We want to solve

$$A^* = (A \otimes A^*) \oplus I$$

One approach is successive iteration

$$A^{k+1} = (A \otimes A^k) \oplus I$$
Example: most reliable path

- Imagine links a subject to “problems”
- A message transits link \(e\) with IID probability \(r_e \in [0, 1]\), which we call the link reliability
- The probability of successfully negotiating a path is

\[
r_p = \prod_{e \in p} r_e
\]

- So we want to solve

\[
A_{ij}^* = \max_{p \in P_{ij}} \prod_{e \in p} r_e,
\]

- The natural semiring to use is the Max-times or Viterbi Semiring

\[
(S, \oplus, \otimes, \bar{0}, \bar{1}) = ([0, 1], \max, \times, 0, 1)
\]
Most reliable path example

$$(S, \oplus, \otimes, \bar{0}, \bar{1}) = ([0, 1], \max, \times, 0, 1)$$

$$A = \begin{pmatrix}
0.0 & 0.5 & 0.9 & 0.1 \\
0.5 & 0.0 & 0.9 & 0.9 \\
0.9 & 0.9 & 0.0 & 0.0 \\
0.1 & 0.9 & 0.0 & 0.0
\end{pmatrix}$$

$$I = \begin{pmatrix}
1.0 & 0.0 & 0.0 & 0.0 \\
0.0 & 1.0 & 0.0 & 0.0 \\
0.0 & 0.0 & 1.0 & 0.0 \\
0.0 & 0.0 & 0.0 & 1.0
\end{pmatrix}$$
Most reliable path example

We are calculating

\[ A^{<1>} = \left( A \otimes A^{<0>} \right) \oplus I \]

Note \( A^{<0>} = I \), so first calculate

\[
A \otimes I = \begin{pmatrix}
0.0 & 0.5 & 0.9 & 0.1 \\
0.5 & 0.0 & 0.9 & 0.9 \\
0.9 & 0.9 & 0.0 & 0.0 \\
0.1 & 0.9 & 0.0 & 0.0 \\
\end{pmatrix} \otimes \begin{pmatrix}
1.0 & 0.0 & 0.0 & 0.0 \\
0.0 & 1.0 & 0.0 & 0.0 \\
0.0 & 0.0 & 1.0 & 0.0 \\
0.0 & 0.0 & 0.0 & 1.0 \\
\end{pmatrix}
\]

\[
= \begin{pmatrix}
0.0 & 0.5 & 0.9 & 0.1 \\
0.5 & 0.0 & 0.9 & 0.9 \\
0.9 & 0.9 & 0.0 & 0.0 \\
0.1 & 0.9 & 0.0 & 0.0 \\
\end{pmatrix}
\]

\[
= A
\]
Most reliable path example

We are calculating

\[ A^{<1>} = \left( A \otimes A^{<0>} \right) \oplus I \]

Now \( A \otimes A^{<0>} = A \), so now

\[
A \oplus I = \begin{pmatrix}
0.0 & 0.5 & 0.9 & 0.1 \\
0.5 & 0.0 & 0.9 & 0.9 \\
0.9 & 0.9 & 0.0 & 0.0 \\
0.1 & 0.9 & 0.0 & 0.0
\end{pmatrix} \oplus \begin{pmatrix}
1.0 & 0.0 & 0.0 & 0.0 \\
0.0 & 1.0 & 0.0 & 0.0 \\
0.0 & 0.0 & 1.0 & 0.0 \\
0.0 & 0.0 & 0.0 & 1.0
\end{pmatrix}
\]

\[
= \begin{pmatrix}
1.0 & 0.5 & 0.9 & 0.1 \\
0.5 & 1.0 & 0.9 & 0.9 \\
0.9 & 0.9 & 1.0 & 0.0 \\
0.1 & 0.9 & 0.0 & 1.0
\end{pmatrix}
\]

This tells us the *most reliable path with 1 hop or less*
Most reliable path example

Second iteration

\[ A^{<2>} = (A \otimes A^{<1>}) \oplus I \]

First calculate

\[ A \otimes A^{<1>} = \begin{pmatrix}
0.0 & 0.5 & 0.9 & 0.1 \\
0.5 & 0.0 & 0.9 & 0.9 \\
0.9 & 0.9 & 0.0 & 0.0 \\
0.1 & 0.9 & 0.0 & 0.0
\end{pmatrix} \otimes \begin{pmatrix}
1.0 & 0.5 & 0.9 & 0.1 \\
0.5 & 1.0 & 0.9 & 0.9 \\
0.9 & 0.9 & 1.0 & 0.0 \\
0.1 & 0.9 & 0.0 & 1.0
\end{pmatrix} = \begin{pmatrix}
0.81 & 0.81 & 0.9 & 0.45 \\
0.81 & 0.81 & 0.9 & 0.9 \\
0.9 & 0.9 & 0.81 & 0.81 \\
0.45 & 0.9 & 0.81 & 0.81
\end{pmatrix} \]
Most reliable path example

Second iteration

\[ A^{<2>} = \left( A \otimes A^{<1>} \right) \oplus I \]

Now add the identity

\[
\left( A \otimes A^{<1>} \right) \oplus I = \begin{pmatrix}
0.81 & 0.81 & 0.9 & 0.45 \\
0.81 & 0.81 & 0.9 & 0.9 \\
0.9 & 0.9 & 0.81 & 0.81 \\
0.45 & 0.9 & 0.81 & 0.81 \\
\end{pmatrix} \oplus \begin{pmatrix}
1.0 & 0.0 & 0.0 & 0.0 \\
0.0 & 1.0 & 0.0 & 0.0 \\
0.0 & 0.0 & 1.0 & 0.0 \\
0.0 & 0.0 & 0.0 & 1.0 \\
\end{pmatrix}
= \begin{pmatrix}
1.0 & 0.81 & 0.9 & 0.45 \\
0.81 & 1.0 & 0.9 & 0.9 \\
0.9 & 0.9 & 1.0 & 0.81 \\
0.45 & 0.9 & 0.81 & 1.0 \\
\end{pmatrix}
\]

This tells us the most reliable path with 2 hops or less

Notice that none of the reliabilities went down. They can’t decrease, because we have more options when we allow longer paths. As values are monotonic and bounded, we know they must converge.
Most reliable path example

Third iteration

\[ A^{<3>} = \left( A \otimes A^{<2>} \right) \oplus I \]

\[
\begin{pmatrix}
1.0 & 0.81 & 0.9 & 0.729 \\
0.81 & 1.0 & 0.9 & 0.9 \\
0.9 & 0.9 & 1.0 & 0.81 \\
0.729 & 0.9 & 0.81 & 1.0
\end{pmatrix}
\]

This tells us the *most reliable path with 3 hops or less*
Most reliable path example

Forth iteration

\[ A^{<4>} = (A \otimes A^{<3>}) \oplus I \]

\[
\begin{pmatrix}
1.0 & 0.81 & 0.9 & 0.729 \\
0.81 & 1.0 & 0.9 & 0.9 \\
0.9 & 0.9 & 1.0 & 0.81 \\
0.729 & 0.9 & 0.81 & 1.0
\end{pmatrix}
\]

This tells us the most reliable path with 4 hops or less.

Note that it is the same as the 3-hop version.
Most reliable path example

Fifth iteration

\[
A^{<5>} = (A \otimes A^{<4>}) \oplus I
\]

\[
= \begin{pmatrix}
1.0 & 0.81 & 0.9 & 0.729 \\
0.81 & 1.0 & 0.9 & 0.9 \\
0.9 & 0.9 & 1.0 & 0.81 \\
0.729 & 0.9 & 0.81 & 1.0
\end{pmatrix}
\]

This tells us the most reliable path with 5 hops or less.
Note that it is the same as the 4-hop version.
Most reliable path example

\[ A^{<1>} = A \]
\[ A^{<2>} = \begin{pmatrix}
1.0 & 0.81 & 0.9 & 0.45 \\
0.81 & 1.0 & 0.9 & 0.9 \\
0.9 & 0.9 & 1.0 & 0.81 \\
0.45 & 0.9 & 0.81 & 1.0 \\
\end{pmatrix} \]
\[ A^{<3>} = \begin{pmatrix}
1.0 & 0.81 & 0.9 & 0.729 \\
0.81 & 1.0 & 0.9 & 0.9 \\
0.9 & 0.9 & 1.0 & 0.81 \\
0.729 & 0.9 & 0.81 & 1.0 \\
\end{pmatrix} \]

- \( A^* = A^{<3>} \)
- In a real algorithm we also need to keep track of the predecessor nodes
- In a real problem we hope that it converges before we reach \( A^{<n-1>} \)
Section 1

Path-problem algorithm properties
Fixed-point iteration

- We want to solve
  \[ A^* = \left( A \otimes A^* \right) \oplus I \]

- One approach is successive iteration
  \[
  A^{<0>} = I \\
  A^{<k+1>} = \left( A \otimes A^{<k>} \right) \oplus I
  \]

- When does
  - the iteration converge to a fixed-point?
  - the equation have a unique result?
  - if the equation has more than one result, then which one would the iteration find?
Fixed-point iteration

Lemma

If we take

\[ A^{<0>} = I \]
\[ A^{<k+1>} = \left( A \otimes A^{<k>} \right) \oplus I \]

then \( A^{<k+1>} = A^{(k+1)} = I \oplus A \oplus \cdots \oplus A^k \).

Proof.

By induction. The \( k = 0 \) case is true by definition. Assume it is true for \( k \), then

\[ A^{<k+1>} = \left( A \otimes A^{<k>} \right) \oplus I \]
\[ = \left( A \otimes (I \oplus A \oplus \cdots \oplus A^k) \right) \oplus I \]
\[ = I \oplus A \oplus \cdots \oplus A^{k+1} \]

Note that distributivity and commutativity of \( \oplus \) is required.
**q-Stability**

Take an arbitrary semiring \((S, \oplus, \otimes, 0, 1)\) where we define powers using these operators, *i.e.*,

\[
a^0 = 1, \quad \text{and} \quad a^k = a \otimes a^{k-1}
\]

and we define

\[
a^{(q)} = a^0 \oplus a^1 \oplus a^2 \oplus \cdots \oplus a^q
\]

\[
a^* = a^0 \oplus a^1 \oplus a^2 \oplus \cdots
\]

**Definition (q-stability)**

If there exists a \(q\) such that \(a^{(q)} = a^{(q+1)}\) then we say \(a\) is \(q\)-stable. We say the semiring \(S\) is \(q\)-stable if every \(a \in S\) is \(q\)-stable.
**q-Stability**

**Lemma**

If $a$ is $q$-stable, then $a^* = a^{(q)}$.

**Proof.**

If $a$ is $q$-stable, then $a^{(q)} = a^{(q+1)}$, and by induction we get $a^{(q)} = a^{(q+t)}$ for all $t \geq 0$. Take $t \to \infty$ and we get the result.
Lemma

If $\overline{1}$ is an annihilator for $\oplus$, then $S$ is 0-stable.

$$a \oplus \overline{1} = \overline{1} \oplus a = \overline{1}, \quad \forall a \in S,$$

Examples:

- Boolean: $a \text{ OR } T = T \text{ OR } a = T$
- Min-plus: $\min(a, 0) = \min(0, a) = 0$
- Viterbi: $\max(a, 1) = \max(1, a) = 1$
- lots of others ...
**q-Stability**

**Lemma**

*If* $\bar{1}$ *is an annihilator for* $\oplus$, i.e.,

$$a \oplus \bar{1} = \bar{1} \oplus a = \bar{1}, \; \forall a \in S,$$

*then* $S$ *is 0-stable.*

**Proof.**

$$a^{(1)} = \bar{1} \oplus a$$

$$= \bar{1}$$

$$= a^{(0)}$$
**Lemma**

If $S$ is 0-stable, then $M_n(S)$ is $(n - 1)$-stable, that is

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

- Intuition: annihilation means we can ignore paths with loops, and so the longest possible path has $n - 1$ hops, so we don’t need any higher powers.
- Or, extend the idea that “shortest paths are built from shortest paths”

\[
(a \otimes x \otimes b) \oplus (a \otimes b) = a \otimes (\overline{1} \oplus x) \otimes b, \text{ by distributivity} \\
= a \otimes \overline{1} \otimes b, \text{ by annihilation} \\
= a \otimes b, \text{ as } \overline{1} \text{ is multiplicative identity}
\]

- Primary consequence is that the fixed-point iteration will always converge in at most $n - 1$ steps.
Uniqueness

**Theorem**

If $A$ is $q$-stable, then $A^*$ exists (and hence solves the equations)

$$X = AX \oplus I$$

and $A^*$ is the “least” solution.

**Proof.**

Existence is shown by stability (above), and that it is a solution to the equations in the last lecture.

The remaining issue is the “least.” To answer this, we need to define an ordering.
Binary Relations

Definition

A relation from $A$ to $B$ is a binary operator $x \mathcal{R} y$ for $x \in A$ and $y \in B$ that either “holds”, or does not hold. We say it is a relation on $A$ if $A = B$.

Examples

- “is the mother of”
- “is a friend of”
- “is a multiple of”
- $=$
- $\leq$
- $\subset$
- $\subseteq$
- ...

Matthew Roughan (School of Mathematical Sciences, University of Adelaide)
Orderings

An ordering is a special type of relation on $A$ (that we’ll denote $\leq$) with the properties

- **reflexivity**: $x \leq x$ for all $x \in A$
- **anti-symmetry**: if $x \leq y$ and $y \leq x$ then $x = y$
- **transitivity**: if $x \leq y$ and $y \leq z$ then $x \leq z$

Further, two elements of $A$ are said to be *comparable* if either $x \leq y$ or $y \leq x$, and *incomparable* otherwise. If all elements of $A$ are comparable then $\leq$ defines a *total order*, otherwise it is a *partial order*.

Examples

- $\leq$ defines total order on $\mathbb{R}$
- $\subset$ defines a partial order for the set of subsets of $A$
Orderings

We will write ordering relation here as $\preceq$ or $\succeq$, where we interpret $a \preceq b$ as meaning $b$ is “at least as good” as $a$, or the preferred path to $a$ in path problem.

- Note that this can be far from the standard meaning
  - e.g., in the shortest-path problem, better means shorter so
    $$2 \succeq 3$$
  - e.g., in path properties algebra, where we deal with subsets, it becomes the subset relation
Orderings

An *idempotent*, *commutative*, and *associative* operator $\oplus$ defines ordering as follows:

$$x \preceq y, \quad \text{if and only if} \quad x \oplus y = y$$

Generally, in *path algebras* like this, we want $\oplus$ to be selective, and hence, idempotent, and hence the $\oplus$ operator defines an ordering, with $\bar{0}$ as the least element, *i.e.*, 

$$\bar{0} \leq x, \quad \text{for all} \ x \in S$$

One implication is that

$$y \preceq x \oplus y$$
$$x \preceq x \oplus y$$

*i.e.*, if we can choose between two paths, the result should be at least as good as either of the choices.
Isotonic operators

**Definition (Isotonic)**

We say that an operator \( a \bullet b \) is *isotonic* if

\[
b \preceq c \Rightarrow a \bullet b \preceq a \bullet c
\]

for all \( a \in S \).

- **Intuition:** Think of \( \otimes \) as extending a path, then this says for an isotonic \( \otimes \) if we extend two alternate paths with the same link, the preferred ordering of the extended paths doesn’t change.

- **When** \( \oplus \) is idempotent (and commutative and associative), then it and \( \otimes \) are isotonic.
Isotonic operators

Lemma

For semiring \((S, \oplus, \otimes, \bar{0}, \bar{1})\), if \(\oplus\) is also idempotent it defines an ordering \(\preceq\), i.e.,

\[ x \preceq y, \quad \text{if and only if} \quad x \oplus y = y \]

and both \(\oplus\) and \(\otimes\) are isotone with respect to this ordering.

Proof.

The relation \(\preceq\) is an ordering because it is

- reflexive: \( x \oplus x = x \) through idempotence
- anti-symmetric: \( x \oplus y = y \oplus x \) through commutativity
- transitive: by associativity, \( i.e., \), if \( x \oplus y = y \) and \( y \oplus z = z \) then

\[ x \oplus z = x \oplus (y \oplus z) = (x \oplus y) \oplus z = y \oplus z = z \]
Isotonic operators

Proof.

The operator $\oplus$ can be seen to be isotonic from the definition of $a \oplus b \leq a \oplus c$, i.e.,

\[
(a \oplus b) \oplus (a \oplus c) = (a \oplus a) \oplus (b \oplus c), \quad \text{associativity and commutativity}
\]
\[
= a \oplus (b \oplus c), \quad \text{idempotence}
\]
\[
= a \oplus c, \quad \text{because } b \leq c
\]

Hence $(a \oplus b) \leq (a \oplus c)$ follows from $b \leq c$.

A similar result follows for $\otimes$ using distributivity.
Lemma

For semiring \((S, \oplus, \otimes, \bar{0}, \bar{1})\), if \(\oplus\) and \(\otimes\) are isotone and \(x\) and \(y\) are stable, then
\[ x \preceq y \implies x^* \preceq y^*. \]

Proof.

The proof follows by noting that if \(x\) and \(y\) are stable they can be expanded as a finite sequence of \(\oplus\) and \(\otimes\) operations with themselves, each of which preserves the original order.

Hence, if \(\oplus\) is idempotent, everything else works!
Solutions

Lemma

For semiring \((S, \oplus, \otimes, \bar{0}, \bar{1})\), if \(\oplus\) is idempotent, then the equation 

\[ y = (a \otimes y) \oplus \bar{1} \]

has a solution \(y = a^*\) and this is the least possible solution.

Proof.

We have already shown that idempotence implies stability, and hence that \(y = a^*\) is a solution to the above equation. Now presume that \(y_0\) is any solution to the equation, we can repeatedly substitute it into the equation itself to get

\[ y_0 = (a \otimes [(a \otimes y_0) \oplus \bar{1}]) \oplus \bar{1} = a^2 \otimes y_0 \oplus (a \oplus \bar{1}) \]
Proof.

Repeating results in

\[ y_0 = a^k y_0 \oplus (\bar{1} \oplus a \oplus a^2 \oplus \cdots \oplus a^{k-1}) \]

If \( k > q \) we have \( a^{(q)} = a^* \) and hence

\[ y_0 = a^k y_0 \oplus a^* \]

and hence (because \( x \oplus y \succeq y \))

\[ y_0 \succeq a^* \]

So \( a^* \) is the least solution.

This is a special case of the more general equation \( y = (a \otimes y) \oplus b \), which has solution \( y = a^* b \).
Transitive Closure

$A^*$ is a special case of a transitive closure

- Take some relation between members of the set
  - as expressed by links in the graph
- Extend the relation to a consistent relation over all pairs
  - as expressed by paths between pairs
Section 2

Issues
So we are finished?

- We have a VERY general approach
  - define a semiring with a idempotent $\oplus$
  - extend it to adjacency matrices
  - and we know we can solve path problems

- We can even solve a particular column of $A^*$ at a time by solving
  \[ y = Ay \oplus e_k \]

  - so we can start to apply techniques for doing fast linear algebra
  - e.g., Gauss-Jordan, and better techniques
  - algorithms, e.g., Dijkstra, can be seen as solution techniques from linear algebra

- Does it cover everything?
Is everything a semiring

- Many simple, obvious binary operators are not semigroup operators (and hence can’t be used in semiring).
  - e.g., the average $a \bullet b = (a + b)/2$ is not associative
    
    $$(1 \bullet 2) \bullet 3 = \frac{9}{4} \neq \frac{7}{4} = 1 \bullet (2 \bullet 3)$$

- Some viable operations don’t distribute over others
  - e.g., multi-objective optimisations are often performed by
    
    $$\text{min } objective_1 \text{ subject to } objective_2 < C$$

    can’t translate this into a semiring (as far as I know) except for special cases

- But, there are a vast set of possibilities, especially when we start to compose semirings, e.g., take lexicographic products ...
Further reading I