Separating words with weighted automata

Zur IZHAKIAN, Glenn MERLET

WATA, 23/04/2021

The problem

Question [Goralcik-Koubek 86] :
For $u, v \in A^*$, find the smallest DFA that accepts u and not v.

The problem

Question [Goralcik-Koubek 86] :
For $u, v \in A^*$, find the smallest DFA that accepts u and not v.

Remarks :

- Symmetric in u and v

The problem

Question [Goralcik-Koubek 86] :
For $u, v \in A^*$, find the smallest DFA that accepts u and not v.

Remarks :

- Symmetric in u and v
- If $|u| \neq |v|$, compute the length mod p for $p \leq 4.4 \log(\max(|u|, |v|))$. (Reversible DFA).

The problem

Question [Goralcik-Koubek 86] :
For $u, v \in A^*$, find the smallest DFA that accepts u and not v.

Remarks :

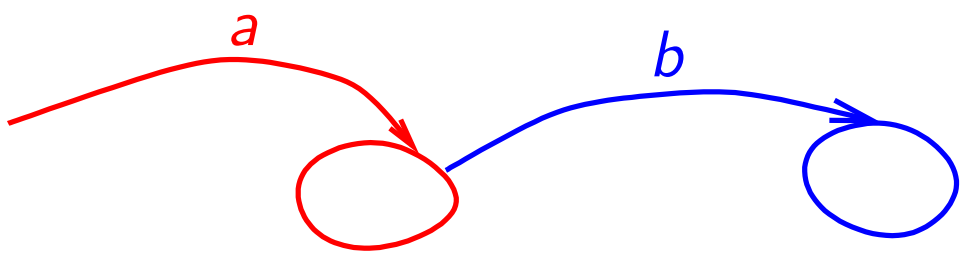
- Symmetric in u and v
- If $|u| \neq |v|$, compute the length mod p for $p \leq 4.4 \log(\max(|u|, |v|))$. (Reversible DFA).
- No DFA with n states can separate $a^{n-1}b^{n-1+\mathrm{lcm}(1,2,\cdots,n)}$ and $a^{n-1+\mathrm{lcm}(1,2,\cdots,n)}b^{n-1}$

The problem

Question [Goralcik-Koubek 86] :
For $u, v \in A^*$, find the smallest DFA that accepts u and not v.

Remarks :

- Symmetric in u and v
- If $|u| \neq |v|$, compute the length mod p for $p \leq 4.4 \log(\max(|u|, |v|))$. (Reversible DFA).
- No DFA with n states can separate $a^{n-1}b^{n-1+\mathrm{lcm}(1,2,\cdots,n)}$ and $a^{n-1+\mathrm{lcm}(1,2,\cdots,n)}b^{n-1}$



The weighted case

Definition

- A weighted automaton $\mathcal{A}$ *separates* two words u and v if $\mathcal{A}(u) \neq \mathcal{A}(v)$.
- $sep_{\mathcal{C}}(N)$ is the smallest number of states needed to separate all pair of distinct words of length N with an element of $\mathcal{C}$.

The weighted case

Definition

- A weighted automaton $\mathcal{A}$ *separates* two words u and v if $\mathcal{A}(u) \neq \mathcal{A}(v)$.
- $sep_{\mathcal{C}}(N)$ is the smallest number of states needed to separate all pair of distinct words of length N with an element of $\mathcal{C}$.

Remarks:

- Enough to consider two letters

The weighted case

Definition

- A weighted automaton $\mathcal{A}$ *separates* two words u and v if $\mathcal{A}(u) \neq \mathcal{A}(v)$.
- $sep_{\mathcal{C}}(N)$ is the smallest number of states needed to separate all pair of distinct words of length N with an element of $\mathcal{C}$.

Remarks:

- Enough to consider two letters
- Consider a and b such that $u_i = a$ and $v_i = b$ at some i.
- Set $\hat{x}_i = a_i$ is $x_i = a_i$, otherwise $\hat{x}_i = b_i$.
- $\mathcal{A}$ separates $\hat{u}$ and $\hat{v}$. Add labels to all transitions labelled b.

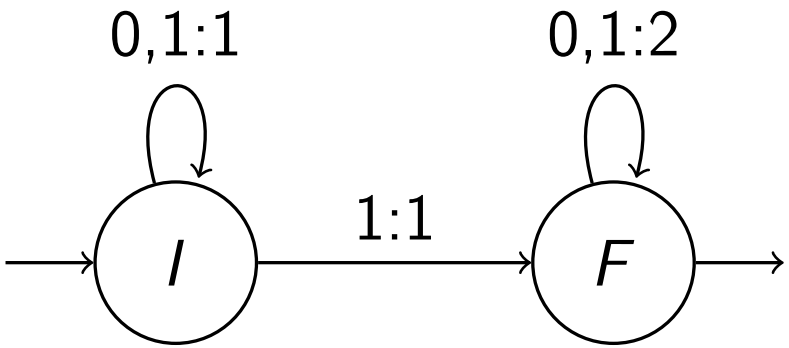
The weighted case

Definition

- A weighted automaton $\mathcal{A}$ *separates* two words u and v if $\mathcal{A}(u) \neq \mathcal{A}(v)$.
- $sep_{\mathcal{C}}(N)$ is the smallest number of states needed to separate all pair of distinct words of length N with an element of $\mathcal{C}$.

Remarks:

- Enough to consider two letters
- $sep_{(+,\times)-\mathrm{WFA}}(N) = 2$:



State of the art

$\mathcal{C}$	$sep_{\mathcal{C}}(N) \leq$	$sep_{\mathcal{C}}(N) \geq$
Rev. DFA	$O(\sqrt{N})$ [Robson 96]	$3/2 \log(N) + o(\log(N))$ [Bulatov et al. 16]
DFA	$O\left(N^{2/5} \log^{3/5}(N)\right)$ [Robson 89]	$\log(N) + o(\log(N))$ [Demaine et al. 11]
NFA		$\log(N) + o(\log(N))$ [Demaine et al. 11]
WDFA		$1/2 \log(N) + o(\log(N))$
$(\max, +)$-WFA		$\Omega\left(\sqrt{\log(N)}\right)$ [Izhakian-M. 18]
$(+, \times)$-WFA	2	2

Semigroup Identities

- Definition : $(u, v) \in \{a, b\}^+$ is a *semigroup identity* for S if $\forall (A, B) \in S^2, u[A, B] = v[A, B]$.

Semigroup Identities

- Definition : $(u, v) \in \{a, b\}^+$ is a *semigroup identity* for S if $\forall (A, B) \in S^2, u[A, B] = v[A, B]$.
- $(u, v) \in \mathrm{Id}\,(\mathcal{M}_n(\mathbb{S})) \iff u$ and v not separable by $\mathbb{S}$-weighted automata with n states.

Semigroup Identities

- Definition : $(u, v) \in \{a, b\}^+$ is a *semigroup identity* for S if $\forall (A, B) \in S^2, u[A, B] = v[A, B]$.
- $(u, v) \in \mathrm{Id}\,(\mathcal{M}_n(\mathbb{S})) \iff u$ and v not separable by $\mathbb{S}$-weighted automata with n states.

Theorem (Wielandt 1950)

The powers of boolean matrices of size n are periodic after at most $(n-1)^2 + 1$ *steps :* $A^{n^2+\mathrm{lcm}(1,\cdots,n)} = A^{n^2}$

Semigroup Identities

- Definition : $(u, v) \in \{a, b\}^+$ is a *semigroup identity* for S if $\forall (A, B) \in S^2, u[A, B] = v[A, B]$.
- $(u, v) \in \mathrm{Id}\,(\mathcal{M}_n(\mathbb{S})) \iff u$ and v not separable by $\mathbb{S}$-weighted automata with n states.

Theorem (Wielandt 1950)

The powers of boolean matrices of size n are periodic after at most $(n-1)^2 + 1$ *steps :* $A^{n^2+\mathrm{lcm}(1,\cdots,n)} = A^{n^2}$ *thus* $A^{n^2+\mathrm{lcm}(1,\cdots,n)} B^{n^2} = A^{n^2} B^{n^2+\mathrm{lcm}(1,\cdots,n)}$

Semigroup Identities

- Definition : $(u, v) \in \{a, b\}^+$ is a *semigroup identity* for S if $\forall (A, B) \in S^2, u[A, B] = v[A, B]$.
- $(u, v) \in \mathrm{Id}(\mathcal{M}_n(\mathbb{S})) \iff u$ and v not separable by $\mathbb{S}$-weighted automata with n states.

Theorem (Wielandt 1950)

The powers of boolean matrices of size n are periodic after at most $(n-1)^2 + 1$ steps : $A^{n^2+\mathrm{lcm}(1,\cdots,n)} = A^{n^2}$ thus $A^{n^2+\mathrm{lcm}(1,\cdots,n)} B^{n^2} = A^{n^2} B^{n^2+\mathrm{lcm}(1,\cdots,n)}$

Theorem (Izahkian-M. 2018)

$\mathcal{M}_n(\mathbb{R}_{\max})$ satisfies a nontrivial semigroup identity.
Its length grows with n as $e^{Cn^2+o(n^2)}$ for some $C \leq \frac{1+\ln(2)}{2}$.

Shitov's induction

Lemma (After Shitov 2014)

Let $W, U, V \in \mathcal{M}_n$ such that $W = PQ$, where $P \in \mathcal{M}_{n\times k}$, $Q \in \mathcal{M}_{k\times n}$, and let $s \in \{a, b\}^+$. Then

$$(sa)[WU, WV] = P\,(s[QBP, QCP])\,QU.$$

Shitov's induction

Lemma (After Shitov 2014)

Let $W, U, V \in \mathcal{M}_n$ such that $W = PQ$, where $P \in \mathcal{M}_{n\times k}$, $Q \in \mathcal{M}_{k\times n}$, and let $s \in \{a, b\}^+$. Then

$$(sa)[WU, WV] = P\,(s[QBP, QCP])\,QU.$$

Lemma (After Shitov 2014)

There are $w, u, v \in \{a, b\}^+$ such that

$$\mathrm{rk}_{det}(w[A, B]) = n \implies u[A, B] = v[A, B].$$

Shitov's induction

Lemma (After Shitov 2014)

Let $W, U, V \in \mathcal{M}_n$ such that $W = PQ$, where $P \in \mathcal{M}_{n\times k}$, $Q \in \mathcal{M}_{k\times n}$, and let $s \in \{a, b\}^+$. Then

$$(sa)[WU, WV] = P\,(s[QBP, QCP])\,QU.$$

Lemma (After Shitov 2014)

There are $w, u, v \in \{a, b\}^+$ such that

$$\mathrm{rk}_{det}(w[A, B]) = n \implies u[A, B] = v[A, B].$$

Theorem (Shitov 2014)

$\mathcal{M}_{3\times 3}(\mathbb{R}_{\max})$ satisfies a non-trivial semigroup identity

Izhakian's theorem for regular matrices

Theorem (Izhakian 2016, Izhakian-M. 2018)

Suppose that $(q, r) \in \mathrm{Id}(\mathcal{U}_n)$, *and that* $A, B \in \mathcal{M}_n$ *satisfy*

$$\mathrm{per}(A) = \mathrm{tr}(A), \ \ \mathrm{per}(B) = \mathrm{tr}(B)$$

$$\text{and} \ \ \mathrm{rk}_{\mathrm{tr}}(q[A, B]) = \mathrm{rk}_{\mathrm{tr}}(r[A, B]) = n.$$

Then, $q[A, B] = r[A, B]$.

Izhakian's theorem for regular matrices

Theorem (Izhakian 2016, Izhakian-M. 2018)

Suppose that $(q, r) \in \mathrm{Id}(\mathcal{U}_n)$, *and that* $A, B \in \mathcal{M}_n$ *satisfy*

$$\mathrm{per}(A) = \mathrm{tr}(A), \ \ \mathrm{per}(B) = \mathrm{tr}(B)$$

$$\text{and} \ \ \mathrm{rk}_{\mathrm{tr}}(q[A, B]) = \mathrm{rk}_{\mathrm{tr}}(r[A, B]) = n.$$

Then, $q[A, B] = r[A, B]$.

Lemma

For $A \in \mathcal{M}_n(\mathbb{R}_{\max})$, *if* $\overline{n} = \mathrm{lcm}(1, \ldots, n)$, *then*

$$\mathrm{rk}_{\mathrm{tr}}(A^{\overline{n}}) = n \implies \mathrm{per}(A^{\overline{n}}) = \mathrm{tr}(A^{\overline{n}}).$$

Izhakian's theorem for regular matrices

Theorem (Izhakian 2016, Izhakian-M. 2018)

Suppose that $(q, r) \in \mathrm{Id}(\mathcal{U}_n)$, *and that* $A, B \in \mathcal{M}_n$ *satisfy*

$$\mathrm{per}(A) = \mathrm{tr}(A), \ \ \mathrm{per}(B) = \mathrm{tr}(B)$$

$$\text{and} \ \ \mathrm{rk}_{\mathrm{tr}}(q[A, B]) = \mathrm{rk}_{\mathrm{tr}}(r[A, B]) = n.$$

Then, $q[A, B] = r[A, B]$.

Lemma

For $A \in \mathcal{M}_n(\mathbb{R}_{\max})$, *if* $\overline{n} = \mathrm{lcm}(1, \ldots, n)$, *then*

$$\mathrm{rk}_{\mathrm{tr}}(A^{\overline{n}}) = n \implies \mathrm{per}(A^{\overline{n}}) = \mathrm{tr}(A^{\overline{n}}).$$

$$w = (qr)[a^{\overline{n}}, b^{\overline{n}}], \ u = q[a^{\overline{n}}, b^{\overline{n}}], \ v = r[a^{\overline{n}}, b^{\overline{n}}]$$

Powers of matrices and Ranks

Theorem (Izhakian-M. 2018)

For any $A \in \mathcal{M}_n(\mathbb{R}_{\max})$ *and* $t \geq (n-1)^2 + 1$, *we have*

$$\mathrm{rk}_{\mathrm{fc}}(A^t) \leq \mathrm{rk}_{\mathrm{tr}}(A).$$

Powers of matrices and Ranks

Theorem (Izhakian-M. 2018)

For any $A \in \mathcal{M}_n(\mathbb{R}_{\max})$ *and* $t \geq (n-1)^2 + 1$, *we have*

$$\mathrm{rk}_{\mathrm{fc}}(A^t) \leq \mathrm{rk}_{\mathrm{tr}}(A).$$

Theorem (After M.-Nowak-Sergeev 2014)

For $t \geq (n-1)^2 + 1$, *there is decomposition indexed by a collection of node-disjoint elementary cycles :*

$$A^t = \bigvee_{\theta \in \Theta} C_\theta (S_\theta)^t R_\theta,$$

the sum of the lengths of the cycles being at most $\mathrm{rk}_f(A)$.

Conclusion

$$w = (qr)^t[a^{\overline{n}}, b^{\overline{n}}],\ u = q[a^{\overline{n}}, b^{\overline{n}}],\ v = r[a^{\overline{n}}, b^{\overline{n}}]$$

Conclusion

$$w = (qr)^t[a^{\overline{n}}, b^{\overline{n}}],\ u = q[a^{\overline{n}}, b^{\overline{n}}],\ v = r[a^{\overline{n}}, b^{\overline{n}}]$$

Theorem

Given $n \in \mathbb{N}$, *let* $\overline{n} = \mathrm{lcm}(1, \ldots, n)$ *and* $t = (n-1)^2 + 1$. *For any* $u, v, q, r, \in \{a, b\}^+$ *such that* $(u, v) \in \mathrm{Id}(\mathcal{M}_{n-1})$ $(q, r) \in \mathrm{Id}(\mathcal{U}_n)$ *and any* $w_1, w_2 \in \{a, b\}^*$, *we have:*

$$(ua, va)\left[((qr)^t w_1\,[q, r])\,[a^{\overline{n}}, b^{\overline{n}}], ((qr)^t w_2\,[q, r])\,[a^{\overline{n}}, b^{\overline{n}}]\right] \in \mathrm{Id}(\mathcal{M}_n).$$

Conclusion

$$w = (qr)^t[a^{\overline{n}}, b^{\overline{n}}],\ u = q[a^{\overline{n}}, b^{\overline{n}}],\ v = r[a^{\overline{n}}, b^{\overline{n}}]$$

Theorem

Given $n \in \mathbb{N}$, *let* $\overline{n} = \mathrm{lcm}(1, \ldots, n)$ *and* $t = (n-1)^2 + 1$. *For any* $u, v, q, r, \in \{a, b\}^+$ *such that* $(u, v) \in \mathrm{Id}(\mathcal{M}_{n-1})$ $(q, r) \in \mathrm{Id}(\mathcal{U}_n)$ *and any* $w_1, w_2 \in \{a, b\}^*$, *we have:*

$$(ua, va)\left[((qr)^t w_1\,[q, r])\,[a^{\overline{n}}, b^{\overline{n}}], ((qr)^t w_2\,[q, r])\,[a^{\overline{n}}, b^{\overline{n}}]\right] \in \mathrm{Id}(\mathcal{M}_n).$$

$$\left.\begin{array}{rcc} \overline{n} & = & e^{n+o(n)} \\ |q| = |r| & = & 2^{n+o(n)} \\ t & = & O(n^2) = e^{o(n)} \\ |w_i| & \leq & 1 \end{array}\right\} \Rightarrow |u_{n+1}| = e^{(1+\ln 2)n}|u_n|.$$

Thank you for your attention.