L11: Algebraic Path Problems with applications to Internet Routing
Lecture 16

Timothy G. Griffin

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

Michaelmas Term, 2014

Dijkstra's algorithm

Input : adjacency matrix $\mathbf{A}$ and source vertex $i \in V$,
Output : the i-th row of $\mathbf{R}$, $\mathbf{R}(i, \_)$.

begin
  $S \leftarrow \{i\}$
  $\mathbf{R}(i, i) \leftarrow \overline{1}$
  for each $q \in V - \{i\}$: $\mathbf{R}(i, q) \leftarrow \mathbf{A}(i, q)$
  while $S \neq V$
    begin
      find $q \in V - S$ such that $\mathbf{R}(i, q)$ is $\leq_{\oplus}^{L}$ -minimal
      $S \leftarrow S \cup \{q\}$
      for each $j \in V - S$
        $\mathbf{R}(i, j) \leftarrow \mathbf{R}(i, j) \oplus (\mathbf{R}(i, q) \otimes \mathbf{A}(q, j))$
    end
end

Classical proofs of Dijkstra's algorithm (for global optimality) assume

Semiring Axioms

$$
\begin{array}{rcrcl}
\text{ADD.ASSOCIATIVE} & : & a \oplus (b \oplus c) & = & (a \oplus b) \oplus c \\
\text{ADD.COMMUTATIVE} & : & a \oplus b & = & b \oplus a \\
\text{ADD.LEFT.ID} & : & \overline{0} \oplus a & = & a \\
\text{MULT.ASSOCIATIVE} & : & a \otimes (b \otimes c) & = & (a \otimes b) \otimes c \\
\text{MULT.LEFT.ID} & : & \overline{1} \otimes a & = & a \\
\text{MULT.RIGHT.ID} & : & a \otimes \overline{1} & = & a \\
\text{MULT.LEFT.ANN} & : & \overline{0} \otimes a & = & \overline{0} \\
\text{MULT.RIGHT.ANN} & : & a \otimes \overline{0} & = & \overline{0} \\
\text{L.DISTRIBUTIVE} & : & a \otimes (b \oplus c) & = & (a \otimes b) \oplus (a \otimes c) \\
\text{R.DISTRIBUTIVE} & : & (a \oplus b) \otimes c & = & (a \otimes c) \oplus (b \otimes c)
\end{array}
$$

Classical proofs of Dijkstra's algorithm assume

Additional axioms

$$
\begin{array}{rcrcl}
\text{ADD.SELECTIVE} & : & a \oplus b & \in & \{a,\ b\} \\
\text{ADD.ANN} & : & \overline{1} \oplus a & = & \overline{1}
\end{array}
$$

Note that we can derive

$$
\text{RIGHT.ABSORBTION} \quad : \quad a \oplus (a \otimes b) \quad = \quad a
$$

and this gives (right) inflationarity, $\forall a, b : a \leq a \otimes b$.

$$
\begin{array}{rcl}
a \oplus (a \otimes b) & = & (a \otimes \overline{1}) \oplus (a \otimes b) \\
 & = & a \otimes (\overline{1} \oplus b) \\
 & = & a \otimes \overline{1} \\
 & = & a
\end{array}
$$

Our goal will be simpler

Theorem 9.1

Given adjacency matrix $\mathbf{A}$ and source vertex $i \in V$, Dijkstra's algorithm will compute $\mathbf{R}(i, \_)$ such that

$$\forall j \in V : \mathbf{R}(i, j) = \mathbf{I}(i,j) \oplus \bigoplus_{q \in V} \mathbf{R}(i, q) \otimes \mathbf{A}(q, j).$$

That is, it computes one row of the solution for the right equation

$$\mathbf{X} = \mathbf{X}\mathbf{A} \oplus \mathbf{I}.$$

What will we assume?

~~Semiring~~ Axioms

ADD.ASSOCIATIVE	:	$a \oplus (b \oplus c)$	$=$	$(a \oplus b) \oplus c$
ADD.COMMUTATIVE	:	$a \oplus b$	$=$	$b \oplus a$
ADD.LEFT.ID	:	$\overline{0} \oplus a$	$=$	a
~~MULT.ASSOCIATIVE~~	:	$\cancel{a \otimes (b \otimes c)}$	$\cancel{=}$	$\cancel{(a \otimes b) \otimes c}$
MULT.LEFT.ID	:	$\overline{1} \otimes a$	$=$	a
~~MULT.RIGHT.ID~~	:	$\cancel{a \otimes \overline{1}}$	$\cancel{=}$	$\cancel{a}$
~~MULT.LEFT.ANN~~	:	$\cancel{\overline{0} \otimes a}$	$\cancel{=}$	$\cancel{\overline{0}}$
~~MULT.RIGHT.ANN~~	:	$\cancel{a \otimes \overline{0}}$	$\cancel{=}$	$\cancel{\overline{0}}$
~~L.DISTRIBUTIVE~~	:	$\cancel{a \otimes (b \oplus c)}$	$\cancel{=}$	$\cancel{(a \otimes b) \oplus (a \otimes c)}$
~~R.DISTRIBUTIVE~~	:	$\cancel{(a \oplus b) \otimes c}$	$\cancel{=}$	$\cancel{(a \otimes c) \oplus (b \otimes c)}$

What will we assume?

Additional axioms

$$
\begin{array}{rcrcl}
\text{ADD.SELECTIVE} & : & a \oplus b & \in & \{a,\ b\} \\
\text{ADD.ANN} & : & \overline{1} \oplus a & = & \overline{1} \\
\text{RIGHT.ABSORBTION} & : & a \oplus (a \otimes b) & = & a
\end{array}
$$

Note that we can no longer derive RIGHT.ABSORBTION, so we must assume it.

Dijkstra's algorithm, annotated version

Subscripts make proofs by induction easier ....

begin
  $S_1 \leftarrow \{i\}$
  $\mathbf{R}_1(i,\ i) \leftarrow \overline{1}$
  for each $q \in V - S_1$: $\mathbf{R}_1(i,\ q) \leftarrow \mathbf{A}(i,\ q)$
  for each $k = 2, 3, \ldots, \mid V \mid$
    begin
      find $q_k \in V - S_{k-1}$ such that $\mathbf{R}(i,\ q)$ is $\leq^{L}_{\oplus}$ -minimal
      $S_k \leftarrow S_{k-1} \cup \{q_k\}$
      for each $j \in V - S_k$
        $\mathbf{R}_k(i,\ j) \leftarrow \mathbf{R}_{k-1}(i,\ j) \oplus (\mathbf{R}_{k-1}(i,\ q_k) \otimes \mathbf{A}(q_k,\ j))$
    end
end

On to the proof ...

Main Claim

$$\forall k : 1 \leq k \leq \mid V \mid \implies \forall j \in S_k : \mathbf{R}_k(i,\ j) = \mathbf{I}(i, j) \oplus \bigoplus_{q \in S_k} \mathbf{R}_k(i,\ q) \otimes \mathbf{A}(q,\ j)$$

Observation 1

$$\forall k : 1 \leq k < \mid V \mid \implies \forall j \in S_{k+1} : \mathbf{R}_k(i,\ j) = \mathbf{R}_{k+1}(i,\ j)$$

This is easy to see — once a node is put into S its weight never changes.

Observation 2

Observation 2

$$\forall k : 1 \leq k \leq \mid V \mid \Longrightarrow \forall q \in S_k : \forall w \in V - S_k : \mathbf{R}_k(i,\ q) \leq \mathbf{R}_k(i,\ w)$$

By induction.
Base : Need $\overline{1} \leq \mathbf{A}(i,\ w)$. OK
Induction. Assume

$$\forall q \in S_k : \forall w \in V - S_k : \mathbf{R}_k(i,\ q) \leq \mathbf{R}_k(i,\ w)$$

and show

$$\forall q \in S_{k+1} : \forall w \in V - S_{k+1} : \mathbf{R}_{k+1}(i,\ q) \leq \mathbf{R}_{k+1}(i,\ w)$$

Since $S_{k+1} = S_k \cup \{q_{k+1}\}$, this is means showing

$$\begin{array}{ll} (1) & \forall q \in S_k : \forall w \in V - S_{k+1} : \mathbf{R}_{k+1}(i,\ q) \leq \mathbf{R}_{k+1}(i,\ w) \\ (2) & \forall w \in V - S_{k+1} : \mathbf{R}_{k+1}(i,\ q_{k+1}) \leq \mathbf{R}_{k+1}(i,\ w) \end{array}$$

By Observation 1, showing (1) is the same as

$$\forall q \in S_k : \forall w \in V - S_{k+1} : \mathbf{R}_k(i,\ q) \leq \mathbf{R}_{k+1}(i,\ w)$$

which expands to (by definition of $\mathbf{R}_{k+1}(i,\ w)$)

$$\forall q \in S_k : \forall w \in V - S_{k+1} : \mathbf{R}_k(i,\ q) \leq \mathbf{R}_k(i,\ w) \oplus (\mathbf{R}_k(i,\ q_{k+1}) \otimes \mathbf{A}(q_{k+1},\ w))$$

But $\mathbf{R}_k(i,\ q) \leq \mathbf{R}_k(i,\ w)$ by the induction hypothesis, and $\mathbf{R}_k(i,\ q) \leq (\mathbf{R}_k(i,\ q_{k+1}) \otimes \mathbf{A}(q_{k+1},\ w))$ by the induction hypothesis and RINF.
Since $a \leq^L_\oplus b \wedge a \leq^L_\oplus c \implies a \leq^L_\oplus (b \oplus c)$, we are done.

By Observation 1, showing (2) is the same as showing

$$\forall w \in V - S_{k+1} : \mathbf{R}_k(i,\ q_{k+1}) \leq \mathbf{R}_{k+1}(i,\ w)$$

which expands to

$$\forall w \in V - S_{k+1} : \mathbf{R}_k(i,\ q_{k+1}) \leq \mathbf{R}_k(i,\ w) \oplus (\mathbf{R}_k(i,\ q_{k+1}) \otimes \mathbf{A}(q_{k+1},\ w))$$

But $\mathbf{R}_k(i,\ q_{k+1}) \leq \mathbf{R}_k(i,\ w)$ since q_{k+1} was chosen to be minimal, and $\mathbf{R}_k(i,\ q_{k+1}) \leq (\mathbf{R}_k(i,\ q_{k+1}) \otimes \mathbf{A}(q_{k+1},\ w))$ by RINF.
Since $a \leq^L_\oplus b \wedge a \leq^L_\oplus c \implies a \leq^L_\oplus (b \oplus c)$, we are done.

Observation 3

Observation 3

$$\forall k : 1 \leq k \leq \mid V \mid \Longrightarrow \forall w \in V - S_k : \mathbf{R}_k(i,\ w) = \bigoplus_{q \in S_k} \mathbf{R}_k(i,\ q) \otimes \mathbf{A}(q,\ w)$$

Proof: By induction:

Base : easy, since

$$\bigoplus_{q \in S_1} \mathbf{R}_1(i,\ q) \otimes \mathbf{A}(q,\ w) = \overline{1} \otimes \mathbf{A}(i,\ w) = \mathbf{A}(i,\ w) = \mathbf{R}_1(i,\ w)$$

Induction step. Assume

$$\forall w \in V - S_k : \mathbf{R}_k(i,\ w) = \bigoplus_{q \in S_k} \mathbf{R}_k(i,\ q) \otimes \mathbf{A}(q,\ w)$$

and show

$$\forall w \in V - S_{k+1} : \mathbf{R}_{k+1}(i,\ w) = \bigoplus_{q \in S_{k+1}} \mathbf{R}_{k+1}(i,\ q) \otimes \mathbf{A}(q,\ w)$$

By Observation 1, and a bit of rewriting, this means we must show

$$\forall w \in V - S_{k+1} : \mathbf{R}_{k+1}(i,\ w) = \mathbf{R}_k(i,\ q_{k+1}) \otimes \mathbf{A}(q_{k+1},\ w) \oplus \bigoplus_{q \in S_k} \mathbf{R}_k(i,\ q) \otimes \mathbf{A}($$

Using the induction hypothesis, this becomes

$$\forall w \in V - S_{k+1} : \mathbf{R}_{k+1}(i,\ w) = \mathbf{R}_k(i,\ q_{k+1}) \otimes \mathbf{A}(q_{k+1},\ w) \oplus \mathbf{R}_k(i,\ w)$$

But this is exactly how $\mathbf{R}_{k+1}(i,\ w)$ is computed in the algorithm.

Proof of Main Claim

Main Claim

$$\forall k : 1 \leq k \leq\mid V \mid \Longrightarrow \forall j \in S_k : \mathbf{R}_k(i,\ j) = \mathbf{I}(i, j) \oplus \bigoplus_{q \in S_k} \mathbf{R}_k(i,\ q) \otimes \mathbf{A}(q,\ j)$$

Proof : By induction on k.
Base case: $S_1 = \{i\}$ and the claim is easy.
Induction: Assume that

$$\forall j \in S_k : \mathbf{R}_k(i,\ j) = \mathbf{I}(i, j) \oplus \bigoplus_{q \in S_k} \mathbf{R}_k(i,\ q) \otimes \mathbf{A}(q,\ j)$$

We must show that

$$\forall j \in S_{k+1} : \mathbf{R}_{k+1}(i,\ j) = \mathbf{I}(i, j) \oplus \bigoplus_{q \in S_{k+1}} \mathbf{R}_{k+1}(i,\ q) \otimes \mathbf{A}(q,\ j)$$

Since $S_{k+1} = S_k \cup \{q_{k+1}\}$, this means we must show

$$\begin{array}{ll} (1) & \forall j \in S_k : \mathbf{R}_{k+1}(i,\ j) = \mathbf{I}(i,j) \oplus \bigoplus_{q \in S_{k+1}} \mathbf{R}_{k+1}(i,\ q) \otimes \mathbf{A}(q,\ j) \\ (2) & \mathbf{R}_{k+1}(i,\ q_{k+1}) = \mathbf{I}(i,q_{k+1}) \oplus \bigoplus_{q \in S_{k+1}} \mathbf{R}_{k+1}(i,\ q) \otimes \mathbf{A}(q,\ q_{k+1}) \end{array}$$

By use Observation 1, showing (1) is the same as showing

$$\forall j \in S_k : \mathbf{R}_k(i,\ j) = \mathbf{I}(i,j) \oplus \bigoplus_{q \in S_{k+1}} \mathbf{R}_k(i,\ q) \otimes \mathbf{A}(q,\ j),$$

which is equivalent to

$$\forall j \in S_k : \mathbf{R}_k(i,\ j) = \mathbf{I}(i,j) \oplus (\mathbf{R}_k(i,\ q_{k+1}) \otimes \mathbf{A}(q_{k+1},\ j)), \oplus \bigoplus_{q \in S_k} \mathbf{R}_k(i,\ q) \otimes \mathbf{A}(q,$$

By the induction hypothesis, this is equivalent to

$$\forall j \in S_k : \mathbf{R}_k(i,\ j) = \mathbf{R}_k(i,\ j) \oplus (\mathbf{R}_k(i,\ q_{k+1}) \otimes \mathbf{A}(q_{k+1},\ j)),$$

Put another way,

$$\forall j \in S_k : \mathbf{R}_k(i,\ j) \le \mathbf{R}_k(i,\ q_{k+1}) \otimes \mathbf{A}(q_{k+1},\ j)$$

By observation 2 we know $\mathbf{R}_k(i,\ j) \le \mathbf{R}_k(i,\ q_{k+1})$, and so

$$\mathbf{R}_k(i,\ j) \le \mathbf{R}_k(i,\ q_{k+1}) \le \mathbf{R}_k(i,\ q_{k+1}) \otimes \mathbf{A}(q_{k+1},\ j)$$

by RINF.

To show (2), we use Observation 1 and $\mathbf{I}(i, q_{k+1}) = \overline{0}$ to obtain

$$\mathbf{R}_k(i,\ q_{k+1}) = \bigoplus_{q \in S_{k+1}} \mathbf{R}_k(i,\ q) \otimes \mathbf{A}(q,\ q_{k+1})$$

which, since $\mathbf{A}(q_{k+1},\ q_{k+1}) = \overline{0}$, is the same as

$$\mathbf{R}_k(i,\ q_{k+1}) = \bigoplus_{q \in S_k} \mathbf{R}_k(i,\ q) \otimes \mathbf{A}(q,\ q_{k+1})$$

This then follows directly from Observation 3.