Lower bound for the length of synchronizing words in partially-synchronizing automata

Wit Foryś, Adam Roman

Instytut Informatyki
Uniwersytet Jagielloński

SOFSEM 2008, Slovakia

Synchronizing words and automata

Definition: An automaton

An automaton is a triple $\mathcal{A} = (Q, A, \delta)$, where:

- Q is a finite set of states
- A is a finite alphabet
- $\delta: \ Q \times A \to Q$ is a transition function

Extending δ

$$\delta : 2^Q \times A^* \to 2^Q$$

$$\delta(P, aw) = \bigcup_{p \in P} \{\delta(\delta(p, a), w)\}, P \subseteq Q, \ a \in A, \ w \in A^*$$

For example, if $\delta(1, a) = 2$, $\delta(2, a) = 3$, $\delta(2, b) = 1$, $\delta(3, b) = 2$, then $\delta(\{1, 2\}, ab) = \{1, 2\}$.

Definition: An automaton

An automaton is a triple $\mathcal{A} = (Q, A, \delta)$, where:

- Q is a finite set of states
- A is a finite alphabet
- $\delta: \ Q \times A \rightarrow Q$ is a transition function

Extending δ

$$\delta : 2^Q \times A^* \rightarrow 2^Q$$

$$\delta(P, aw) = \bigcup_{p \in P} \{\delta(\delta(p, a), w)\}, P \subseteq Q, \ a \in A, \ w \in A^*$$

For example, if $\delta(1, a) = 2$, $\delta(2, a) = 3$, $\delta(2, b) = 1$, $\delta(3, b) = 2$, then $\delta(\{1, 2\}, ab) = \{1, 2\}$.

Definition: An automaton

An automaton is a triple $\mathcal{A} = (Q, A, \delta)$, where:

- Q is a finite set of states
- A is a finite alphabet
- $\delta : \; Q \times A \rightarrow Q$ is a transition function

Extending δ

$$\delta : 2^Q \times A^* \rightarrow 2^Q$$

$$\delta(P, aw) = \bigcup_{p \in P} \{\delta(\delta(p, a), w)\}, P \subseteq Q, \; a \in A, \; w \in A^*$$

For example, if $\delta(1, a) = 2$, $\delta(2, a) = 3$, $\delta(2, b) = 1$, $\delta(3, b) = 2$, then $\delta(\{1, 2\}, ab) = \{1, 2\}$.

Definition: An automaton

An automaton is a triple $\mathcal{A} = (Q, A, \delta)$, where:

- Q is a finite set of states
- A is a finite alphabet
- $\delta : \ Q \times A \rightarrow Q$ is a transition function

Extending δ

$$\delta : 2^Q \times A^* \rightarrow 2^Q$$

$$\delta(P, aw) = \bigcup_{p \in P} \{\delta(\delta(p, a), w)\}, P \subseteq Q, \ \ a \in A, \ \ w \in A^*$$

For example, if $\delta(1, a) = 2$, $\delta(2, a) = 3$, $\delta(2, b) = 1$, $\delta(3, b) = 2$, then $\delta(\{1, 2\}, ab) = \{1, 2\}$.

Definition: An automaton

An automaton is a triple $\mathcal{A} = (Q, A, \delta)$, where:

- Q is a finite set of states
- A is a finite alphabet
- $\delta : \; Q \times A \to Q$ is a transition function

Extending δ

$$\delta : 2^Q \times A^* \to 2^Q$$

$$\delta(P, aw) = \bigcup_{p \in P} \{\delta(\delta(p, a), w)\}, P \subseteq Q, \; a \in A, \; w \in A^*$$

For example, if $\delta(1, a) = 2$, $\delta(2, a) = 3$, $\delta(2, b) = 1$, $\delta(3, b) = 2$, then $\delta(\{1, 2\}, ab) = \{1, 2\}$.

"Classical" version of synchronization

Let $\mathcal{A} = (Q, A, \delta)$ be a full, deterministic and strongly connected automaton. If

$$\exists w \in A^* : \quad \forall p, q \in Q \ \delta(p, w) = \delta(q, w),$$

then we say that $\mathcal{A}$ is synchronizing, and w is a synchronizing word. We also say that w synchronizes $\mathcal{A}$.

Remark

If w synchronizes $\mathcal{A}$, then each word uwv ($u, v \in A^*$) also does it.

"Classical" version of synchronization

Let $\mathcal{A} = (Q, A, \delta)$ be a full, deterministic and strongly connected automaton. If

$$\exists w \in A^* : \quad \forall p, q \in Q \ \delta(p, w) = \delta(q, w),$$

then we say that $\mathcal{A}$ is synchronizing, and w is a synchronizing word. We also say that w synchronizes $\mathcal{A}$.

Remark

If w synchronizes $\mathcal{A}$, then each word uwv $(u, v \in A^*)$ also does it.

Definition

We say w is a minimal synchronizing word for $\mathcal{A}$, if w synchronizes $\mathcal{A}$, and for each v synchronizing $\mathcal{A}$ we have $|v| \geqslant |w|$.

The problem

What are the upper and lower bounds for the length of minimal synchronizing words for an n-state automaton?

Definition

We say w is a minimal synchronizing word for $\mathcal{A}$, if w synchronizes $\mathcal{A}$, and for each v synchronizing $\mathcal{A}$ we have $|v| \geqslant |w|$.

The problem

What are the upper and lower bounds for the length of minimal synchronizing words for an n-state automaton?

Lower and upper bounds

Notation

- $m(\mathcal{A})$ - the length of minimal synchronizing word for $\mathcal{A}$.
- $SYN(n)$ - the set of all n-state synchronizing automata.
- $M(n) = \max_{\mathcal{A} \in SYN(n)} \min_{w \in A^*} \{|w| : |\delta(Q, w)| = 1\}$.

Černý Conjecture, 1964

$$\mathcal{A} \in SYN(n) \Rightarrow m(\mathcal{A}) \leqslant (n-1)^2.$$

Notation

- $m(\mathcal{A})$ - the length of minimal synchronizing word for $\mathcal{A}$.
- $SYN(n)$ - the set of all n-state synchronizing automata.
- $M(n) = \max_{\mathcal{A} \in SYN(n)} \min_{w \in A^*} \{|w| : |\delta(Q, w)| = 1\}$.

Černý Conjecture, 1964

$$\mathcal{A} \in SYN(n) \Rightarrow m(\mathcal{A}) \leqslant (n-1)^2.$$

Notation

- $m(\mathcal{A})$ - the length of minimal synchronizing word for $\mathcal{A}$.
- $SYN(n)$ - the set of all n-state synchronizing automata.
- $M(n) = \max_{\mathcal{A} \in SYN(n)} \min_{w \in A^*} \{|w| : |\delta(Q, w)| = 1\}$.

Černý Conjecture, 1964

$$\mathcal{A} \in SYN(n) \Rightarrow m(\mathcal{A}) \leqslant (n-1)^2.$$

Notation

- $m(\mathcal{A})$ - the length of minimal synchronizing word for $\mathcal{A}$.
- $SYN(n)$ - the set of all n-state synchronizing automata.
- $M(n) = \max_{\mathcal{A} \in SYN(n)} \min_{w \in A^*} \{|w| : |\delta(Q, w)| = 1\}$.

Černý Conjecture, 1964

$$\mathcal{A} \in SYN(n) \Rightarrow m(\mathcal{A}) \leqslant (n-1)^2.$$

Notation

- $m(\mathcal{A})$ - the length of minimal synchronizing word for $\mathcal{A}$.
- $SYN(n)$ - the set of all n-state synchronizing automata.
- $M(n) = \max_{\mathcal{A} \in SYN(n)} \min_{w \in A^*} \{|w| : |\delta(Q, w)| = 1\}$.

Černý Conjecture, 1964

$$\mathcal{A} \in SYN(n) \Rightarrow m(\mathcal{A}) \leqslant (n-1)^2.$$

Lower bound

For each n there exists an n-state Černý automaton, that is, an automaton for which $m(\mathcal{A}) = (n-1)^2$. So: $M(n) \geqslant (n-1)^2$.

Theorem – Pin; Klyachko, Rystsov, Spivak

$$\mathcal{A} \in SYN(n) \Rightarrow m(\mathcal{A}) \leqslant \frac{n^3 - n}{6}.$$

Conclusion

For synchronization in the "classical" case we have

$$(n-1)^2 \leqslant M(n) \leqslant \frac{n^3 - n}{6}.$$

Lower bound

For each n there exists an n-state Černý automaton, that is, an automaton for which $m(\mathcal{A}) = (n-1)^2$. So: $M(n) \geqslant (n-1)^2$.

Theorem - Pin; Klyachko, Rystsov, Spivak

$$\mathcal{A} \in SYN(n) \Rightarrow m(\mathcal{A}) \leqslant \frac{n^3 - n}{6}.$$

Conclusion

For synchronization in the "classical" case we have

$$(n-1)^2 \leqslant M(n) \leqslant \frac{n^3 - n}{6}.$$

Lower bound

For each n there exists an n-state Černý automaton, that is, an automaton for which $m(\mathcal{A}) = (n-1)^2$. So: $M(n) \geqslant (n-1)^2$.

Theorem - Pin; Klyachko, Rystsov, Spivak

$$\mathcal{A} \in SYN(n) \Rightarrow m(\mathcal{A}) \leqslant \frac{n^3 - n}{6}.$$

Conclusion

For synchronization in the "classical" case we have

$$(n-1)^2 \leqslant M(n) \leqslant \frac{n^3 - n}{6}.$$

Extended notion of synchronization

Definition

Let $\mathcal{A}$ be an automaton as above but δ is not necessarily a total function - $\delta(q, a)$ can be undefined for some states and letters.

How does the synchronization look like?

An automaton $\mathcal{A} = (Q, A, \delta)$ with a non-total δ is synchronized by $w = a_1 a_2 \ldots a_k$, if each of the sets $P_i = \delta(Q, a_1 \ldots a_i)$ is well defined and $|P_k| = 1$.

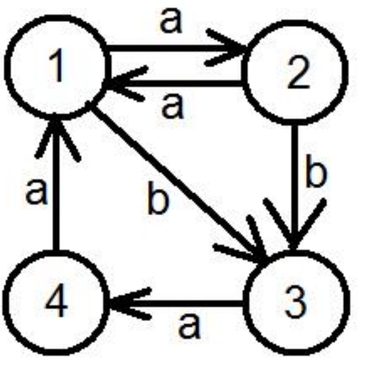
Definition

Let $\mathcal{A}$ be an automaton as above but δ is not necessarily a total function - $\delta(q, a)$ can be undefined for some states and letters.

How does the synchronization look like?

An automaton $\mathcal{A} = (Q, A, \delta)$ with a non-total δ is synchronized by $w = a_1 a_2 \ldots a_k$, if each of the sets $P_i = \delta(Q, a_1 \ldots a_i)$ is well defined and $|P_k| = 1$.

An example



How to synchronize it?

$\delta(Q, a) = \{1, 2, 4\}$

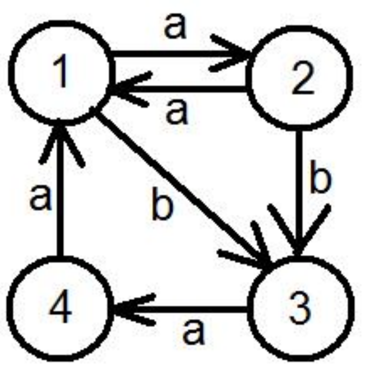
$\delta(\{1, 2, 4\}, b)$ - undefined!

$\delta(\{1, 2, 4\}, a) = \{1, 2\}$

$\delta(\{1, 2\}, b) = \{3\}$

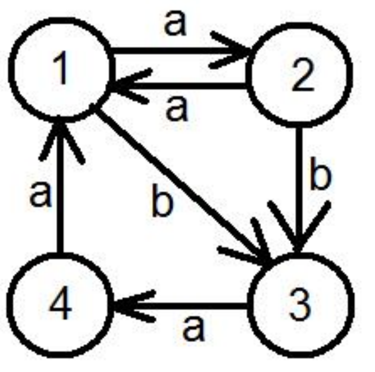
$w = aab$.

An example



How to synchronize it?
$\delta(Q, a) = \{1, 2, 4\}$
$\delta(\{1, 2, 4\}, b)$ - undefined!
$\delta(\{1, 2, 4\}, a) = \{1, 2\}$
$\delta(\{1, 2\}, b) = \{3\}$
$w = aab.$

An example



How to synchronize it?

$\delta(Q, a) = \{1, 2, 4\}$

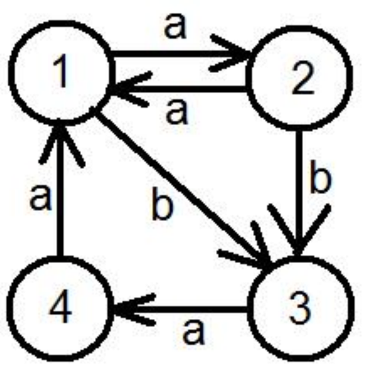
$\delta(\{1, 2, 4\}, b)$ - undefined!

$\delta(\{1, 2, 4\}, a) = \{1, 2\}$

$\delta(\{1, 2\}, b) = \{3\}$

$w = aab$.

An example



How to synchronize it?
$\delta(Q, a) = \{1, 2, 4\}$
$\delta(\{1, 2, 4\}, b)$ - undefined!
$\delta(\{1, 2, 4\}, a) = \{1, 2\}$
$\delta(\{1, 2\}, b) = \{3\}$
$w = aab$.

Notation

For partial automata we will use $M^*(n)$ in the same meaning as $M(n)$. $M^*(n)$ is the longest word among all minimal synchronizing words for n-state partial automata.

Theorem (M. Ito, K. Shikishima-Tsuji)

For n even $2^{\frac{n}{2}} + 1 \leqslant M^*(n) \leqslant 2^n - 2^{n-2} - 1$.
For n odd $3 \cdot 2^{\frac{n-3}{2}} + 1 \leqslant M^*(n) \leqslant 2^n - 2^{n-2} - 1$.

Theorem (P. Martjugin)

For $n = 3k$ $M^*(n) \geqslant 3 \cdot 3^{\frac{n}{3}} - 2$
For $n = 3k + 1$ $M^*(n) \geqslant 4 \cdot 3^{\frac{n-1}{3}} - 2$
For $n = 3k + 2$ $M^*(n) \geqslant 6 \cdot 3^{\frac{n-2}{3}} - 2$.

Notation

For partial automata we will use $M^*(n)$ in the same meaning as $M(n)$. $M^*(n)$ is the longest word among all minimal synchronizing words for n-state partial automata.

Theorem (M. Ito, K. Shikishima-Tsuji)

For n even $2^{\frac{n}{2}} + 1 \leqslant M^*(n) \leqslant 2^n - 2^{n-2} - 1$.
For n odd $3 \cdot 2^{\frac{n-3}{2}} + 1 \leqslant M^*(n) \leqslant 2^n - 2^{n-2} - 1$.

Theorem (P. Martjugin)

For $n = 3k$ $M^*(n) \geqslant 3 \cdot 3^{\frac{n}{3}} - 2$
For $n = 3k+1$ $M^*(n) \geqslant 4 \cdot 3^{\frac{n-1}{3}} - 2$
For $n = 3k+2$ $M^*(n) \geqslant 6 \cdot 3^{\frac{n-2}{3}} - 2$.

Notation

For partial automata we will use $M^*(n)$ in the same meaning as $M(n)$. $M^*(n)$ is the longest word among all minimal synchronizing words for n-state partial automata.

Theorem (M. Ito, K. Shikishima-Tsuji)

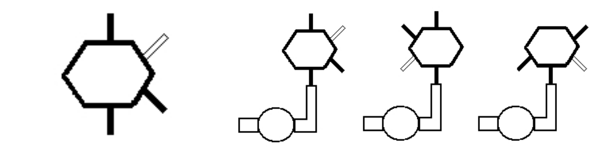
For n even $2^{\frac{n}{2}} + 1 \leqslant M^*(n) \leqslant 2^n - 2^{n-2} - 1$.
For n odd $3 \cdot 2^{\frac{n-3}{2}} + 1 \leqslant M^*(n) \leqslant 2^n - 2^{n-2} - 1$.

Theorem (P. Martjugin)

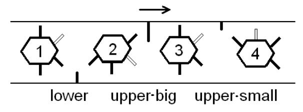
For $n = 3k$ $M^*(n) \geqslant 3 \cdot 3^{\frac{n}{3}} - 2$
For $n = 3k + 1$ $M^*(n) \geqslant 4 \cdot 3^{\frac{n-1}{3}} - 2$
For $n = 3k + 2$ $M^*(n) \geqslant 6 \cdot 3^{\frac{n-2}{3}} - 2$.

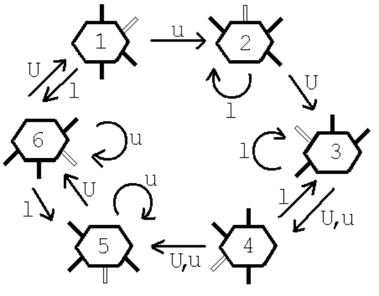
Generalized notion of synchronization

An example



An example





Generalization

- An automaton is a partial one
- The synchronization can start in an arbitrary subset of Q.

Definitoin: k-synchronizing automaton

An n-state automaton $\mathcal{A}$ is k-synchronizing automaton ($k \leqslant n$), if there exists a k-subset P of Q and $w \in A^*$, such that:

- $\delta(P, w)$ is well-defined
- $|\delta(P, w)| = 1$
- there is no set greater than P with above properties.

Generalization

- An automaton is a partial one
- The synchronization can start in an arbitrary subset of Q.

Definitoin: k-synchronizing automaton

An n-state automaton $\mathcal{A}$ is k-synchronizing automaton ($k \leqslant n$), if there exists a k-subset P of Q and $w \in A^*$, such that:

- $\delta(P, w)$ is well-defined
- $|\delta(P, w)| = 1$
- there is no set greater than P with above properties.

Generalization

- An automaton is a partial one
- The synchronization can start in an arbitrary subset of Q.

Definitoin: k-synchronizing automaton

An n-state automaton $\mathcal{A}$ is k-synchronizing automaton ($k \leqslant n$), if there exists a k-subset P of Q and $w \in A^*$, such that:

- $\delta(P, w)$ is well-defined
- $|\delta(P, w)| = 1$
- there is no set greater than P with above properties.

Generalization

- An automaton is a partial one
- The synchronization can start in an arbitrary subset of Q.

Definitoin: k-synchronizing automaton

An n-state automaton $\mathcal{A}$ is k-synchronizing automaton ($k \leqslant n$), if there exists a k-subset P of Q and $w \in A^*$, such that:

- $\delta(P, w)$ is well-defined
- $|\delta(P, w)| = 1$
- there is no set greater than P with above properties.

Generalization

- An automaton is a partial one
- The synchronization can start in an arbitrary subset of Q.

Definitoin: k-synchronizing automaton

An n-state automaton $\mathcal{A}$ is k-synchronizing automaton ($k \leqslant n$), if there exists a k-subset P of Q and $w \in A^*$, such that:

- $\delta(P, w)$ is well-defined
- $|\delta(P, w)| = 1$
- there is no set greater than P with above properties.

Notation

By $M^{\diamondsuit}(n)$ we denote the longest word among the minimal synchronizing words for k-synchronizing n-state automata (for arbitrary $k = 1, 2, ..., n$).

It seems that...

taking the arbitrary subset of Q as the starting point of the synchronization process will result in shorter value of the minimal synchronizing word's length (we start from the smaller set, so we have fewer number of combinations of states during the synchr. process). In other words: it seems that $M^{\diamondsuit}(n) < M^{*}(n)$.

Notation

By $M^{\diamondsuit}(n)$ we denote the longest word among the minimal synchronizing words for k-synchronizing n-state automata (for arbitrary $k = 1, 2, ..., n$).

It seems that...

taking the arbitrary subset of Q as the starting point of the synchronization process will result in shorter value of the minimal synchronizing word's length (we start from the smaller set, so we have fewer number of combinations of states during the synchr. process). In other words: it seems that $M^{\diamondsuit}(n) < M^{*}(n)$.

but...

it is exactly the opposite! Generalized synchronization causes the elongation of minimal synchronizing words.

Why?

In case of classical and "partial-type" synchronization there must exist a letter $a \in A$ such that $\delta(\cdot, a)$ is defined for all $q \in Q$. This fact prevented to achieve possibly long minimal synchronizing word.

but...

it is exactly the opposite! Generalized synchronization causes the elongation of minimal synchronizing words.

Why?

In case of classical and "partial-type" synchronization there must exist a letter $a \in A$ such that $\delta(\cdot, a)$ is defined for all $q \in Q$. This fact prevented to achieve possibly long minimal synchronizing word.

Main theorem

Let $n = 2k$. There exists $\frac{n}{2}$-synchronizing automaton, for which the length of minimal synchronizing word is

$$|w| = \binom{n+1}{\frac{n}{2}} - \frac{n}{2} - 2.$$

Comparision with Martjugin results

$\lvert Q\rvert$	$M^*(\lvert Q\rvert)$	$M^{\diamondsuit}(\lvert Q\rvert)$	$\lvert Q\rvert$	$M^*(\lvert Q\rvert)$	$M^{\diamondsuit}(\lvert Q\rvert)$
8	52	120	22	8746	1 352 065
10	106	455	24	19 681	5 200 286
12	241	1 708	26	39 364	20 058 285
14	484	6 424	28	78 730	77 558 744
16	970	24 300	30	177 145	300 540 178
18	2 185	92 367	32	354 292	1 166 803 092
20	4 372	352 704	34	708 586	4 537 567 631

Main theorem

Let $n = 2k$. There exists $\frac{n}{2}$-synchronizing automaton, for which the length of minimal synchronizing word is

$$|w| = \binom{n+1}{\frac{n}{2}} - \frac{n}{2} - 2.$$

Comparision with Martjugin results

$\lvert Q\rvert$	$M^*(\lvert Q\rvert)$	$M^{\Diamond}(\lvert Q\rvert)$	$\lvert Q\rvert$	$M^*(\lvert Q\rvert)$	$M^{\Diamond}(\lvert Q\rvert)$
8	52	120	22	8746	1 352 065
10	106	455	24	19 681	5 200 286
12	241	1 708	26	39 364	20 058 285
14	484	6 424	28	78 730	77 558 744
16	970	24 300	30	177 145	300 540 178
18	2 185	92 367	32	354 292	1 166 803 092
20	4 372	352 704	34	708 586	4 537 567 631

Possible fields of research

- better lower bound for M^*?
- better lower bound for $M^\Diamond$?
- a nontrivial upper bound for $M^\Diamond$?

Possible fields of research

- better lower bound for M^*?
- better lower bound for $M^{\diamondsuit}$?
- a nontrivial upper bound for $M^{\diamondsuit}$?

Possible fields of research

- better lower bound for M^*?
- better lower bound for $M^\diamondsuit$?
- a nontrivial upper bound for $M^\diamondsuit$?

Possible fields of research

- better lower bound for M^*?
- better lower bound for $M^{\diamondsuit}$?
- a nontrivial upper bound for $M^{\diamondsuit}$?

THE END.