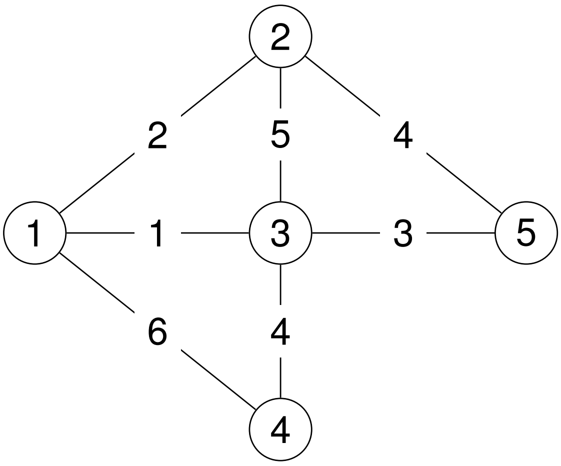
L11: Algebraic Path Problems with applications to Internet Routing

Timothy G. Griffin

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

Michaelmas Term, 2019

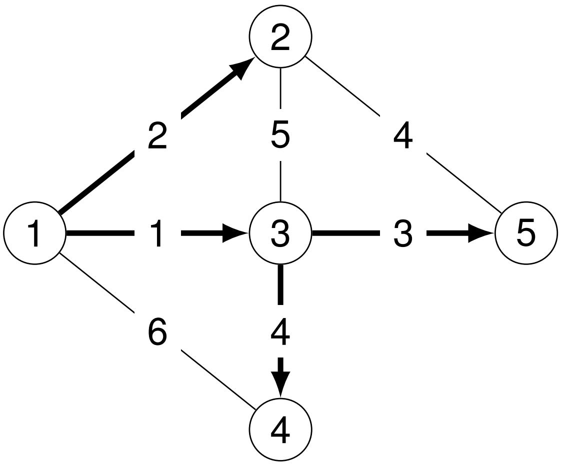
Shortest paths example, $\mathrm{sp} = (\mathbb{N}^{\infty},\ \min,\ +, \infty,\ 0)$



The adjacency matrix

$$
\mathbf{A} \;=\; \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{array}
\begin{array}{c} \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array} \\
\left[\begin{array}{ccccc}
\infty & 2 & 1 & 6 & \infty \\
2 & \infty & 5 & \infty & 4 \\
1 & 5 & \infty & 4 & 3 \\
6 & \infty & 4 & \infty & \infty \\
\infty & 4 & 3 & \infty & \infty
\end{array}\right] \end{array}
$$

Shortest paths solution



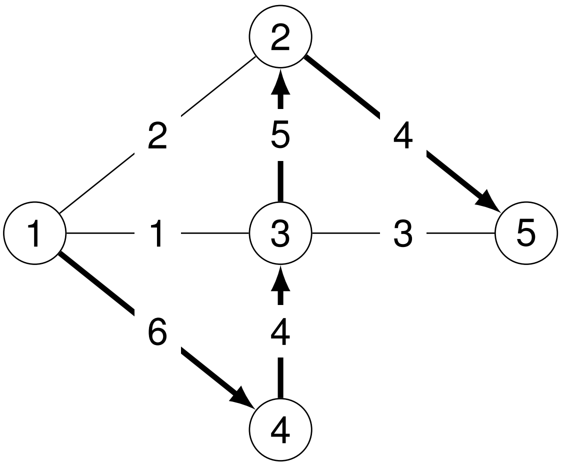
$$\mathbf{A}^* = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{array} \begin{array}{c} \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array} \\ \left[\begin{array}{ccccc} 0 & 2 & 1 & 5 & 4 \\ 2 & 0 & 3 & 7 & 4 \\ 1 & 3 & 0 & 4 & 3 \\ 5 & 7 & 4 & 0 & 7 \\ 4 & 4 & 3 & 7 & 0 \end{array} \right] \end{array}$$

solves this global optimality problem:

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

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

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



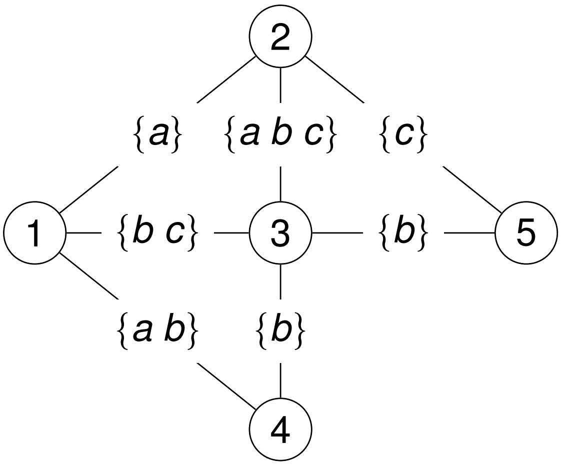
$$\mathbf{A}^* = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{array} \begin{array}{c} \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array} \\ \left[\begin{array}{ccccc} \infty & 4 & 4 & 6 & 4 \\ 4 & \infty & 5 & 4 & 4 \\ 4 & 5 & \infty & 4 & 4 \\ 6 & 4 & 4 & \infty & 4 \\ 4 & 4 & 4 & 4 & \infty \end{array} \right] \end{array}$$

solves this global optimality problem:

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

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

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



We want $\mathbf{A}^*$ to solve this global optimality problem:

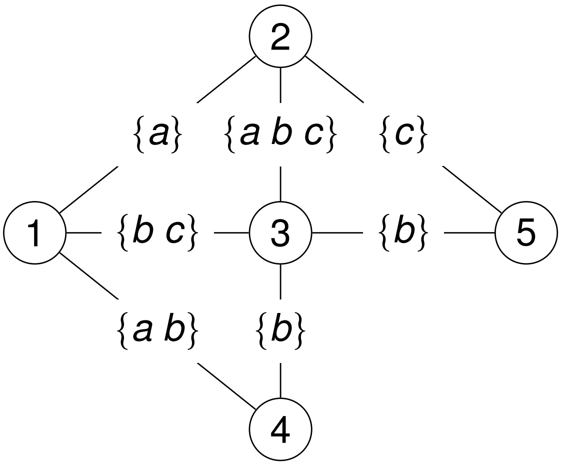
$$\mathbf{A}^*(i,\ j) = \bigcup_{p \in \pi(i,\ j)} w(p),$$

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

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

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

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



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

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

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

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

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

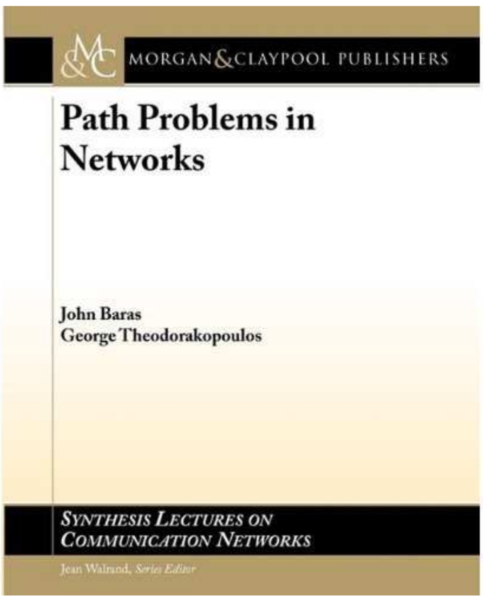
Semirings (generalise $(\mathbb{R}, +, \times, 0, 1)$)

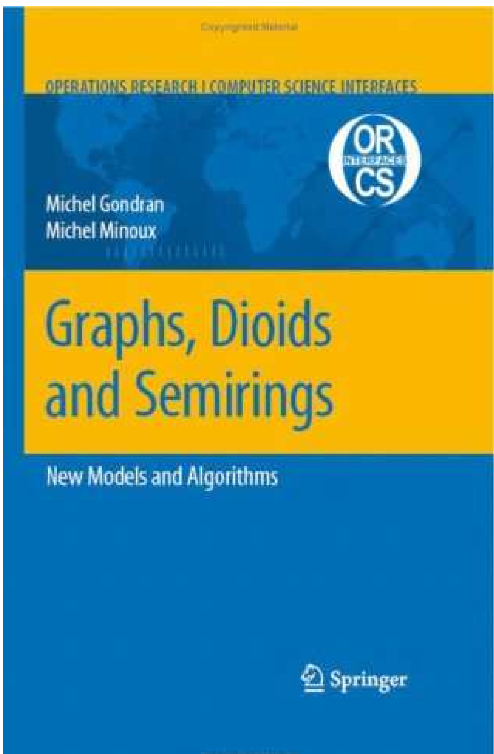
name	S	$\oplus$,	$\otimes$	$\overline{0}$	$\overline{1}$	possible routing use
sp	$\mathbb{N}^{\infty}$	min	$+$	∞	0	minimum-weight routing
bw	$\mathbb{N}^{\infty}$	max	min	0	∞	greatest-capacity routing
rel	$[0, 1]$	max	$\times$	0	1	most-reliable routing
use	$\{0, 1\}$	max	min	0	1	usable-path routing
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

Recommended (on reserve in CL library)





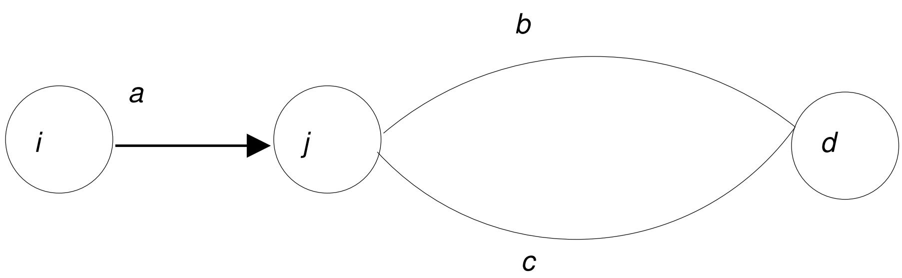
Semiring axioms ...

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

distributivity

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

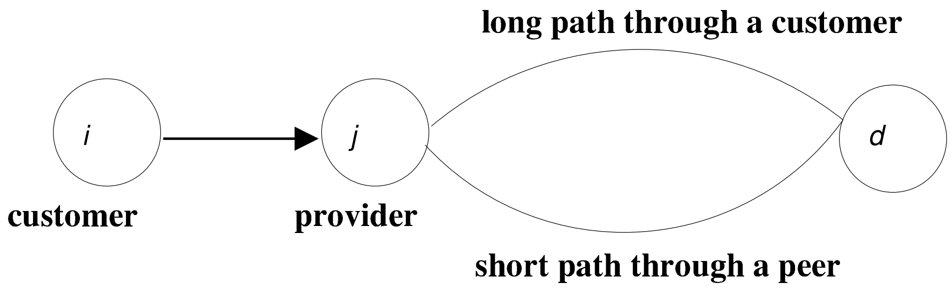
Distributivity, illustrated



$$a \otimes (b \oplus c) \quad = \quad (a \otimes b) \oplus (a \otimes c)$$

j makes the choice $=$ i makes the choice

Should distributivity hold in Internet Routing?

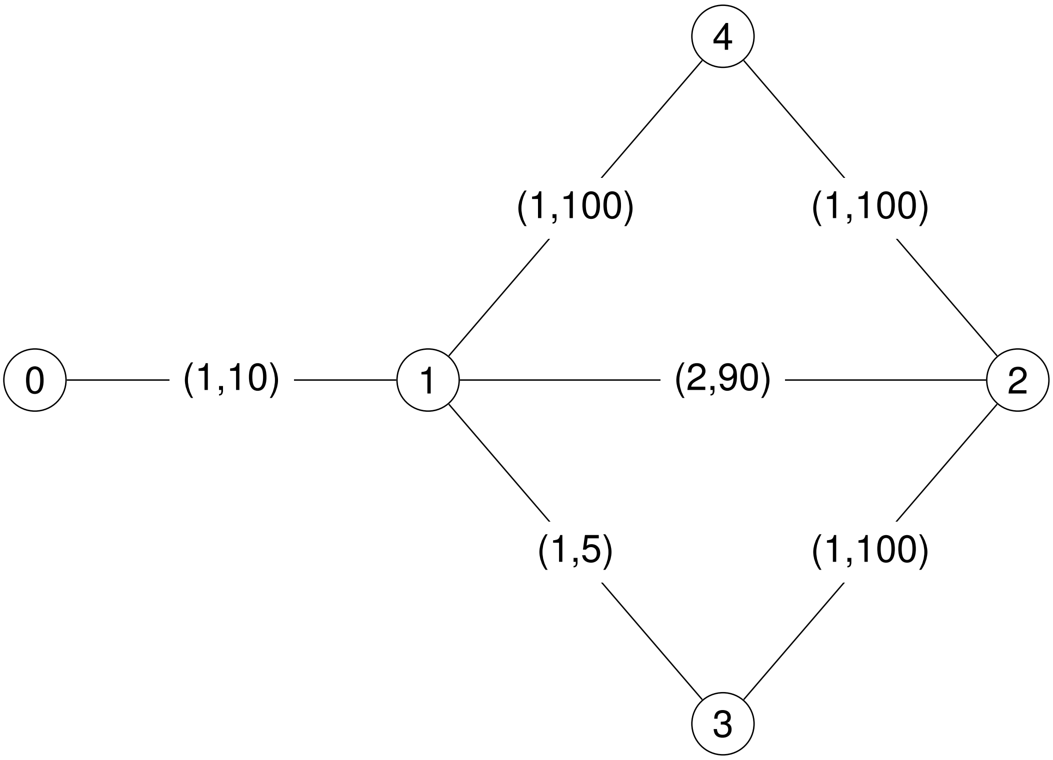


- *j* prefers long path though one of its customers (not the shorter path through a competitor)
- given two routes from a provider, *i* prefers the one with a shorter path
- More on inter-domain routing in the Internet later in the term ...

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.

Widest shortest-paths



Weights are globally optimal (we have a semiring)

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

R =

	0	1	2	3	4
0	$(0, \infty)$	$(1, 10)$	$(3, 10)$	$(2, 5)$	$(2, 10)$
1	$(1, 10)$	$(0, \infty)$	$(2, 100)$	$(1, 5)$	$(1, 100)$
2	$(3, 10)$	$(2, 100)$	$(0, \infty)$	$(1, 100)$	$(1, 100)$
3	$(2, 5)$	$(1, 5)$	$(1, 100)$	$(0, \infty)$	$(2, 100)$
4	$(2, 10)$	$(1, 100)$	$(1, 100)$	$(2, 100)$	$(0, \infty)$

But what about the paths themselves?

Four optimal paths of weight $(3, 10)$.

$$\mathbf{P}_{\text{optimal}}(0,2) = \{(0,1,2),\ (0,1,4,2)\}$$
$$\mathbf{P}_{\text{optimal}}(2,0) = \{(2,1,0),\ (2,4,1,0)\}$$

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

Do these extended algorithms find all optimal paths?

Surprise!

Four optimal paths of weight $(3, 10)$

$$\mathbf{P}_{\text{optimal}}(0,2) = \{(0,1,2),\ (0,1,4,2)\}$$
$$\mathbf{P}_{\text{optimal}}(2,0) = \{(2,1,0),\ (2,4,1,0)\}$$

Paths computed by (extended) Dijkstra

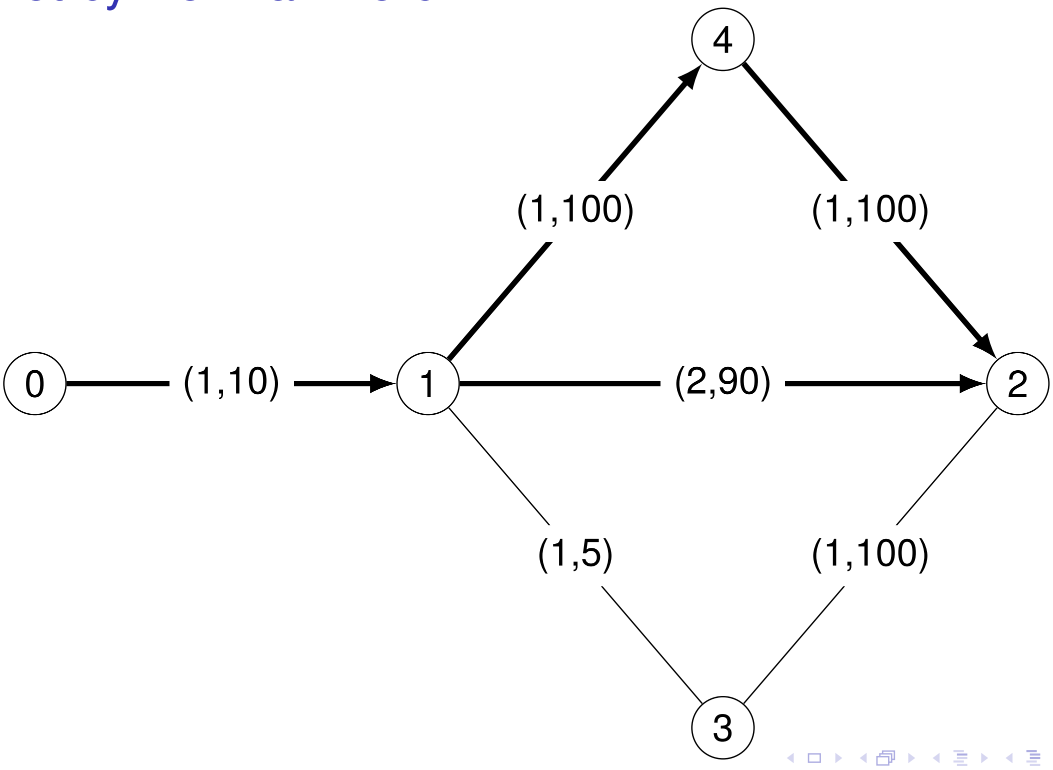
$$\mathbf{P}_{\text{Dijkstra}}(0,2) = \{(0,1,2),\ (0,1,4,2)\}$$
$$\mathbf{P}_{\text{Dijkstra}}(2,0) = \{(2,4,1,0)\}$$

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

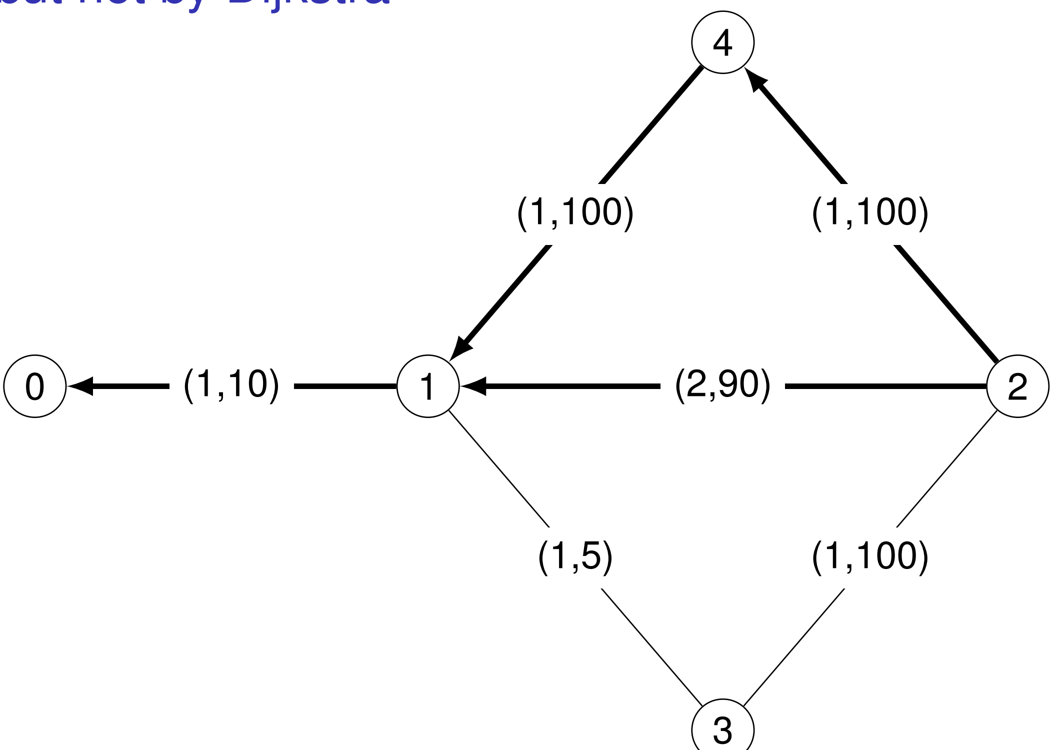
Paths computed by distributed Bellman-Ford

$$\mathbf{P}_{\text{Bellman}}(0,2) = \{(0,1,4,2)\}$$
$$\mathbf{P}_{\text{Bellman}}(2,0) = \{(2,1,0),\ (2,4,1,0)\}$$

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



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



How can we understand this (algebaically)?

The Algorithm to Algebra (A2A) method

$$\left(\begin{array}{c}\text{original metric} \\ + \\ \text{complex algorithm}\end{array}\right) \rightarrow \left(\begin{array}{c}\text{modified metric} \\ + \\ \text{matrix equations (generic algorithm)}\end{array}\right)$$

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! ($a \min b = a \min c$ does not imply that $b = c$)

Towards a non-classical theory of algebraic path finding

We need theory that can accept algebras that violate distributivity.

Global optimality

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

Left local optimality (distributed Bellman-Ford)

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

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.

Lectures 2, 3

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

Semigroups

Semigroup

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

$$\mathbb{AS} \quad \text{associative} \quad \equiv \quad \forall a, b, c \in S, \; a \bullet (b \bullet c) = (a \bullet b) \bullet c$$

Important Assumption — We will ignore trival semigroups

We will impicitly assume that $2 \leqslant \mid S \mid$.

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	$\equiv$	$\exists \alpha \in S,\ \forall a \in S,\ a = \alpha \bullet a = a \bullet \alpha$
$\mathbb{AN}$	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

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

A few concrete semigroups

S	$\bullet$	description	α	ω	$\mathbb{CM}$	$\mathbb{SL}$	$\mathbb{IP}$
S	left	x left $y = x$				$\star$	$\star$
S	right	x right $y = y$				$\star$	$\star$
S^*	$\cdot$	concatenation	ϵ				
S^+	$\cdot$	concatenation					
$\{t,\ f\}$	$\wedge$	conjunction	t	f	$\star$	$\star$	$\star$
$\{t,\ f\}$	$\vee$	disjunction	f	t	$\star$	$\star$	$\star$
$\mathbb{N}$	min	minimum		0	$\star$	$\star$	$\star$
$\mathbb{N}$	max	maximum	0		$\star$	$\star$	$\star$
2^W	$\cup$	union	$\{\}$	W	$\star$		$\star$
2^W	$\cap$	intersection	W	$\{\}$	$\star$		$\star$
$\text{fin}(2^U)$	$\cup$	union	$\{\}$		$\star$		$\star$
$\text{fin}(2^U)$	$\cap$	intersection		$\{\}$	$\star$		$\star$
$\mathbb{N}$	$+$	addition	0		$\star$		
$\mathbb{N}$	$\times$	multiplication	1	0	$\star$		

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

A few abstract semigroups

S	$\bullet$	description	α	ω	$\mathbb{CM}$	$\mathbb{SL}$	$\mathbb{IP}$
2^U	$\cup$	union	$\{\}$	U	$\star$		$\star$
2^U	$\cap$	intersection	U	$\{\}$	$\star$		$\star$
$2^{U\times U}$	$\bowtie$	relational join	$\mathcal{I}_U$	$\{\}$			
$X \to X$	$\circ$	composition	$\lambda x.x$				

U an infinite set
$X \bowtie Y \equiv \{(x, z) \in U \times U \mid \exists y \in U,\ (x,\ y) \in X \wedge (y,\ z) \in Y\}$
$\mathcal{I}_U \equiv \{(u,\ u) \mid u \in U\}$

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 $\leqslant \subseteq\ S \times S$

Definition (Important Order Properties)

$$\begin{array}{llcl} \mathbb{RX} & \text{reflexive} & \equiv & a \leqslant a \\ \mathbb{TR} & \text{transitive} & \equiv & a \leqslant b \wedge b \leqslant c \to a \leqslant c \\ \mathbb{AY} & \text{antisymmetric} & \equiv & a \leqslant b \wedge b \leqslant a \to a = b \\ \mathbb{TO} & \text{total} & \equiv & a \leqslant b \vee b \leqslant a \end{array}$$

	pre-order	partial order	preference order	total order
$\mathbb{RX}$	$\star$	$\star$	$\star$	$\star$
$\mathbb{TR}$	$\star$	$\star$	$\star$	$\star$
$\mathbb{AY}$		$\star$		$\star$
$\mathbb{TO}$			$\star$	$\star$

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 $\bullet$ implies that these relations are transitive.

Proof.

Note that $a \trianglelefteq^R_\bullet b$ means $\exists c_1 \in S : b = a \bullet c_1$, and $b \trianglelefteq^R_\bullet c$ 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 $a \trianglelefteq^R_\bullet c$. The proof for $\trianglelefteq^L_\bullet$ is similar. □

Canonically Ordered Semigroup

Definition (Canonically Ordered Semigroup)

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

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 $a \trianglelefteq^{L}_{\bullet} b$. In a similar way, $b \trianglelefteq^{R}_{\bullet} a$. Therefore $a = b$. □

Natural Orders

Definition (Natural orders)

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

$$a \leqslant^{L}_{\bullet} b \quad \equiv \quad a = a \bullet b$$
$$a \leqslant^{R}_{\bullet} b \quad \equiv \quad b = a \bullet b$$

Lemma

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

Proof.

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

□

Special elements and natural orders

Lemma (Natural Bounds)

- *If α exists, then for all a, a $\leqslant^L_\bullet$ α and α $\leqslant^R_\bullet$ a*
- *If ω exists, then for all a, ω $\leqslant^L_\bullet$ a and a $\leqslant^R_\bullet$ ω*
- *If α and ω exist, then S is bounded.*

$$\begin{array}{ccccc} \omega & \leqslant^L_\bullet & a & \leqslant^L_\bullet & \alpha \\ \alpha & \leqslant^R_\bullet & a & \leqslant^R_\bullet & \omega \end{array}$$

Remark (Thanks to Iljitsch van Beijnum)

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

$$\begin{array}{ccccc} 0 & \leqslant^L_{\min} & a & \leqslant^L_{\min} & \infty \\ \infty & \leqslant^R_{\min} & a & \leqslant^R_{\min} & 0 \end{array}$$

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

Examples of special elements

S	$\bullet$	α	ω	$\leqslant^L_\bullet$	$\leqslant^R_\bullet$
$\mathbb{N}^{\infty}$	min	∞	0	$\leqslant$	$\geqslant$
$\mathbb{N}^{-\infty}$	max	0	$-\infty$	$\geqslant$	$\leqslant$
$\mathcal{P}(W)$	$\cup$	$\{\}$	W	$\subseteq$	$\supseteq$
$\mathcal{P}(W)$	$\cap$	W	$\{\}$	$\supseteq$	$\subseteq$

Property Management

Lemma

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

1. $\mathbb{IP}(S,\ \bullet) \iff \mathbb{RX}(S,\ \leqslant^D_\bullet)$
2. $\mathbb{CM}(S,\ \bullet) \implies \mathbb{AY}(S,\ \leqslant^D_\bullet)$
3. $\mathbb{AS}(S,\ \bullet) \implies \mathbb{TR}(S,\ \leqslant^D_\bullet)$
4. $\mathbb{CM}(S,\ \bullet) \implies (\mathbb{SL}(S,\ \bullet) \iff \mathbb{TO}(S,\ \leqslant^D_\bullet))$

Proof.

1. $a \leqslant^D_\bullet a \iff a = a \bullet a$,
2. $a \leqslant^L_\bullet b \wedge b \leqslant^L_\bullet a \iff a = a \bullet b \wedge b = b \bullet a \implies a = b$
3. $a \leqslant^L_\bullet b \wedge b \leqslant^L_\bullet c \iff a = a \bullet b \wedge b = b \bullet c \implies a = a \bullet (b \bullet c) = (a \bullet b) \bullet c = a \bullet c \implies a \leqslant^L_\bullet c$
4. $a = a \bullet b \vee b = a \bullet b \iff a \leqslant^L_\bullet b \vee b \leqslant^L_\bullet a$

□

Bounds

Suppose $(S,\ \leqslant)$ 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 $c = a \text{ glb } b$, if it is a lower bound ($c \leqslant a$ and $c \leqslant b$), and for every $d \in S$ with $d \leqslant a$ and $d \leqslant b$, we have $d \leqslant c$.

least upper bound

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

Semi-lattices

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

meet-semilattice

S is a meet-semilattice if $a \, \mathrm{glb} \, b$ exists for each $a, b \in S$.

join-semilattice

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

Fun Facts

Fact 1

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

- $(S, \leqslant^L_\bullet)$ is a meet-semilattice with $a \, \mathrm{glb} \, b = a \bullet b$.
- $(S, \leqslant^R_\bullet)$ is a join-semilattice with $a \, \mathrm{lub} \, b = a \bullet b$.

Fact 2

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

- If $(S, \leqslant)$ is a meet-semilattice, then (S, glb) is a commutative and idempotent semigroup.
- If $(S, \leqslant)$ 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.

Lecture 3

- Semirings
- Matrix semirings
- Shortest paths
- Minimax

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,

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

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....

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!

Fix that ...

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

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

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

J and I

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

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

Associativity

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

$$\begin{array}{lll}
& (\mathbf{A} \otimes (\mathbf{B} \otimes \mathbf{C}))(i,\ j) & \\
= & \bigoplus_{1 \leqslant u \leqslant n} \mathbf{A}(i,\ u) \otimes (\mathbf{B} \otimes \mathbf{C})(u,\ j) & (\text{def} \rightarrow) \\
= & \bigoplus_{1 \leqslant u \leqslant n} \mathbf{A}(i,\ u) \otimes (\bigoplus_{1 \leqslant v \leqslant n} \mathbf{B}(u,\ v) \otimes \mathbf{C}(v,\ j)) & (\text{def} \rightarrow) \\
= & \bigoplus_{1 \leqslant u \leqslant n} \bigoplus_{1 \leqslant v \leqslant n} \mathbf{A}(i,\ u) \otimes (\mathbf{B}(u,\ v) \otimes \mathbf{C}(v,\ j)) & (\mathbb{LD}) \\
= & \bigoplus_{1 \leqslant v \leqslant n} \bigoplus_{1 \leqslant u \leqslant n} (\mathbf{A}(i,\ u) \otimes \mathbf{B}(u,\ v)) \otimes \mathbf{C}(v,\ j) & (\mathbb{AS}, \mathbb{CM}) \\
= & \bigoplus_{1 \leqslant v \leqslant n} (\bigoplus_{1 \leqslant u \leqslant n} \mathbf{A}(i,\ u) \otimes \mathbf{B}(u,\ v)) \otimes \mathbf{C}(v,\ j) & (\mathbb{RD}) \\
= & \bigoplus_{1 \leqslant v \leqslant n} (\mathbf{A} \otimes \mathbf{B})(i,\ v) \otimes \mathbf{C}(v,\ j) & (\text{def} \leftarrow) \\
= & ((\mathbf{A} \otimes \mathbf{B}) \otimes \mathbf{C})(i,\ j) & (\text{def} \leftarrow)
\end{array}$$

Left Distributivity

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

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

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 path weights

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

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

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

How can we solve this problem?

Stability

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

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

Matrix methods

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

$$\begin{aligned} \mathbf{A}^0 &= \mathbf{I} \\ \mathbf{A}^{k+1} &= \mathbf{A} \otimes \mathbf{A}^k \end{aligned}$$

Closure, $\mathbf{A}^*$

$$\begin{aligned} \mathbf{A}^{(k)} &= \mathbf{I} \oplus \mathbf{A}^1 \oplus \mathbf{A}^2 \oplus \cdots \oplus \mathbf{A}^k \\ \mathbf{A}^* &= \mathbf{I} \oplus \mathbf{A}^1 \oplus \mathbf{A}^2 \oplus \cdots \oplus \mathbf{A}^k \oplus \cdots \end{aligned}$$

Note: $\mathbf{A}^*$ might not exist. Why?

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

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

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: $k = 0$.

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

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

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

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

Proof of (1)

Induction step.

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

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,

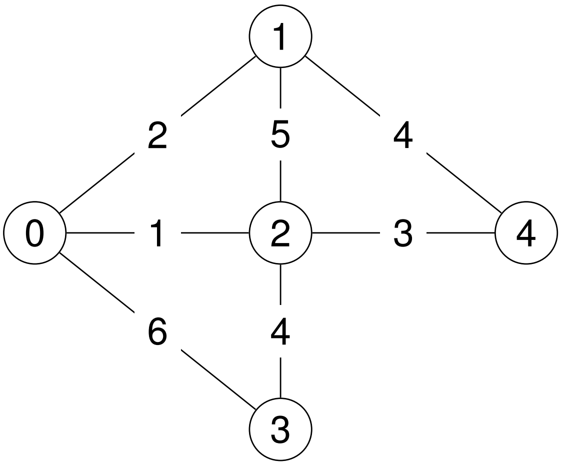
$$\mathbf{A}^* = \mathbf{A}^{(n-1)} = \mathbf{I} \oplus \mathbf{A}^1 \oplus \mathbf{A}^2 \oplus \cdots \oplus \mathbf{A}^{n-1}$$

Why? Because we can ignore paths with loops.

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

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

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



The adjacency matrix

$$\mathbf{A} = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \\ 4 \end{array} \begin{array}{c} \begin{array}{ccccc} 0 & 1 & 2 & 3 & 4 \end{array} \\ \left[\begin{array}{ccccc} \infty & 2 & 1 & 6 & \infty \\ 2 & \infty & 5 & \infty & 4 \\ 1 & 5 & \infty & 4 & 3 \\ 6 & \infty & 4 & \infty & \infty \\ \infty & 4 & 3 & \infty & \infty \end{array}\right] \end{array}$$

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

$(\text{min}, +)$ example

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

$$\mathbf{A}^* = \mathbf{A}^{(4)} = \mathbf{I} \text{ min } \mathbf{A} \text{ min } \mathbf{A}^2 \text{ min } \mathbf{A}^3 \text{ min } \mathbf{A}^4 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \\ 4 \end{array} \begin{array}{c} \begin{array}{ccccc} 0 & 1 & 2 & 3 & 4 \end{array} \\ \left[\begin{array}{ccccc} 0 & 2 & 1 & 5 & 4 \\ 2 & 0 & 3 & 7 & 4 \\ 1 & 3 & 0 & 4 & 3 \\ 5 & 7 & 4 & 0 & 7 \\ 4 & 4 & 3 & 7 & 0 \end{array}\right] \end{array}$$

$(\min, +)$ example

$$\mathbf{A} = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \\ 4 \end{array} \begin{array}{c} \begin{array}{ccccc} 0 & 1 & 2 & 3 & 4 \end{array} \\ \left[\begin{array}{ccccc} \infty & \underline{2} & \underline{1} & 6 & \infty \\ \underline{2} & \infty & 5 & \infty & \underline{4} \\ \underline{1} & 5 & \infty & \underline{4} & \underline{3} \\ 6 & \infty & \underline{4} & \infty & \infty \\ \infty & \underline{4} & \underline{3} & \infty & \infty \end{array}\right] \end{array} \quad \mathbf{A}^3 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \\ 4 \end{array} \begin{array}{c} \begin{array}{ccccc} 0 & 1 & 2 & 3 & 4 \end{array} \\ \left[\begin{array}{ccccc} 8 & 4 & 3 & 8 & 10 \\ 4 & 8 & 7 & \underline{7} & 6 \\ 3 & 7 & 8 & 6 & 5 \\ 8 & \underline{7} & 6 & 11 & 10 \\ 10 & 6 & 5 & 10 & 12 \end{array}\right] \end{array}$$

$$\mathbf{A}^2 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \\ 4 \end{array} \begin{array}{c} \begin{array}{ccccc} 0 & 1 & 2 & 3 & 4 \end{array} \\ \left[\begin{array}{ccccc} 2 & 6 & 7 & \underline{5} & \underline{4} \\ 6 & 4 & \underline{3} & 8 & 8 \\ 7 & \underline{3} & 2 & 7 & 9 \\ \underline{5} & 8 & 7 & 8 & \underline{7} \\ \underline{4} & 8 & 9 & \underline{7} & 6 \end{array}\right] \end{array} \quad \mathbf{A}^4 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \\ 4 \end{array} \begin{array}{c} \begin{array}{ccccc} 0 & 1 & 2 & 3 & 4 \end{array} \\ \left[\begin{array}{ccccc} 4 & 8 & 9 & 7 & 6 \\ 8 & 6 & 5 & 10 & 10 \\ 9 & 5 & 4 & 9 & 11 \\ 7 & 10 & 9 & 10 & 9 \\ 6 & 10 & 11 & 9 & 8 \end{array}\right] \end{array}$$

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

$\mathbf{A}$ vs $\mathbf{A} \oplus \mathbf{I}$

Lemma

If $\oplus$ is idempotent, then

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

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

$$\begin{array}{rcl} (\mathbf{A} \oplus \mathbf{I})^{k+1} & = & (\mathbf{A} \oplus \mathbf{I})(\mathbf{A} \oplus \mathbf{I})^k \\ & = & (\mathbf{A} \oplus \mathbf{I})\mathbf{A}^{(k)} \\ & = & \mathbf{A}\mathbf{A}^{(k)} \oplus \mathbf{A}^{(k)} \\ & = & \mathbf{A}(\mathbf{I} \oplus \mathbf{A} \oplus \cdots \oplus \mathbf{A}^k) \oplus \mathbf{A}^{(k)} \\ & = & \mathbf{A} \oplus \mathbf{A}^2 \oplus \cdots \oplus \mathbf{A}^{k+1} \oplus \mathbf{A}^{(k)} \\ & = & \mathbf{A}^{k+1} \oplus \mathbf{A}^{(k)} \\ & = & \mathbf{A}^{(k+1)} \end{array}$$

back to $(\min, +)$ example

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

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

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

Semigroup properties (so far)

$$\begin{array}{rcl}
\mathbb{AS}(S,\ \bullet) & \equiv & \forall a, b, c \in S,\ a \bullet (b \bullet c) = (a \bullet b) \bullet c \\
\mathbb{IID}(S,\ \bullet,\ \alpha) & \equiv & \forall a \in S,\ a = \alpha \bullet a = a \bullet \alpha \\
\mathbb{ID}(S,\ \bullet) & \equiv & \exists \alpha \in S,\ \mathbb{IID}(S,\ \bullet,\ \alpha) \\
\mathbb{IAN}(S,\ \bullet,\ \omega) & \equiv & \forall a \in S,\ \omega = \omega \bullet a = a \bullet \omega \\
\mathbb{AN}(S,\ \bullet) & \equiv & \exists \omega \in S,\ \mathbb{IAN}(S,\ \bullet,\ \omega) \\
\mathbb{CM}(S,\ \bullet) & \equiv & \forall a, b \in S,\ a \bullet b = b \bullet a \\
\mathbb{SL}(S,\ \bullet) & \equiv & \forall a, b \in S,\ a \bullet b \in \{a,\ b\} \\
\mathbb{IP}(S,\ \bullet) & \equiv & \forall a \in S,\ a \bullet a = a \\
\mathbb{IR}(S,\ \bullet) & \equiv & \forall s, t \in S, s \bullet t = t \\
\mathbb{IL}(S,\ \bullet) & \equiv & \forall s, t \in S, s \bullet t = s
\end{array}$$

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

Bisemigroup properties (so far)

$$
\begin{array}{rcl}
\mathbb{AAS}(S,\ \oplus,\ \otimes) & \equiv & \mathbb{AS}(S,\ \oplus) \\
\mathbb{AID}(S,\ \oplus,\ \otimes) & \equiv & \mathbb{ID}(S,\ \oplus) \\
\mathbb{ACM}(S,\ \oplus,\ \otimes) & \equiv & \mathbb{CM}(S,\ \oplus) \\
\mathbb{MAS}(S,\ \oplus,\ \otimes) & \equiv & \mathbb{AS}(S,\ \otimes) \\
\mathbb{MID}(S,\ \oplus,\ \otimes) & \equiv & \mathbb{ID}(S,\ \otimes) \\
\mathbb{LD}(S,\ \oplus,\ \otimes) & \equiv & \forall a, b, c \in S,\ a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c) \\
\mathbb{RD}(S,\ \oplus,\ \otimes) & \equiv & \forall a, b, c \in S,\ (a \oplus b) \otimes c = (a \otimes c) \oplus (b \otimes c) \\
\mathbb{ZA}(S,\ \oplus,\ \otimes) & \equiv & \exists \overline{0} \in S,\ \mathbb{IID}(S,\ \oplus,\ \overline{0}) \wedge \mathbb{IAN}(S,\ \otimes,\ \overline{0}) \\
\hline
\mathbb{OA}(S,\ \oplus,\ \otimes) & \equiv & \exists \overline{1} \in S,\ \mathbb{IID}(S,\ \otimes,\ \overline{1}) \wedge \mathbb{IAN}(S,\ \oplus,\ \overline{1}) \\
\mathbb{ASL}(S,\ \oplus,\ \otimes) & \equiv & \mathbb{SL}(S,\ \oplus) \\
\mathbb{AIP}(S,\ \oplus,\ \otimes) & \equiv & \mathbb{IP}(S,\ \oplus)
\end{array}
$$

A Minimax Semiring

$$\text{minimax} \equiv (\mathbb{N}^{\infty},\ \min,\ \max,\ \infty,\ 0)$$

$$17 \min \infty = 17$$

$$17 \max \infty = \infty$$

How can we interpret this?

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

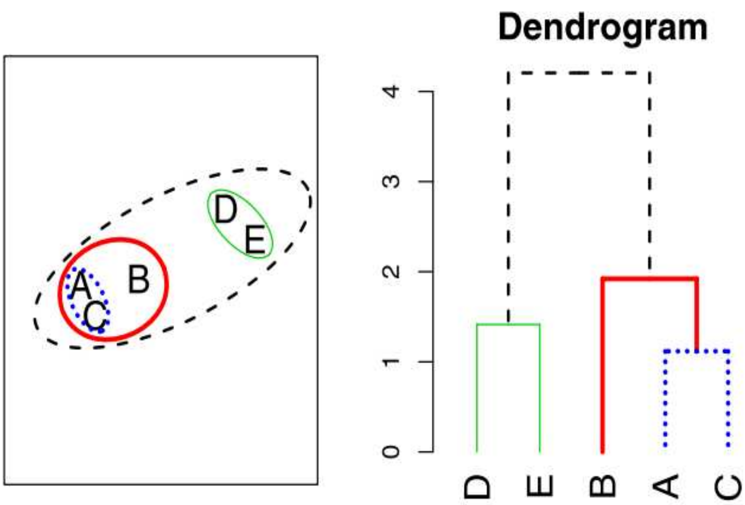
One possible interpretation of Minimax

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

Many uses

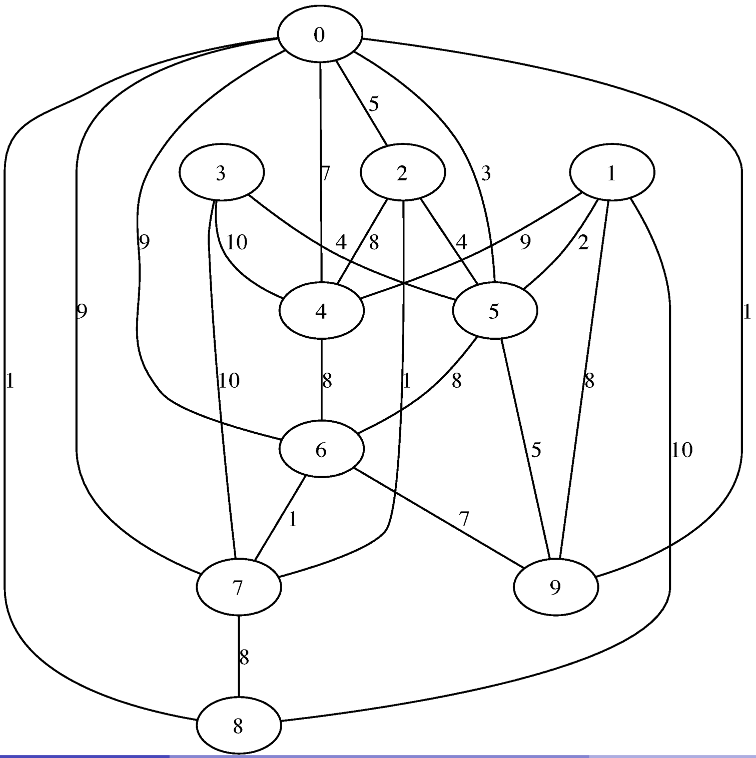
- Hierarchical clustering of large data sets
- Classification in Machine Learning
- Computational phylogenetics
- ...

Dendrograms

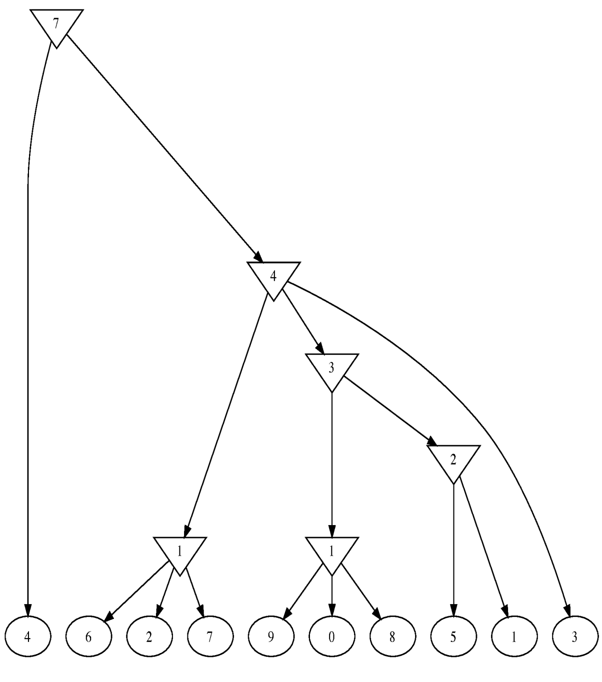


from **Hierarchical Clustering With Prototypes via Minimax Linkage**, Bien and Tibshirani, 2011.

A minimax graph



The solution $\mathbf{A}^*$ drawn as a dendrogram



Hierarchical clustering? Why?

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

Metric

A metric for set X over $(Y, \leqslant, +)$ is a function $d \in X \times X \rightarrow Y$ such that

- $\forall x, y \in X,\ d(x, y) = 0 \Leftrightarrow x = y$
- $\forall x, y \in X,\ d(x, y) = d(y, x)$
- $\forall x, y, z \in X,\ d(x, y) \leqslant d(x, z) + d(z, y)$

Ultrametric

An ultrametric for set X over $(Y, \leqslant)$ is a function $d \in X \times X \rightarrow Y$ such that

- $\forall x \in X,\ d(x, x) = 0$
- $\forall x, y \in X,\ d(x, y) = d(y, x)$
- $\forall x, y, z \in X,\ d(x, y) \leqslant d(x, z) \max d(z, y)$

Fun Facts

Fact 5

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

Fact 6

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

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

is a minimum spanning tree.

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