L11: Algebraic Path Problems with applications to Internet Routing Lecture 3

Timothy G. Griffin

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

Michaelmas Term, 2018



Lecture 3

- Semirings
- Matrix semirings
- Matrix encoding of a path problem
- A* solves a path problem
- Computing A*
- A* as a solution to certain matrix equations

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

- ullet (S, \oplus, \otimes) is a bi-semigroup
- is commutative

and left- and right-distributivity hold,

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

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

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	⊕,	\otimes	0	1
min_plus	\mathbb{N}	min	+		0
max_min	\mathbb{N}	max	min	0	

Semirings

name	S	\oplus ,	\otimes	$\overline{0}$	1
sp	M_{∞}	min	+	∞	0
bw	M_{∞}	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 "0 is an annihilator for ⊗"? No!

Fix that ...

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

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

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

Left Distributivity

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

$$\begin{array}{ll} (\mathbf{A} \otimes (\mathbf{B} \oplus \mathbf{C}))(i,j) \\ = & \bigoplus_{1 \leqslant q \leqslant n} \mathbf{A}(i,q) \otimes (\mathbf{B} \oplus \mathbf{C})(q,j) \\ = & \bigoplus_{1 \leqslant q \leqslant n} \mathbf{A}(i,q) \otimes (\mathbf{B}(q,j) \oplus \mathbf{C}(q,j)) \\ = & \bigoplus_{1 \leqslant q \leqslant n} (\mathbf{A}(i,q) \otimes \mathbf{B}(q,j)) \oplus (\mathbf{A}(i,q) \otimes \mathbf{C}(q,j)) \\ = & \bigoplus_{1 \leqslant q \leqslant n} \mathbf{A}(i,q) \otimes \mathbf{B}(q,j)) \oplus (\bigoplus_{1 \leqslant q \leqslant n} \mathbf{A}(i,q) \otimes \mathbf{C}(q,j)) \end{array}$$
 (\$\text{LD}\$)
$$= & (\bigoplus_{1 \leqslant q \leqslant n} \mathbf{A}(i,q) \otimes \mathbf{B}(q,j)) \oplus (\bigoplus_{1 \leqslant q \leqslant n} \mathbf{A}(i,q) \otimes \mathbf{C}(q,j))$$
 (\$\text{AS}, \text{CM}\$)
$$= & ((\mathbf{A} \otimes \mathbf{B}) \oplus (\mathbf{A} \otimes \mathbf{C}))(i,j)$$
 (\$\text{def} \lefta \cdot \text{Odef} \lefta \cdot

Matrix encoding path problems

- $(S, \oplus, \otimes, \overline{0}, \overline{1})$ a semiring
- G = (V, E) a directed graph
- $w \in E \rightarrow S$ a weight function

Path weight

The weight of a path $p = i_1, i_2, i_3, \dots, i_k$ is

$$\textbf{\textit{w}}(\textbf{\textit{p}}) = \textbf{\textit{w}}(\textbf{\textit{i}}_1, \ \textbf{\textit{i}}_2) \otimes \textbf{\textit{w}}(\textbf{\textit{i}}_2, \ \textbf{\textit{i}}_3) \otimes \cdots \otimes \textbf{\textit{w}}(\textbf{\textit{i}}_{k-1}, \ \textbf{\textit{i}}_k).$$

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 **A*** such that for all $i, j \in V$

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

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

How can we solve this problem?

Stability

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

$a \in S$, define powers a^k

$$a^0 = \overline{1}$$

 $a^{k+1} = a \otimes a^k$

Closure, a*

$$a^{(k)} = a^0 \oplus a^1 \oplus a^2 \oplus \cdots \oplus a^k$$

 $a^* = a^0 \oplus a^1 \oplus a^2 \oplus \cdots \oplus a^k \oplus \cdots$

Definition (q stability)

If there exists a q such that $a^{(q)}=a^{(q+1)}$, then a is q-stable. By induction: $\forall t, 0 \leq t, a^{(q+t)}=a^{(q)}$. Therefore, $a^*=a^{(q)}$.

Matrix methods

Matrix powers, \mathbf{A}^k

$$A^0 = I$$

$$\mathbf{A}^{k+1} = \mathbf{A} \otimes \mathbf{A}^k$$

Closure, A*

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

$$\mathbf{A}^* = \mathbf{I} \oplus \mathbf{A}^1 \oplus \mathbf{A}^2 \oplus \cdots \oplus \mathbf{A}^k \oplus \cdots$$

Note: A* might not exist. Why?

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

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

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

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.

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

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,

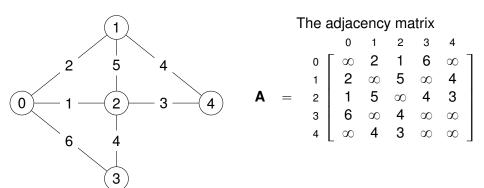
$$\mathbf{A}^* = \mathbf{A}^{(n-1)} = \mathbf{I} \oplus \mathbf{A}^1 \oplus \mathbf{A}^2 \oplus \cdots \oplus \mathbf{A}^{n-1}$$

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



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

(min, +) example

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

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

(min, +) example

$$\mathbf{A} = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 0 & 2 & 1 & 6 & \infty \\ 2 & \infty & 5 & \infty & 4 \\ 1 & 5 & \infty & 4 & 3 \\ 6 & \infty & 4 & \infty & \infty \\ 4 & 2 & 3 & \infty & \infty \end{bmatrix} \quad \mathbf{A}^3 = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 8 & 4 & 3 & 8 & 10 \\ 4 & 8 & 7 & 7 & 6 \\ 3 & 7 & 8 & 6 & 5 \\ 8 & 7 & 6 & 11 & 10 \\ 10 & 6 & 5 & 10 & 12 \end{bmatrix}$$

$$\mathbf{A}^{2} = \begin{bmatrix} 2 & 6 & 7 & \frac{5}{5} & \frac{4}{4} \\ 6 & 4 & \frac{3}{3} & 8 & 8 \\ 7 & \frac{3}{2} & 2 & 7 & 9 \\ \frac{5}{4} & 8 & 9 & \frac{7}{6} \end{bmatrix} \qquad \mathbf{A}^{4} = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 6 & 4 & \frac{3}{3} & 8 & 8 \\ 1 & \frac{3}{4} & \frac{7}{4} & \frac{7}$$

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

A vs A \oplus I

Lemma

If \oplus is idempotent, then

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

Proof. Base case: When k = 0 both expressions are **I**.

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

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

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

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

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

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

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

$$= \mathbf{A}^{(k+1)}$$

back to (min, +) example

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

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

Solving (some) equations

Theorem 6.1

If **A** is q-stable, then **A*** solves the equations

$$L = AL \oplus I$$

and

$$R = RA \oplus I$$
.

For example, to show $\mathbf{L} = \mathbf{A}^*$ solves the first equation:

$$\begin{array}{lll} \mathbf{A}^* &=& \mathbf{A}^{(q)} \\ &=& \mathbf{A}^{(q+1)} \\ &=& \mathbf{A}^{q+1} \oplus \mathbf{A}^q \oplus \ldots \oplus \mathbf{A}^2 \oplus \mathbf{A} \oplus \mathbf{I} \\ &=& \mathbf{A}(\mathbf{A}^q \oplus \mathbf{A}^{q-1} \oplus \ldots \oplus \mathbf{A} \oplus \mathbf{I}) \oplus \mathbf{I} \\ &=& \mathbf{A}\mathbf{A}^{(q)} \oplus \mathbf{I} \\ &=& \mathbf{A}\mathbf{A}^* \oplus \mathbf{I} \end{array}$$

Note that if we replace the assumption "**A** is q-stable" with "**A*** exists," then we require that \otimes distributes over <u>infinite</u> sums.

A more general result

Theorem Left-Right

If **A** is q-stable, then $\mathbf{L} = \mathbf{A}^* \mathbf{B}$ solves the equation

$$L = AL \oplus B$$

and $\mathbf{R} = \mathbf{B}\mathbf{A}^*$ solves

$$R = RA \oplus B$$
.

For the first equation:

$$\mathbf{A}^*\mathbf{B} = \mathbf{A}^{(q)}\mathbf{B}$$

$$= \mathbf{A}^{(q+1)}\mathbf{B}$$

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

$$= (\mathbf{A}^{q+1} \oplus \mathbf{A}^q \oplus \dots \oplus \mathbf{A}^2 \oplus \mathbf{A})\mathbf{B} \oplus \mathbf{B}$$

$$= \mathbf{A}(\mathbf{A}^q \oplus \mathbf{A}^{q-1} \oplus \dots \oplus \mathbf{A} \oplus \mathbf{I})\mathbf{B} \oplus \mathbf{B}$$

$$= \mathbf{A}(\mathbf{A}^{(q)}\mathbf{B}) \oplus \mathbf{B}$$

$$= \mathbf{A}(\mathbf{A}^*\mathbf{B}) \oplus \mathbf{B}$$

The "best" solution

Suppose Y is a matrix such that

$$\mathbf{Y} = \mathbf{AY} \oplus \mathbf{I}$$

If **A** is q-stable and q < k, then

$$\mathbf{Y} = \mathbf{A}^k \mathbf{Y} \oplus \mathbf{A}^*$$

$$\mathbf{Y} = \mathbf{A}\mathbf{Y} \oplus \mathbf{I} \\
= \mathbf{A}^{1}\mathbf{Y} \oplus \mathbf{A}^{(0)} \\
= \mathbf{A}((\mathbf{A}\mathbf{Y} \oplus \mathbf{I})) \oplus \mathbf{I} \\
= \mathbf{A}^{2}\mathbf{Y} \oplus \mathbf{A} \oplus \mathbf{I} \\
= \mathbf{A}^{2}\mathbf{Y} \oplus \mathbf{A}^{(1)} \\
\vdots \vdots \vdots \\
= \mathbf{A}^{k+1}\mathbf{Y} \oplus \mathbf{A}^{(k)}$$

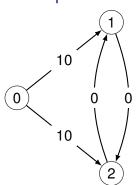
$$\mathbf{Y} \leq^{\underline{L}}_{\oplus} \mathbf{A}^*$$

and if \oplus is idempotent, then

$$\mathbf{Y} \leqslant^{\mathit{L}}_{\oplus} \mathbf{A}^*$$

So **A*** is the largest solution. What does this mean in terms of the sp semiring?

Example with zero weighted cycles using sp semiring



$$\mathbf{A} = \begin{bmatrix} 0 & 1 & 2 \\ 0 & 0 & 10 & 10 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

 A^* (= $A \oplus I$ in this case) solves

$$X = XA \oplus I$$
.

But so does this (dishonest) matrix!

$$\mathbf{F} = \begin{bmatrix} 0 & 1 & 2 \\ 0 & 9 & 9 \\ \infty & 0 & 0 \\ 2 & \infty & 0 & 0 \end{bmatrix}$$

For example:

$$\mathbf{A} = \begin{bmatrix} 0 & 10 & 10 \\ 0 & \infty & \infty & 0 \\ 0 & 0 & \infty \end{bmatrix}$$

$$= \begin{bmatrix} \mathbf{FA} \oplus \mathbf{I})(0,1) \\ 0 & \infty & 0 \\ 0 & 0 & \infty \end{bmatrix}$$

$$= \begin{bmatrix} \mathbf{FA} \oplus \mathbf{I})(0,1) \\ 0 & \mathbf{F}(0,q) + \mathbf{A}(q,1) \\ 0 & \mathbf{F}(0,1,2) \\ 0 & \mathbf{F}(0,1) \end{bmatrix}$$

$$= \begin{bmatrix} \mathbf{FA} \oplus \mathbf{I} \\ 0 & \mathbf{I} \\ 0 & \mathbf{F}(0,1) \end{bmatrix}$$