L11: Algebraic Path Problems with applications to Internet Routing Lectures 5 and 6

Timothy G. Griffin

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

Michaelmas Term, 2016



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

▲ロト ▲聞 ト ▲ 国 ト ▲ 国 ト ― 国

Bisemigroup prop	erti	es (so far)
$\mathbb{AAS}(\boldsymbol{S}, \oplus, \otimes)$	\equiv	$\mathbb{AS}(\boldsymbol{S}, \oplus)$
$\mathbb{AID}(\boldsymbol{S},\oplus,\otimes)$	\equiv	$\mathbb{ID}(\mathcal{S},\oplus)$
$\mathbb{ACM}(\boldsymbol{S}, \oplus, \otimes)$	\equiv	$\mathbb{CM}(\mathcal{S},\oplus)$
$\mathbb{MAS}(\boldsymbol{S}, \oplus, \otimes)$	\equiv	$\mathbb{AS}(\boldsymbol{S}, \otimes)$
$\mathbb{MID}(\boldsymbol{S}, \oplus, \otimes)$	\equiv	$\mathbb{ID}(\mathcal{S},\otimes)$
$\mathbb{LD}(\mathcal{S}, \oplus, \otimes)$	\equiv	$\forall a, b, c \in S, \ a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$
$\mathbb{RD}(\mathcal{S}, \oplus, \otimes)$	\equiv	$\forall a, b, c \in S, \ (a \oplus b) \otimes c = (a \otimes c) \oplus (b \otimes c)$
$\mathbb{ZA}(\boldsymbol{S}, \oplus, \otimes)$	\equiv	$\exists \overline{0} \in \boldsymbol{S}, \ \mathbb{IID}(\boldsymbol{S}, \oplus, \ \overline{0}) \land \mathbb{IAN}(\boldsymbol{S}, \otimes, \ \overline{0})$
$\mathbb{OA}(\boldsymbol{S},\oplus,\otimes)$	=	$\exists \overline{1} \in \boldsymbol{S}, \ \mathbb{IID}(\boldsymbol{S}, \otimes, \ \overline{1}) \land \mathbb{IAN}(\boldsymbol{S}, \oplus, \ \overline{1})$
$\mathbb{ASL}(\mathcal{S}, \oplus, \otimes)$	\equiv	$\mathbb{SL}(\mathcal{S},\oplus)$
$\mathbb{AIP}(\boldsymbol{S}, \oplus, \otimes)$	≡	$\mathbb{IP}(\mathcal{S},\oplus)$



Operations for adding a zero, a one

$$\operatorname{AddZero}(\overline{0}, (S, \oplus, \otimes)) \equiv (S \uplus \{\overline{0}\}, \bigoplus_{\overline{0}}^{\operatorname{id}}, \otimes_{\overline{0}}^{\operatorname{an}})$$
$$\operatorname{AddOne}(\overline{1}, (S, \oplus, \otimes)) \equiv (S \uplus \{\overline{1}\}, \bigoplus_{\overline{1}}^{\operatorname{an}}, \otimes_{\overline{1}}^{\operatorname{id}})$$

Recall

$$a \bullet_{\alpha}^{\mathrm{id}} b \equiv \begin{cases} a & (\mathrm{if} \ b = \mathrm{inr}(\alpha)) \\ b & (\mathrm{if} \ a = \mathrm{inr}(\alpha)) \\ \mathrm{inl}(x \bullet y) & (\mathrm{if} \ a = \mathrm{inl}(x), \ b = \mathrm{inl}(y)) \end{cases}$$
$$a \bullet_{\omega}^{\mathrm{an}} b \equiv \begin{cases} \mathrm{inr}(\omega) & (\mathrm{if} \ b = \mathrm{inr}(\omega)) \\ \mathrm{inr}(\omega) & (\mathrm{if} \ a = \mathrm{inr}(\omega)) \\ \mathrm{inl}(x \bullet y) & (\mathrm{if} \ a = \mathrm{inl}(x), \ b = \mathrm{inl}(y)) \end{cases}$$

<ロ> < 回 > < 回 > < 回 > < 回 >

T.G.Griffin©

æ

We can "inherit" semigroup rules





Property management for AddZero

"Inherited" rules
$\begin{array}{llllllllllllllllllllllllllllllllllll$
Easy Exercises
$ \begin{array}{llllllllllllllllllllllllllllllllllll$
<ロト・(部ト・注下・注・)の(
tgg22 (cl.cam.ac.uk) L11: Algebraic Path Problems with applica T.G.Griffin@2015 6 / 3

Easy Exercises?

Consider left distributivity (\mathbb{LD})								
а	b	С	$a \otimes_{\overline{0}}^{\operatorname{an}} (b \oplus_{\overline{0}}^{\operatorname{id}} c)$	$(a \otimes_{\overline{0}}^{\operatorname{an}} b) \oplus_{\overline{0}}^{\operatorname{id}} (a \otimes_{\overline{0}}^{\operatorname{an}} c)$				
$\operatorname{inl}(\boldsymbol{a}')$	$\operatorname{inl}(\boldsymbol{b}')$	$\operatorname{inl}(\mathbf{C}')$	$\operatorname{inl}(\mathbf{a}'\otimes(\mathbf{b}'\oplus\mathbf{c}'))$	$\operatorname{inl}((\boldsymbol{a}'\otimes\boldsymbol{b}')\oplus(\boldsymbol{a}'\otimes\boldsymbol{c}'))$				
$inr(\overline{0})$	$\operatorname{inl}(\boldsymbol{b'})$	$\operatorname{inl}(\mathbf{C'})$	$\operatorname{inr}(\overline{0})$	$inr(\overline{0})$				
$\operatorname{inl}(\mathbf{a}')$	$inr(\overline{0})$	$\operatorname{inl}(\mathbf{C}')$	$\operatorname{inl}(\mathbf{a}'\oplus\mathbf{c}')$	$\operatorname{inl}(\boldsymbol{a}'\oplus \boldsymbol{c}')$				
$\operatorname{inl}(\boldsymbol{a}')$	$\operatorname{inl}(\boldsymbol{b}')$	$inr(\overline{0})$	$\operatorname{inl}(\mathbf{a'}\oplus\mathbf{b'})$	$\operatorname{inl}(\textit{a}' \oplus \textit{b}')$				
$\operatorname{inl}(\boldsymbol{a}')$	$inr(\overline{0})$	$inr(\overline{0})$	$inr(\overline{0})$	$inr(\overline{0})$				
$inr(\overline{0})$	$inr(\overline{0})$	$inr(\overline{0})$	$\operatorname{inr}(\overline{0})$	$inr(\overline{0})$				
taa22 (イロトイ部トイヨトイヨト ヨークへで tag22 (cl.cam.ac.uk) I 11: Algebraic Path Problems with applies TG Griffipの2015 7/36							

However, adding a one is more complicated!

Consider left distributivity (\mathbb{LD})						
а	b	С	$a \otimes_{\overline{1}}^{\operatorname{id}} (b \oplus_{\overline{1}}^{\operatorname{an}} c)$	$(\boldsymbol{a} \otimes_{\overline{1}}^{\operatorname{id}} \boldsymbol{b}) \oplus_{\overline{1}}^{\operatorname{an}} (\boldsymbol{a} \otimes_{\overline{1}}^{\operatorname{id}} \boldsymbol{c})$		
$\operatorname{inl}(\mathbf{a}')$	$\operatorname{inl}(\boldsymbol{b}')$	$\operatorname{inl}(\mathbf{C}')$	$\operatorname{inl}(\boldsymbol{a}'\otimes(\boldsymbol{b}'\oplus\boldsymbol{c}'))$	$\operatorname{inl}((\boldsymbol{a}'\otimes\boldsymbol{b}')\oplus(\boldsymbol{a}'\otimes\boldsymbol{c}'))$		
$\operatorname{inr}(\overline{1})$	$\operatorname{inl}(\boldsymbol{b}')$	$\operatorname{inl}(\mathbf{C'})$	$\operatorname{inl}({\it b}'\oplus{\it c}')$	$\operatorname{inl}({\it b}'\oplus{\it c}')$		
$\operatorname{inl}(\mathbf{a}')$	$inr(\overline{1})$	$\operatorname{inl}(\mathbf{C}')$	$\operatorname{inl}(\boldsymbol{a'})$	$\operatorname{inl}((\mathbf{a'} \oplus (\mathbf{a'} \otimes \mathbf{c'}))$		
$\operatorname{inl}(\mathbf{a}')$	$\operatorname{inl}(\boldsymbol{b}')$	$inr(\overline{1})$	inl(a ')	$\operatorname{inl}((\operatorname{\textit{a}}'\otimes\operatorname{\textit{b}}')\oplus\operatorname{\textit{a}}')$		
$\operatorname{inl}(\mathbf{a}')$	$\operatorname{inr}(\overline{1})$	$inr(\overline{1})$	inl(a')	$\operatorname{inl}(\mathbf{a'}\oplus\mathbf{a'})$		
$inr(\overline{1})$	$inr(\overline{1})$	$inr(\overline{1})$	$\operatorname{inr}(\overline{1})$	$\operatorname{inr}(\overline{1})$		
イロトイ昂トイヨト ヨーのへの tag22(cl.cam.ac.uk) 11: Algebraic Path Problems with applics TC Criffinの2015 8/26						

T.G.Griffin © 2015

What is this?

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

Suppose \oplus is idempotent and commutative and we let $a \le b \equiv a = a \oplus b$. We know that

$$b \leqslant c \Rightarrow a \otimes b \leqslant a \otimes c$$

since $b = b \oplus c$ implies $a \otimes b = a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$. That is \otimes is order preserving. Now $a = (a \otimes b) \oplus a$ is telling us something else, that

$$a \leq a \otimes b$$
.

That is, that multiplication is inflationary.



Absorption

$$\begin{split} & \mathbb{AB} \text{sorption properties (name is from lattice theory)} \\ & \mathbb{RAB}(S, \oplus, \otimes) \equiv \forall a, b \in S, \ a = (a \otimes b) \oplus a = a \oplus (a \otimes b) \\ & \mathbb{LAB}(S, \oplus, \otimes) \equiv \forall a, b \in S, \ a = (b \otimes a) \oplus a = a \oplus (b \otimes a) \\ \end{split}$$

ロト・日本・モート・

590

10/36

Rules for absorption? Consider \mathbb{RAB}

AddZer	0				
	а	b	$(\boldsymbol{a}\otimes_{\overline{0}}^{\mathrm{an}}\boldsymbol{b})\oplus_{\overline{0}}^{\mathrm{id}}\boldsymbol{a}$	$a \oplus_{\overline{0}}^{\operatorname{id}} (a \otimes_{\overline{0}}^{\operatorname{an}} b)$	
	inl(<i>a</i> ′)	inl(b ')	$\operatorname{inl}((a'\otimes b')\oplus a)$	$\operatorname{inl}(a' \oplus (a' \otimes b'))$	
	$inr(\overline{0})$	inl(b ')	$\operatorname{inr}(\overline{0})$	$inr(\overline{0})$	
	$\operatorname{inl}(\boldsymbol{a}')$	$inr(\overline{0})$	inl(a ')	$\operatorname{inl}(a')$	
	$inr(\overline{0})$	$\operatorname{inr}(\overline{0})$	$\operatorname{inr}(\overline{0})$	$inr(\overline{0})$	
	RAB(A LAB(A	AddZero(AddZero($ar{0},\ (oldsymbol{\mathcal{S}},\ \oplus,\ \otimes))) \Leftrightarrow ar{0},\ (oldsymbol{\mathcal{S}},\ \oplus,\ \otimes))) \Leftrightarrow$	$ \mathbb{RAB}(\boldsymbol{S}, \oplus, \otimes) $ $ \mathbb{LAB}(\boldsymbol{S}, \oplus, \otimes) $	
tgg22	2 (cl.cam.ac.uk)	L1:	1: Algebraic Path Problems with	< □ > < ⊡ > < ⊡ > < ≧ > < ≧ > < ≧ > < ≧	うへで 11/36

Rules for absorption? Consider \mathbb{RAB}

AddOne	;				
	а	b	$(\boldsymbol{a} \otimes_{\overline{1}}^{\operatorname{id}} \boldsymbol{b}) \oplus_{\overline{1}}^{\operatorname{an}} \boldsymbol{a}$	$\pmb{a} \oplus_{\overline{1}}^{\operatorname{an}} (\pmb{a} \otimes_{\overline{1}}^{\operatorname{id}} \pmb{b})$	
	$\operatorname{inl}(a')$	inl(b ')	$\operatorname{inl}((a'\otimes b')\oplus a)$	$\operatorname{inl}(a' \oplus (a' \otimes b'))$	
	$\operatorname{inr}(\overline{1})$	inl(b ')	$\operatorname{inr}(\overline{1})$	$inr(\overline{1})$	
	$\operatorname{inl}(a')$	$inr(\overline{1})$	$\operatorname{inl}(\boldsymbol{a'})$	$\operatorname{inl}(\mathbf{a}'\oplus\mathbf{a}')$	
	$inr(\overline{1})$	$inr(\overline{1})$	$\operatorname{inr}(\overline{1})$	$inr(\overline{1})$	

< ⊡ >

< ∃ >

< ∃ >

Property management for AddOne

"Inherited" rules		
$\mathbb{AAS}(\mathrm{AddOne}(\overline{1}, \ (\boldsymbol{S}, \oplus, \otimes)))$	\Leftrightarrow	$\mathbb{AS}(\boldsymbol{S},\oplus)$
$\mathbb{AID}(\mathrm{AddOne}(\overline{1}, \ (\boldsymbol{S}, \ \oplus, \ \otimes)))$	\Leftrightarrow	$\mathbb{ID}(\boldsymbol{S},\oplus)$
$\mathbb{ACM}(\mathrm{AddOne}(\overline{1}, \ (\boldsymbol{S}, \ \oplus, \ \otimes)))$	\Leftrightarrow	$\mathbb{CM}(\boldsymbol{S},\oplus)$
$\mathbb{ASL}(\mathrm{AddOne}(\overline{1}, \ (\boldsymbol{S}, \ \oplus, \ \otimes)))$	\Leftrightarrow	$\mathbb{SL}(\boldsymbol{S}, \oplus)$
$\mathbb{AIP}(\text{AddOne}(\overline{1}, (\boldsymbol{S}, \oplus, \otimes)))$	\Leftrightarrow	$\mathbb{IP}(\boldsymbol{S}, \oplus)$
$\mathbb{MAS}(\mathrm{AddOne}(\overline{1}, \ (\boldsymbol{S}, \ \oplus, \ \otimes)))$	\Leftrightarrow	$\mathbb{AS}(\boldsymbol{S}, \otimes)$
$\mathbb{MID}(\mathrm{AddOne}(\overline{1}, \ (\boldsymbol{S}, \ \oplus, \ \otimes)))$	\Leftrightarrow	TRUE



Property management for AddOne

$\mathbb{LD}(\text{AddOne}(\overline{1}, \ (\textbf{\textit{S}}, \ \oplus, \ \otimes)))$	\Leftrightarrow	$\mathbb{LD}(\boldsymbol{S},\oplus,\otimes)\wedge\mathbb{RAB}(\boldsymbol{S},\oplus,\otimes)$
$\mathbb{RD}(\text{AddOne}(\overline{1}, \ (\boldsymbol{S}, \oplus, \otimes)))$	\Leftrightarrow	$ ^{\Lambda} \mathbb{IP}(\boldsymbol{S}, \oplus) \\ \mathbb{RD}(\boldsymbol{S}, \oplus, \otimes) \wedge \mathbb{LAB}(\boldsymbol{S}, \oplus, \otimes) $
$\mathbb{ZA}(\text{AddOne}(\overline{1}, (S, \oplus, \otimes)))$	\Leftrightarrow	$\wedge \mathbb{IP}(\boldsymbol{S}, \oplus)$ $\mathbb{ZA}(\boldsymbol{S}, \oplus, \otimes)$
$\mathbb{OA}(\text{AddOne}(\overline{1}, (S, \oplus, \otimes)))$	\Leftrightarrow	TRUE
$\mathbb{RAB}(\mathrm{AddOne}(\overline{1}, \ (\boldsymbol{S}, \oplus, \otimes)))$	\Leftrightarrow	$\mathbb{RAB}(\boldsymbol{S},\oplus,\otimes)\wedge\mathbb{IP}(\boldsymbol{S},\oplus)$
$\mathbb{LAB}(\mathrm{AddOne}(\overline{1}, \ (\boldsymbol{\mathcal{S}}, \ \oplus, \ \otimes)))$	\Leftrightarrow	$\mathbb{LAB}(\boldsymbol{S}, \oplus, \otimes) \land \mathbb{IP}(\boldsymbol{S}, \oplus)$

< 日 > < 四 > < 臣 > < 臣 > 、

9 Q (?

We have to start somewhere!

S	\oplus	\otimes	0	1	\mathbb{LD}	\mathbb{RD}	$\mathbb{Z}\mathbb{A}$	\mathbb{Q}	LAB	RAB
\mathbb{N}	min	+		0	*	*		*	*	*
\mathbb{N}	max	+	0	0	*	*			*	*
\mathbb{N}	max	min	0		*	*	*		*	*
\mathbb{N}	min	max		0	*	*		*	*	*



Introducing Minimax

$$\begin{array}{lll} \text{minimax} &\equiv & \text{AddZero}(\infty, \ (\mathbb{N}, \ \text{min}, \ \text{max})) \\ \\ &= & (\mathbb{N} \uplus \{\infty\}, \ \text{min}_{\overline{\infty}}^{\text{id}}, \ \text{max}_{\overline{\infty}}^{\text{an}}) \end{array}$$

Some examples ...

$$\operatorname{inl}(17) \operatorname{min}_{\overline{\infty}}^{\operatorname{id}} \operatorname{inr}(\infty) = \operatorname{inl}(17)$$

 $inl(17) \max_{\overline{\infty}}^{an} inr(\infty) = inr(\infty)$

... which we will usually write as $17 \min \infty = 17$ $17 \max \infty = \infty$ < ロ > < @ > < 注 > < 注 > < 注 > < 注 500

tgg22	(cl.cam.ac.uk)
-99	

Dendrograms



tgg22 (cl.cam.ac.uk)	L11: Algebraic Path Problems with applica	T.G.Griffin©2015	17 / 36

An application 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 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 phylogenetic
- ...

A (random) minimax matrix A drawn as a graph



The solution A* drawn as a dendrogram



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

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

tgg22 (cl.cam.ac.uk)

L11: Algebraic Path Problems with applica

Fun Facts

minimax and ultrametrics

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

minimax and spanning trees

The set of arcs

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

contain a spanning tree

ロト (日) (モ) (モ)

T.G.Griffin © 2015

21 / 36

500

22 / 36

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



Recall



- 4 回 ト 4 回 ト 4 回 ト

Saa

Lexicographic product for Bi-semigroups



	4	- ▲ 重 ▶ ▲ 重 ▶	€
tgg22 (cl.cam.ac.uk)	L11: Algebraic Path Problems with applica	T.G.Griffin © 2015	25 / 36

Examples

Distributivity?

Theorem: If \bigoplus_{S} is commutative and selective, then

$$\begin{split} \mathbb{LD}((\boldsymbol{S}, \oplus_{\boldsymbol{S}}, \otimes_{\boldsymbol{S}}) \stackrel{\scriptstyle{\times}}{\times} (\boldsymbol{T}, \oplus_{\boldsymbol{T}}, \otimes_{\boldsymbol{T}})) \Leftrightarrow \\ \mathbb{LD}(\boldsymbol{S}, \oplus_{\boldsymbol{S}}, \otimes_{\boldsymbol{S}}) \wedge \mathbb{LD}(\boldsymbol{T}, \oplus_{\boldsymbol{T}}, \otimes_{\boldsymbol{T}}) \wedge (\mathbb{LC}(\boldsymbol{S}, \otimes_{\boldsymbol{S}}) \vee \mathbb{LK}(\boldsymbol{T}, \otimes_{\boldsymbol{T}})) \end{split}$$

 $\mathbb{RD}((S, \oplus_{S}, \otimes_{S}) \times (T, \oplus_{T}, \otimes_{T})) \Leftrightarrow \\\mathbb{RD}(S, \oplus_{S}, \otimes_{S}) \wedge \mathbb{RD}(T, \oplus_{T}, \otimes_{T}) \wedge (\mathbb{RC}(S, \otimes_{S}) \vee \mathbb{RK}(T, \otimes_{T}))$

Left and Right Cancellative

$$\begin{split} \mathbb{L}\mathbb{C}(X, \bullet) &\equiv \forall a, b, c \in X, \ c \bullet a = c \bullet b \Rightarrow a = b \\ \mathbb{R}\mathbb{C}(X, \bullet) &\equiv \forall a, b, c \in X, \ a \bullet c = b \bullet c \Rightarrow a = b \end{split}$$



Why bisemigroups?

But wait! How could any semiring satisfy either of these properties?

 $\mathbb{LC}(X, \bullet) \equiv \forall a, b, c \in X, \ c \bullet a = c \bullet b \Rightarrow a = b \\ \mathbb{LK}(X, \bullet) \equiv \forall a, b, c \in X, \ c \bullet a = c \bullet b$

- For LC, note that we always have 0 ⊗ a = 0 ⊗ b, so LC could only hold when S = {0}.
- For $\mathbb{L}\mathbb{K}$, let $a = \overline{1}$ and $b = \overline{0}$ and $\mathbb{L}\mathbb{K}$ leads to the conclusion that every *c* is equal to $\overline{0}$ (again!).

Normally we will add a zero and/or a one as the last step(s) of constructing a semiring. Alternatively, we might want to complicate our properties so that things work for semirings. A design trade-off!

tgg22 (cl.cam.ac.uk)

୬ ୯.୯ 28 / 36

Proof of \Leftarrow for \mathbb{LD}

Assume

- (1) $\mathbb{LD}(S, \oplus_S, \otimes_S)$
- (2) $\mathbb{LD}(T, \oplus_T, \otimes_T)$
- (3) $\mathbb{LC}(S, \otimes_S) \vee \mathbb{LK}(T, \otimes_T)$
- (4) $\mathbb{IP}(S, \oplus_S)$.

Let $\oplus \equiv \oplus_S \times \oplus_T$ and $\otimes \equiv \otimes_S \times \otimes_T$. Suppose

$$(s_1, t_1), (s_2, t_2), (s_3, t_3) \in S \times T.$$

We want to show that

$$lhs \equiv (\mathbf{s}_1, t_1) \otimes ((\mathbf{s}_2, t_2) \oplus (\mathbf{s}_3, t_3)) \\ = ((\mathbf{s}_1, t_1) \otimes (\mathbf{s}_2, t_2)) \oplus ((\mathbf{s}_1, t_1) \otimes (\mathbf{s}_3, t_3)) \\ \equiv rhs$$



Proof of \Leftarrow for \mathbb{LD}

We have

$$\begin{aligned} \text{lhs} &\equiv (\mathbf{S}_1, t_1) \otimes ((\mathbf{S}_2, t_2) \oplus (\mathbf{S}_3, t_3)) \\ &= (\mathbf{S}_1, t_1) \otimes (\mathbf{S}_2 \oplus_S \mathbf{S}_3, t_{\text{lhs}}) \\ &= (\mathbf{S}_1 \otimes_S (\mathbf{S}_2 \oplus_S \mathbf{S}_3), t_1 \otimes_T t_{\text{lhs}}) \end{aligned} \\ \text{rhs} &\equiv ((\mathbf{S}_1, t_1) \otimes (\mathbf{S}_2, t_2)) \oplus ((\mathbf{S}_1, t_1) \otimes (\mathbf{S}_3, t_3)) \\ &= (\mathbf{S}_1 \otimes_S \mathbf{S}_2, t_1 \otimes_T t_2) \oplus (\mathbf{S}_1 \otimes_S \mathbf{S}_3, t_1 \otimes_T t_3) \\ &= ((\mathbf{S}_1 \otimes_S \mathbf{S}_2) \oplus_S (\mathbf{S}_1 \otimes_S \mathbf{S}_3), t_{\text{rhs}}) \\ &= (\mathbf{S}_1 \otimes_S (\mathbf{S}_2 \oplus_S \mathbf{S}_3), t_{\text{rhs}}) \end{aligned}$$

where t_{lhs} and t_{rhs} are determined by the appropriate case in the definition of \oplus . Finally, note that

 $lhs = rhs \Leftrightarrow t_{rhs} = t_1 \otimes t_{lhs}.$

tgg22 (cl.cam.ac.uk)	L11: Algebraic Path Problems with applica	T.G.Griffin © 2015	30 / 36

◆□▶ ◆□▶ ◆ 臣▶ ◆ 臣▶ 臣 のへぐ

Proof by cases on $s_2 \oplus_S s_3$

Case 1 : $s_2 = s_2 \oplus_S s_3 = s_3$. Then $t_{\text{lhs}} = t_2 \oplus_T t_3$ and

$$t_1 \otimes_{\mathcal{T}} t_{\text{lhs}} = t_1 \otimes_{\mathcal{T}} (t_2 \oplus_{\mathcal{T}} t_3) =_{(2)} (t_1 \otimes_{\mathcal{T}} t_2) \oplus_{\mathcal{T}} (t_1 \otimes_{\mathcal{T}} t_3).$$

Since $s_2 = s_3$ we have $s_1 \otimes_S s_2 = s_1 \otimes_S s_3$ and

$$s_1 \otimes_S s_2 =_{(4)} (s_1 \otimes_S s_2) \oplus_S (s_1 \otimes_S s_3) =_{(4)} s_1 \otimes_S s_3.$$

Therefore,

$$t_{\rm rhs} = (t_1 \otimes_T t_2) \oplus (t_1 \otimes_T t_3) = t_1 \otimes_T t_{\rm lhs}.$$

Case 2 : $s_2 = s_2 \oplus_S s_3 \neq s_3$. Then $t_{lhs} = t_2$ and

$$t_1 \otimes_T t_{\text{lhs}} = t_1 \otimes_T t_2.$$

Since $s_2 = s_2 \oplus_S s_3$ we have

$$\mathbf{s}_1 \otimes_S \mathbf{s}_2 = \mathbf{s}_1 \otimes_S (\mathbf{s}_2 \oplus_S \mathbf{s}_3) =_{(1)} (\mathbf{s}_1 \otimes_S \mathbf{s}_2) \oplus_S (\mathbf{s}_1 \otimes_S \mathbf{s}_3).$$

tag22 (cl.com.ac.uk)	111: Algebraic Bath Problems, with applic	T.G. Griffin @2015	31/36
igyzz (ci.cam.ac.uk)	LTT. Algebraic Failt Froblems with applica	1.0.0111110/2013	51750

Case 2.1 $s_1 \otimes_S s_2 \neq s_1 \otimes_S s_3$. Then $t_{rhs} = t_1 \otimes_T t_2 = t_1 \otimes_T t_{lhs}$. Case 2.2 $s_1 \otimes_S s_2 = s_1 \otimes_S s_3$. Then

$$t_{\rm rhs} = (t_1 \otimes_{\mathcal{T}} t_2) \oplus_{\mathcal{T}} (t_1 \otimes_{\mathcal{T}} t_3) =_{(2)} t_1 \otimes_{\mathcal{T}} (t_2 \oplus_{\mathcal{T}} t_3)$$

We need to consider two subcases.

Case 2.2.1: Assume $\mathbb{LC}(S, \otimes_S)$. But $s_1 \otimes_S s_2 = s_1 \otimes_S s_3 \Rightarrow s_2 = s_3$, which is a contradiction.

Case 2.2.2 : Assume $\mathbb{LK}(T, \otimes_T)$. In this case we know

$$\forall a, b \in X, t_1 \otimes_T a = t_1 \otimes_T b.$$

Letting $a = t_2 \oplus_T t_3$ and $b = t_2$ we have

$$t_{\rm rhs} = t_1 \otimes_{\mathcal{T}} (t_2 \oplus_{\mathcal{T}} t_3) = t_1 \otimes_{\mathcal{T}} t_2 = t_1 \otimes_{\mathcal{T}} t_{\rm lhs}.$$

Case 3 : $s_2 \neq s_2 \oplus_S s_3 = s_3$. Similar to Case 2.

tgg22 (cl.cam.ac.uk)	L11: Algebraic Path Problems with applica	T.G.Griffin © 2015
----------------------	---	--------------------

୬ ୯. ୯ 32 / 36

Other direction, \Rightarrow

Prove this:

 $\begin{array}{l} \neg \mathbb{LD}(\boldsymbol{S}, \oplus_{\boldsymbol{S}}, \otimes_{\boldsymbol{S}}) \lor \neg \mathbb{LD}(\boldsymbol{T}, \oplus_{\boldsymbol{T}}, \otimes_{\boldsymbol{T}}) \lor (\neg \mathbb{LC}(\boldsymbol{S}, \otimes_{\boldsymbol{S}}) \land \neg \mathbb{LK}(\boldsymbol{T}, \otimes_{\boldsymbol{T}})) \\ \Rightarrow \neg \mathbb{LD}((\boldsymbol{S}, \oplus_{\boldsymbol{S}}, \otimes_{\boldsymbol{S}}) \stackrel{\prec}{\times} (\boldsymbol{T}, \oplus_{\boldsymbol{T}}, \otimes_{\boldsymbol{T}})). \end{array}$

Case 1: $\neg \mathbb{LD}(S, \oplus_S, \otimes_S)$. That is

$$\exists a, b, c \in S, \ a \otimes_S (b \oplus_S c) \neq (a \otimes_S b) \oplus_S (a \otimes_S c).$$

Pick any $t \in T$. Then for some $t_1, t_2, t_3 \in T$ we have

 $(a, t) \otimes ((b, t) \oplus (c, t))$ $= (a, t) \otimes (b \oplus_S c, t_1)$ $= (a, \otimes_S (b \oplus_S c), t_2)$ $\neq ((a \otimes_S b) \oplus_S (a \otimes_S c), t_3)$ $= (a \otimes_S b, t \otimes_T t) \oplus (a \otimes_S c, t \otimes_T t)$ $= ((a, t) \otimes (b, t)) \oplus ((a, t) \otimes (c, t))$

Case 2: $\neg \mathbb{LD}(T, \oplus_T, \otimes_T)$. Similar.tgg22 (cl.cam.ac.uk)L11: Algebraic Path Problems with applicaT.G.Griffin@201533 / 36

Case 3: $(\neg \mathbb{LC}(S, \otimes_S) \land \neg \mathbb{LK}(T, \otimes_T))$. That is

$$\exists a, b, c \in S, \ c \otimes_S a = c \otimes_S b \land a \neq b$$

and

$$\exists x, y, z \in T, \ z \otimes_T x \neq z \otimes_T y.$$

Since \bigoplus_S is selective and $a \neq b$, we have $a = a \bigoplus_S b$ or $b = a \bigoplus_S b$. Assume without loss of generality that $a = a \bigoplus_S b \neq b$. Suppose that $t_1, t_2, t_3 \in T$. Then

$$lhs \equiv (c, t_1) \otimes ((a, t_2) \oplus (b, t_3)) = (c, t_1) \otimes (a, t_2) = (c \otimes_S a, t_1 \otimes_T t_2) rhs \equiv ((c, t_1) \otimes (a, t_2)) \oplus ((c, t_1) \otimes (b, t_3)) = (c \otimes_S a, t_1 \otimes_T t_2) \oplus (c \otimes_S b, t_1 \otimes_T t_3) = (c \otimes_S a, (t_1 \otimes_T t_2) \oplus_T (t_1 \otimes_T t_3))$$

▲ロト ▲聞 ト ▲ 国 ト ▲ 国 ト ― 国

Our job now is to select t_1, t_2, t_3 so that

$$t_{\text{lhs}} \equiv t_1 \otimes_T t_2 \neq (t_1 \otimes_T t_2) \oplus_T (t_1 \otimes_T t_3) \equiv t_{\text{rhs}}.$$

We don't have very much to work with! Only

$$\exists x, y, z \in T, \ z \otimes_T x \neq z \otimes_T y.$$

In addition, we can assume $\mathbb{LD}(T, \oplus_T, \otimes_T)$ (otherwise, use Case 2!), SO

$$t_{\rm rhs} = t_1 \otimes_T (t_2 \oplus_T t_3).$$



We need to select t_1, t_2, t_3 so that $t_{\text{lhs}} \equiv t_1 \otimes_T t_2 \neq t_1 \otimes_T (t_2 \oplus_T t_3) \equiv t_{\text{rhs}}.$ Case 3.1: $z \otimes_T x = z \otimes_T (x \oplus_T y)$. Then letting $t_1 = z$, $t_2 = y$, and $t_3 = x$ we have

$$t_{\mathrm{lhs}} = z \otimes_{\mathcal{T}} y \neq z \otimes_{\mathcal{T}} x = z \otimes_{\mathcal{T}} (x \oplus_{\mathcal{T}} y) = t_{\mathrm{rhs}}.$$

Case 3.2: $z \otimes_T y = z \otimes_T (x \oplus_T y)$. Then letting $t_1 = z$, $t_2 = x$, and $t_3 = y$ we have

$$t_{\text{lhs}} = z \otimes_T x \neq z \otimes_T y = z \otimes_T (x \oplus_T y) = t_{\text{rhs}}.$$

Case 3.3: $z \otimes_T x \neq z \otimes_T (x \oplus_T y) \neq z \otimes_T y$. Then letting $t_1 = z$, $t_2 = x$, and $t_3 = y$ we have

$$t_{\rm lhs} = z \otimes_T x \neq z \otimes_T (x \oplus_T y) = t_{\rm rhs}.$$

▲□ ▶ ▲ 臣 ▶ ▲ 臣 ▶