Automates, algèbre, applications - AAA

CM 1

Uli Fahrenberg Sven Dziadek Philipp Schlehuber
Adrien Pommellet Etienne Renault

EPITA

S6 2022

Foreword

Program of the course

1. CM 1 : Weighted automata — 5 May
2. TD : Weighted automata — 12 May
3. CM 2 : ω-Automata — 19 May

5. TP : ω-Automata — 2 June
6. CM 3 : Automata learning — 16 June
7. CM 4 : LTL model checking — 16 June

Program of the course

1. CM 1 : Weighted automata — 5 May
2. TD : Weighted automata — 12 May
3. CM 2 : ω-Automata — 19 May
4. DM (noté)
5. TP : ω-Automata — 2 June
6. CM 3 : Automata learning — 16 June
7. CM 4 : LTL model checking — 16 June

CM 1 : Weighted automata

1. Semirings
2. Weighted automata
3. Matrix semirings
4. Stars of matrices
5. Power series
6. Kleene-Schützenberger theorem

Sources:

- my "book" covers almost everything, except for the last two slides
- for these, see Chapter 4 of the *Handbook* (which also covers many more things)

Other things to note

DM noté / graded homework:

- énoncé available just after CM 2, 19 May
- to be handed in three days after CM 4, 19 June 13:37 (Paris time)
- exercises mostly on the topics of CM 1 & CM 2 (and TD and TP), but also a bit on CM 3 and CM4 (!)

Automates et applications

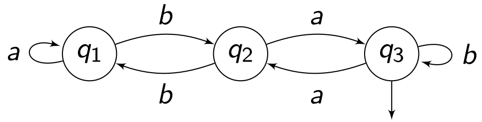
This is an électif developed and given by most of the Automata & applications (A∀) group at LRDE:

We're always happy for research students / internships etc. $\ddot{\smile}$

Introduction

THLR DM 4 exo 6

A :



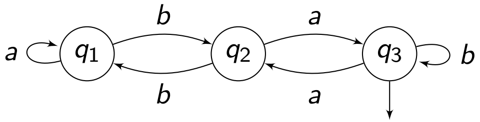
- Let L_i be the language recognized by A with initial state q_i

$$\Rightarrow \quad \begin{aligned} L_1 &= \{a\}L_1 \cup \{b\}L_2 \\ L_2 &= \{a\}L_3 \cup \{b\}L_1 \\ L_3 &= \{a\}L_2 \cup \{b\}L_3 \cup \{\varepsilon\} \end{aligned}$$

- or, as matrix-vector equation: $\begin{bmatrix} L_1 \\ L_2 \\ L_3 \end{bmatrix} = \begin{bmatrix} a & b & \emptyset \\ b & \emptyset & a \\ \emptyset & a & b \end{bmatrix} \begin{bmatrix} L_1 \\ L_2 \\ L_3 \end{bmatrix} \cup \begin{bmatrix} \emptyset \\ \emptyset \\ \varepsilon \end{bmatrix}$

THLR DM 4 exo 6

A :



- Let L_i be the language recognized by A with initial state q_i

$$\Rightarrow \quad \begin{aligned} L_1 &= \{a\}L_1 \cup \{b\}L_2 \\ L_2 &= \{a\}L_3 \cup \{b\}L_1 \\ L_3 &= \{a\}L_2 \cup \{b\}L_3 \cup \{\varepsilon\} \end{aligned}$$

- or, as matrix-vector equation:

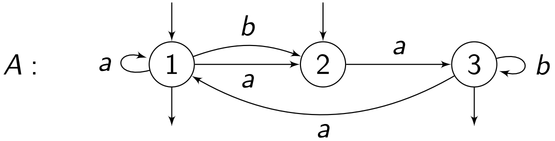
$$\begin{bmatrix} L_1 \\ L_2 \\ L_3 \end{bmatrix} = \begin{bmatrix} a & b & \emptyset \\ b & \emptyset & a \\ \emptyset & a & b \end{bmatrix} \begin{bmatrix} L_1 \\ L_2 \\ L_3 \end{bmatrix} \cup \begin{bmatrix} \emptyset \\ \emptyset \\ \varepsilon \end{bmatrix}$$

$$\vec{L} = M\,\vec{L} \cup \vec{f}$$

Slogan

A finite automaton on Σ is an affine transformation in a "vector space" on the semiring $\mathcal{P}(\Sigma^*)$.

Another example



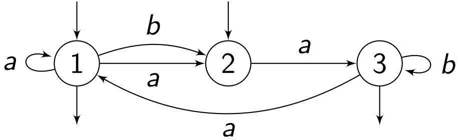
Definition

A weighted automaton with n states on a semiring S is given by a matrix $M \in S^{n\times n}$ and two vectors $\vec{i}, \vec{f} \in S^n$.

- here: $S = \mathcal{P}(\Sigma^*)$, $M = \begin{bmatrix} \{a\} & \{a,b\} & \emptyset \\ \emptyset & \emptyset & \{a\} \\ \{a\} & \emptyset & \{b\} \end{bmatrix}$, $\vec{i} = \begin{bmatrix} \{\varepsilon\} \\ \{\varepsilon\} \\ \emptyset \end{bmatrix}$, $\vec{f} = \begin{bmatrix} \{\varepsilon\} \\ \emptyset \\ \{\varepsilon\} \end{bmatrix}$

Another example

$A:$



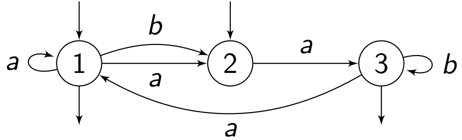
Definition

A weighted automaton with n states on a semiring S is given by a matrix $M \in S^{n\times n}$ and two vectors $\vec{i}, \vec{f} \in S^n$.

- here: $S = \mathcal{P}(\Sigma^*)$, $M = \begin{bmatrix} \{a\} & \{a,b\} & \emptyset \\ \emptyset & \emptyset & \{a\} \\ \{a\} & \emptyset & \{b\} \end{bmatrix}$, $\vec{i} = \begin{bmatrix} \{\varepsilon\} \\ \{\varepsilon\} \\ \emptyset \end{bmatrix}$, $\vec{f} = \begin{bmatrix} \{\varepsilon\} \\ \emptyset \\ \{\varepsilon\} \end{bmatrix}$

1. compute fixed point to
$$\vec{L} = M\,\vec{L} + \vec{f}$$
2. then $L(A) = \vec{i}\,\vec{L}$

Another example

$A :$ 

Definition

A weighted automaton with n states on a semiring S is given by a matrix $M \in S^{n \times n}$ and two vectors $\vec{i}, \vec{f} \in S^n$.

- here: $S = \mathcal{P}(\Sigma^*)$, $M = \begin{bmatrix} \{a\} & \{a,b\} & \emptyset \\ \emptyset & \emptyset & \{a\} \\ \{a\} & \emptyset & \{b\} \end{bmatrix}$, $\vec{i} = \begin{bmatrix} \{\varepsilon\} \\ \{\varepsilon\} \\ \emptyset \end{bmatrix}$, $\vec{f} = \begin{bmatrix} \{\varepsilon\} \\ \emptyset \\ \{\varepsilon\} \end{bmatrix}$

1. compute fixed point to
$$\vec{L} = M\,\vec{L} + \vec{f}$$
2. then $L(A) = \vec{i}\,\vec{L}$

1. compute fixed point to
$$\vec{L'} = \vec{L'}\,M + \vec{i}$$
2. then $L(A) = \vec{L'}\vec{f}$

Lots to unpack . . .

« Automata are affine transformations in "vector spaces" over semirings, and their languages are fixed points to these transformations. »

- What is a semiring?
- What are "vector spaces" (semimodules) over semirings?
- How to compute fixed points to affine transformations in semimodules?
- And to what use is all this? $\ddot\smile$

Semirings

Definition

Remember STAI ?

A ring: algebraic structure $(S, +, \cdot, 0, 1)$

- $+$ associative, commutative, neutral element 0, inverses
- $\cdot$ associative, neutral element 1 may be non-commutative
- distributivity: $a(b+c) = ab + ac$, $(a+b)c = ac + bc$

Canonical example: $\mathbb{Z}$

Definition

Remember STAI ?

A ring: algebraic structure $(S, +, \cdot, 0, 1)$

- $+$ associative, commutative, neutral element 0, inverses
- $\cdot$ associative, neutral element 1 may be non-commutative
- distributivity: $a(b+c) = ab + ac$, $(a+b)c = ac + bc$

Canonical example: $\mathbb{Z}$

Definition

A semiring: algebraic structure $(S, +, \cdot, 0, 1)$

- $+$ associative, commutative, neutral element 0

  may have no inverses
- $\cdot$ associative, neutral element 1
- distributivity: $a(b+c) = ab + ac$, $(a+b)c = ac + bc$
- annihilation: $a0 = 0a = 0$

Annihilation?

Lemma

In any ring, $a0 = 0a = 0$ holds for every a.

Annihilation?

Lemma

In any ring, $a0 = 0a = 0$ holds for every a.

Proof.

$a0 = a(1 - 1) = a - a = 0$

- in semirings, no « $-$ » !

Examples

Definition

A semiring: algebraic structure $(S, +, \cdot, 0, 1)$

- $+$ associative, commutative, neutral element 0
- $\cdot$ associative, neutral element 1
- distributivity: $a(b+c) = ab + ac$, $(a+b)c = ac + bc$
- annihilation: $a0 = 0a = 0$

- to avoid confusion, sometimes write $(S, \oplus, \otimes, \mathbb{0}, \mathbb{1})$

Examples

Definition

A semiring: algebraic structure $(S, +, \cdot, 0, 1)$

- $+$ associative, commutative, neutral element 0
- $\cdot$ associative, neutral element 1
- distributivity: $a(b+c) = ab + ac$, $(a+b)c = ac + bc$
- annihilation: $a0 = 0a = 0$

- natural numbers: $(\mathbb{N}, +, \cdot, 0, 1)$
  - commutative semiring
  - also $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$

Examples

Definition

A semiring: algebraic structure $(S, +, \cdot, 0, 1)$

- $+$ associative, commutative, neutral element 0
- $\cdot$ associative, neutral element 1
- distributivity: $a(b+c) = ab + ac$, $(a+b)c = ac + bc$
- annihilation: $a0 = 0a = 0$

- natural numbers: $(\mathbb{N}, +, \cdot, 0, 1)$
- min-plus semiring: $(\mathbb{R} \cup \{\infty\}, \min, +, \infty, 0)$
  - commutative semiring
  - also $\mathbb{R}_+ \cup \{\infty\}$ or $\mathbb{N} \cup \{\infty\}$

Examples

Definition

A semiring: algebraic structure $(S, +, \cdot, 0, 1)$

- $+$ associative, commutative, neutral element 0
- $\cdot$ associative, neutral element 1
- distributivity: $a(b+c) = ab + ac$, $(a+b)c = ac + bc$
- annihilation: $a0 = 0a = 0$

- natural numbers: $(\mathbb{N}, +, \cdot, 0, 1)$
- min-plus semiring: $(\mathbb{R} \cup \{\infty\}, \min, +, \infty, 0)$
- boolean semiring: $(\{\mathtt{true}, \mathtt{false}\}, \vee, \wedge, \mathtt{false}, \mathtt{true})$
  - commutative semiring
  - self-dual: $(\{\mathtt{true}, \mathtt{false}\}, \wedge, \vee, \mathtt{true}, \mathtt{false})$

Examples

Definition

A semiring: algebraic structure $(S, +, \cdot, 0, 1)$

- $+$ associative, commutative, neutral element 0
- $\cdot$ associative, neutral element 1
- distributivity: $a(b+c) = ab + ac$, $(a+b)c = ac + bc$
- annihilation: $a0 = 0a = 0$

- natural numbers: $(\mathbb{N}, +, \cdot, 0, 1)$
- min-plus semiring: $(\mathbb{R} \cup \{\infty\}, \min, +, \infty, 0)$
- boolean semiring: $(\{\texttt{true}, \texttt{false}\}, \vee, \wedge, \texttt{false}, \texttt{true})$
- language semirings: $(\mathcal{P}(\Sigma^*), \cup, \cdot, \emptyset, \{\varepsilon\})$
  - for any Σ
  - « $\cdot$ » is concatenation of languages
  - non-commutative for $|\Sigma| \geq 2$

Min-plus semiring

The min-plus semiring: $(\mathbb{R} \cup \{\infty\}, \min, +, \infty, 0)$

- min associative, commutative, neutral element ∞ ?

Min-plus semiring

The min-plus semiring: $(\mathbb{R} \cup \{\infty\}, \min, +, \infty, 0)$

- min associative, commutative, neutral element ∞ ?
    - $\min(\min(a, b), c) = \min(a, \min(b, c))$?

Min-plus semiring

The min-plus semiring: $(\mathbb{R} \cup \{\infty\}, \min, +, \infty, 0)$

- min associative, commutative, neutral element ∞ ?
  - $\min(\min(a, b), c) = \min(a, \min(b, c))$
  - $\min(a, b) = \min(b, a)$?

Min-plus semiring

The min-plus semiring: $(\mathbb{R} \cup \{\infty\}, \min, +, \infty, 0)$

- min associative, commutative, neutral element ∞ ?
  - $\min(\min(a, b), c) = \min(a, \min(b, c))$
  - $\min(a, b) = \min(b, a)$
  - $\min(a, \infty) = a$?

Min-plus semiring

The min-plus semiring: $(\mathbb{R} \cup \{\infty\}, \min, +, \infty, 0)$

- min associative, commutative, neutral element ∞
  - $\min(\min(a, b), c) = \min(a, \min(b, c))$
  - $\min(a, b) = \min(b, a)$
  - $\min(a, \infty) = a$
- $+$ associative, *commutative*, neutral element 0 ?

Min-plus semiring

The min-plus semiring: $(\mathbb{R} \cup \{\infty\}, \min, +, \infty, 0)$

- min associative, commutative, neutral element ∞
  - $\min(\min(a, b), c) = \min(a, \min(b, c))$
  - $\min(a, b) = \min(b, a)$
  - $\min(a, \infty) = a$
- $+$ associative, *commutative*, neutral element 0
- distributivity: $a + \min(b, c) = \min(a + b, a + c)$?
  - (was $a \otimes (b \oplus c) = a \otimes b \oplus a \otimes c$)

Min-plus semiring

The min-plus semiring: $(\mathbb{R} \cup \{\infty\}, \min, +, \infty, 0)$

- min associative, commutative, neutral element ∞
  - $\min(\min(a, b), c) = \min(a, \min(b, c))$
  - $\min(a, b) = \min(b, a)$
  - $\min(a, \infty) = a$
- $+$ associative, *commutative*, neutral element 0
- distributivity: $a + \min(b, c) = \min(a + b, a + c)$
  - (was $a \otimes (b \oplus c) = a \otimes b \oplus a \otimes c$)
- annihilation: $a + \infty = \infty$?
  - (was $a \otimes 0 = 0$)
  - by convention . . .

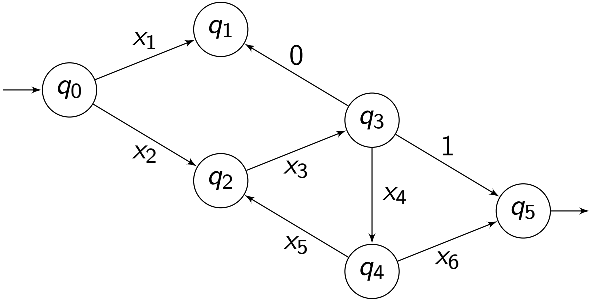
Weighted automata

Definition

Definition

A weighted automaton over a semiring S: structure (Q, I, F, T)

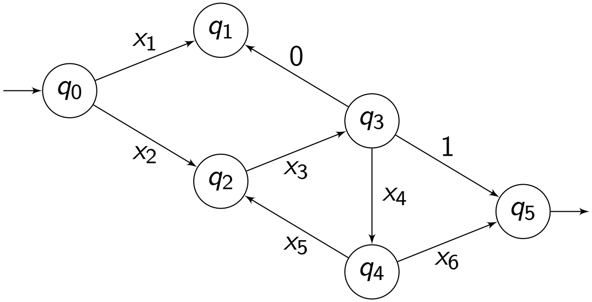
- Q: finite set of states
- $I, F \subseteq Q$: initial and accepting states
- $T \subseteq Q \times S \times Q$: finite transition relation



Paths

- Paths are sequences of transitions (as usual)
- The value of path $\pi = q_1 \xrightarrow{x_1} q_2 \xrightarrow{x_2} \cdots \xrightarrow{x_n} q_{n+1}$:

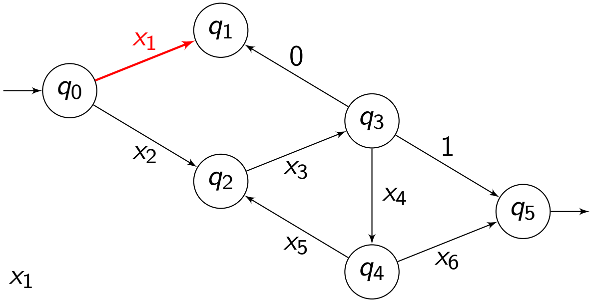
$$|\pi| = x_1 x_2 \cdots x_n$$



Paths

- Paths are sequences of transitions (as usual)
- The value of path $\pi = q_1 \xrightarrow{x_1} q_2 \xrightarrow{x_2} \cdots \xrightarrow{x_n} q_{n+1}$:

$$|\pi| = x_1 x_2 \cdots x_n$$

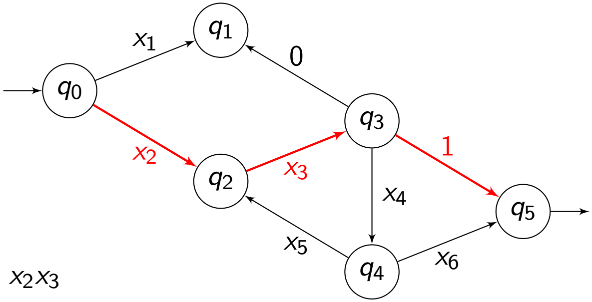


$|\pi| = x_1$

Paths

- Paths are sequences of transitions (as usual)
- The value of path $\pi = q_1 \xrightarrow{x_1} q_2 \xrightarrow{x_2} \cdots \xrightarrow{x_n} q_{n+1}$:

$$|\pi| = x_1 x_2 \cdots x_n$$

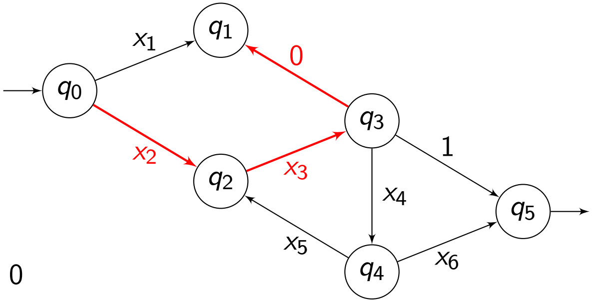


$|\pi| = x_2 x_3$

Paths

- Paths are sequences of transitions (as usual)
- The value of path $\pi = q_1 \xrightarrow{x_1} q_2 \xrightarrow{x_2} \cdots \xrightarrow{x_n} q_{n+1}$:

$$|\pi| = x_1 x_2 \cdots x_n$$

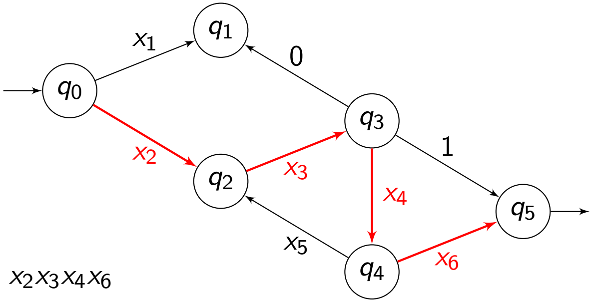


$|\pi| = 0$

Paths

- Paths are sequences of transitions (as usual)
- The value of path $\pi = q_1 \xrightarrow{x_1} q_2 \xrightarrow{x_2} \cdots \xrightarrow{x_n} q_{n+1}$:

$$|\pi| = x_1 x_2 \cdots x_n$$

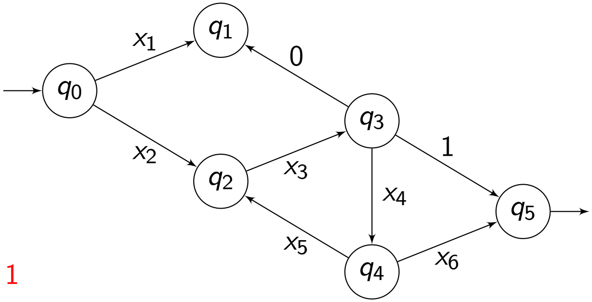


$|\pi| = x_2 x_3 x_4 x_6$

Paths

- Paths are sequences of transitions (as usual)
- The value of path $\pi = q_1 \xrightarrow{x_1} q_2 \xrightarrow{x_2} \cdots \xrightarrow{x_n} q_{n+1}$:

$$|\pi| = x_1 x_2 \cdots x_n$$

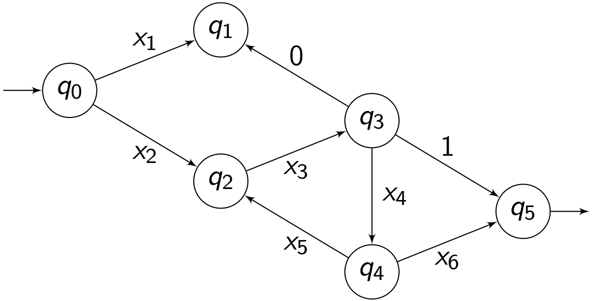


$|\varepsilon| = 1$

"Languages"

- Accepting paths: as usual
- The value of automaton A:

$$|A| = \bigoplus \{\!\{ |\pi| \mid \pi \text{ accepting path in } A \}\!\}$$

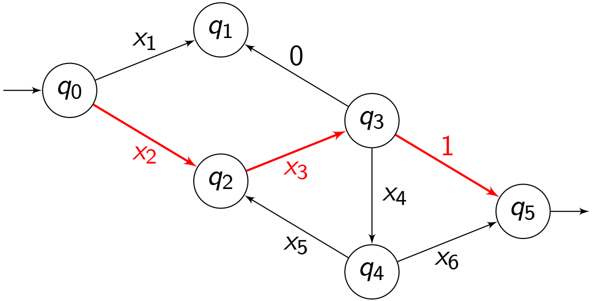


$|A| =$

"Languages"

- Accepting paths: as usual
- The value of automaton A:

$$|A| = \bigoplus \{\!\{ |\pi| \mid \pi \text{ accepting path in } A \}\!\}$$

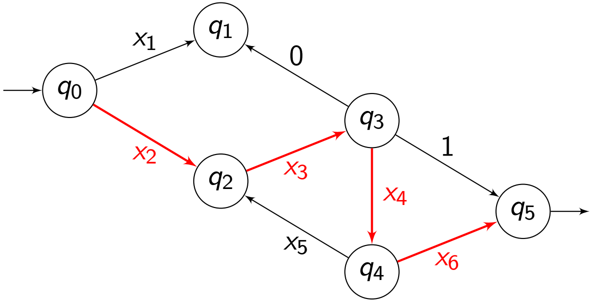


$|A| = x_2 x_3$

"Languages"

- Accepting paths: as usual
- The value of automaton A:

$$|A| = \bigoplus \{\!\{ |\pi| \mid \pi \text{ accepting path in } A \}\!\}$$

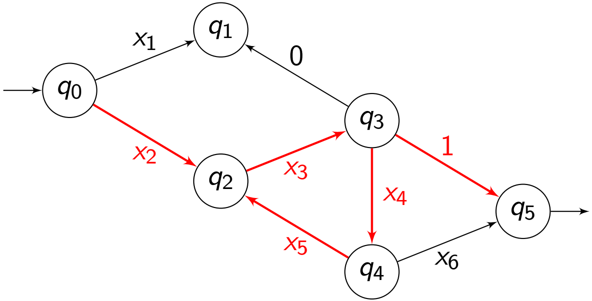


$$|A| = x_2x_3 + x_2x_3x_4x_6$$

"Languages"

- Accepting paths: as usual
- The value of automaton A:

$$|A| = \bigoplus \{\!\{ |\pi| \mid \pi \text{ accepting path in } A \}\!\}$$

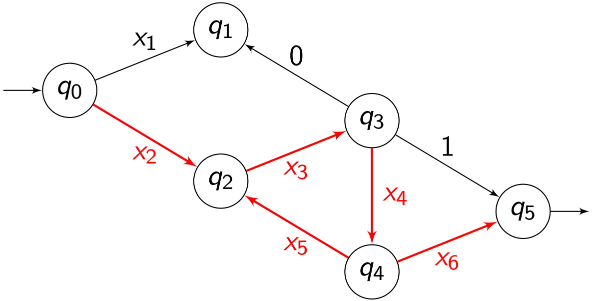


$$|A| = x_2x_3 + x_2x_3x_4x_6 + x_2x_3x_4x_5x_3$$

“Languages”

- Accepting paths: as usual
- The value of automaton A:

$$|A| = \bigoplus \{\!\{ |\pi| \mid \pi \text{ accepting path in } A \}\!\}$$



$$|A| = x_2x_3 + x_2x_3x_4x_6 + x_2x_3x_4x_5x_3 + x_2x_3x_4x_5x_3x_4x_6 + \cdots$$

- an infinite sum !?

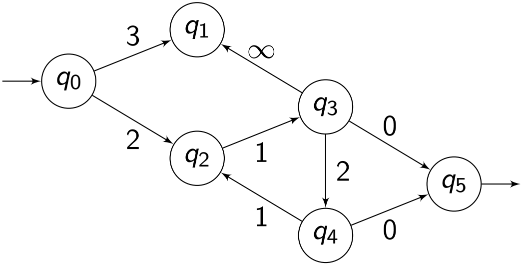
Values of weighted automata

- The value of a path is the product of its labels.
- The value of a weighted automaton is the sum of the values of all its accepting paths, if that sum exists.

$$|A| = \bigoplus \{\!\{ |\pi| \mid \pi \text{ accepting path in } A \}\!\}$$

- So, how to make sure that $|A|$ exists?

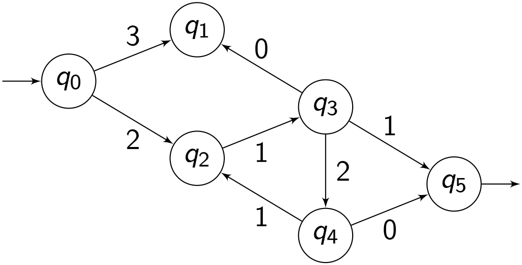
Example: min-plus semiring



$$
\begin{aligned}
|A| &= \bigoplus \{\!\{ |\pi| \mid \pi \text{ accepting path in } A \}\!\} \\
&= \min \{ |\pi| \mid \pi \text{ accepting path in } A \} \\
&= \min \{ 2+1+0, 2+1+2+0, 2+1+2+1+1+0, \dots \} \\
&= 3
\end{aligned}
$$

- In the min-plus semiring, $|A|$ is the length of a shortest path
- ... and $|A|$ always exists

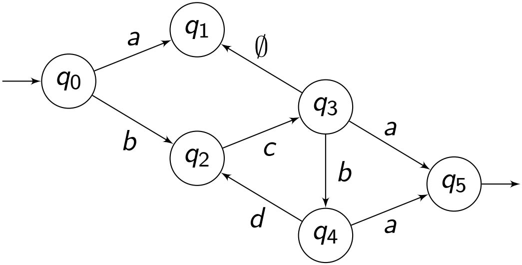
Example: natural numbers



$$
\begin{aligned}
|A| &= \bigoplus \{\!\{ |\pi| \mid \pi \text{ accepting path in } A \}\!\} \\
&= \bigoplus \{\!\{ 2\cdot 1\cdot 1, 2\cdot 1\cdot 2\cdot 0, 2\cdot 1\cdot 2\cdot 1\cdot 1\cdot 1, \dots \}\!\} \\
&= \bigoplus \{\!\{ 2, 0, 4, \dots \}\!\} \\
&= \bigoplus \{\!\{ 2, 4, 8, 16, \dots \}\!\} \to \infty
\end{aligned}
$$

- In $\mathbb{N}$, $|A|$ does not always exist

Example: languages



$$
\begin{aligned}
|A| &= \bigoplus \{\!\{ |\pi| \mid \pi \text{ accepting path in } A \}\!\} \\
&= \{ bca, bcba, bcbdca, bcbdcba, \dots \} \\
&= \{b\} \cdot \{cbd\}^* \cdot \{ca, cba\}
\end{aligned}
$$

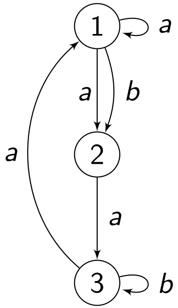
- In $\mathcal{P}(\Sigma^*)$, $|A| = L(A)$, the usual language
- It seems we might need a star...

Linear algebra over semirings

Weighted automata as matrices

- Let (Q, I, F, T) be a weighted automaton over S
- Write $Q = \{1, \dots, n\}$
- Define a matrix $M \in S^{n \times n}$ by

$$M_{pq} = \bigoplus \{\!\{ x \mid (p, x, q) \in T \}\!\}$$



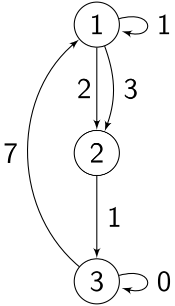
$$S = \mathcal{P}(\Sigma^*)$$

$$M = \begin{bmatrix} \{a\} & \{a, b\} & \emptyset \\ \emptyset & \emptyset & \{a\} \\ \{a\} & \emptyset & \{b\} \end{bmatrix}$$

Weighted automata as matrices

- Let (Q, I, F, T) be a weighted automaton over S
- Write $Q = \{1, \dots, n\}$
- Define a matrix $M \in S^{n \times n}$ by

$$M_{pq} = \bigoplus \{\!\{ x \mid (p, x, q) \in T \}\!\}$$



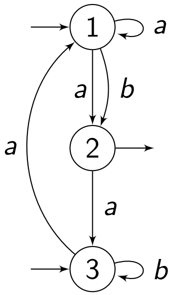
$S = \mathbb{N}$

$$M = \begin{bmatrix} 1 & 5 & 0 \\ 0 & 0 & 1 \\ 7 & 0 & 0 \end{bmatrix}$$

Weighted automata as matrices, II

- (Q, I, F, T) weighted automaton over S, $Q = \{1, \dots, n\}$
- $M \in S^{n \times n}$ given by $M_{pq} = \bigoplus \{\!\{ x \mid (p, x, q) \in T \}\!\}$
- Define vectors $\vec{i}, \vec{f} \in \{0, 1\}^n$ by

$$\vec{i}_q = \begin{cases} 1 & \text{if } q \in I \\ 0 & \text{otherwise} \end{cases} \qquad \vec{f}_q = \begin{cases} 1 & \text{if } q \in F \\ 0 & \text{otherwise} \end{cases}$$



$$S = \mathcal{P}(\Sigma^*)$$

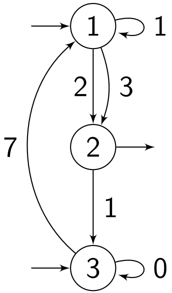
$$M = \begin{bmatrix} \{a\} & \{a, b\} & \emptyset \\ \emptyset & \emptyset & \{a\} \\ \{a\} & \emptyset & \{b\} \end{bmatrix}$$

$$\vec{i} = \begin{bmatrix} \{\varepsilon\} \\ \emptyset \\ \{\varepsilon\} \end{bmatrix} \qquad \vec{f} = \begin{bmatrix} \emptyset \\ \{\varepsilon\} \\ \emptyset \end{bmatrix}$$

Weighted automata as matrices, II

- (Q, I, F, T) weighted automaton over S, $Q = \{1, \dots, n\}$
- $M \in S^{n \times n}$ given by $M_{pq} = \bigoplus \{\!\{ x \mid (p, x, q) \in T \}\!\}$
- Define vectors $\vec{i}, \vec{f} \in \{0, 1\}^n$ by

$$\vec{i}_q = \begin{cases} 1 & \text{if } q \in I \\ 0 & \text{otherwise} \end{cases} \qquad \vec{f}_q = \begin{cases} 1 & \text{if } q \in F \\ 0 & \text{otherwise} \end{cases}$$



$S = \mathbb{N}$

$$M = \begin{bmatrix} 1 & 5 & 0 \\ 0 & 0 & 1 \\ 7 & 0 & 0 \end{bmatrix}$$

$$\vec{i} = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} \qquad \vec{f} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$$

Weighted automata as matrices, III

- (Q, I, F, T) weighted automaton over S, $Q = \{1, \dots, n\}$
- $M \in S^{n \times n}$ given by $M_{pq} = \bigoplus \{\!\{x \mid (p, x, q) \in T\}\!\}$
- $\vec{i}, \vec{f} \in \{0, 1\}^n$ given by $\vec{i}_q = 1$ iff $q \in I$, $\vec{f}_q = 1$ iff $q \in F$
- Conversely, if we have $(\vec{i}, M, \vec{f})$, we can define (Q, I, F, T):
  - $Q = \{1, \dots, n\}$
  - $I = \{q \in Q \mid \vec{i}_q = 1\}$, $F = \{q \in Q \mid \vec{f}_q = 1\}$
  - $T = \{(p, M_{pq}, q) \mid p, q \in Q\}$

Weighted automata as matrices, III

- (Q, I, F, T) weighted automaton over S, $Q = \{1, \dots, n\}$
- $M \in S^{n \times n}$ given by $M_{pq} = \bigoplus \{\!\{ x \mid (p, x, q) \in T \}\!\}$
- $\vec{i}, \vec{f} \in \{0, 1\}^n$ given by $\vec{i}_q = 1$ iff $q \in I$, $\vec{f}_q = 1$ iff $q \in F$
- Conversely, if we have $(\vec{i}, M, \vec{f})$, we can define (Q, I, F, T):
  - $Q = \{1, \dots, n\}$
  - $I = \{q \in Q \mid \vec{i}_q = 1\}$, $F = \{q \in Q \mid \vec{f}_q = 1\}$
  - $T = \{(p, M_{pq}, q) \mid p, q \in Q\}$

Re-definition

A weighted automaton with n states on a semiring S is given by a matrix $M \in S^{n \times n}$ and two vectors $\vec{i}, \vec{f} \in S^n$.

- "no transition $p \to q$" is equivalent to $M_{pq} = 0$
- have generalized $\vec{i}$ and $\vec{f}$ from $\in \{0, 1\}^n$ to $\in S^n$

Computing values

Theorem

Let $A = (\vec{i}, M, \vec{f})$ *be a weighted automaton. If* $|A|$ *exists, then*

$$|A| = \bigoplus_{n \geq 0} \vec{i}\, M^n\, \vec{f}$$

Proof (sketch):

Computing values

Theorem

Let $A = (\vec{i}, M, \vec{f})$ be a weighted automaton. If $|A|$ exists, then

$$|A| = \bigoplus_{n \geq 0} \vec{i}\, M^n\, \vec{f}$$

Proof (sketch):

- M collects values of paths of length 1

Computing values

Theorem

Let $A = (\vec{i}, M, \vec{f})$ be a weighted automaton. If $|A|$ exists, then

$$|A| = \bigoplus_{n \geq 0} \vec{i}\, M^n\, \vec{f}$$

Proof (sketch):

- M collects values of paths of length 1
- M^2 collects values of paths of length 2, etc.

Computing values

Theorem

Let $A = (\vec{i}, M, \vec{f})$ be a weighted automaton. If $|A|$ exists, then

$$|A| = \bigoplus_{n \geq 0} \vec{i}\, M^n\, \vec{f}$$

Proof (sketch):

- M collects values of paths of length 1
- M^2 collects values of paths of length 2, etc.
- $\vec{i}\, M^n\, \vec{f}$ selects paths of length n which start in an initial state and end in an accepting state

Computing values

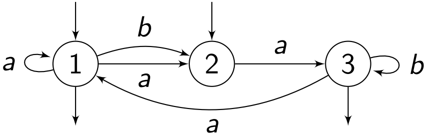
Theorem

Let $A = (\vec{i}, M, \vec{f})$ be a weighted automaton. If $|A|$ exists, then

$$|A| = \bigoplus_{n \geq 0} \vec{i}\, M^n\, \vec{f}$$

Proof (sketch):

- M collects values of paths of length 1
- M^2 collects values of paths of length 2, etc.
- $\vec{i}\, M^n\, \vec{f}$ selects paths of length n which start in an initial state and end in an accepting state



$$M = \begin{bmatrix} \{a\} & \{a, b\} & \emptyset \\ \emptyset & \emptyset & \{a\} \\ \{a\} & \emptyset & \{b\} \end{bmatrix}$$

Computing values

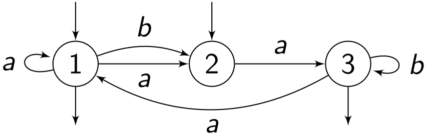
Theorem

Let $A = (\vec{i}, M, \vec{f})$ be a weighted automaton. If $|A|$ exists, then

$$|A| = \bigoplus_{n \geq 0} \vec{i}\, M^n\, \vec{f}$$

Proof (sketch):

- M collects values of paths of length 1
- M^2 collects values of paths of length 2, etc.
- $\vec{i}\, M^n\, \vec{f}$ selects paths of length n which start in an initial state and end in an accepting state



$$M^2 = \begin{bmatrix} \{aa\} & \{aa, ab\} & \{aa, ba\} \\ \{aa\} & \emptyset & \{ab\} \\ \{aa, ba\} & \{aa, ab\} & \{bb\} \end{bmatrix}$$

Infinite distributivity

Let $A = (\vec{i}, M, \vec{f})$ be a weighted automaton. If $|A|$ exists, then

$$|A| = \bigoplus_{n \geq 0} \vec{i}\, M^n\, \vec{f}$$

Infinite distributivity

Let $A = (\vec{i}, M, \vec{f})$ be a weighted automaton. If $|A|$ exists, then

$$|A| = \bigoplus_{n \geq 0} \vec{i}\, M^n\, \vec{f} = \vec{i} \left(\bigoplus_{n \geq 0} M^n \right) \vec{f}$$

- ... if we assume infinite distributivity
- But wait, $\bigoplus_{n \geq 0} M^n$ is a geometric series

Infinite distributivity

Let $A = (\vec{i}, M, \vec{f})$ be a weighted automaton. If $|A|$ exists, then

$$|A| = \bigoplus_{n \geq 0} \vec{i}\, M^n\, \vec{f} = \vec{i} \left(\bigoplus_{n \geq 0} M^n \right) \vec{f}$$

- ... if we assume infinite distributivity
- But wait, $\bigoplus_{n \geq 0} M^n$ is a geometric series

$$??? \qquad \bigoplus_{n \geq 0} M^n = \frac{1}{1 - M} \qquad ???$$

- in a semiring, no subtraction nor division ...

Star-continuous semirings

Definition

A semiring S is star-continuous if

1. the infinite sums $\bigoplus_{n\geq 0} a^n$ exist for all $a \in S$
2. for all $a, b, c \in S$, $\bigoplus_{n\geq 0} ab^n c = a \left(\bigoplus_{n\geq 0} b^n \right) c$

- geometric series plus infinite distributivity

Star-continuous semirings

Definition

A semiring S is star-continuous if

1. the infinite sums $\bigoplus_{n\geq 0} a^n$ exist for all $a \in S$
2. for all $a, b, c \in S$, $\bigoplus_{n\geq 0} ab^n c = a\left(\bigoplus_{n\geq 0} b^n\right) c$

- geometric series plus infinite distributivity

Definition

In a star-continuous semiring, $a^* = \bigoplus_{n\geq 0} a^n$

Examples

$$a^* = \bigoplus_{n\geq 0} a^n$$

- in $\mathcal{P}(\Sigma^*)$: $L^* = \bigcup_{n\geq 0} L^n = L^*$
- $\mathbb{N}$ is not star-continuous: $\bigcup_{n\geq 0} 2^n \to \infty$
- in min-plus $\mathbb{N} \cup \{\infty\}$: $a^* = \min\{0, a, a+a, a+a+a, \dots\} = 0$

Examples

$$a^* = \bigoplus_{n \geq 0} a^n$$

- in $\mathcal{P}(\Sigma^*)$: $L^* = \bigcup_{n \geq 0} L^n = L^*$
- $\mathbb{N}$ is not star-continuous: $\bigcup_{n \geq 0} 2^n \to \infty$
- in min-plus $\mathbb{N} \cup \{\infty\}$: $a^* = \min \{0, a, a+a, a+a+a, \dots\} = 0$

Operationally, stars are loops

- in min-plus, shortest paths never include loops

Stars are fixed points

Look:

$$
\begin{aligned}
& & a^* = \bigoplus_{n\geq 0} a^n = \frac{1}{1-a} \\
&\iff & (1-a)a^* = 1 \\
&\iff & a^* - aa^* = 1 \\
&\iff & a^* = 1 + aa^*
\end{aligned}
$$

Stars are fixed points

Look:

$$\left.\begin{aligned} a^* = \bigoplus_{n\geq 0} a^n &= \frac{1}{1-a} \\ \iff \quad (1-a)a^* &= 1 \\ \iff \quad a^* - aa^* &= 1 \end{aligned}\right\} \text{illegal}$$

$$\iff \quad a^* = 1 + aa^* \quad \Leftarrow \text{true}$$

Lemma

If S is star-continuous, then $a^* = aa^* + 1 = a^*a + 1$ for all $a \in S$.

Matrices

If S is a semiring (and $n \geq 1$), then $S^{n\times n}$ is also a semiring

- with usual matrix addition and matrix multiplication

Lemma

If S is star-continuous, then so is $S^{n\times n}$, with

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^* = \begin{bmatrix} (a+bd^*c)^* & (a+bd^*c)^*bd^* \\ (d+ca^*b)^*ca^* & (d+ca^*b)^* \end{bmatrix}$$

for any block matrix.

- so this is recursive: a, b, c, d may be matrices themselves
- see Floyd-Warshall! see Brzozowski-McCluskey!

Stars of matrices

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^* = \begin{bmatrix} (a + bd^*c)^* & (a + bd^*c)^*bd^* \\ (d + ca^*b)^*ca^* & (d + ca^*b)^* \end{bmatrix}$$

Floyd-Warshall:

for $p \in Q$ **do**
  for $q \in Q$ **do**
    for $r \in Q$ **do**
      $M_{pq} \leftarrow \min\left(M_{pq}, M_{pr} + M_{rq}\right)$

- aka $M_{pq} \leftarrow M_{pq} \oplus M_{pr} \otimes M_{rq}$
- why no star?

Stars of matrices

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^* = \begin{bmatrix} (a+bd^*c)^* & (a+bd^*c)^*bd^* \\ (d+ca^*b)^*ca^* & (d+ca^*b)^* \end{bmatrix}$$

Brzozowski-McCluskey (one step):

Choose $r \in Q$
for $p \in Q$ **do**
  for $q \in Q$ **do**
    $M_{pq} \leftarrow M_{pq} + M_{pr} M_{rr}^* M_{rq}$
$Q \leftarrow Q \setminus \{r\}$

Putting things together

« Automata are affine transformations in "vector spaces" over semirings, and their languages are fixed points to these transformations. »

- a weighted automaton over S with n states: $(\vec{i}, M, \vec{f})$
  - $\vec{i}, \vec{f} \in S^n$, $M \in S^{n \times n}$

Putting things together

« Automata are affine transformations in "vector spaces" over semirings, and their languages are fixed points to these transformations. »

- a weighted automaton over S with n states: $(\vec{i}, M, \vec{f})$
  - $\vec{i}, \vec{f} \in S^n$, $M \in S^{n \times n}$
- if $\vec{L}$ is the vector of values with initial states i, then $\vec{L} = M\vec{L} + \vec{f}$
  - $\vec{x} \mapsto M\vec{x} + \vec{f}$ is an affine transformation $S^n \to S^n$
  - viewing S^n as a semimodule over S

Putting things together

« Automata are affine transformations in "vector spaces" over semirings, and their languages are fixed points to these transformations. »

- a weighted automaton over S with n states: $(\vec{i}, M, \vec{f})$
  - $\vec{i}, \vec{f} \in S^n$, $M \in S^{n\times n}$
- if $\vec{L}$ is the vector of values with initial states i, then $\vec{L} = M\,\vec{L} + \vec{f}$
  - $\vec{x} \mapsto M\,\vec{x} + \vec{f}$ is an affine transformation $S^n \to S^n$
  - viewing S^n as a semimodule over S
- $M^* = M\,M^* + 1 \Rightarrow M^*\vec{f} = M\,M^*\vec{f} + \vec{f}$
  - so $\vec{L} = M^*\vec{f}$ is a fixed point!

$$\Rightarrow \quad |A| = \vec{i}\,M^*\vec{f}$$

Semimodules and Linear Transformations

- a vector space over a field K: an abelian group $(V, +, 0)$ and an action $\cdot : K \times V \to V$:
  - $x(u+v) = xu+xv$, $(x+y)v = xv+yv$, $(xy)v = x(yv)$, $1v = v$

Semimodules and Linear Transformations

- a vector space over a field K: an abelian group $(V, +, 0)$ and an action $\cdot : K \times V \to V$:
  - $x(u+v) = xu+xv$, $(x+y)v = xv+yv$, $(xy)v = x(yv)$, $1v = v$
- a left module over a ring R: an abelian group $(V, +, 0)$ and an action $\cdot : R \times V \to V$:
  - same axioms as above
  - right module: $\cdot : V \times R \to V$ (why the difference?)

Semimodules and Linear Transformations

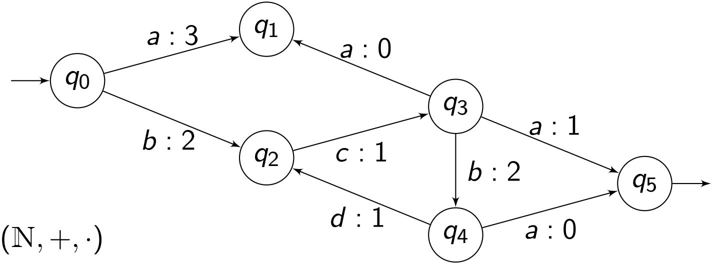
- a vector space over a field K: an abelian group $(V,+,0)$ and an action $\cdot : K \times V \to V$:
  - $x(u+v) = xu+xv$, $(x+y)v = xv+yv$, $(xy)v = x(yv)$, $1v = v$
- a left module over a ring R: an abelian group $(V,+,0)$ and an action $\cdot : R \times V \to V$:
  - same axioms as above
  - right module: $\cdot : V \times R \to V$
- a left semimodule over a semiring S: a commutative monoid $(V,+,0)$ and an action $\cdot : S \times V \to V$:
  - same axioms, plus $0v = 0$ and $x0 = 0$ (why?)

Semimodules and Linear Transformations

- a vector space over a field K: an abelian group $(V, +, 0)$ and an action $\cdot : K \times V \to V$:
  - $x(u+v) = xu+xv$, $(x+y)v = xv+yv$, $(xy)v = x(yv)$, $1v = v$
- a left module over a ring R: an abelian group $(V, +, 0)$ and an action $\cdot : R \times V \to V$:
  - same axioms as above
  - right module: $\cdot : V \times R \to V$
- a left semimodule over a semiring S: a commutative monoid $(V, +, 0)$ and an action $\cdot : S \times V \to V$:
  - same axioms, plus $0v = 0$ and $x0 = 0$
- a right-linear transformation $f : U \to V$ of right semimodules U, V over S:
  - $f(u+v) = f(u) + f(v)$, $f(vx) = f(v)x$
  - equivalent to functions $v \mapsto Mv$

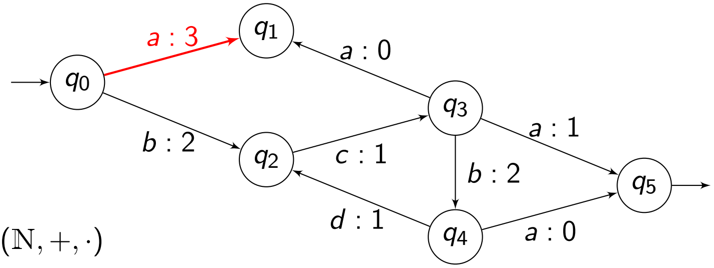
Bonus: Formal power series

Weighted automata with input



$S = (\mathbb{N}, +, \cdot)$

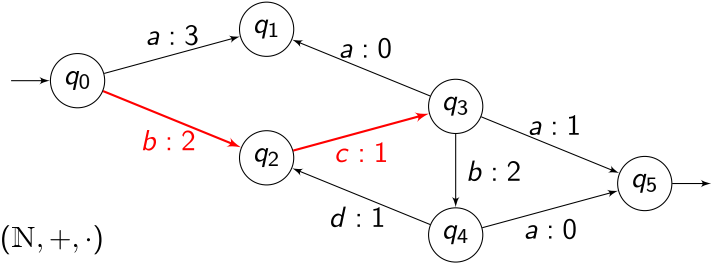
Weighted automata with input



$S = (\mathbb{N}, +, \cdot)$

- $|A|(a) = 0$

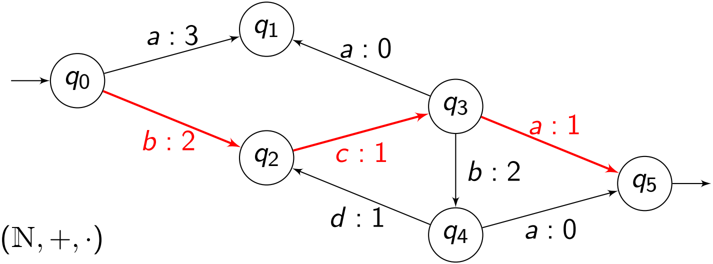
Weighted automata with input



$S = (\mathbb{N}, +, \cdot)$

- $|A|(a) = 0$
- $|A|(bc) = 0$

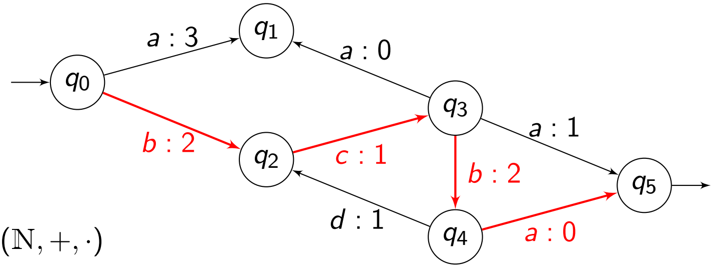
Weighted automata with input



$S = (\mathbb{N}, +, \cdot)$

- $|A|(a) = 0$
- $|A|(bc) = 0$
- $|A|(bca) = 2 \cdot 1 \cdot 1 = 2$

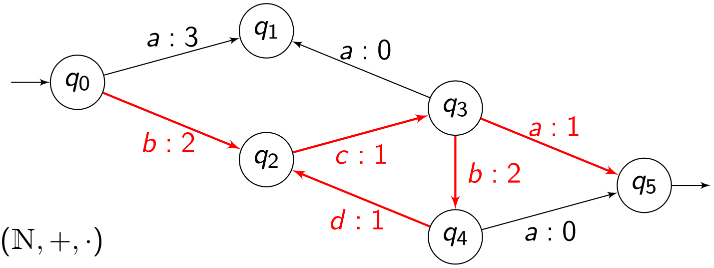
Weighted automata with input



$S = (\mathbb{N}, +, \cdot)$

- $|A|(a) = 0$
- $|A|(bc) = 0$
- $|A|(bca) = 2 \cdot 1 \cdot 1 = 2$
- $|A|(bcba) = 0$

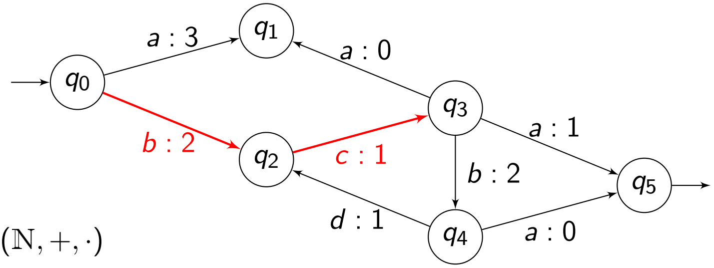
Weighted automata with input



$S = (\mathbb{N}, +, \cdot)$

- $|A|(a) = 0$
- $|A|(bc) = 0$
- $|A|(bca) = 2 \cdot 1 \cdot 1 = 2$
- $|A|(bcba) = 0$
- $|A|(bcbdca) = 4$

Weighted automata with input



$S = (\mathbb{N}, +, \cdot)$

- $|A|(a) = 0$
- $|A|(bc) = 0$
- $|A|(bca) = 2 \cdot 1 \cdot 1 = 2$
- $|A|(bcba) = 0$
- $|A|(bcbdca) = 4$

$$L(A)(w) = \begin{cases} 2^{n+1} & \text{for } w = b(cbd)^n ca \\ 0 & \text{otherwise} \end{cases}$$

Weighted automata with input, II

Definition

A weighted automaton with input over alphabet Σ and semiring S: structure (Q, I, F, T)

- Q: finite set of states
- $I, F \subseteq Q$: initial and accepting states
- $T \subseteq Q \times \Sigma \times S \times Q$: finite transition relation

- $|A|$ is now a function $\Sigma^* \to S$:

$$|A|(w) = \bigoplus \{\!\{ |\pi| \mid \pi \text{ accepting path over } w \text{ in } A \}\!\}$$

Weighted automata with input, II

Definition

A weighted automaton with input over alphabet Σ and semiring S: structure (Q, I, F, T)

- Q: finite set of states
- $I, F \subseteq Q$: initial and accepting states
- $T \subseteq Q \times \Sigma \times S \times Q$: finite transition relation

- $|A|$ is now a function $\Sigma^* \to S$:

$$|A|(w) = \bigoplus \{\!\{ |\pi| \mid \pi \text{ accepting path over } w \text{ in } A \}\!\}$$

- Functions $\Sigma^* \to S$ are called (formal) power series
- the set of all these is denoted $S\langle\!\langle \Sigma^* \rangle\!\rangle$

Operations on power series

Let $r_1, r_2 \in S\langle\langle \Sigma^* \rangle\rangle$

- addition: $(r_1 + r_2)(w) = r_1(w) + r_2(w)$
  - neutral element $\mathbb{0}$ given by $\mathbb{0}(w) = 0$

Operations on power series

Let $r_1, r_2 \in S\langle\langle\Sigma^*\rangle\rangle$

- addition: $(r_1 + r_2)(w) = r_1(w) + r_2(w)$
  - neutral element $\mathbb{0}$ given by $\mathbb{0}(w) = 0$
- Cauchy product: $(r_1 r_2)(w) = \bigoplus \{\{ r_1(u) r_2(v) \mid w = uv \}\}$
  - all possible splits of w into uv

  $\Rightarrow$ $(r_1 r_2)(ab) = r_1(\varepsilon) r_2(ab) + r_1(a) r_2(b) + r_1(ab) r_2(\varepsilon)$
  - neutral element $\mathbb{1}$ given by

Operations on power series

Let $r_1, r_2 \in S\langle\langle\Sigma^*\rangle\rangle$

- addition: $(r_1 + r_2)(w) = r_1(w) + r_2(w)$
  - neutral element $\mathbb{0}$ given by $\mathbb{0}(w) = 0$
- Cauchy product: $(r_1 r_2)(w) = \bigoplus \{\!\{ r_1(u) r_2(v) \mid w = uv \}\!\}$
  - all possible splits of w into uv

  $\Rightarrow$ $(r_1 r_2)(ab) = r_1(\varepsilon) r_2(ab) + r_1(a) r_2(b) + r_1(ab) r_2(\varepsilon)$
  - neutral element $\mathbb{1}$ given by $\mathbb{1}(w) = \begin{cases} 1 & \text{if } w = \varepsilon \\ 0 & \text{otherwise} \end{cases}$

Operations on power series

Let $r_1, r_2 \in S\langle\langle\Sigma^*\rangle\rangle$

- addition: $(r_1 + r_2)(w) = r_1(w) + r_2(w)$
  - neutral element $\mathbb{0}$ given by $\mathbb{0}(w) = 0$
- Cauchy product: $(r_1 r_2)(w) = \bigoplus \{\!\{ r_1(u) r_2(v) \mid w = uv \}\!\}$
  - all possible splits of w into uv

  $\Rightarrow$ $(r_1 r_2)(ab) = r_1(\varepsilon) r_2(ab) + r_1(a) r_2(b) + r_1(ab) r_2(\varepsilon)$
  - neutral element $\mathbb{1}$ given by $\mathbb{1}(w) = \begin{cases} 1 & \text{if } w = \varepsilon \\ 0 & \text{otherwise} \end{cases}$
- in fact, $(S\langle\langle\Sigma^*\rangle\rangle, +, \cdot, \mathbb{0}, \mathbb{1})$ forms itself a semiring

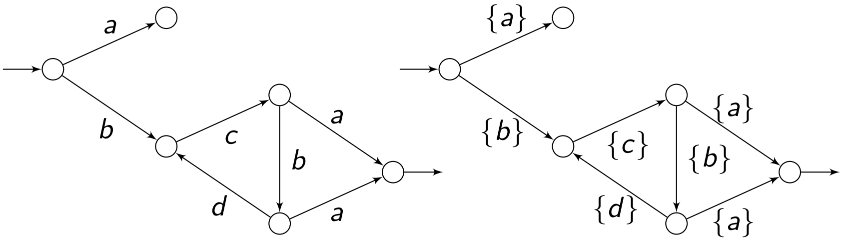
Weighted automata with input are weighted automata

weighted automaton with input over Σ and S

$\hat{=}$

weighted automaton over $S\langle\langle\Sigma^*\rangle\rangle$

- example, for $S = \{\texttt{true}, \texttt{false}\}$:



Rational series

- monomials in $S\langle\langle\Sigma^*\rangle\rangle$: $[w \mapsto x](u) = \begin{cases} x & \text{if } u = w \\ 0 & \text{otherwise} \end{cases}$
- star of $r \in \langle\langle\Sigma^*\rangle\rangle$: $r^*(w) = \bigoplus_{n\geq 0} r^n(w)$
  - exists iff $r(\varepsilon) = 0$

Rational series

- monomials in $S\langle\langle\Sigma^*\rangle\rangle$: $[w \mapsto x](u) = \begin{cases} x & \text{if } u = w \\ 0 & \text{otherwise} \end{cases}$
- star of $r \in \langle\langle\Sigma^*\rangle\rangle$: $r^*(w) = \bigoplus_{n\geq 0} r^n(w)$
  - exists iff $r(\varepsilon) = 0$

Definition (Rational power series)

- $[\{\varepsilon\} \mapsto x]$ and $[\{a\} \mapsto x]$ are rational for all $x \in S$ and $a \in \Sigma$
- if r_1 and r_2 are rational, then so are $r_1 + r_2$ and $r_1 r_2$
- if r is rational and r^* is defined, then r^* is rational

Definition (Recognizable power series)

A formal power series $r \in \langle\langle\Sigma^*\rangle\rangle$ is recognizable if there exists a weighted automaton A with input on Σ and S such that $|A| = r$

Kleene on steroids

Theorem (Schützenberger)

A formal power series is recognizable iff it is rational.


That's all Folks!