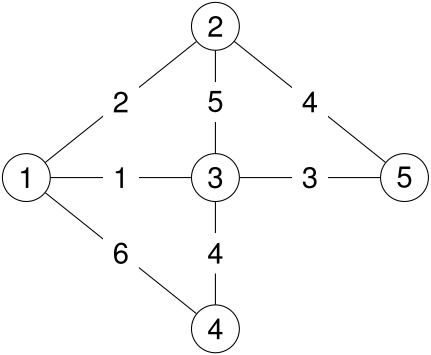
L11: Algebraic Path Problems with applications to Internet Routing Lectures 1 and 2

Timothy G. Griffin

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

Michaelmas Term, 2018

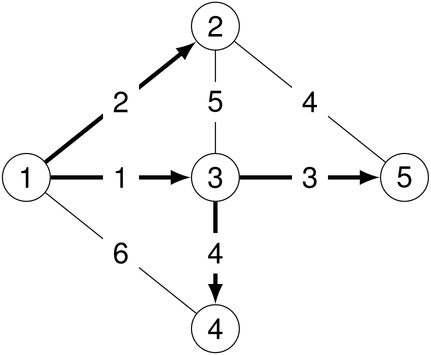
Shortest paths example, $\mathrm{sp} = (\mathbb{N}^{\infty},\ \min,\ +, \infty,\ 0)$



The adjacency matrix

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

Shortest paths solution



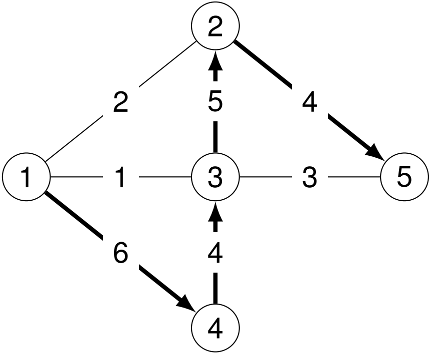
$$\mathbf{A}^* = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{array} \begin{array}{c} \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array} \\ \left[\begin{array}{ccccc} 0 & 2 & 1 & 5 & 4 \\ 2 & 0 & 3 & 7 & 4 \\ 1 & 3 & 0 & 4 & 3 \\ 5 & 7 & 4 & 0 & 7 \\ 4 & 4 & 3 & 7 & 0 \end{array}\right] \end{array}$$

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



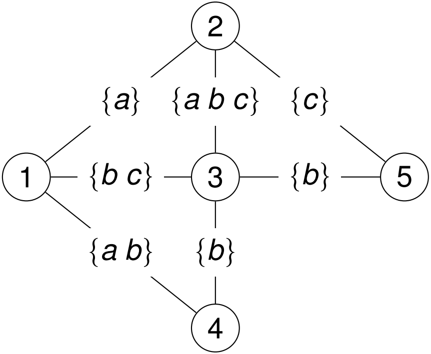
$$\mathbf{A}^* = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{array} \begin{array}{c} \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array} \\ \left[\begin{array}{ccccc} \infty & 4 & 4 & 6 & 4 \\ 4 & \infty & 5 & 4 & 4 \\ 4 & 5 & \infty & 4 & 4 \\ 6 & 4 & 4 & \infty & 4 \\ 4 & 4 & 4 & 4 & \infty \end{array}\right]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

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:

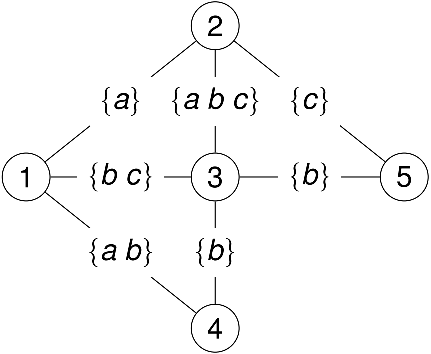
$$\mathbf{A}^*(i,\ j) = \bigcup_{p \in \pi(i,\ j)} w(p),$$

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.

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

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.

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

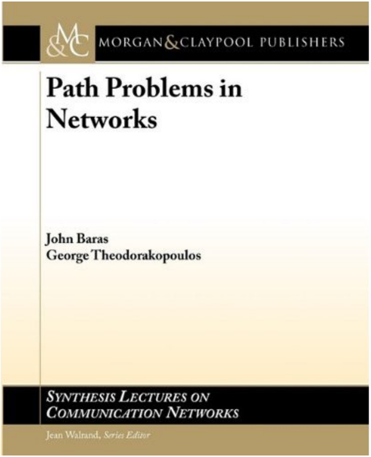
Semirings (generalise $(\mathbb{R}, +, \times, 0, 1)$)

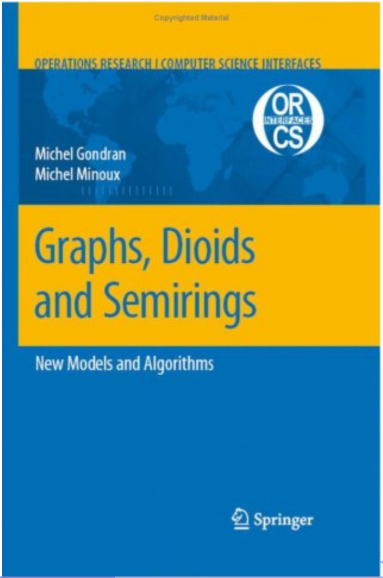
name	S	$\oplus$,	$\otimes$	$\overline{0}$	$\overline{1}$	possible routing use
sp	$\mathbb{N}^{\infty}$	min	$+$	∞	0	minimum-weight routing
bw	$\mathbb{N}^{\infty}$	max	min	0	∞	greatest-capacity routing
rel	$[0, 1]$	max	$\times$	0	1	most-reliable routing
use	$\{0, 1\}$	max	min	0	1	usable-path routing
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





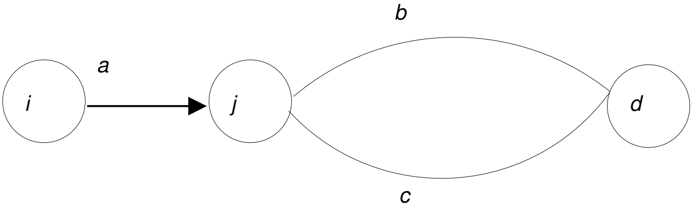
Semiring axioms ...

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

distributivity

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

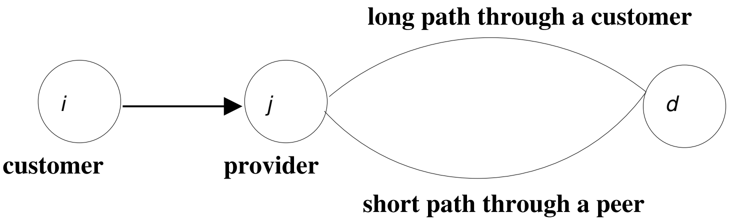
Distributivity, illustrated



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

j makes the choice = *i* makes the choice

Should distributivity hold in Internet Routing?

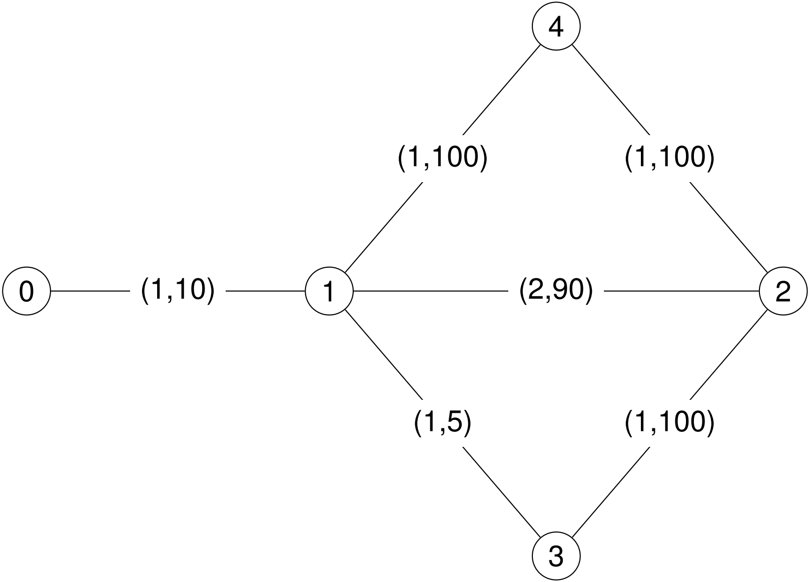


- *j* prefers long path though one of its customers (not the shorter path through a competitor)
- given two routes from a provider, *i* prefers the one with a shorter path
- More on inter-domain routing in the Internet later in the term ...

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

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

But what about the paths themselves?

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

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

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 $(3, 10)$

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

Paths computed by (extended) **Dijkstra**

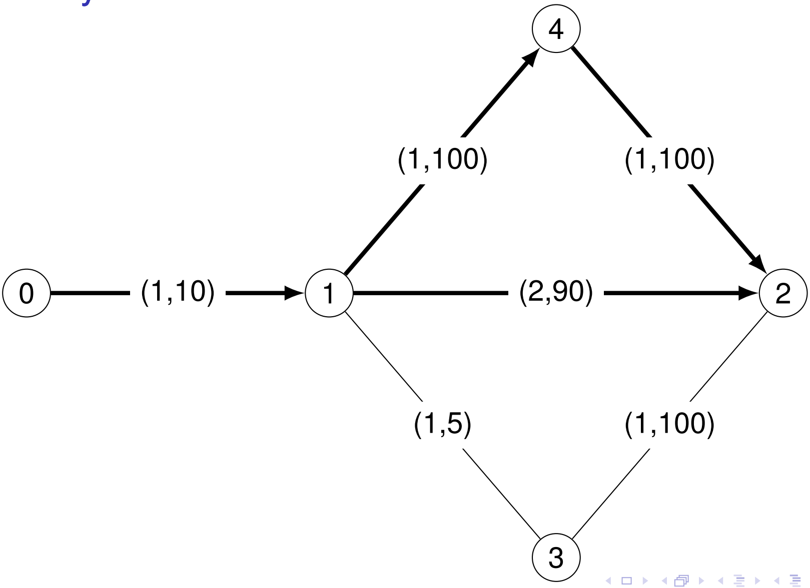
$$\begin{array}{rcl} \mathbf{P}_{\text{Dijkstra}}(0, 2) & = & \{(0, 1, 2),\ (0, 1, 4, 2)\} \\ \mathbf{P}_{\text{Dijkstra}}(2, 0) & = & \{(2, 4, 1, 0)\} \end{array}$$

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

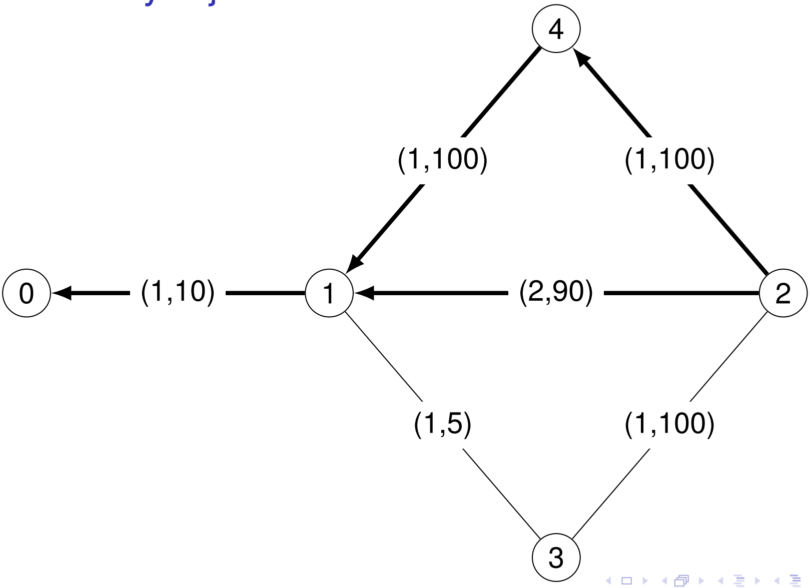
Paths computed by **distributed Bellman-Ford**

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

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.

Lecture 2

- 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	$\{\}$	$\star$		$\star$
$\mathrm{fin}(2^U)$	$\cup$	union	$\{\}$		$\star$		$\star$
$\mathrm{fin}(2^U)$	$\cap$	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, $\mathrm{fin}(Y) \equiv \{X \in Y \mid X \text{ is finite}\}$

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)

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

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

Canonical Pre-order of a Commutative Semigroup

Definition (Canonical pre-orders)

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

Lemma (Sanity check)

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

Proof.

Note that $a \trianglelefteq_{\bullet}^{R} b$ means $\exists c_1 \in S : b = a \bullet c_1$, and $b \trianglelefteq_{\bullet}^{R} c$ 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 $a \trianglelefteq_{\bullet}^{R} c$. The proof for $\trianglelefteq_{\bullet}^{L}$ 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 $a \bullet a^{-1} = a^{-1} \bullet a = \alpha$.

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 $a = b$. □

Natural Orders

Definition (Natural orders)

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

$$
\begin{array}{lcl}
a \leqslant^{L}_{\bullet} b & \equiv & a = a \bullet b \\
a \leqslant^{R}_{\bullet} b & \equiv & b = a \bullet b
\end{array}
$$

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.

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

□

Special elements and natural orders

Lemma (Natural Bounds)

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

$$\begin{array}{ccccc} \omega & \leqslant_{\bullet}^{L} & a & \leqslant_{\bullet}^{L} & \alpha \\ \alpha & \leqslant_{\bullet}^{R} & a & \leqslant_{\bullet}^{R} & \omega \end{array}$$

Remark (Thanks to Iljitsch van Beijnum)

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

$$\begin{array}{ccccc} 0 & \leqslant_{\min}^{L} & a & \leqslant_{\min}^{L} & \infty \\ \infty & \leqslant_{\min}^{R} & a & \leqslant_{\min}^{R} & 0 \end{array}$$

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

Examples of special elements

S	$\bullet$	α	ω	$\leqslant_{\bullet}^{\mathrm{L}}$	$\leqslant_{\bullet}^{\mathrm{R}}$
$\mathbb{N}^{\infty}$	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. $\mathbb{IP}(S,\ \bullet) \iff \mathbb{RX}(S,\ \leqslant_{\bullet}^{D})$
2. $\mathbb{CM}(S,\ \bullet) \implies \mathbb{AY}(S,\ \leqslant_{\bullet}^{D})$
3. $\mathbb{AS}(S,\ \bullet) \implies \mathbb{TR}(S,\ \leqslant_{\bullet}^{D})$
4. $\mathbb{CM}(S,\ \bullet) \implies (\mathbb{SL}(S,\ \bullet) \iff \mathbb{TO}(S,\ \leqslant_{\bullet}^{D}))$

Proof.

1. $a \leqslant_{\bullet}^{D} a \iff a = a \bullet a,$
2. $a \leqslant_{\bullet}^{L} b \wedge b \leqslant_{\bullet}^{L} a \iff a = a \bullet b \wedge b = b \bullet a \implies a = b$
3. $a \leqslant_{\bullet}^{L} b \wedge b \leqslant_{\bullet}^{L} c \iff a = a \bullet b \wedge b = b \bullet c \implies a = a \bullet (b \bullet c) = (a \bullet b) \bullet c = a \bullet c \implies a \leqslant_{\bullet}^{L} c$
4. $a = a \bullet b \vee b = a \bullet b \iff a \leqslant_{\bullet}^{L} b \vee b \leqslant_{\bullet}^{L} a$

□

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 $c = a \mathrm{\ glb\ } b$, 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 $c = a \mathrm{\ lub\ } b$, 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.

- $(S, \leqslant_{\bullet}^{L})$ is a meet-semilattice with $a \,\mathrm{glb}\, b = a \bullet b$.
- $(S, \leqslant_{\bullet}^{R})$ 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.