Lower bounds for the length of reset words in eulerian automata

Vladimir V. Gusev

Ural Federal University, Russia
University of Turku, Finland

September 28, 2011

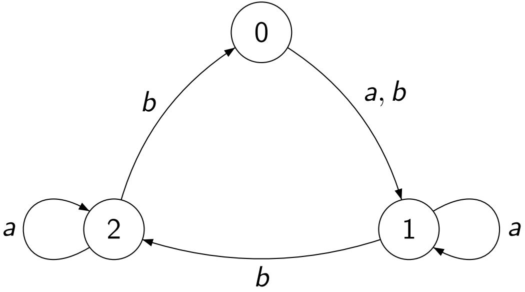
We consider DFA: $\mathscr{A} = \langle Q, \Sigma, \delta \rangle$.

- Q the state set
- Σ the input alphabet
- $\delta : Q \times \Sigma \to Q$ the transition function

$\mathscr{A}$ is called synchronizing if there exists a word $w \in \Sigma^*$ whose action resets $\mathscr{A}$, that is, leaves the automaton in one particular state no matter which state in Q it started at: $\delta(q, w) = \delta(q', w)$ for all $q, q' \in Q$.

Any w with this property is a synchronizing word for $\mathscr{A}$.

The minimum length of synchronizing words for $\mathscr{A}$ is called the reset threshold of $\mathscr{A}$ denoted by $rt(\mathscr{A})$.



Here a synchronizing word is *abba*.

It resets the automaton to state 1.
Reset threshold equal to 4.

Černý (1964): For each $n \geq 2$, there is an automaton $\mathscr{C}_n$ with n states whose reset threshold is $(n-1)^2$.

Černý's conjecture (1964): The reset threshold of every synchronizing automaton with n states is not greater than $(n-1)^2$.

This problem is still open.

(Pin, 1983) reset threshold is at most $\frac{n^3-n}{6}$

(Trakhtman, FCT2011) $\frac{7n^3+6n^2-16n}{48}$

No quadratic upper bound for the reset threshold of synchronizing automata with n states is known.

Confirmed for various restricted classes of synchronizing automata.

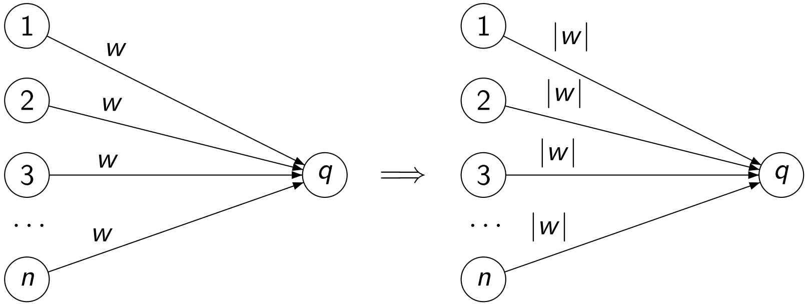
Natural idea:

Focus on automata whose reset threshold is close to $(n-1)^2$.

One series was given in (Ananichev, Volkov, Zaks, DLT 2006).

Several series of such automata were presented
in (Ananichev, Gusev, Volkov, MFCS2010).

Automata with large reset threshold were obtained from digraphs with large exponent.



We say that $\mathscr{A}$ is 0-primitive:
$\exists t, q$ such that $\forall p$ there is a path of length t from p to q.

Smallest such t is called 0-exponent of $\mathscr{A}$.

Every synchronizing automaton $\mathscr{A}$ is 0-primitive and following holds:

$$rt(\mathscr{A}) \geq exp_0(\mathscr{A})$$

We consider only strongly connected automata.
Enough to confirm Černý's conjecture for them.

0-primitive:
$\exists t, q$ such that $\forall p$ there is a path of length t from p to q.

Automaton $\mathscr{A}$ is primitive:
$\exists \ell$ such that $\forall p, s$ there is a path of length ℓ from p to s.

The least ℓ with this property is called the exponent of $\mathscr{A}$

0-primitivity $\Rightarrow$ primitivity:

Path between p and s of length $exp_0(\mathscr{A}) + n - 1$

From p to p'	From p' to q	From q to s
$n - 1 - k$ steps	Exactly $exp_0(\mathscr{A})$	$k \leq n - 1$ steps

$$exp_0(\mathscr{A}) + n - 1 \geq exp(\mathscr{A}) \geq exp_0(\mathscr{A})$$

We know a lot about exponents!

(Wielandt, 1950):
The exponent of primitive automaton with n states is at most $(n-1)^2+1$ and this bound is tight.

(Dulmage, Mendelson, Shao, Lewin, Vitek, Zhang 1964 - 1987):
Set of all possible exponents depending on number of states is described.

Bounds on exponents are obtained for various special classes.

Big question:

How close the notion of reset threshold is connected to the notion of 0-exponent?

Is this a universal approach for every class of automata?

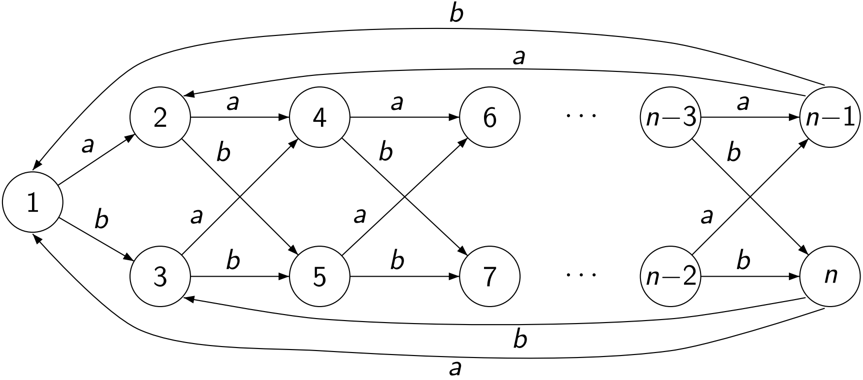
We say that automaton $\mathscr{A}$ is Eulerian if indegree of every state is equal to outdegree.

(Kari, 2003) Reset threshold of Eulerian automaton with n states is at most $n^2 - 3n + 3$.

But there is no corresponding lower bound.

Let's shoot both targets.

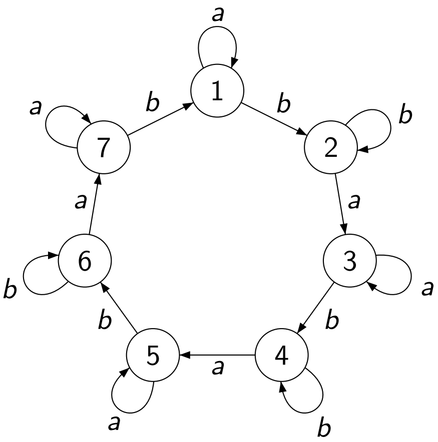
(Shen, 2000) Primitive Eulerian automaton with outdegree 2 and $n \geq 8$ vertices has exponent at most $\frac{(n-1)^2}{4} + 1$. Bound is reached by $\mathscr{D}_n$.



Automaton $\mathscr{D}_n$

$$rt(\mathscr{D}_n) \geq exp_0(\mathscr{D}_n) = \frac{n^2}{4} + o(n^2)$$

But there are examples with reset threshold $\frac{n^2}{2} + o(n^2)$!



Automaton $\mathscr{M}_7$

$\mathscr{M}_n$ is defined for odd n only.

$rt(\mathscr{M}_n) = \frac{n^2-3n+4}{2}$.

$exp_0(\mathscr{M}_n) = n - 1$.

0-exponent is too weak

We have discarded too much information

Let's save more!

Let $\Sigma = \{a_1, a_2, \ldots, a_k\}$.

We say that $u \in \Sigma^*$ is a factor of $w \in \Sigma^*$ if $w = xuy$, where $x, y \in \Sigma^*$.

We denote $|w|_u$ number of different occurrences of u in w as a factor.

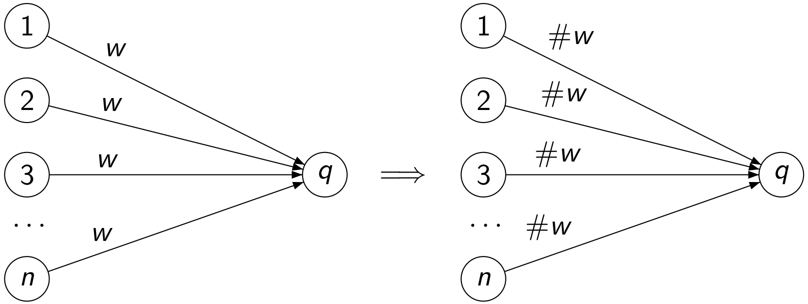
Parikh vector $\#w$ of a word w is vector $\#w = (|w|_{a_1}, |w|_{a_2}, \ldots, |w|_{a_k})$.

For example:
$w = bab$ $\quad \#w = (1, 2)$
$w = abbaaba$ $\quad \#w = (4, 3)$

Length of vector is the sum of its components.

If path α labelled by w we say that path α has Parikh vector $\#w$.

Note: Length of path equal to the length of its Parikh vector.



We say that $\mathscr{A}$ is 1-primitive:

$\exists$ vector v, $\exists$ state q such that $\forall p$ there is a path from p to q with v as its Parikh vector.

Smallest length of such vectors v is called 1-exponent of $\mathscr{A}$.

Every synchronizing automaton $\mathscr{A}$ is 1-primitive and following holds:

$$rt(\mathscr{A}) \geq exp_1(\mathscr{A})$$

Very useful notion.

Earlier $\mathscr{C}_n$ was related to a family of automata with large 0-exponent via special unlooping trick.

1-exponent of $\mathscr{C}_n$ is close to $(n-1)^2$.

More natural proof of $rt(\mathscr{C}_n) = (n-1)^2$.

Uniqueness of shortest synchronizing word for $\mathscr{C}_n$ has been shown as corollary.

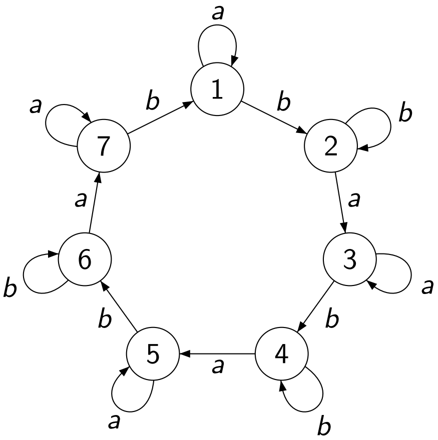
In (Olesky, Shader, van den Driessche, Suwilo, 2002, 2003) similar notion was studied.

Asymptotic bounds for NFA.

Corollary:

$O(n^{k+1})$ bound on 1-exponent of 1-primitive DFA over k letters.

1-exponent is too weak for $\mathscr{M}_n$.



Automaton $\mathscr{M}_7$

$$exp_1(\mathscr{M}_n) \leq 4n$$

Paths from every state p to 1 with the same Parikh vector

- Round trip from p to p
  n letters
- Trip from state p to 1
  $< n$ letters
- Use loops to make same amount of letters in paths
  $\leq 2n$ letters

$\mathscr{A}$ has $\{1, 2, \ldots n\}$ as state set

We say that $\mathscr{A}$ is k-primitive:

there are words $u_1, u_2, \ldots, u_n$ such that

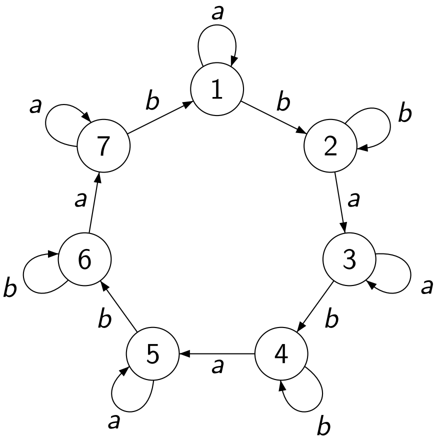
- $1 \cdot u_1 = 2 \cdot u_2 = \ldots = n \cdot u_n$
- $|u_1|_v = |u_2|_v = \ldots = |u_n|_v$ for every word v of length at most k.

Note that $u_1, u_2, \ldots, u_n$ have the same length.

Minimal length of words that witness k-primitivity
is called k-exponent of $\mathscr{A}$.

Every synchronizing automaton $\mathscr{A}$ is k-primitive and following holds:

$$rt(\mathscr{A}) \geq exp_k(\mathscr{A})$$



$exp_2(\mathscr{M}_n) = \frac{n^2}{2} + o(n^2)$

2-exponent witnesses:

$2 = 1 \cdot u_1 = 2 \cdot u_2 = \ldots = n \cdot u_n$

$k = |u_2|_{ab}$

u_2 divided into blocks:
$b^*(a^+b^+)^{\frac{n-1}{2}}ba^*b$

Every block has either $\frac{n-1}{2}$ or $\frac{n+1}{2}$ occurrences of ab.

k is a non-negative integer combination of $\frac{n-1}{2}$ and $\frac{n+1}{2}$.

$2 \cdot (ab)^t = j$

$2 \cdot (ab)^t u_j = 2$

Since $|u_j|_{ab} = |u_2|_{ab} = k$ word ab appears $t + k$ times as a factor in $(ab)^t u_j$.

$t + k$ is a non-negative integer combination of $\frac{n-1}{2}$ and $\frac{n+1}{2}$ for every natural t.

Largest number which is not expressible as non-negative integer combination of coprime numbers p and q is $pq - p - q$.

$k > \frac{n-1}{2} \cdot \frac{n+1}{2} - \frac{n-1}{2} - \frac{n+1}{2} = \frac{n^2}{4} + o(n^2)$.

$exp_2(\mathscr{M}_n) = \frac{n^2}{2} + o(n^2)$

General approach:

Let $\mathscr{A}$ be synchronizing automaton

$exp_k(\mathscr{A})$ is well defined

$exp_k(\mathscr{A}) \leq rt(\mathscr{A})$

$$exp_0(\mathscr{A}) \leq exp_1(\mathscr{A}) \leq \cdots \leq exp_k(\mathscr{A}) = exp_{k+1}(\mathscr{A}) = \cdots = rt(\mathscr{A})$$

Way to study special classes of automata

Quadratic upper bound on k-exponent for every k
leads to quadratic upper bound on reset threshold.

Main Contribution:

New lower bound on reset threshold of Eulerian automata: $\frac{n^2-3n+4}{2}$.

Framework for analysis of synchronizing properties of automata(k-primitivity, k-exponents).

Future work and open questions:

Quadratic upper bound on 1-exponent for automata?

Bounds on k-exponents for $k \geq 2$.

How to check if automaton is k-primitive?

Relations between k-exponents and synchronizability.

Is there automaton which is k-primitive for every k but not synchronizing?