Synchronizing Finite Automata

VIII. Automata vs Matrices

Mikhail Volkov

Ural State University, Ekaterinburg, Russia

CSClub, St Petersburg, November 21, 2010

1. Recap

Deterministic finite automata (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 $q, q' \in Q$.

$|Q\,.\,w| = 1$. Here $Q\,.\,v = \{\delta(q, v) \mid q \in Q\}$.

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

1. Recap

Deterministic finite automata (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 $q, q' \in Q$.

$|Q\,.\,w| = 1$. Here $Q\,.\,v = \{\delta(q, v) \mid q \in Q\}$.

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

1. Recap

Deterministic finite automata (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 $q, q' \in Q$.
$|Q\,.\,w| = 1$. Here $Q\,.\,v = \{\delta(q, v) \mid q \in Q\}$.

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

1. Recap

Deterministic finite automata (DFA): $\mathscr{A} = \langle Q, \Sigma, \delta \rangle$.

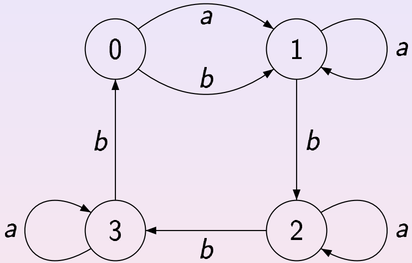
- Q the state set
- Σ the input alphabet
- $\delta : Q \times \Sigma \to Q$ the transition function

$\mathscr{A}$ 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 $q, q' \in Q$.

$|Q\,.\,w| = 1$. Here $Q\,.\,v = \{\delta(q, v) \mid q \in Q\}$.

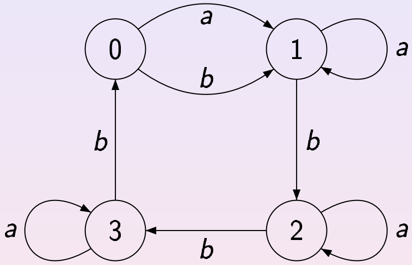
Any w with this property is a reset word for $\mathscr{A}$.

2. Example



A reset word is *abbbabbba*. In fact, we have verified that this is the shortest reset word for this automaton.

2. Example



A reset word is *abbbabbba*. In fact, we have verified that this is the shortest reset word for this automaton.

3. Černý Conjecture

The Černý conjecture is the claim that every synchronizing automaton with n states possesses a reset word of length $(n-1)^2$. The validity of the conjecture is main open problem of the area.

Define the *Černý function* $C(n)$ as the maximum length of shortest reset words for synchronizing automata with n states. In terms of this function, our current knowledge can be summarized in one line:

The Černý conjecture thus claims that in fact $C(n) = (n-1)^2$.

The Černý conjecture is the claim that every synchronizing automaton with n states possesses a reset word of length $(n-1)^2$. The validity of the conjecture is main open problem of the area.

Define the *Černý function* $C(n)$ as the maximum length of shortest reset words for synchronizing automata with n states. In terms of this function, our current knowledge can be summarized in one line:

The Černý conjecture thus claims that in fact $C(n) = (n-1)^2$.

3. Černý Conjecture

The Černý conjecture is the claim that every synchronizing automaton with n states possesses a reset word of length $(n-1)^2$. The validity of the conjecture is main open problem of the area.

Define the *Černý function* $C(n)$ as the maximum length of shortest reset words for synchronizing automata with n states. In terms of this function, our current knowledge can be summarized in one line:

The Černý conjecture thus claims that in fact $C(n) = (n-1)^2$.

The Černý conjecture is the claim that every synchronizing automaton with n states possesses a reset word of length $(n-1)^2$. The validity of the conjecture is main open problem of the area.

Define the *Černý function* $C(n)$ as the maximum length of shortest reset words for synchronizing automata with n states. In terms of this function, our current knowledge can be summarized in one line:

The Černý conjecture thus claims that in fact $C(n) = (n-1)^2$.

3. Černý Conjecture

The Černý conjecture is the claim that every synchronizing automaton with n states possesses a reset word of length $(n-1)^2$. The validity of the conjecture is main open problem of the area.

Define the *Černý function* $C(n)$ as the maximum length of shortest reset words for synchronizing automata with n states. In terms of this function, our current knowledge can be summarized in one line:

$$\text{(Černý, 1964)} \quad (n-1)^2 \leq C(n)$$

The Černý conjecture thus claims that in fact $C(n) = (n-1)^2$.

3. Černý Conjecture

The Černý conjecture is the claim that every synchronizing automaton with n states possesses a reset word of length $(n-1)^2$. The validity of the conjecture is main open problem of the area.

Define the *Černý function* $C(n)$ as the maximum length of shortest reset words for synchronizing automata with n states. In terms of this function, our current knowledge can be summarized in one line:

$$\text{(Černý, 1964)}\quad (n-1)^2 \leq C(n) \leq \frac{n^3-n}{6} \quad \text{(Pin–Frankl, 1983).}$$

The Černý conjecture thus claims that in fact $C(n) = (n-1)^2$.

3. Černý Conjecture

The Černý conjecture is the claim that every synchronizing automaton with n states possesses a reset word of length $(n-1)^2$. The validity of the conjecture is main open problem of the area.

Define the *Černý function* $C(n)$ as the maximum length of shortest reset words for synchronizing automata with n states. In terms of this function, our current knowledge can be summarized in one line:

$$\text{(Černý, 1964)}\quad (n-1)^2 \leq C(n) \leq \frac{n^3-n}{6} \quad \text{(Pin–Frankl, 1983).}$$

The Černý conjecture thus claims that in fact $C(n) = (n-1)^2$.

4. Recent Discovery

Vladimir Gusev, a PhD student of mine, has performed a massive series of experiments searching exhaustively through automata with a modest number of states in order to find new examples of “slowly” synchronizing automata. He has used an approach due to Marco Almeida, Nelma Moreira and Rogério Reis, Enumeration and generation with a string automata representation, Theor. Comput. Sci., 387 (2007) 93–102.

4. Recent Discovery

Vladimir Gusev, a PhD student of mine, has performed a massive series of experiments searching exhaustively through automata with a modest number of states in order to find new examples of "slowly" synchronizing automata. He has used an approach due to Marco Almeida, Nelma Moreira and Rogério Reis, Enumeration and generation with a string automata representation, Theor. Comput. Sci., 387 (2007) 93–102.

5. Second Gap

The next tables present the distribution of non-isomorphic synchronizing automata with 8 and 9 states and 2 letters with respect to the minimum length of their reset words.

5. Second Gap

The next tables present the distribution of non-isomorphic synchronizing automata with 8 and 9 states and 2 letters with respect to the minimum length of their reset words.

8 states:

Reset word length	49	48	47	46	45	44	43	42	41	40
# of automata	1	0	0	0	0	1	1	3	1	5

5. Second Gap

The next tables present the distribution of non-isomorphic synchronizing automata with 8 and 9 states and 2 letters with respect to the minimum length of their reset words.

8 states:

Reset word length	49	48	47	46	45	44	43	42	41	40
# of automata	1	0	0	0	0	1	1	3	1	5

5. Second Gap

The next tables present the distribution of non-isomorphic synchronizing automata with 8 and 9 states and 2 letters with respect to the minimum length of their reset words.

8 states:

Reset word length	49	48	47	46	45	44	43	42	41	40
# of automata	1	0	0	0	0	1	1	3	1	5

9 states:

Reset word length	64	63	62	61	60	59	58	57	56	55
# of automata	1	0	0	0	0	0	1	2	3	0

Reset word length	54	53	52	51
# of automata	0	0	4	4

5. Second Gap

The next tables present the distribution of non-isomorphic synchronizing automata with 8 and 9 states and 2 letters with respect to the minimum length of their reset words.

8 states:

Reset word length	49	48	47	46	45	44	43	42	41	40
# of automata	1	0	0	0	0	1	1	3	1	5

9 states:

Reset word length	64	63	62	61	60	59	58	57	56	55
# of automata	1	0	0	0	0	0	1	2	3	0

Reset word length	54	53	52	51
# of automata	0	0	4	4

Thus, the pattern is:

$(n-1)^2$ the first gap the "island" the second gap

The second gap first appears at 9 states and grows rather regularly with the number of states. The size of the island depends only on the parity of the number of states.

The very same pattern appears in the distribution of exponents of non-negative matrices.

Thus, the pattern is:

$(n-1)^2$ the first gap the “island” the second gap

The second gap first appears at 9 states and grows rather regularly with the number of states. The size of the island depends only on the parity of the number of states.

The very same pattern appears in the distribution of exponents of non-negative matrices.

Thus, the pattern is:

$(n-1)^2$ the first gap the "island" the second gap

The second gap first appears at 9 states and grows rather regularly with the number of states. The size of the island depends only on the parity of the number of states.

The very same pattern appears in the distribution of exponents of non-negative matrices.

A non-negative matrix A is said to be primitive if some power A^k is positive. The minimum k with this property is called the exponent of A, denoted $\exp A$.

Helmut Wielandt proved in 1950 that for any primitive $n \times n$-matrix A, one has $\exp A \leq n^2 - 2n + 2 = (n-1)^2 + 1$, and this bound is tight. Possible exponents of $n \times n$-matrices were intensively studied in the 1960s, and it was discovered that two extreme values are each attained by a unique matrix, then there is a gap followed by an island followed by another gap. The sizes of the gaps and of the island perfectly match the sizes of the gaps and of the islands in possible lengths of shortest reset words for synchronizing automata with n steps – basically one has the same picture shifted by 1. Clearly, this cannot be a mere coincidence.

7. Exponents of Non-negative Matrices

A non-negative matrix A is said to be primitive if some power A^k is positive. The minimum k with this property is called the exponent of A, denoted $\exp A$.

Helmut Wielandt proved in 1950 that for any primitive $n \times n$-matrix A, one has $\exp A \leq n^2 - 2n + 2 = (n-1)^2 + 1$, and this bound is tight. Possible exponents of $n \times n$-matrices were intensively studied in the 1960s, and it was discovered that two extreme values are each attained by a unique matrix, then there is a gap followed by an island followed by another gap. The sizes of the gaps and of the island perfectly match the sizes of the gaps and of the islands in possible lengths of shortest reset words for synchronizing automata with n steps – basically one has the same picture shifted by 1. Clearly, this cannot be a mere coincidence.

7. Exponents of Non-negative Matrices

A non-negative matrix A is said to be primitive if some power A^k is positive. The minimum k with this property is called the exponent of A, denoted $\exp A$.

Helmut Wielandt proved in 1950 that for any primitive $n \times n$-matrix A, one has $\exp A \leq n^2 - 2n + 2 = (n-1)^2 + 1$, and this bound is tight. Possible exponents of $n \times n$-matrices were intensively studied in the 1960s, and it was discovered that two extreme values are each attained by a unique matrix, then there is a gap followed by an island followed by another gap. The sizes of the gaps and of the island perfectly match the sizes of the gaps and of the islands in possible lengths of shortest reset words for synchronizing automata with n steps – basically one has the same picture shifted by 1. Clearly, this cannot be a mere coincidence.

7. Exponents of Non-negative Matrices

A non-negative matrix A is said to be primitive if some power A^k is positive. The minimum k with this property is called the exponent of A, denoted $\exp A$.

Helmut Wielandt proved in 1950 that for any primitive $n \times n$-matrix A, one has $\exp A \leq n^2 - 2n + 2 = (n-1)^2 + 1$, and this bound is tight. Possible exponents of $n \times n$-matrices were intensively studied in the 1960s, and it was discovered that two extreme values are each attained by a unique matrix, then there is a gap followed by an island followed by another gap. The sizes of the gaps and of the island perfectly match the sizes of the gaps and of the islands in possible lengths of shortest reset words for synchronizing automata with n steps – basically one has the same picture shifted by 1. Clearly, this cannot be a mere coincidence.

7. Exponents of Non-negative Matrices

A non-negative matrix A is said to be primitive if some power A^k is positive. The minimum k with this property is called the exponent of A, denoted $\exp A$.

Helmut Wielandt proved in 1950 that for any primitive $n \times n$-matrix A, one has $\exp A \leq n^2 - 2n + 2 = (n-1)^2 + 1$, and this bound is tight. Possible exponents of $n \times n$-matrices were intensively studied in the 1960s, and it was discovered that two extreme values are each attained by a unique matrix, then there is a gap followed by an island followed by another gap. The sizes of the gaps and of the island perfectly match the sizes of the gaps and of the islands in possible lengths of shortest reset words for synchronizing automata with n steps – basically one has the same picture shifted by 1. Clearly, this cannot be a mere coincidence.

8. Digraphs and Matrices

A directed graph (digraph) is a pair $D = \langle V, E \rangle$.

- V set of vertices
- $E \subseteq V \times V$ set of edges

This definition allows loops but excludes multiple edges.

The matrix of a digraph $D = \langle V, E \rangle$ is just the incidence matrix of the edge relation, that is, a $V \times V$-matrix whose entry in the row v and the column v' is 1 if $(v, v') \in E$ and 0 otherwise.

8. Digraphs and Matrices

A directed graph (digraph) is a pair $D = \langle V, E \rangle$.

- V set of vertices
- $E \subseteq V \times V$ set of edges

This definition allows loops but excludes multiple edges.

The matrix of a digraph $D = \langle V, E \rangle$ is just the incidence matrix of the edge relation, that is, a $V \times V$-matrix whose entry in the row v and the column v' is 1 if $(v, v') \in E$ and 0 otherwise.

A directed graph (digraph) is a pair $D = \langle V, E \rangle$.

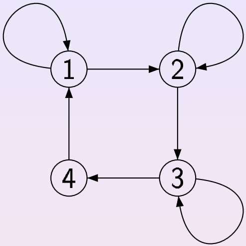
- V set of vertices
- $E \subseteq V \times V$ set of edges

This definition allows loops but excludes multiple edges.

The matrix of a digraph $D = \langle V, E \rangle$ is just the incidence matrix of the edge relation, that is, a $V \times V$-matrix whose entry in the row v and the column v' is 1 if $(v, v') \in E$ and 0 otherwise.

9. Digraphs and Matrices

For instance, the matrix of the digraph

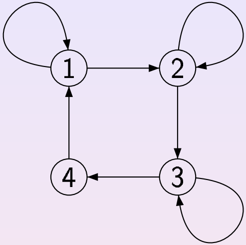


(with respect to the chosen numbering of its vertices) is $\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$.

Conversely, given an $n \times n$-matrix $P = (p_{ij})$ with non-negative real entries, we assign to it a digraph $D(P)$ on the set $\{1, 2, \ldots, n\}$ as follows: (i, j) is an edge of $D(P)$ if and only if $p_{ij} > 0$.

This 'two-way' correspondence allows us to reformulate in terms of digraphs several important notions and results which originated in the classical Perron–Frobenius theory of non-negative matrices.

For instance, the matrix of the digraph

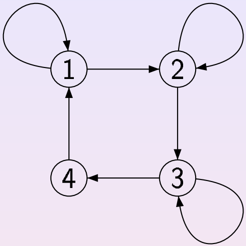


(with respect to the chosen numbering of its vertices) is $\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$.

Conversely, given an $n \times n$-matrix $P = (p_{ij})$ with non-negative real entries, we assign to it a digraph $D(P)$ on the set $\{1, 2, \ldots, n\}$ as follows: (i, j) is an edge of $D(P)$ if and only if $p_{ij} > 0$.

This 'two-way' correspondence allows us to reformulate in terms of digraphs several important notions and results which originated in the classical Perron–Frobenius theory of non-negative matrices.

For instance, the matrix of the digraph



(with respect to the chosen numbering of its vertices) is $\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$.

Conversely, given an $n \times n$-matrix $P = (p_{ij})$ with non-negative real entries, we assign to it a digraph $D(P)$ on the set $\{1, 2, \dots, n\}$ as follows: (i, j) is an edge of $D(P)$ if and only if $p_{ij} > 0$.

This 'two-way' correspondence allows us to reformulate in terms of digraphs several important notions and results which originated in the classical Perron–Frobenius theory of non-negative matrices.

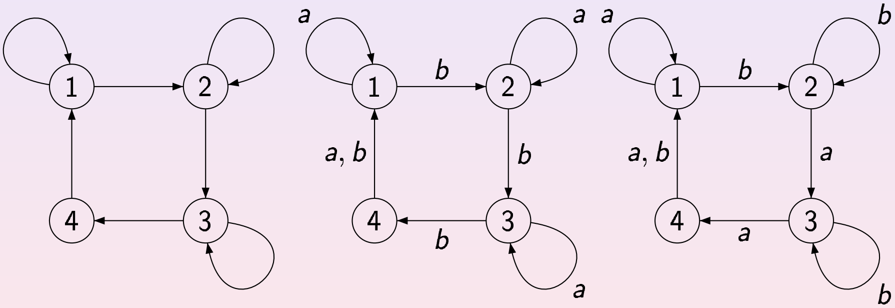
10. Digraphs and Colorings

Informally, by a coloring of a digraph we mean assigning labels from an alphabet Σ to edges such that the digraph labelled this way becomes a DFA.

By the underlying digraph of a DFA we mean the digraph obtained by erasing letters and identifying multiple edges in the diagram of the DFA.

11. Example

A digraph and two of its colorings



12. Primitive Digraphs

A digraph D is primitive if D is strongly connected and the greatest common divisor of the lengths of all cycles in D is equal to 1.

A digraph D is primitive if and only if there exists $t \in \mathbb{N}$ such that for each pair of vertices there exists a path between them of length exactly t. (This goes back to Frobenius's theory of non-negative matrices.)

The least t with this property is called the exponent of the digraph D and is denoted by $\gamma(D)$.

13. Road Coloring

There are tight connections between the notion of a primitive digraph and that of a synchronizing automaton:

1977, Adler, Goodwyn, Weiss:
Underlying digraphs of strongly connected synchronizing automata are primitive.

Road Coloring Conjecture: Every primitive digraph admits a synchronizing coloring.

Confirmed by Trahtman in 2007.

Is there a connection between numerical characteristics of these notions: exponent and reset length?

14. Exponents

We know a lot about exponents of digraphs.

1950, Wielandt:
The exponent of every primitive digraph on n vertices is not greater than $(n-1)^2+1$ and this bound is tight.

1964, Dulmage-Mendelsohn:
There is exactly one primitive digraph on n vertices with exponent equal to $(n-1)^2+1$ and exactly one primitive digraph on n vertices with exponent equal to $(n-1)^2$.

If $n>4$ is even, then there is no primitive digraph D on n vertices such that $n^2-4n+6<\gamma(D)<(n-1)^2$.

If $n>3$ is odd, then there is no primitive digraph D on n vertices such that $n^2-3n+4<\gamma(D)<(n-1)^2$,
or $n^2-4n+6<\gamma(D)<n^2-3n+2$.

15. Experimental Results

Exponents of primitive digraphs with 9 vertices vs reset lengths of 2-letter strongly connected synchronizing automata with 9 states

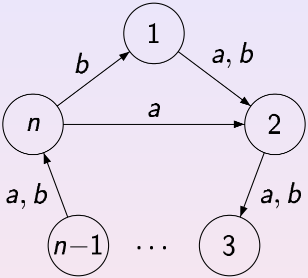
N	65	64	63	62	61	60	59	58	57	56	55	54	53	52	51
# of primitive digraphs with exponent N	1	1	0	0	0	0	0	1	1	2	0	0	0	0	4
# of 2-letter synchronizing automata with reset length N	0	1	0	0	0	0	0	1	2	3	0	0	0	4	4

At MFCS 2006, Trahtman reported the first gap in the upper part of the sequence of possible reset lengths.

The existence of the second gap have not been reported yet.

16. Wielandt Automaton

The Wielandt automaton $\mathscr{W}_n$ has $\gamma(\mathscr{W}_n) = (n-1)^2 + 1$



$$rl(\mathscr{W}_n) = n^2 - 3n + 3$$

Using the inequality $\gamma(\mathscr{W}_n) \le rl(\mathscr{W}_n) + n - 1$,
one can obtain $n^2 - 3n + 2 \le rl(\mathscr{W}_n)$.

Every digraph with large exponent produces slowly synchronizing automata.

17. Hybrid Conjecture

$\mathscr{W}_n$ possesses an essentially unique coloring.

In the general case, there can be a lot of colorings.

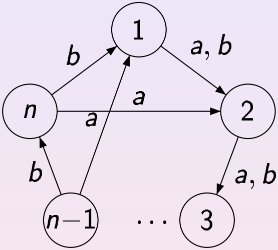
Problem: If a primitive digraph has n vertices, what is the minimum reset length for its synchronizing colorings?

Conjecture: Every primitive digraph with n vertices has a synchronizing coloring with reset length at most $n^2 - 3n + 3$.

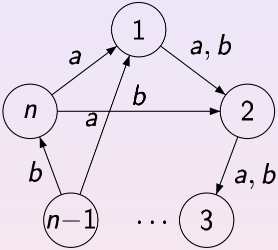
The graph $\mathscr{W}_n$ shows that this bound cannot be lowered.

18. Further Automata

Colorings of digraph with exponent $(n-1)^2$



$n^2 - 3n + 4$



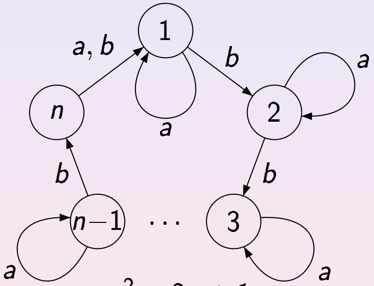
$n^2 - 3n + 2$

Left: The slowest automaton after $\mathscr{C}_n$.
Right: None of the letters act as a cyclic permutation.

However, not every slowly synchronizing automaton we discovered can be obtained in such a way.

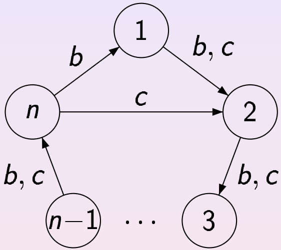
19. Černý Automaton

A reduction from the Černý automaton $\mathscr{C}_n$ to $\mathscr{W}_n$.



$n^2 - 2n + 1$

$\gamma(\mathscr{C}_n) = n - 1$



$n^2 - 3n + 3$

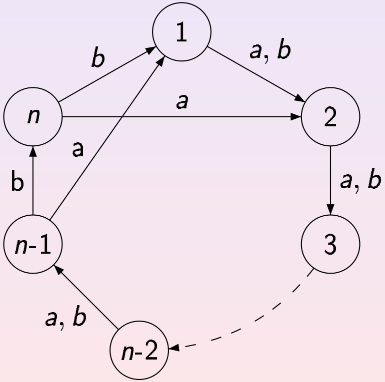
$\gamma(\mathscr{W}_n) = n^2 - 2n + 2$

$\mathscr{C}_n$ induces $\mathscr{W}_n$ by the actions of b and $c = ab$.
Every shortest synchronizing word of $\mathscr{C}_n$ transforms to a synchronizing word of $\mathscr{W}_n$.

20. Further Examples

All other automata from the 'island' can be explained via this 'unlooping' trick.

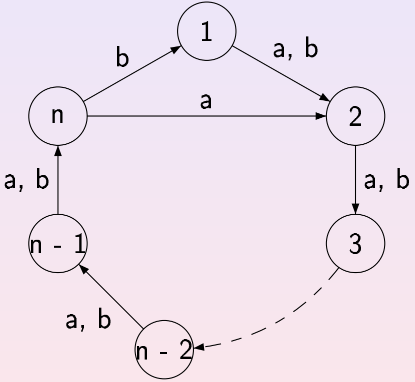
1 0 0 0 0 0 1 2 3 0 0 0 4 4



$n^2 - 3n + 4$

21. Further Examples

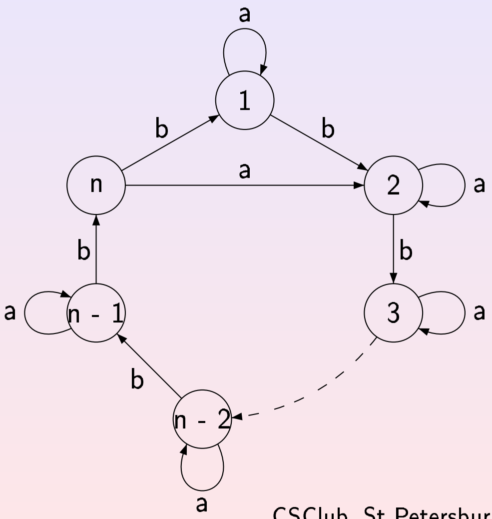
1 0 0 0 0 0 1 2 3 0 0 0 4 4



$n^2 - 3n + 3$

22. Further Examples

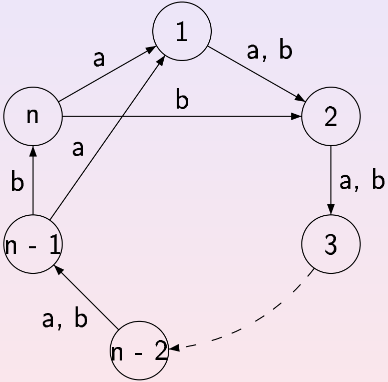
1 0 0 0 0 0 1 2 3 0 0 0 4 4



$n^2 - 3n + 3$, n odd

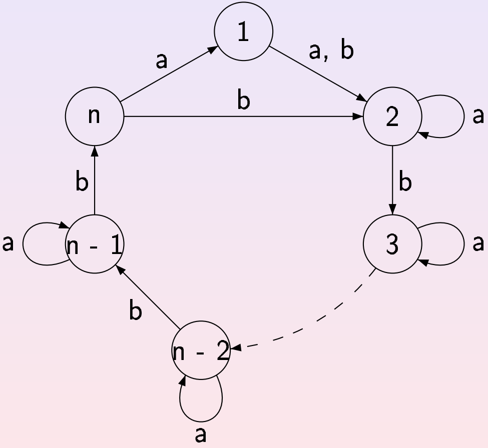
23. Further Examples

1 0 0 0 0 0 1 2 3 0 0 0 4 4



$n^2 - 3n + 2$

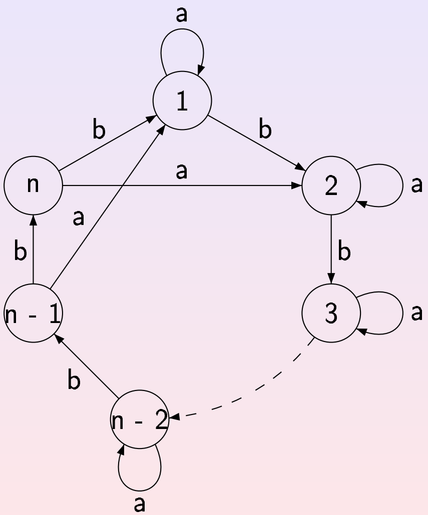
1 0 0 0 0 0 1 2 3 0 0 0 4 4



$n^2 - 3n + 2$

25. Further Examples

1 0 0 0 0 0 1 2 3 0 0 0 4 4



$n^2 - 3n + 2$, n odd

26. Conclusion

Main Contribution: Primitive digraphs with large exponent stand – directly or via unlooping – behind all known slowly synchronizing digraphs.

Future work:
Use this connection and the information of exponents of primitive digraphs in order to progress towards a proof of Černý's conjecture.