimes	0	1
max_plus	\mathbb{N}	max	+	0	0

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

Fix that					
name	S	\oplus	\otimes	ō	1
$\max_{\text{plus}}^{-\infty}$	$\mathbb{M} \oplus \{-\infty\}$	max	+	$-\infty$	0

T.G.Griffin © 2017 41 / 107

Matrix Semirings

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

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

J and I

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

Associativity

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



Left Distributivity

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

$$\begin{array}{rcl} (\mathbf{A}\otimes(\mathbf{B}\oplus\mathbf{C}))(i,\,j) \\ = & \bigoplus_{1\leqslant q\leqslant n} \mathbf{A}(i,\,q)\otimes(\mathbf{B}\oplus\mathbf{C})(q,\,j) & (\operatorname{def}\rightarrow) \\ = & \bigoplus_{1\leqslant q\leqslant n} \mathbf{A}(i,\,q)\otimes(\mathbf{B}(q,\,j)\oplus\mathbf{C}(q,\,j)) & (\operatorname{def}\rightarrow) \\ = & \bigoplus_{1\leqslant q\leqslant n} (\mathbf{A}(i,\,q)\otimes\mathbf{B}(q,\,j))\oplus(\mathbf{A}(i,\,q)\otimes\mathbf{C}(q,\,j)) & (\mathbb{LD}) \\ = & (\bigoplus_{1\leqslant q\leqslant n} \mathbf{A}(i,\,q)\otimes\mathbf{B}(q,\,j))\oplus(\bigoplus_{1\leqslant q\leqslant n} \mathbf{A}(i,\,q)\otimes\mathbf{C}(q,\,j)) & (\mathbb{AS},\mathbb{CM}) \\ = & ((\mathbf{A}\otimes\mathbf{B})\oplus(\mathbf{A}\otimes\mathbf{C}))(i,\,j) & (\operatorname{def}\leftarrow) \end{array}$$

 $((\mathbf{A} \otimes \mathbf{B}) \oplus (\mathbf{A} \otimes \mathbf{C}))(I, J)$

Э.

イロト イヨト イヨト イヨト

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

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

L11: Algebraic Path Problems with applica

The general problem of finding globally optimal path weights

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

$$\mathbf{A}^*(i, j) = \bigoplus_{\boldsymbol{p} \in \pi(i, j)} \boldsymbol{w}(\boldsymbol{p})$$

where $\pi(i, j)$ represents the set of all paths from *i* to *j*.

How can we solve this problem?

不得る とうちょうちょ

Stability

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

$a \in S$, define 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. By induction: $\forall t, 0 \leq t, a^{(q+t)} = a^{(q)}$. Therefore, $a^* = a^{(q)}$.

э.

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?

æ

Matrix methods can compute optimal path weights

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

Theorem
(1)
$$\mathbf{A}^{k}(i, j) = \bigoplus_{\substack{p \in \pi^{k}(i, j) \\ p \in \pi^{(k)}(i, j)}} \mathbf{w}(p)$$

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

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

T.G.Griffin © 2017 49 / 107

イベト イモト イモト

Proof of (1)

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

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

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

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

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

E N 4 E N

< 17 ▶

Proof of (1)

Induction step.

 $\mathbf{A}^{k+1}(i,j) = (\mathbf{A} \otimes \mathbf{A}^k)(i,j)$ = \bigoplus $\mathbf{A}(i, q) \otimes \mathbf{A}^{k}(q, j)$ 1*≤q≤n* $= \bigoplus \mathbf{A}(i, q) \otimes (\bigoplus w(p))$ $1 \leq q \leq n$ $p \in \pi^k(q, j)$ = \bigoplus \bigoplus $\mathbf{A}(i, q) \otimes w(p)$ $1 \leq q \leq n p \in \pi^k(q, j)$ \bigoplus $w(i, q) \otimes w(p)$ = $(i, q) \in E p \in \pi^k(q,j)$ = (+) w(p) $p \in \pi^{k+1}(i, j)$

T.G.Griffin@2017

4 E 5

э.

51 / 107

< 6 b

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

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

Why? Because we can ignore paths with loops.

$$(\mathbf{a}\otimes\mathbf{c}\otimes\mathbf{b})\oplus(\mathbf{a}\otimes\mathbf{b})=\mathbf{a}\otimes(\overline{\mathbf{1}}\oplus\mathbf{c})\otimes\mathbf{b}=\mathbf{a}\otimes\overline{\mathbf{1}}\otimes\mathbf{b}=\mathbf{a}\otimes\mathbf{b}$$

Think of *c* as the weight of a loop in a path with weight $a \otimes b$.

3

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



Note that the longest shortest path is (1, 0, 2, 3) of length 3 and weight 7.

(min,+) example

Our theorem tells us that $\mathbf{A}^* = \mathbf{A}^{(n-1)} = \mathbf{A}^{(4)}$

$$\mathbf{A}^{*} = \mathbf{A}^{(4)} = \mathbf{I} \min \mathbf{A} \min \mathbf{A}^{2} \min \mathbf{A}^{3} \min \mathbf{A}^{4} = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 0 & 2 & 1 & 5 & 4 \\ 1 & 2 & 0 & 3 & 7 & 4 \\ 1 & 3 & 0 & 4 & 3 \\ 3 & 5 & 7 & 4 & 0 & 7 \\ 4 & 4 & 3 & 7 & 0 \end{bmatrix}$$

2

L11: Algebraic Path Problems with applica

tgg22 (cl.cam.ac.uk)

 $(\min, +)$ example



First appearance of final value is in red and <u>underlined</u>. Remember: we are looking at all paths of a given length, even those with cycles!

A vs **A** ⊕ **I**

Lemma

If \oplus is idempotent, then

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

Proof. Base case: When k = 0 both expressions are I. Assume $(\mathbf{A} \oplus \mathbf{I})^k = \mathbf{A}^{(k)}$. Then

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

< 回 > < 回 > < 回 >

back to (min, +) example

$$(\mathbf{A} \oplus \mathbf{I})^{1} = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 0 & 2 & 1 & 6 & \infty \\ 2 & 0 & 5 & \infty & 4 \\ 1 & 5 & 0 & 4 & 3 & (\mathbf{A} \oplus \mathbf{I})^{3} &= \begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 0 & 2 & 1 & 5 & 4 \\ 2 & 0 & 3 & 7 & 4 \\ 1 & 3 & 0 & 4 & 3 \\ 6 & \infty & 4 & 0 & \infty \\ \infty & 4 & 3 & \infty & 0 \end{bmatrix}$$

$$(\mathbf{A} \oplus \mathbf{I})^{2} = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 0 & 2 & 1 & 5 & 4 \\ 2 & 0 & 3 & 8 & 4 \\ 1 & 3 & 0 & 4 & 3 \\ 5 & 8 & 4 & 0 & 7 \\ 4 & 4 & 3 & 7 & 0 \end{bmatrix}$$

æ

イロト イヨト イヨト イヨト

Semigroup properties (so far)



Recall that is right (IR) and is left (IL) are forced on us by wanting an \Leftrightarrow -rule for $SL((S, \bullet) \times (T, \diamond))$

Bisemigroup properties (so far)



T.G.Griffin © 2017 59 / 107

イロト 不得 トイヨト イヨト ニヨー

A Minimax Semiring

minimax \equiv (\mathbb{N}^{∞} , min, max, ∞ , **0**)

 $17 \min \infty = 17$

 $17 \max \infty = \infty$

How can we interpret this?

$$\mathbf{A}^*(i, j) = \min_{\boldsymbol{p} \in \pi(i, j)} \max_{(u, v) \in \boldsymbol{p}} \mathbf{A}(u, v),$$

tgg22 (cl.cam.ac.uk)

L11: Algebraic Path Problems with applica

T.G.Griffin@2017 60 / 107

▲□▶ ▲□▶ ▲□▶ ▲□▶ ▲□ ● のへで

One possible interpretation of Minimax

- Given an adjacency matrix A over minimax,
- suppose that $\mathbf{A}(i, j) = \mathbf{0} \Leftrightarrow i = j$,
- suppose that **A** is symmetric ($\mathbf{A}(i, j) = \mathbf{A}(j, i)$,
- interpret $\mathbf{A}(i, j)$ as <u>measured</u> dissimilarity of *i* and *j*,
- interpret $\mathbf{A}^*(i, j)$ as <u>inferred</u> dissimilarity of *i* and *j*,

Many uses

o ...

- Hierarchical clustering of large data sets
- Classification in Machine Learning
- Computational phylogenetics

< 口 > < 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 > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ >

Dendrograms



from **Hierarchical Clustering With Prototypes via Minimax Linkage**, Bien and Tibshirani, 2011.

tgg22 (cl.cam.ac.uk)

L11: Algebraic Path Problems with applica

T.G.Griffin@2017 62 / 107

A minimax graph



The solution A* drawn as a dendrogram



3 > 4 3

< A

Hierarchical clustering? Why?

Suppose $(Y, \leq, +)$ is a totally ordered with least element 0.

Metric

A <u>metric</u> for set *X* over $(Y, \leq, +)$ is a function $d \in X \times X \rightarrow Y$ such that

•
$$\forall x, y \in X, \ d(x, \ y) = 0 \Leftrightarrow x = y$$

•
$$\forall x, y \in X, d(x, y) = d(y, x)$$

•
$$\forall x, y, z \in X, \ d(x, \ y) \leq d(x, \ z) + d(z, \ y)$$

Ultrametric

An <u>ultrametric</u> for set X over (Y, \leq) is a function $d \in X \times X \rightarrow Y$ such that

•
$$\forall x \in X, \ d(x, x) = 0$$

•
$$\forall x, y \in X, \ d(x, \ y) = d(y, \ x)$$

• $\forall x, y, z \in X, \ d(x, \ y) \leq d(x, \ z) \max d(z, \ y)$

Fun Facts

Fact 5

If **A** is an $n \times n$ symmetric minimax adjacency matrix, then **A**^{*} is a finite ultrametric for $\{0, 1, ..., n-1\}$ over $(\mathbb{N}^{\infty}, \leq)$).

Fact 6

Suppose each arc weight is unique. Then the set of arcs

$$\{(i, j) \in \boldsymbol{E} \mid \boldsymbol{\mathsf{A}}(i, j) = \boldsymbol{\mathsf{A}}^*(i, j)\}$$

is a minimum spanning tree.

A spanning tree derived from **A** and **A***

