

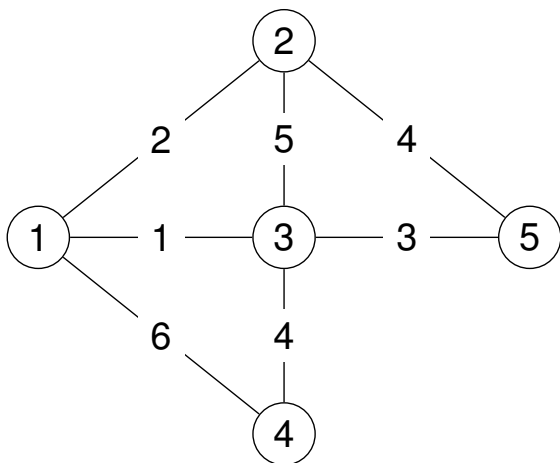
L11: Algebraic Path Problems with applications to Internet Routing Lectures 01 – 03

Timothy G. Griffin

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

Michaelmas Term, 2017

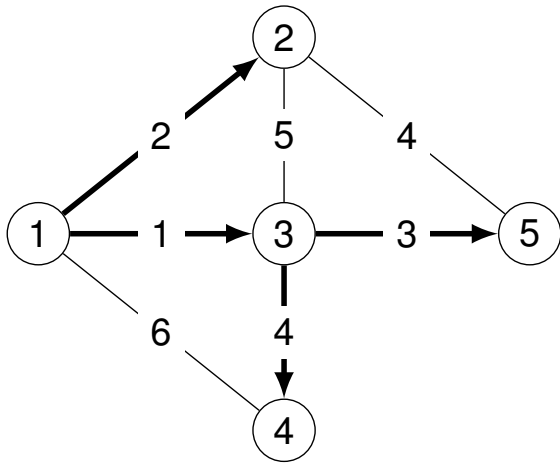
Shortest paths example, $sp = (\mathbb{N}^\infty, \min, +, \infty, 0)$



The adjacency matrix

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

Shortest paths solution



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

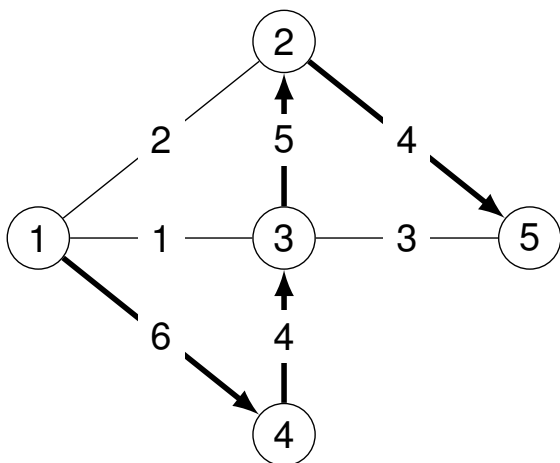
solves this **global optimality** problem:

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

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

Navigation icons: back, forward, search, etc.

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



$$\mathbf{A}^* = \begin{matrix} & \begin{matrix} 1 & 2 & 3 & 4 & 5 \end{matrix} \\ \begin{matrix} 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{matrix} & \begin{bmatrix} \infty & 4 & 4 & 6 & 4 \\ 4 & \infty & 5 & 4 & 4 \\ 4 & 5 & \infty & 4 & 4 \\ 6 & 4 & 4 & \infty & 4 \\ 4 & 4 & 4 & 4 & \infty \end{bmatrix} \end{matrix}$$

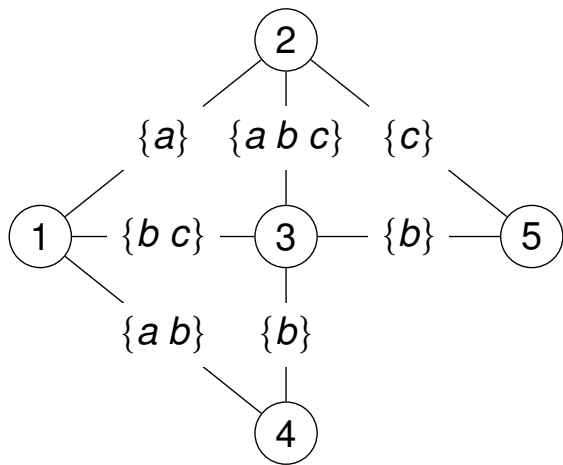
solves this global optimality problem:

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

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

Navigation icons: back, forward, search, etc.

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



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

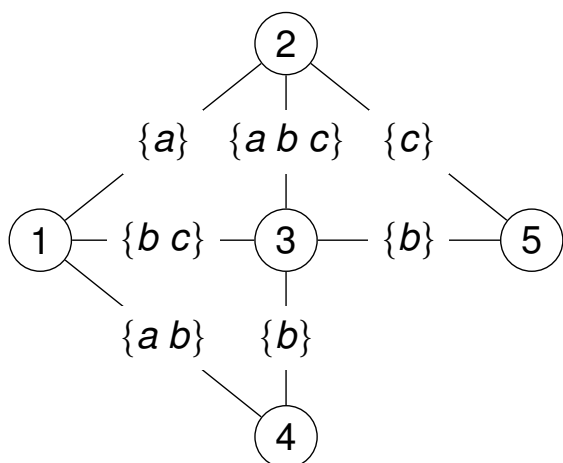
$$\mathbf{A}^*(i, j) = \bigcup_{p \in P(i, j)} w(p),$$

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

For $x \in \{a, b, c\}$, interpret $x \in \mathbf{A}^*(i, j)$ 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 \mathbf{R} to solve this global optimality problem:

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

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

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

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

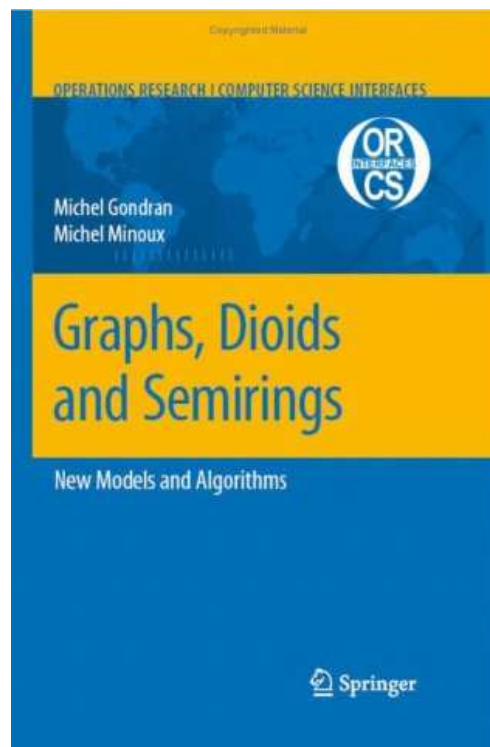
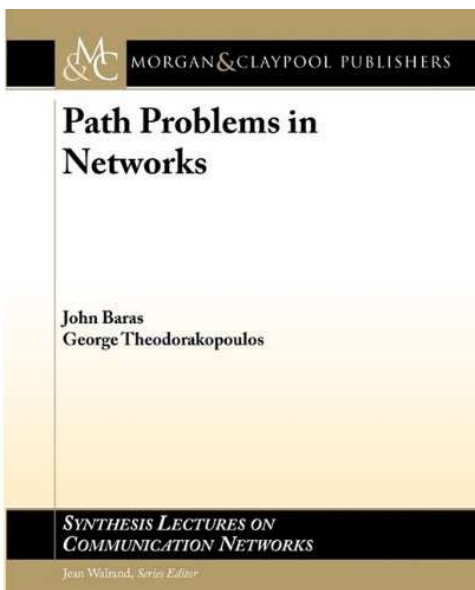
Semirings (generalise $(\mathbb{R}, +, \times, 0, 1)$)

name	S	$\oplus,$	\otimes	$\bar{0}$	$\bar{1}$	possible routing use
sp	\mathbb{N}^∞	min	+	∞	0	minimum-weight routing
bw	\mathbb{N}^∞	max	min	0	∞	greatest-capacity routing
rel	$[0, 1]$	max	\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}^∞	Natural numbers, plus infinity
$\bar{0}$	Identity for \oplus
$\bar{1}$	Identity for \otimes

Recommended (on reserve in CL library)



Semiring axioms ...

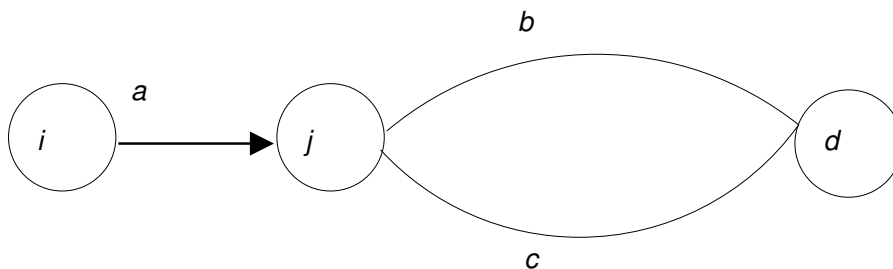
We will look at all of the axioms of semirings, but the most important are

distributivity

$$\text{LD} : a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$$

$$\text{RD} : (a \oplus b) \otimes c = (a \otimes c) \oplus (b \otimes c)$$

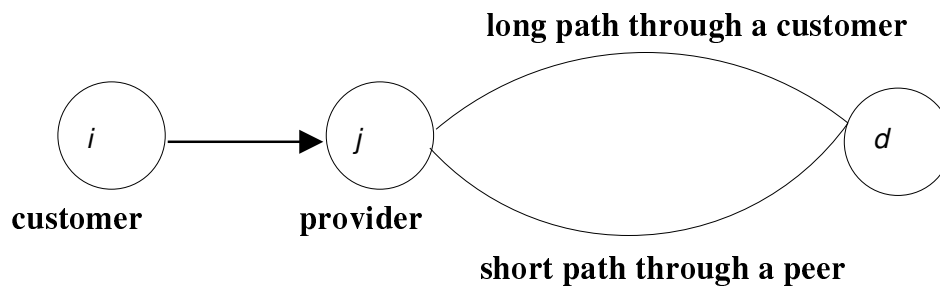
Distributivity, illustrated



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

j makes the choice = i makes the choice

Should distributivity hold in Internet Routing?

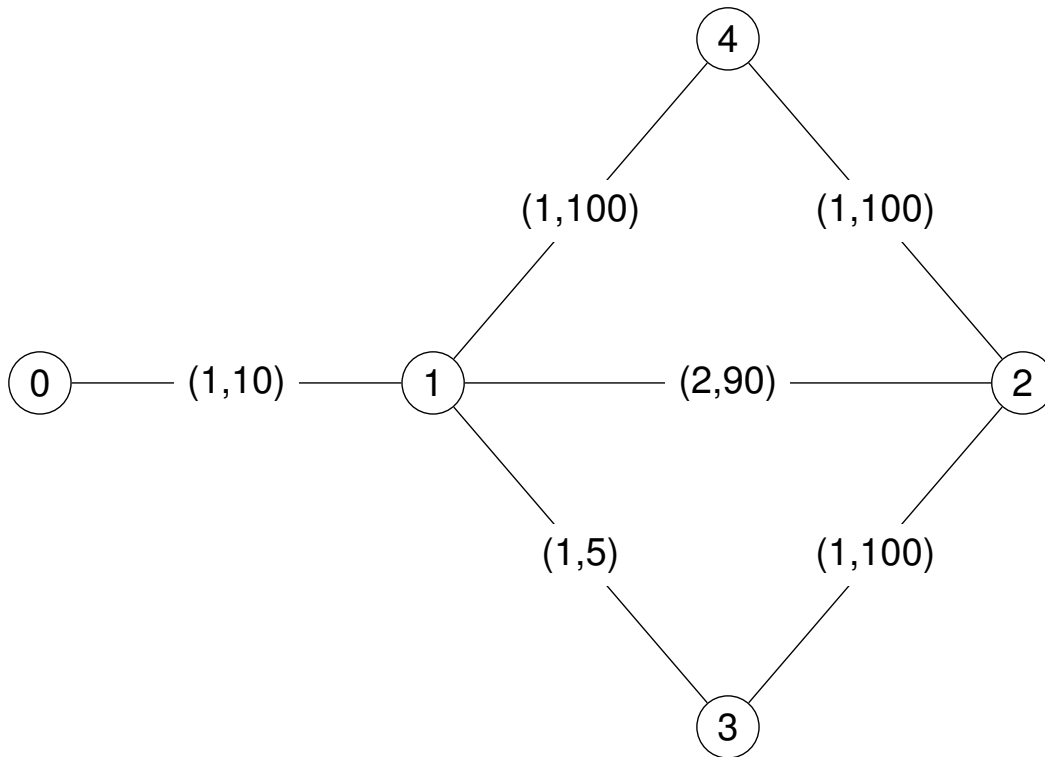


- *j* prefers long path through one of its customers (not the shorter path through a competitor)
- given two routes from a provider, *i* prefers the one with a shorter path
- More on inter-domain routing in the Internet later in the term ...

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



Navigation icons: back, forward, search, etc.

Weights are globally optimal (we have a semiring)

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

$$\mathbf{R} = \begin{matrix} & \begin{matrix} 0 & 1 & 2 & 3 & 4 \end{matrix} \\ \begin{matrix} 0 \\ 1 \\ 2 \\ 3 \\ 4 \end{matrix} & \left[\begin{array}{ccccc} (0, \infty) & (1, 10) & (3, 10) & (2, 5) & (2, 10) \\ (1, 10) & (0, \infty) & (2, 100) & (1, 5) & (1, 100) \\ (3, 10) & (2, 100) & (0, \infty) & (1, 100) & (1, 100) \\ (2, 5) & (1, 5) & (1, 100) & (0, \infty) & (2, 100) \\ (2, 10) & (1, 100) & (1, 100) & (2, 100) & (0, \infty) \end{array} \right] \end{matrix}$$

Navigation icons: back, forward, search, etc.

But what about the paths themselves?

Four optimal paths of weight (3, 10).

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

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)

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

Paths computed by (extended) **Dijkstra**

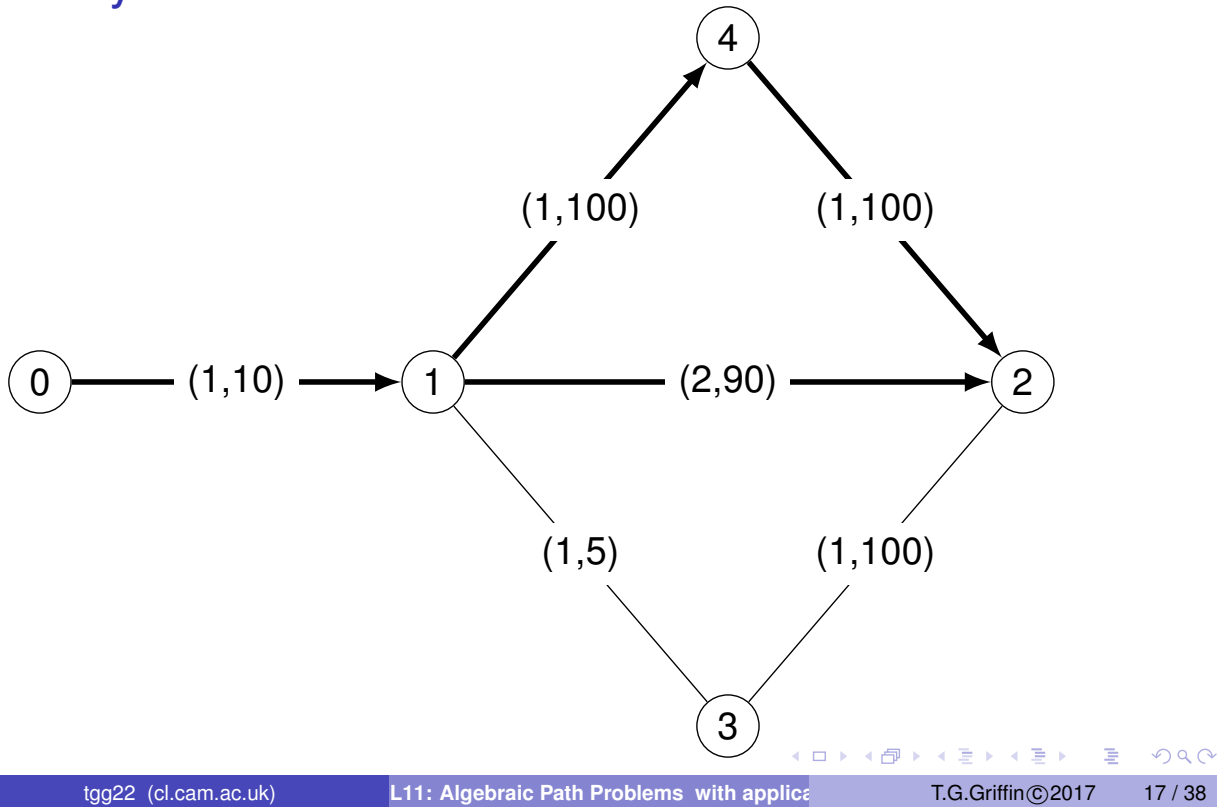
$$\begin{aligned}\mathbf{P}_{\text{Dijkstra}}(0, 2) &= \{(0, 1, 2), (0, 1, 4, 2)\} \\ \mathbf{P}_{\text{Dijkstra}}(2, 0) &= \{(2, 4, 1, 0)\}\end{aligned}$$

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

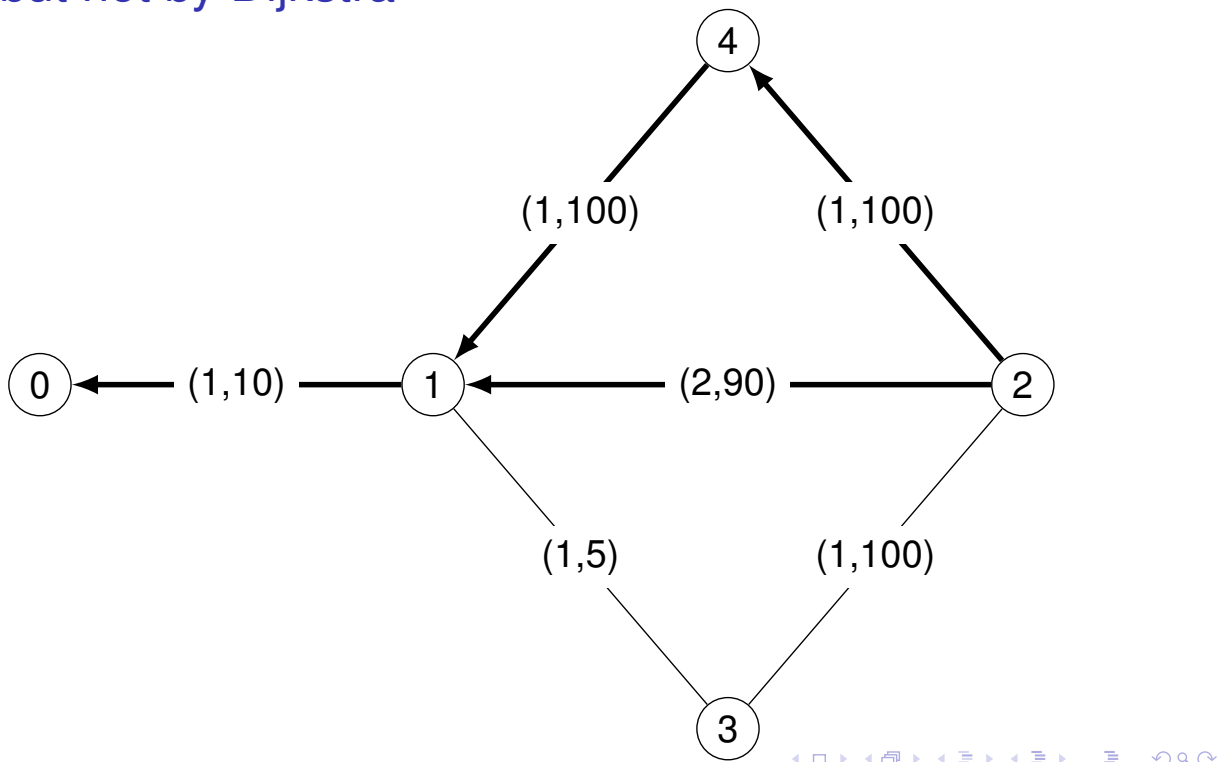
Paths computed by **distributed Bellman-Ford**

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

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 (algebraically)?

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.

Assessment

Five homeworks, with only best four counted, each 25%.

	due
1	October 16
2	October 27
3	November 6
4	November 17
5	December 1

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

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

Important Assumption — We will ignore trivial semigroups

We will implicitly assume that $2 \leq |S|$.

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

IID	identity	$\equiv \exists \alpha \in S, \forall a \in S, a = \alpha \bullet a = a \bullet \alpha$
AN	annihilator	$\equiv \exists \omega \in S, \forall a \in S, \omega = \omega \bullet a = a \bullet \omega$
CM	commutative	$\equiv \forall a, b \in S, a \bullet b = b \bullet a$
SL	selective	$\equiv \forall a, b \in S, a \bullet b \in \{a, b\}$
IP	idempotent	$\equiv \forall a \in S, a \bullet a = a$

A semigroup with an identity is called a **monoid**.

Note that

$$SL(S, \bullet) \implies IP(S, \bullet)$$

A few concrete semigroups

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

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	CM	SL	IP
2^U	\cup	union	$\{\}$	U	*		*
2^U	\cap	intersection	U	$\{\}$	*		*
$2^{U \times U}$	\bowtie	relational join	\mathcal{I}_U	$\{\}$			
$X \rightarrow X$	\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 $\leq \subseteq S \times S$

Definition (Important Order Properties)

RX	reflexive	$\equiv a \leq a$
TR	transitive	$\equiv a \leq b \wedge b \leq c \rightarrow a \leq c$
AY	antisymmetric	$\equiv a \leq b \wedge b \leq a \rightarrow a = b$
TO	total	$\equiv a \leq b \vee b \leq a$

	pre-order	partial order	preference order	total order
RX	*	*	*	*
TR	*	*	*	*
AY		*		*
TO			*	*

Navigation icons: back, forward, search, etc.

Canonical Pre-order of a Commutative Semigroup

Definition (Canonical pre-orders)

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

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

Lemma (Sanity check)

Associativity of \bullet implies that these relations are transitive.

Proof.

Note that $a \leq_{\bullet}^R b$ 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. □

Navigation icons: back, forward, search, etc.

Canonically Ordered Semigroup

Definition (Canonically Ordered Semigroup)

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

Canonically Ordered Semigroups vs. Groups

Lemma (THE BIG DIVIDE)

Only a trivial group is canonically ordered.

Proof.

If $a, b \in S$, then $a = \alpha \bullet a = (b \bullet b^{-1}) \bullet a = b \bullet (b^{-1} \bullet a) = b \bullet c$, for $c = b^{-1} \bullet a$, so $a \trianglelefteq^L b$. In a similar way, $b \trianglelefteq^R a$. Therefore $a = b$. \square

Natural Orders

Definition (Natural orders)

Let (S, \bullet) be a semigroup.

$$a \leq_{\bullet}^L b \equiv a = a \bullet b$$

$$a \leq_{\bullet}^R b \equiv b = a \bullet b$$

Lemma

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

Proof.

$$\begin{aligned} a \leq_{\bullet}^R b &\iff b = a \bullet c = (a \bullet a) \bullet c = a \bullet (a \bullet c) \\ &= a \bullet b \iff a \leq_{\bullet}^R b \end{aligned}$$

$$\begin{aligned} a \leq_{\bullet}^L b &\iff a = b \bullet c = (b \bullet b) \bullet c = b \bullet (b \bullet c) \\ &= b \bullet a = a \bullet b \iff a \leq_{\bullet}^L b \end{aligned}$$

Special elements and natural orders

Lemma (Natural Bounds)

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

$$\begin{array}{ccc} \omega & \leq_{\bullet}^L & a & \leq_{\bullet}^L & \alpha \\ \alpha & \leq_{\bullet}^R & a & \leq_{\bullet}^R & \omega \end{array}$$

Remark (Thanks to Iljitsch van Beijnum)

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

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

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

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 $c = a \text{ glb } b$, 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 least upper bound of a and b , written $c = a \text{ lub } b$, 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 meet-semilattice if $a \text{ glb } b$ exists for each $a, b \in S$.

join-semilattice

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

Fun Facts

Fact 1

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

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

Fact 2

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

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

Homework 1 (due 16 October)

Prove Fun Fun Facts 1 and 2.