Ângela Filipa Pereira Cardoso

The Černý Conjecture and Other Synchronization Problems

Departamento de Matemática
Faculdade de Ciências da Universidade do Porto

Março de 2014

Ângela Filipa Pereira Cardoso

The Černý Conjecture and Other Synchronization Problems

U.PORTO

FC FACULDADE DE CIÊNCIAS
UNIVERSIDADE DO PORTO

Tese submetida à Faculdade de Ciências da Universidade do Porto
para obtenção do grau de Doutor em Matemática
orientada pelo Professor Jorge Almeida

Departamento de Matemática
Faculdade de Ciências da Universidade do Porto
Março de 2014

Agradecimentos

Esta tese foi financiada com uma bolsa de investigação da Fundação para a Ciência e a Tecnologia (referência SFRH/BD/33099/2007) no âmbito do programa POPH, financiado pelo Fundo Social Europeu e pelo Governo Português.

Em primeiro lugar, quero agradecer ao meu orientador, o Professor Jorge Almeida, pela sua incansável dedicação, por tudo o que me ensinou e pela paciência que sempre teve comigo. Muito dificilmente conseguiria imaginar um orientador melhor.

Um agradecimento ao Departamento de Matemática da Faculdade de Ciências da Universidade do Porto e a todas as pessoas que dele fazem parte. Além de serem responsáveis por praticamente toda a minha formação nesta área, providenciaram-me excelentes condições para realizar os meus trabalhos de doutoramento, quer nas instalações e nos recursos científicos e informáticos, quer no ambiente acolhedor. Agradeço também ao Departamento de Matemática da Universidade de Coimbra, especialmente aos docentes que fazem parte do Programa Inter-Universitário de Doutoramento em Matemática.

Estou grata ao Centro de Matemática da Universidade do Porto, pelo apoio financeiro prestado, que me permitiu estabelecer ligações científicas fundamentais na minha área de investigação.

O meu agradecimento à Universidade Estatal dos Urais, em Ekaterinburg, e especialmente ao Professor Volkov e aos seus alunos, que calorosamente me acolheram.

Ao Millennium bcp, por me ter permitido dedicar tempo à conclusão desta tese, e a todos os meus colegas de trabalho, pelo esforço que fizeram para que eu pudesse ter esse tempo. Agradeço particularmente àqueles que tanto me encorajaram nesta fase final.

Agradeço aos meus colegas de doutoramento que partilharam este desafio comigo. À minha família e aos meus amigos que tanto me incentivaram. Um obrigada muito especial à Ana e à Joana, não estaria aqui sem vocês. E à Margarida, que esteve sempre ao meu lado e do meu lado.

Aos meus pais, por gostarem incondicionalmente de mim. Por todo o vosso apoio e por acreditarem que eu era capaz. Estou-vos eternamente grata.

Resumo

Esta tese considera essencialmente três problemas relacionados com a Conjetura de Černý e, mais geralmente, com a sincronização de autómatos.

Primeiro estudamos a sincronização de digrafos. Apresentamos duas classes de digrafos totalmente sincronizáveis: a classe de digrafos monótonos e a classe de digrafos monótonos generalizados, que por sua vez coincide com as classes de digrafos acíclicos e de digrafos aperiódicos. Para estas classes, apresentamos majorantes ótimos para o comprimento de palavras sincronizantes universais mais curtas. Mostramos ainda que, para obter um majorante do comprimento de palavras sincronizantes universais mais curtas para todos os autómatos totalmente sincronizáveis, basta fazê-lo para autómatos com um único ponto fixo acessível e autómatos totalmente sincronizáveis fortemente conexos.

O segundo problema considerado está relacionado com a sincronização de autómatos aperiódicos fortemente conexos. É apresentada uma família destes autómatos. Esta família tem a propriedade de que o nível de monotonia fraca dos seus autómatos cresce com o número de estados. Isto inviabiliza um possível método para melhorar o majorante conhecido para o comprimento de palavras sincronizantes mais curtas para esta classe de autómatos, que consiste em estabelecer um majorante melhor para autómatos com níveis baixos de monotonia fraca.

Finalmente, dedicamos a nossa atenção à sincronização de subconjuntos de estados de autómatos sincronizáveis. Apresentamos uma conjetura para um majorante do comprimento de palavras mais curtas que sincronizam subconjuntos de estados de um determinado tamanho. Reduzimo-la à classe dos autómatos fortemente conexos, estabelecendo-a para autómatos com um único ponto fixo acessível. Provamos a nossa conjetura para uma subclasse de autómatos circulares fracamente orientados, que são um caso particular de autómatos fortemente conexos. Também obtemos um majorante para autómatos circulares, mas não é tão bom como o majorante conjeturado. Apresentamos evidência adicional a favor da nossa conjetura, estabelecendo-a para todos os exemplos conhecidos de autómatos de sincronização extrema e de sincronização lenta. Em particular, para o autómato de Černý, que também é usado para mostrar que o majorante que propomos não pode ser melhorado. Também provamos a Conjetura de Černý para autómatos fracamente orientados, obtendo assim uma generalização e uma simplificação da solução de Eppstein para autómatos orientados.

Abstract

This thesis mainly considers three problems related to the Černý Conjecture and, more generally, automata synchronization.

First we study digraph synchronization. We present two classes of totally synchronizing digraphs: the class of monotonic digraphs and the class of generalized monotonic digraphs, which coincides with the classes of acyclic digraphs and aperiodic digraphs. For these classes, we provide tight upper bounds on the length of shortest universal synchronizing words. We also establish that, in order to find an upper bound on the length of shortest universal synchronizing words for all totally synchronizing digraphs, it is enough to do so for digraphs with a unique sink and totally synchronizing strongly connected digraphs.

The second problem considered is related to the synchronization of strongly connected aperiodic automata. A family of such automata is presented. This family has the property that the level of weak monotonicity of its automata grows with the number of states. This undermines a possible method to improve the best known upper bound on the length of shortest synchronizing words for this class of automata, which consists of establishing a better bound for automata with low levels of weak monotonicity.

Finally we devote our attention to the synchronization of subsets of states of synchronizing automata. We present a conjecture on the upper bound on the length of shortest synchronizing words for subsets of a given size. We reduce it to the class of strongly connected automata, by establishing it for automata with a unique sink. We prove our conjecture for a subclass of weakly oriented circular automata, which are a special case of strongly connected automata. We also obtain an upper bound for circular automata, although it is not as good as the conjectured one. We provide further evidence for our conjecture, by establishing it for all extreme and slowly synchronizing automata known. In particular for the Černý automaton, that is also used to show that our proposed upper bound cannot be improved. We also prove Černý's Conjecture for weakly oriented automata, thus obtaining a generalization and a simplification of Eppstein's solution for oriented automata.

Contents

Chapter 1

Introduction

An automaton is said to be synchronizing if there is a word that sends every state to a single fixed state. In 1964, Černý [13] presented a family of synchronizing automata with n states whose shortest synchronizing words have length $(n-1)^2$ and conjectured that for every automaton with n states, if there is a synchronizing word, then there is one with at most $(n-1)^2$ letters. Several advances have been made towards the proof of this conjecture [4, 5, 7, 9, 11, 12, 16, 17, 21, 23, 29, 33–37, 40–43, 46, 47], but the general case remains open.

For more than 30 years now, the best known upper bound is $(n^3-n)/6$, usually attributed to Pin [31], who reduced it to a nontrivial combinatorial result, that was proven by Frankl in [19]. The full story of this result is actually more complex. The first time it appeared in the literature was in [18], where it was reduced to a combinatorial result similar to the one proven by Frankl. Since that combinatorial result was not established at the time, the paper was eventually forgotten. Later, the bound was rediscovered independently in [24]. Recently an improvement of this upper bound to $\frac{n(7n^2+6n-16)}{48}$ was published by Trahtman [45]. But later the author himself announced that an error was found in a key lemma and that the main result of the paper is not proved.[1]

A generalization of Černý's Conjecture was suggested by Pin [30], stating that if a given automaton with n states admits a word of rank r, that is a word that sends all states to a subset with r states, then there is such a word of length at most $(n-r)^2$. However, Kari [22] gave a counterexample to this conjecture. A reformulated version of Pin's Conjecture known as the Rank or Černý-Pin Conjecture still remains open; it states that if an automaton with n states has rank r, then there is a rank r word with at most $(n-r)^2$ letters.

Another well known problem related to automata synchronization that remained open for more than 30 years is the road coloring problem. In 1970, Adler and Weiss [2], raised the following question: given a strongly connected digraph with constant outdegree, when is it possible to label its edges in order to obtain a synchronizing automaton? Later, in 1977, jointly with Goodwyn [1], they explicitly stated the problem. The authors verified

[1]See http://arxiv.org/abs/1104.2409v7. The author thanks M. V. Volkov for this reference.

that it is a necessary condition that the greatest common divisor of all cycle lengths of the digraph is 1. They also conjectured that this condition, together with being strongly connected and having constant outdegree would be sufficient. In 2009, Trahtman [44] gave a positive answer to this conjecture.

Automata theory has many well known practical applications. Automata are used to describe machines and computers, in text processing and linguistics, in compilers, programming languages and artificial intelligence, and even in biology and neuroscience. In most cases, the same automaton will be used repeatedly, hence having a method to reset the automaton to a known state is naturally helpful.

Since not all automata are synchronizing, one may try to obtain characteristics that guarantee that a given automaton is synchronizing. Also, it is of clear interest to search for fast algorithms that decide if a given automaton can be synchronized, or that find synchronizing words if they exist. Moreover, since shorter synchronizing words mean faster synchronization, it is important to consider the question of what is the minimum length of a shortest synchronizing word.

Automata synchronization has also been linked to representation theory [4, 5] and to symbolic dynamics [1, 2], as well as other mathematical applications.

In 2008, at the School on Algebraic Theory of Automata in Lisbon, M. V. Volkov suggested several problems related to the road coloring problem and the Černý Conjecture. Among those problems was the question of characterizing totally synchronizing digraphs, that is, digraphs such that all their suitable labelings lead to synchronizing automata. Another problem was that of finding universal synchronizing words for such digraphs as well as computing an upper bound on the length of shortest universal synchronizing words. These words are synchronizing words for every automaton that can be obtained from the digraph. Relating the Rank Conjecture to these problems, one obtains the rank problem for digraphs, that is, the problem of computing shortest minimum rank words for such digraphs.

In Chapter 3, we consider these synchronization problems for digraphs. In particular, we obtain some results for the classes of monotonic and generalized monotonic digraphs, which are related to monotonic and generalized monotonic automata. We also obtain a result that states that to solve the problem of finding an upper bound on the length of shortest universal synchronizing words for digraphs, one needs to solve it only for the classes of strongly connected digraphs and digraphs with a sink. Even though we could not find a tight upper bound for the length of universal synchronizing words for strongly connected digraphs nor digraphs with a sink, we show that totally synchronizing monotonic digraphs constitute a subclass of digraphs with a sink.

Just like automata synchronization can be used to regain control of a machine whose current state is unknown, digraph synchronization can have the same use. But in this case we can regain control of a machine even if we have a much more limited understanding of it. To be precise, suppose that we had an automaton which described the machine but somehow we lost the labelings of the arcs, thus obtaining a digraph. If that digraph is totally synchronizing, a universal synchronizing word could be used to bring the machine to a specific state. The biggest difference is that the state to which the machine arrives after we apply such a word may depend on the original automaton, but still a universal synchronizing word would be useful.

To see another application of these notions, think of the digraph described by the street map of some amusement park or museum, with the paths and their directions providing the arcs and the attractions providing the vertices of the digraph. If we construct this digraph carefully we can make sure that it has constant outdegree, simply by turning some paths into multiple arcs. Now suppose that the manager of such a tourist spot decides to make maps with colored streets, in such a way that from each attraction there is always one and only one outgoing path with each of the chosen colors. This map would describe a finite automaton whose underlying digraph is as above. If the automaton is synchronizing the manager can include with the map a synchronizing sequence of colors, that would take every visitor to the exit independently of where that person is. But if the digraph is synchronizing, the manager can publish the map without coloring the paths and still include a universal synchronizing color sequence, the difference is that it is no longer guaranteed that this sequence brings all visitors to the exit, only that it joins all the people using the same coloring. This way, if a group of tourists buys this map and proceeds to color the streets following the rules that would lead them to obtain an automaton, then they can use the universal synchronizing color sequence to find each other if some of them get lost.

Note that there is a known upper bound on the length of shortest universal synchronizing words for a given totally synchronizing digraph G with n states and k letters. Indeed, a $(n-1)$-collapsing word on k elements [6] is a word that synchronizes every synchronizing automaton with n states and k letters; in particular, such a word is a universal synchronizing word for G. According to [26], the length of a shortest $(n-1)$-collapsing word on k elements is at most $k^{\frac{(n-1)(n-2)}{2}}$. Thus, $k^{\frac{(n-1)(n-2)}{2}}$ is an upper bound on the length of a shortest universal synchronizing word for G. It does not seem likely however that this bound is tight, since such a word synchronizes every synchronizing automaton with n states and k letters and not just the ones that share the same underlying digraph G.[2]

In Chapter 4, we show that, given a natural number l, there is a synchronizing strongly

[2]The author thanks E. Rodaro for this reference.

connected aperiodic automaton that is weakly monotonic of level l. The reason to search for strongly connected and aperiodic automata is the fact that in [47] the author suspects that the synchronizing bound $\lfloor n(n+1)/6 \rfloor$ for strongly connected weakly monotonic automata, can be further improved for this particular case. In a private communication, M. V. Volkov asked whether there is a bound on the level of weak monotonicity of strongly connected aperiodic automata, in the hope that such a property would entail fast synchronization. This was joint work with my supervisor, Professor Jorge Almeida, and is published in the International Journal of Algebra [3].

Chapter 5 is devoted to finding the length of the shortest synchronizing words for subsets of states of a given automaton. If the automata we are considering describe a certain machine, we may have some incomplete information on the current state of the machine. Perhaps we do not know the precise state it is in, but we know a subset of possible current states. This is where subset synchronization is useful, to take the machine to a known fixed state, we would only need to synchronize the subset of possible current states.

In the maps and museum examples given above, if the number of visitors is known, then we have an upper bound on the size of the set of current locations of the visitors. Therefore, it is natural to wonder about the length of a shortest set of instructions to gather all visitors in the same place, depending on the total number of locations and on the number of visitors.

Yet another possible application of subset synchronization is synchronization with high probability. Suppose that for each state of the automaton, we know the probability that it is the current state of the automaton. Then in order to obtain a word that has a high probability of bringing the automaton to a known fixed state, one may focus on finding a synchronizing word for the subset of states which have the highest probabilities of being the current state. In the museum example, one may assume that the visitors have a higher probability of being in the locations of the most popular attractions, and then use a synchronizing sequence for those locations to gather most of the visitors if not all.

Although our focus is on synchronizing subsets of synchronizing automata, the case of non synchronizing automata has been studied several times. Indeed, it is known that given an automaton and a set of states S deciding wether there is a synchronizing word for S is PSPACE-complete, see Natarajan [27] and Sandberg [39]. This contrasts with deciding wether a given automaton is synchronizing, which can be done in polynomial time, as was established by Černý [13]. Recently, Vorel [48] has shown that the problem mentioned above remains PSPACE-complete for strongly connected automata with an alphabet of size 2. It has been shown independently by Lee and Yannakakis [25] and A. Salomaa [38] that the length of a shortest synchronizing word for a subset of states of an automaton with n states may be $\lfloor \sqrt[3]{n} \rfloor !$. In [48], Vorel also shows that there is a strongly connected automaton with n states and 2 letters, with a subset of states S, such that the shortest synchronizing word for S has $2^{\Omega(n)}$ letters. This new lower bound is tight and substantially raises the previous known one for the general case, because $\lfloor \sqrt[3]{n} \rfloor !$ lies in $2^{o(n)}$.[3]

We state a conjecture on the length of shortest synchronizing words for subsets of a given size. Then we establish this conjecture for several well known classes and families of automata. Namely, we prove it for automata with a sink and for a subclass of weakly oriented circular automata. We provide a slightly larger upper bound for the class of circular automata. We verify that all extreme synchronizing automata satisfy our conjecture. This is true in particular for Černý family of automata that we use to show that our proposed upper bound cannot be improved. We also verify that all known families of slowly synchronizing automata satisfy our conjecture. We show that, to find an upper bound on the length of shortest synchronizing words for subsets of a given size, it is enough to do so for the class of strongly connected automata. Finally, although we are not able to obtain our conjecture for weakly oriented automata, we do provide a proof of Černý's Conjecture for this class of automata. This is a generalization as well as a simplification of Eppstein's result [17], which gives the Černý Conjecture for oriented automata. M. V. Volkov pointed to the author that this result is not new, since it was established in [7]. The proof obtained however is new and much simpler. Finally, there is some experimental evidence that further supports our conjecture. These results were obtained by Marek Szykuła, upon request by M. V. Volkov.

[3]The author thanks M. V. Volkov for the reference to the work of Vorel [48].

Chapter 2

Preliminaries

2.1 Digraphs and automata

For our purposes we define a *digraph* G as a triple (Q, X, ϕ), where Q is a finite nonempty set of *vertices*, X is a finite set disjoint from Q of *arcs*, and ϕ is an *incidence function* that associates to each element of X an ordered pair of (not necessarily distinct) elements of Q. Given an arc $x \in X$, if $\phi(x) = (p, q)$, for $p, q \in Q$, then we say that the arc x has *origin* p and *destination* q. Note that our digraphs may contain *loops*, that is, arcs whose origin and destination are one and the same vertex, as well as *multiple arcs*, that is arcs sharing the same origin and the same destination. The *outdegree* of a vertex is the number of arcs whose origin is that vertex. A *path* in the graph G is a sequence of arcs $x_1, x_2, \ldots, x_j$ such that for each $i \in \{1, 2, \ldots, j-1\}$ the destination of x_i and the origin of x_{i+1} are the same vertex. A *cycle* is a path such that the origin of the first arc and the destination of the last arc are the same vertex. Note that loops are cycles of length 1. If every cycle in G is a loop, then we say that G is *acyclic*. We say that the digraph G is *strongly connected* if for every pair of distinct vertices p, q there is a directed path in G going from p to q. A *subgraph* of the digraph $G = (Q, X, \phi)$ is a digraph of the form $H = (S, Y, \bar{\phi})$, where $S \subseteq Q$, $Y \subseteq X$, and $\bar{\phi}$ represents the restriction of ϕ to Y. We define a *special subgraph* of the digraph $G = (Q, X, \phi)$ as a subgraph $H = (S, Y, \bar{\phi})$ for which $\phi^{-1}(S \times Q) = \phi^{-1}(S \times S) \subseteq Y$. Note that this notion is stronger than what in the literature is called an induced subgraph.

We define an *automaton* $\mathcal{G}$ as a triple (Q, A, δ), where Q represents the set of *states*, A is the *alphabet*, whose elements are *letters*, and δ is the *transition function* that associates to each pair $(q, a) \in Q \times A$ a state from Q. The function δ is extended on the second component to the set A^* of all *words* in the alphabet A in the following way: if $w, \bar{w} \in A^*$ and $a \in A$ are such that $w = a\bar{w}$, then $\delta(q, w) = \delta(\delta(q, a), \bar{w})$, for every state $q \in Q$. Another way to look at an automaton is as a digraph with labeled arcs, where the labels are the letters from A and for each vertex p and each letter a there is an arc leaving p whose label is a. In the general literature, the automata we are considering are actually complete deterministic finite automata without sets of initial and final states.

Given a digraph G with constant outdegree l and an alphabet A with l letters, we say that a labeling of the arcs in G using the letters from A is *suitable* if it turns G into an automaton $\mathcal{G} = (Q, A, \delta)$. A transition function δ associated with a suitable labeling of the arcs in G will also be called *suitable*. If the digraph G is such that the outdegree of each vertex is at most l and we label the edges in G using the letters from A in such a way that no two vertices with the same origin share the same label, that labeling will still be called *suitable*. A *fixed point* is a vertex q of G such that all arcs leaving q are loops. A *sink* is a fixed point q such that for every vertex p in G there is a path connecting it to p. From these definitions we conclude that a digraph G cannot have more than one sink, but it can have several fixed points. We say that the automaton $\mathcal{G}$ is *strongly connected* if its underlying digraph is strongly connected.

2.2 Synchronizing automata

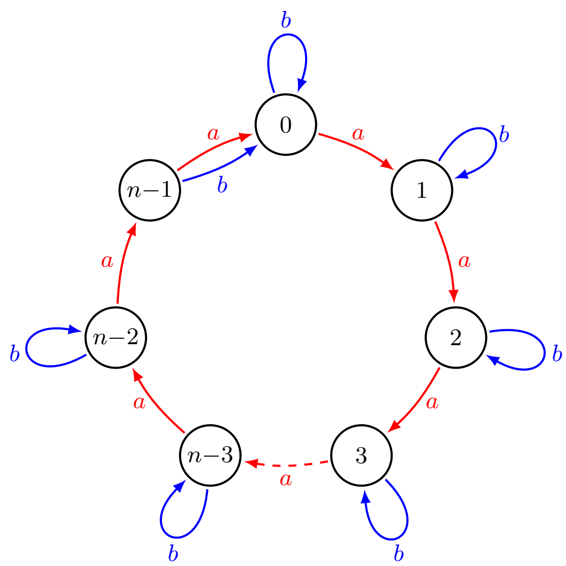

Figure 2.2.1: Černý automaton $\mathcal{C}_n$

The automaton $\mathcal{G} = (Q, A, \delta)$ is said to be *synchronizing* if there is a word $w \in A^*$ such that the set $\delta(Q, w)$ is a singleton. Such a word is called a *synchronizing word*. We denote by $\mathrm{len}(\mathcal{G})$ the length of the shortest word that synchronizes $\mathcal{G}$. This notion was first introduced in 1964 by Černý [13], who presented a family of synchronizing automata with n states whose shortest synchronizing words have length $(n-1)^2$. The Černý automaton, represented in Figure 2.2.1, is defined for each integer $n > 1$ as the automaton $\mathcal{C}_n$ with state set $Q = \{0, 1, \ldots, n-1\}$, alphabet $A_{\mathcal{C}_n} = \{a, b\}$ and transition function $\delta_{\mathcal{C}_n}$ such that, given $q \in Q$,

$$\delta_{\mathcal{C}_n}(q,a) = \begin{cases} q+1 & \text{if } q \neq n-1, \\ 0 & \text{if } q = n-1, \end{cases} \qquad \delta_{\mathcal{C}_n}(q,b) = \begin{cases} q & \text{if } q \neq n-1, \\ 0 & \text{if } q = n-1. \end{cases}$$

In general, when we draw such a diagram, with dashed arrows, we represent a family of automata. A dashed arrow with label a indicates a path in which all arcs have label a. It should be clear from the context which vertices such a path traverses. In Figure 2.2.1, there may be no arc labeled with a going from 3 to $n-3$, but there is always such an arc going from each vertex to the next in the cyclic order, thus forming a path from 3 to $n-3$. A shortest synchronizing word for $\mathcal{C}_n$ is $(ba^{n-1})^{n-1}$. It is easy to see that this word synchronizes the automaton, but not so simple to prove that there is no shorter synchronizing word. In Chapter 5, we will make use of the technique introduced by Černý to establish this fact. Černý believed that his automata represent the worst case scenario. In other words, he made the following conjecture.

Conjecture 2.2.1 ([13])**.** *Given a synchronizing automaton $\mathcal{G} = (Q, A, \delta)$ with n states, there is a synchronizing word for $\mathcal{G}$ whose length is at most $(n-1)^2$.*

If we denote by $\operatorname{len}(n)$ the maximum value of $\operatorname{len}(\mathcal{G})$, where $\mathcal{G}$ is a synchronizing automaton with n states, then Černý's Conjecture simply states that $\operatorname{len}(n) = (n-1)^2$.

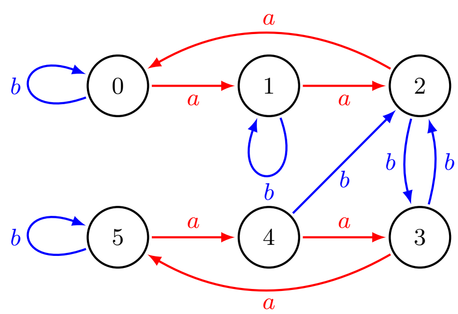

Figure 2.2.2: Kari automaton $\mathcal{X}_6$

Given an automaton $\mathcal{G} = (Q, A, \delta)$ and a word $w \in A^*$, we say that w has *rank* r if $\delta(Q, w)$ has exactly r elements. The *rank* of the automaton $\mathcal{G}$ is the minimum of the ranks of all the words in A^*. The following generalization of Černý's Conjecture was suggested by Pin [30]: if for a given automaton with n states there is a word of rank r, then there is such a word of length at most $(n-r)^2$. However, Kari [22] gave a counterexample to this conjecture, which we will denote by $\mathcal{X}_6$ and is represented in Figure 2.2.2. This automaton is synchronizing and the shortest words of rank 2 have length $17 > (6-2)^2$. A reformulated version of Pin's Conjecture known as the Rank or Černý-Pin Conjecture still remains open.

Conjecture 2.2.2. *Given an automaton $\mathcal{G} = (Q, A, \delta)$ with n states and rank r, there is a word of rank r, whose length is at most $(n-r)^2$.*

Note that Černý's Conjecture is the particular case where $r = 1$. Also, Kari's automaton does not provide a counter example for this conjecture since its rank is 1 and we will later see that its shortest synchronizing word has length $(6-1)^2 = 25$.

Černý's Conjecture remains open, it has only been established for some classes of automata. However, there is an upper bound for the general case, which may be found for example in [31].[1]

Theorem 2.2.3 ([31])**.** *Given a synchronizing automaton $\mathcal{G} = (Q, A, \delta)$ with n states, there is a synchronizing word for $\mathcal{G}$ with at most $(n^3 - n)/6$ letters.*

Of the several classes of automata for which Černý's Conjecture has been established, we will give special attention to some, that will be of use in the following chapters.

2.3 Monotonic and generalized monotonic automata

The automaton $\mathcal{G} = (Q, A, \delta)$ is said to be *monotonic* [8] if there is a total linear order $\leq$ on the state set Q such that given $p, q \in Q$ and $a \in A$, if $p \leq q$ then $\delta(p, a) \leq \delta(q, a)$. A linear order $\leq$ in these conditions will be called *perfect*.

Given a complete deterministic finite automaton $\mathcal{G} = (Q, A, \delta)$, a binary relation $\rho \subseteq Q \times Q$ in $\mathcal{G}$ is *stable* if for every $a \in A$ and every $p, q \in Q$, $(p, q) \in \rho$ implies $(\delta(p, a), \delta(q, a)) \in \rho$. The equivalence closure of a binary relation ρ, denoted by $\mathrm{Eq}(\rho)$, is the smallest equivalence relation that contains ρ. Of course, if ρ is stable so is $\mathrm{Eq}(\rho)$. A *congruence* over $\mathcal{G}$ is a stable equivalence relation $\pi \subseteq Q \times Q$. Denote by $[q]_\pi$ the π-class that contains the state $q \in Q$. We define the *quotient automaton* $\mathcal{G}/\pi$ as the automaton $(Q/\pi, A, \delta_\pi)$, with set of states $Q/\pi = \{[q]_\pi : q \in Q\}$ and transition function δ_π such that for every π-class $[p]_\pi$, we have $\delta_\pi([p]_\pi, x) = [\delta(p, x)]_\pi$.

Consider a congruence π on the automaton $\mathcal{G} = (Q, A, \delta)$. We say that $\mathcal{G}$ is π-*monotonic*, see [9], if there is a partial order $\leq$ on the state set Q for which:

- the states p and q are $\leq$-comparable if and only if $(p, q) \in \pi$;
- for all $p, q \in Q$ and $x \in A$, $p \leq q$ implies $\delta(p, x) \leq \delta(q, x)$.

An automaton $\mathcal{G}$ is said to be *generalized monotonic of level l* [9], if there is a sequence of congruences on $\mathcal{G}$, $\pi_0 \subsetneq \pi_1 \subsetneq \cdots \subsetneq \pi_l$, such that π_0 is the equality relation, π_l is the

[1] For further details see the Introduction.

universal relation and $\mathcal{G}/\pi_{i-1}$ is π_i/π_{i-1}-monotonic for every $i \in \{1, 2, \ldots, l\}$. This way, generalized monotonic automata of level 1 are just monotonic automata. We say that the automaton $\mathcal{G}$ is *generalized monotonic* if it is generalized monotonic of level l for some l.

The Rank Conjecture for monotonic automata was established in [8]. That result was then extended to the class of generalized monotonic automata [9]. Actually, the linear bound $n - r$ was obtained in both cases.

Theorem 2.3.1 ([9]). *Given a generalized monotonic automaton $\mathcal{G}$ with n states and rank r, there is a rank r word for $\mathcal{G}$ whose length is at most $n - r$.*

2.4 Automata with a sink

It is a known result, which is considered folklore [47], that automata with a sink satisfy the Černý Conjecture. A proof of this result can be found for example in [35], where the author also provides an example that shows that the upper bound obtained is tight.

Theorem 2.4.1 ([35]). *Given a synchronizing automaton $\mathcal{G}$ with n states and a sink, there is a synchronizing word for $\mathcal{G}$ whose length is at most $\frac{n(n-1)}{2}$.*

The Rystsov automaton is defined for each integer $n > 1$ as the automaton $\mathcal{R}_n$, represented in Figure 2.4.1, with state set $Q = \{0, 1, \ldots, n-1\}$, alphabet $A_{\mathcal{R}_n} = \{a_1, a_2, \ldots, a_{n-1}\}$ and transition function $\delta_{\mathcal{R}_n}$ such that for every $i \in \{2, 3, \ldots, n-1\}$ and every $q \in Q$,

$$\delta_{\mathcal{R}_n}(q, a_1) = \begin{cases} 0 & \text{if } q \in \{0, 1\}, \\ q & \text{if } q > 1, \end{cases} \qquad \delta_{\mathcal{R}_n}(q, a_i) = \begin{cases} q & \text{if } q \notin \{i-1, i\}, \\ q+1 & \text{if } q = i-1, \\ q-1 & \text{if } q = i. \end{cases}$$

Note that this automaton clearly has a sink, namely the state 0. It is synchronizing, since for every state there is a directed path connecting it to 0. Rystsov [35] used this automaton to show that $\frac{n(n-1)}{2}$ is a lower bound on the length of synchronizing words for synchronizing automata with n states and a sink.

It is a well known result that the Černý Conjecture remains open only for the class of strongly connected automata. A proof of this result can be found in [47]. Actually, the author provides a generalization of this fact.

A *subautomaton* of the automaton $\mathcal{G} = (Q, A, \delta)$ is an automaton $\bar{\mathcal{G}} = (\bar{Q}, \bar{A}, \bar{\delta})$ such that $\bar{Q} \subseteq Q$, $\bar{A} \subseteq A$ and $\bar{\delta}$ is the restriction of δ to $\bar{Q} \times \bar{A}$.

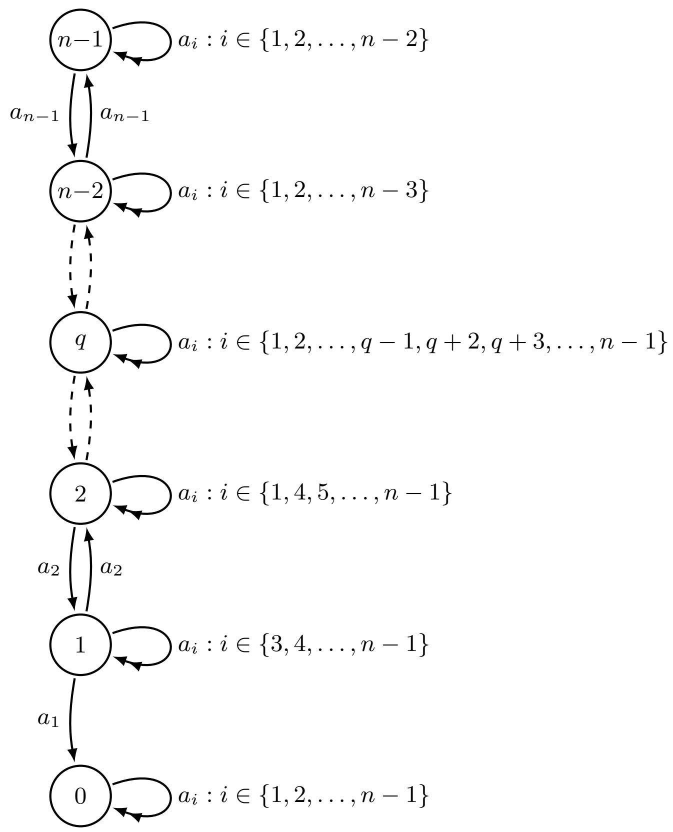

Figure 2.4.1: Rystsov automaton $\mathcal{R}_n$

Proposition 2.4.2 ([47]). *Let* $\mathbf{C}$ *be a class of synchronizing automata closed for subautomata and quotients. Denote by* $\mathbf{C}_n$ *the class of all automata in* $\mathbf{C}$ *with* n *states. Consider a function* $f : \mathbb{Z}^+ \longrightarrow \mathbb{N}$ *such that, for all integers* n, m *with* $n \geq m \geq 1$*,*

$$f(n) \geq f(n-m+1) + f(m) \tag{2.4.1}$$

Suppose that for every positive integer n *and every automaton* $\mathcal{H}$ *in* $\mathbf{C}_n$ *which either is strongly connected or has a sink,* $\operatorname{len}(\mathcal{H}) \leq f(n)$*. Then, for every automaton* $\mathcal{G}$ *in* $\mathbf{C}_n$*,* $\operatorname{len}(\mathcal{G}) \leq f(n)$*.*

Note that the function $f(n) = (n-1)^2$ satisfies the inequality (2.4.1), hence for the class of all synchronizing automata, since Černý's Conjecture is established for automata with a sink, all that is left is the strongly connected case.

2.5 Circular automata

Given an integer α, we denote by $\underline{\alpha} \in \{0, 1, \ldots, n-1\}$ the remainder of the integer division of α by n. Given a set $Q = \{0, 1, \ldots, n-1\}$, we define a *circular permutation* on Q as a bijection $f : Q \longrightarrow Q$ for which there is some $j \in \{1, 2, \ldots, n-1\}$ such that the greatest common divisor between j and n is 1 and $f(q) = \underline{q+j}$, for every $q \in Q$. Note that this is equivalent to defining a circular permutation on Q as a cycle of length $|Q|$. The automaton $\mathcal{G} = (Q, A, \delta)$ with n states is said to be *circular* if there is a letter $a \in A$, such that $\delta(\cdot, a) : Q \longrightarrow Q$ is a circular permutation. Whenever we deal with circular automata we will always assume that the letter $a \in A$ acts as a circular permutation. Also, we will define the positive integer $\lambda \in \{1, 2, \ldots, n-1\}$ such that λ and n are co-prime and $\delta(q, a) = \underline{q + \lambda}$ for every state $q \in Q$ as the *jump* of a.

In 1978, Pin [29] proved the Černý Conjecture for circular automata with a prime number of states. Later, in 1998, Dubuc [16] generalized this result for the class of all circular automata. In fact, the following result was obtained.

Theorem 2.5.1 ([16])**.** *Given a synchronizing circular automaton $\mathcal{G} = (Q, A, \delta)$ with n states and a proper subset S of Q, there is some word $w \in A^*$ such that $|w| \leq n$ and $|\delta^{-1}(S, w)| > |S|$.*

Using Theorem 2.5.1 it is simple to prove the Černý Conjecture for circular automata. Indeed, given a synchronizing automaton $\mathcal{G} = (Q, A, \delta)$ with n states, there are some state $q \in Q$ and some letter $b \in A$ such that $|\delta^{-1}(q, b)| \geq 2$. Then, if $\mathcal{G}$ is circular, using Theorem 2.5.1 recursively one obtains increasingly larger subsets of Q until the whole set is obtained. The synchronizing word w obtained has at most $1 + n(n-2) = (n-1)^2$ letters.

Theorem 2.5.2 ([16])**.** *Given a synchronizing circular automaton $\mathcal{G} = (Q, A, \delta)$ with n states, there is a synchronizing word for $\mathcal{G}$ with at most $(n-1)^2$ letters.*

2.6 Oriented automata

Given an automaton $\mathcal{G} = (Q, A, \delta)$ with n states and a cyclic order $q_0, q_1, \ldots, q_{n-1}, q_0$ on the set of states Q, we write $\langle q_i, q, q_j \rangle$ to indicate that q is between q_i and q_j in the cyclic order. In other words, q_i, q, q_j is a subsequence of some circular permutation of $q_0, q_1, \ldots, q_{n-1}$. We denote by $[q_i, q_j]$ the subset $\{q \in Q : \langle q_i, q, q_j \rangle\}$. We define an *interval* I as a subset of Q such that, given $q_i, q_j \in I$, either $[q_i, q_j] \subseteq I$ or $[q_j, q_i] \subseteq I$. The *size* of an interval is the number of elements it contains. We say that $\mathcal{G}$ is *oriented* whenever the cyclic order is *preserved* by the transition function δ, that is, for every $q_i, q_j, q_k \in Q$, such that $\langle q_i, q_j, q_k \rangle$ and every letter $a \in A$, we have $\langle \delta(q_i, a), \delta(q_j, a), \delta(q_k, a) \rangle$. If a cyclic order is preserved by the transition function δ, then we will call it a *preserved order*.

The synchronization of an arbitrary automaton which preserves some cyclic order was studied by Eppstein in [17], where the word monotonic is used instead of oriented. Later, in [8], an automaton that preserves some linear order is called monotonic, and Eppstein's automata are called oriented.

The following lemma was used in [17] to establish the Černý Conjecture for oriented automata.

Lemma 2.6.1 ([17]). *Given an oriented automaton $\mathcal{G} = (Q, A, \delta)$, for every word $w \in A^*$ and every interval I of the state set Q, the set $\delta^{-1}(I, w)$ is an interval of Q.*

Theorem 2.6.2 ([17]). *Given a synchronizing oriented automaton $\mathcal{G}$ with n states, there is a synchronizing word for $\mathcal{G}$ whose length is at most $(n-1)^2$.*

2.7 Aperiodic automata

Given an automaton $\mathcal{G} = (Q, A, \delta)$ and a nonempty word $w \in A^+$, we define δ_w as the relation $\{(p, q) \in Q \times Q : \delta(p, w) = q\}$. The *transition semigroup* of the automaton $\mathcal{G} = (Q, A, \delta)$ is defined as $\mathsf{S}(\mathcal{G}) = \{\delta_w : w \in A^+\}$, with the product

$$\delta_w \delta_v = \delta_{wv} = \{(p, q) \in Q \times Q \mid \exists s \in Q : (p, s) \in \delta_w \wedge (s, q) \in \delta_v\}.$$

Note that $\mathsf{S}(\mathcal{G})$ is generated by $\{\delta_a : a \in A\}$.

A finite semigroup S is said to be *aperiodic* if every $\mathsf{s} \in \mathsf{S}$ is *aperiodic*, that is, there is some positive integer l such that $\mathsf{s}^l = \mathsf{s}^{l+1}$. An automaton $\mathcal{G} = (Q, A, \delta)$ whose transition semigroup is aperiodic is called *aperiodic* as well, which is equivalent to saying that, for every $w \in A^*$, there is some positive integer l such that $w^{l+1} = w^l$, in the sense that for every $q \in Q$, $\delta(q, w^{l+1}) = \delta(q, w^l)$. In [43], Trahtman proved that Černý's Conjecture is valid for aperiodic automata.

Theorem 2.7.1 ([43]). *Given a synchronizing aperiodic automaton $\mathcal{G}$ with n states, there is a synchronizing word for $\mathcal{G}$ whose length is at most $\frac{n(n-1)}{2}$.*

2.8 Weakly monotonic automata

The bound obtained in Theorem 2.7.1 was improved for the case of strongly connected aperiodic automata by Volkov in [47]. In fact, a larger class of strongly connected automata was considered.

The complete deterministic finite automaton $\mathcal{G} = (Q, A, \delta)$ is called *weakly monotonic of level l* [47], if there is a strictly increasing chain of stable binary relations $\rho^0 \subsetneq \rho^1 \subsetneq \cdots \subsetneq \rho^l$ on $\mathcal{G}$ such that:

- ρ^0 is the equality relation $\{(q, q) : q \in Q\}$;
- for each $i \in \{1, 2, \ldots, l\}$, $\pi^{i-1} = \mathrm{Eq}(\rho^{i-1}) \subsetneq \rho^i$ and ρ^i/π^{i-1} is a partial order on Q/π^{i-1};
- $\pi^l = \mathrm{Eq}(\rho^l)$ is the universal relation on Q.

The automaton $\mathcal{G}$ is said to be *weakly monotonic* if it is weakly monotonic of level l for some positive integer l. The following two results show that this class of automata contains other classes previously mentioned.

Proposition 2.8.1 ([47]). *Every aperiodic automaton is weakly monotonic.*

Proposition 2.8.2 ([47]). *Every automaton with a sink is weakly monotonic.*

Since an automaton with a sink may not be aperiodic the following result was also obtained.

Corollary 2.8.3 ([47]). *The class of weakly monotonic automata strictly contains the class of aperiodic automata.*

In [47], Proposition 2.4.2 is used on the class of weakly monotonic automata to restrict the problem to strongly connected weakly monotonic automata (containing in particular strongly connected aperiodic automata) for which the following result is obtained.

Theorem 2.8.4 ([47]). *Given a strongly connected weakly monotonic synchronizing automaton $\mathcal{G}$ with n states, there is a synchronizing word for $\mathcal{G}$ of length at most $\lfloor \frac{n(n+1)}{6} \rfloor$.*

2.9 Extreme and slowly synchronizing automata

We say that the synchronizing automaton $\mathcal{G}$ with n states is *extreme* [46] if its shortest synchronizing word has length $(n-1)^2$. Even though the Černý Conjecture has only

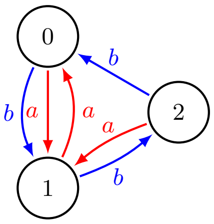

Figure 2.9.1: Automaton $\mathcal{X}_3^1$

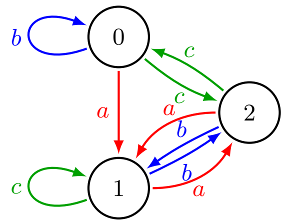

Figure 2.9.2: Automaton $\mathcal{X}_3^2$

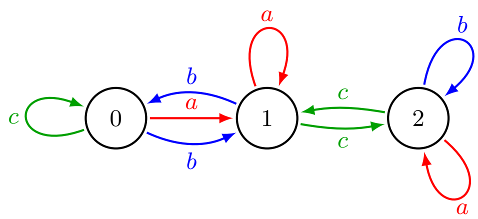

Figure 2.9.3: Automaton $\mathcal{X}_3^3$

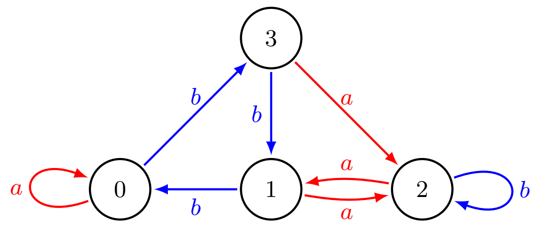

Figure 2.9.4: Automaton $\mathcal{X}_4^1$

been established for some classes of automata, and the best known upper bound for the general case [31] is cubic in n, as seen in Theorem 2.2.3, the number of known examples of extreme synchronizing automata is very reduced. Indeed, the Černý family of automata is the only known infinite series of extreme synchronizing automata. Aside from that, we know only a few small examples:

- three examples with 3 states, that seem to be due to Černý, Pirická and Rosenauerová [14] and which we denote by $\mathcal{X}_3^1, \mathcal{X}_3^2$ and $\mathcal{X}_3^3$ and are represented in Figures 2.9.1, 2.9.2 and 2.9.3, respectively;
- three examples with 4 states, that seem to be due to Černý, Pirická and Rosenauerová [14] and which we denote by $\mathcal{X}_4^1, \mathcal{X}_4^2$ and $\mathcal{X}_4^3$ and are represented in Figures 2.9.4, 2.9.5 and 2.9.6, respectively;
- one example with 5 states due to Roman [32], which we denote by $\mathcal{X}_5$ and is represented in Figure 2.9.7;
- the Kari automaton $\mathcal{X}_6$ with 6 states, mentioned above and which is represented in Figure 2.2.2.

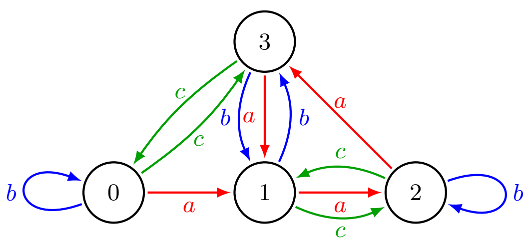

Figure 2.9.5: Automaton $\mathcal{X}_4^2$

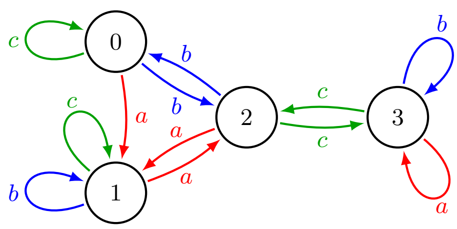

Figure 2.9.6: Automaton $\mathcal{X}_4^3$

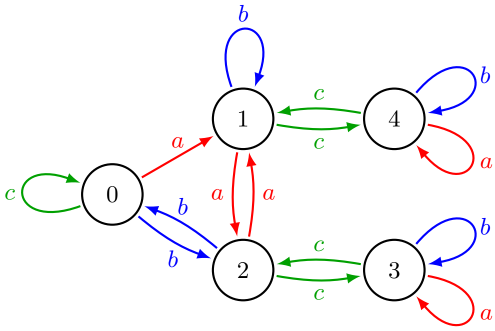

Figure 2.9.7: Roman automaton $\mathcal{X}_5$

Given an automaton $\mathcal{G} = (Q, A, \delta)$, the *power automaton* of $\mathcal{G}$ is the automaton $\mathcal{G}_{\mathcal{P}} = (Q_{\mathcal{P}}, A, \delta)$, where $Q_{\mathcal{P}}$ is the set formed by all non empty subsets of Q and given $S \subseteq Q$ and $a \in A$, $\delta(S, a) = \{\delta(s, a) : s \in S\}$. If $\mathcal{G}$ is synchronizing then, in the power automaton $\mathcal{G}_{\mathcal{P}}$, there is a path from the state $Q \in Q_{\mathcal{P}}$ to a singleton set $\{q\} \in Q_{\mathcal{P}}$, and it is labeled by a synchronizing word for $\mathcal{G}$. Hence, one can find the length of the shortest synchronizing word by counting the number of edges in a shortest path from Q to a singleton in $\mathcal{G}_{\mathcal{P}}$. This method can be used to verify that the automata $\mathcal{X}_3^1, \mathcal{X}_3^2, \mathcal{X}_3^3, \mathcal{X}_4^1, \mathcal{X}_4^2, \mathcal{X}_4^3, \mathcal{X}_5$ and $\mathcal{X}_6$ are indeed extreme synchronizing automata.

Let us say that the automaton $\mathcal{G}$ with n states is *slowly synchronizing* if it is synchronizing and $\operatorname{len}(\mathcal{G}) = \Theta(n^i)$ for some positive integer $i \geq 2$. Of course, if Černý's Conjecture is valid, then there is no slowly synchronizing automaton $\mathcal{G}$ such that $\operatorname{len}(\mathcal{G}) = \Theta(n^i)$ for $i > 2$. Even though Černý's Conjecture is only established for some cases, and the best known upper bound for the general case [45] is $\mathcal{O}(n^3)$, slowly synchronizing automata seem to be rare and there are probabilistic arguments that support this claim [11, 28]. However, in [10] several examples of infinite families of slowly synchronizing automata are given. We will list these examples here, as they will be of use in Chapter 5. In order to keep our convention that, given a circular automaton $\mathcal{G}$, the letter a always represents the circular permutation, our representations of these examples differ from [10] because the actions of the letters a and b are switched. Also, we use the state set $Q = \{0, 1, \ldots, n-1\}$ instead of $\{1, 2, \ldots, n\}$. Finally, for some of the examples, namely the automata $\mathcal{F}_n, \mathcal{B}_n$ and $\mathcal{J}_n$ (which in [10] is denoted by $\mathcal{G}_n$), our representations are significantly different from those in [10], in order to show that they belong to a class of automata that will be considered in Chapter 5. In any case, we will exhibit the precise isomorphism between these three automata and their counterparts in [10].

The automaton $\mathcal{D}'_n$ [10], represented in Figure 2.9.8, is defined for each integer $n > 3$ as the automaton with state set $Q = \{0, 1, \ldots, n-1\}$, alphabet $A_{\mathcal{D}'_n} = \{a, b\}$ and transition

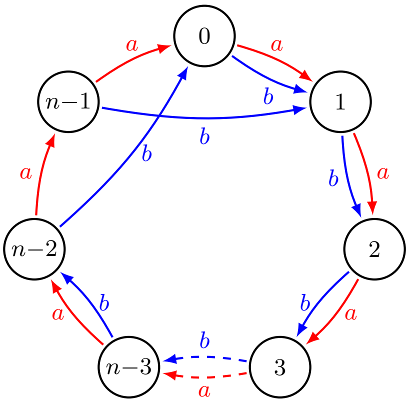

Figure 2.9.8: Automaton $\mathcal{D}'_n$

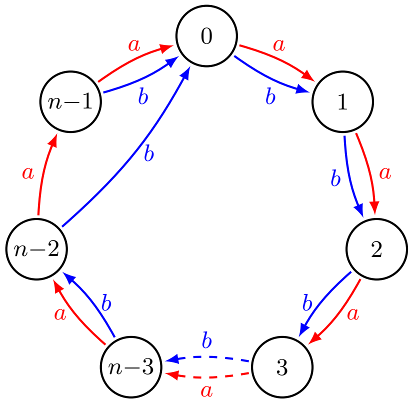

Figure 2.9.9: Wielandt automaton $\mathcal{W}_n$

function $\delta_{\mathcal{D}'_n}$ such that, given $q \in Q$,

$$\delta_{\mathcal{D}'_n}(q,a) = \underline{q+1}, \quad \delta_{\mathcal{D}'_n}(q,b) = \begin{cases} q+1 & \text{if } q \notin \{n-2, n-1\}, \\ \underline{q+2} & \text{if } q \in \{n-2, n-1\}. \end{cases}$$

Theorem 2.9.1 ([10])**.** *Given an integer $n > 3$, a shortest synchronizing word for $\mathcal{D}'_n$ is $(ba^{n-2})^{n-2}ba$, whose length is $n^2 - 3n + 4$.*

The Wielandt automaton $\mathcal{W}_n$ [10], represented in Figure 2.9.9, is defined for each integer $n > 2$ as the automaton with state set $Q = \{0, 1, \ldots, n-1\}$, alphabet $A_{\mathcal{W}_n} = \{a, b\}$ and transition function $\delta_{\mathcal{W}_n}$ such that, given $q \in Q$,

$$\delta_{\mathcal{W}_n}(q,a) = \underline{q+1}, \quad \delta_{\mathcal{W}_n}(q,b) = \begin{cases} q+1 & \text{if } q \notin \{n-2, n-1\}, \\ 0 & \text{if } q \in \{n-2, n-1\}. \end{cases}$$

Theorem 2.9.2 ([10])**.** *Given an integer $n > 2$, a shortest synchronizing word for $\mathcal{W}_n$ is $(ba^{n-2})^{n-2}b$, whose length is $n^2 - 3n + 3$.*

The automaton $\mathcal{F}_n$ [10], represented in Figure 2.9.10, is defined for each odd integer $n > 1$ as the automaton with state set $Q = \{0, 1, \ldots, n-1\}$, alphabet $A_{\mathcal{F}_n} = \{a, b\}$ and transition function $\delta_{\mathcal{F}_n}$ such that, given $q \in Q$,

$$\delta_{\mathcal{F}_n}(q,a) = \underline{q + \tfrac{n-1}{2}}, \quad \delta_{\mathcal{F}_n}(q,b) = \begin{cases} q & \text{if } q \neq 1, \\ 0 & \text{if } q = 1. \end{cases}$$

Theorem 2.9.3 ([10])**.** *Given an odd integer $n > 1$, a shortest synchronizing word for $\mathcal{F}_n$ is $(ba^{n-2})^{n-2}b$, whose length is $n^2 - 3n + 3$.*

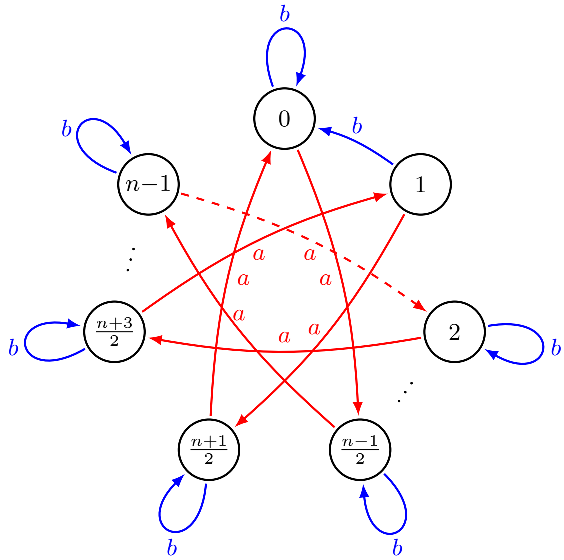

Figure 2.9.10: Automaton $\mathcal{F}_n$, n odd

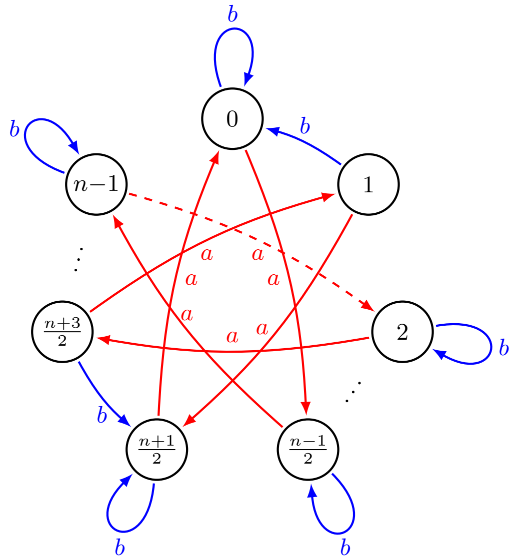

Figure 2.9.11: Automaton $\mathcal{B}_n$, n odd

The automaton $\mathcal{B}_n$ [11], represented in Figure 2.9.11, is defined for each odd integer $n > 3$ as the automaton with state set $Q = \{0, 1, \ldots, n-1\}$, alphabet $A_{\mathcal{B}_n} = \{a, b\}$ and transition function $\delta_{\mathcal{B}_n}$ such that, given $q \in Q$,

$$\delta_{\mathcal{B}_n}(q,a) = \underline{q + \tfrac{n-1}{2}}, \quad \delta_{\mathcal{B}_n}(q,b) = \begin{cases} q & \text{if } q \notin \{1, \frac{n+1}{2}\}, \\ q-1 & \text{if } q \in \{1, \frac{n+1}{2}\}. \end{cases}$$

Theorem 2.9.4 ([11]). *Given an odd integer $n > 3$, a shortest synchronizing word for $\mathcal{B}_n$ is $(ba^{n-2})^{\frac{n-3}{2}} ba^{n-3} (ba^{n-2})^{\frac{n-3}{2}} b$, whose length is $n^2 - 3n + 2$.*

As mentioned before, $\mathcal{F}_n$ and $\mathcal{B}_n$ have very different representations in [10] and [11]. Those representations, that we denote by $\bar{\mathcal{F}}_n = (\bar{Q}, \bar{A}, \bar{\delta}_{\bar{\mathcal{F}}_n})$ and $\bar{\mathcal{B}}_n = (\bar{Q}, \bar{A}, \bar{\delta}_{\bar{\mathcal{B}}_n})$, respectively, with $\bar{Q} = \{1, 2, \ldots, n\}$ and $\bar{A} = \{a, b\}$, can be found in Figures 2.9.12 and 2.9.13. Also, let $A = A_{\mathcal{F}_n} = A_{\mathcal{B}_n} = \{a, b\}$. The isomorphism that transforms $\mathcal{F}_n$ into $\bar{\mathcal{F}}_n$ and $\mathcal{B}_n$ into $\bar{\mathcal{B}}_n$ is given by the bijections

$$\begin{aligned} \xi : Q &\longrightarrow \bar{Q} \\ q &\longmapsto \underline{-2q+1} + 1 \end{aligned} \qquad \text{and} \qquad \begin{aligned} \psi : A &\longrightarrow \bar{A} \\ a &\longmapsto b \\ b &\longmapsto a. \end{aligned} \tag{2.9.1}$$

The automaton $\mathcal{D}''_n$ [10], represented in Figure 2.9.14, is defined for each integer $n > 3$ as the automaton with state set $Q = \{0, 1, \ldots, n-1\}$, alphabet $A_{\mathcal{D}''_n} = \{a, b\}$ and transition function $\delta_{\mathcal{D}''_n}$ such that, given $q \in Q$,

$$\delta_{\mathcal{D}''_n}(q,a) = \begin{cases} q+1 & \text{if } q \notin \{n-2, n-1\}, \\ 0 & \text{if } q \in \{n-2, n-1\}, \end{cases} \qquad \delta_{\mathcal{D}'_n}(q,b) = \begin{cases} q+1 & \text{if } q \neq n-1, \\ 1 & \text{if } q = n-1. \end{cases}$$

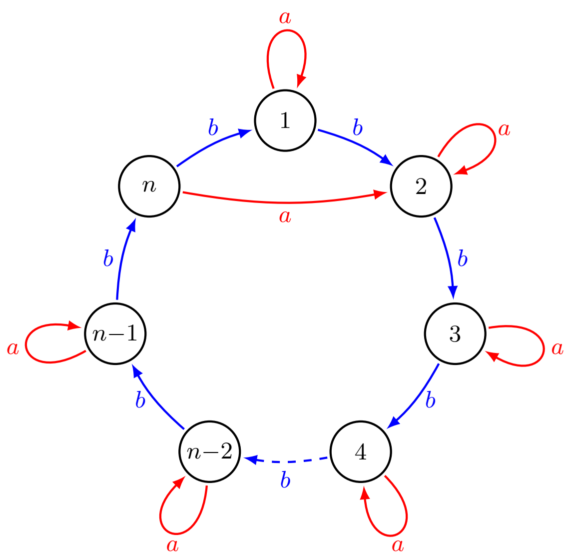

Figure 2.9.12: Automaton $\bar{\mathcal{F}}_n$, n odd

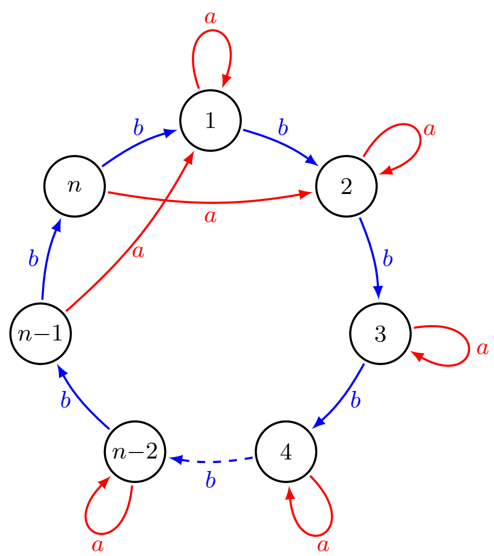

Figure 2.9.13: Automaton $\bar{\mathcal{B}}_n$, n odd

Theorem 2.9.5 ([10])**.** *Given an integer $n > 3$, a shortest synchronizing word for $\mathcal{D}''_n$ is $(ba^{n-1})^{n-3}ba$, whose length is $n^2 - 3n + 2$.*

The automaton $\mathcal{E}_n$ [10], represented in Figure 2.9.15, is defined for each integer $n > 2$ as the automaton with state set $Q = \{0, 1, \dots, n-1\}$, alphabet $A_{\mathcal{E}_n} = \{a, b\}$ and transition function $\delta_{\mathcal{E}_n}$ such that, given $q \in Q$,

$$\delta_{\mathcal{E}_n}(q, a) = \begin{cases} q + 1 & \text{if } q \notin \{n-2, n-1\}, \\ 0 & \text{if } q \in \{n-2, n-1\}, \end{cases} \quad \delta_{\mathcal{E}_n}(q, b) = \begin{cases} q & \text{if } q \notin \{n-2, n-1\}, \\ \underline{q+1} & \text{if } \in \{n-2, n-1\}. \end{cases}$$

Theorem 2.9.6 ([10])**.** *Given an integer $n > 2$, a shortest synchronizing word for $\mathcal{E}_n$ is $(b^2a^{n-2})^{n-3}a^2$, whose length is $n^2 - 3n + 2$.*

The automaton $\mathcal{J}_n$ [10], represented in Figure 2.9.16, is defined for each odd integer $n > 3$ as the automaton with state set $Q = \{0, 1, \dots, n-1\}$, alphabet $A_{\mathcal{J}_n} = \{a, b\}$ and transition function $\delta_{\mathcal{J}_n}$ such that, given $q \in Q$,

$$\delta_{\mathcal{J}_n}(q, a) = \underline{q + \tfrac{n-1}{2}}, \quad \delta_{\mathcal{J}_n}(q, b) = \begin{cases} \underline{q + \frac{n-1}{2}} & \text{if } q \notin \{1, 2\}, \\ q + \frac{n-3}{2} & \text{if } q \in \{1, 2\}. \end{cases}$$

Theorem 2.9.7 ([10])**.** *Given an odd integer $n > 1$, a shortest synchronizing word for $\mathcal{J}_n$ is $b^2(abab^{n-3})^{n-4}abab^2$, whose length is $n^2 - 4n + 7$.*

As mentioned before, the automaton $\mathcal{J}_n$ is isomorphic to the automaton $\mathcal{G}_n$ in [10], represented in Figure 2.9.17. If we make $\mathcal{G}_n = (\bar{Q}, \bar{A}, \bar{\delta})$ then the isomorphism given by the functions in (2.9.1) takes $\mathcal{J}_n$ to its representation $\mathcal{G}_n$ in [10].

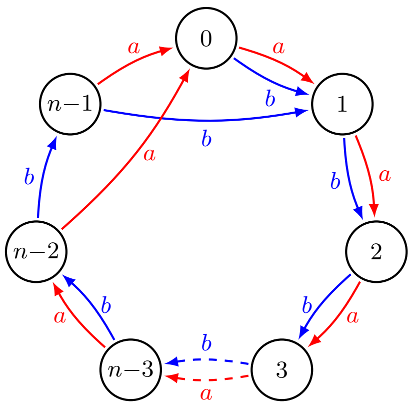

Figure 2.9.14: Automaton $\mathcal{D}''_n$

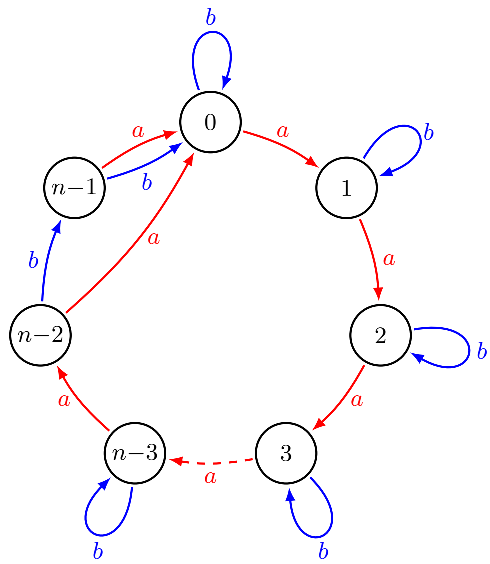

Figure 2.9.15: Automaton $\mathcal{E}_n$

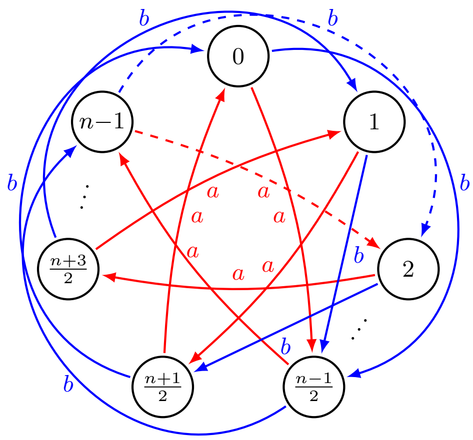

Figure 2.9.16: Automaton $\mathcal{J}_n$, n odd

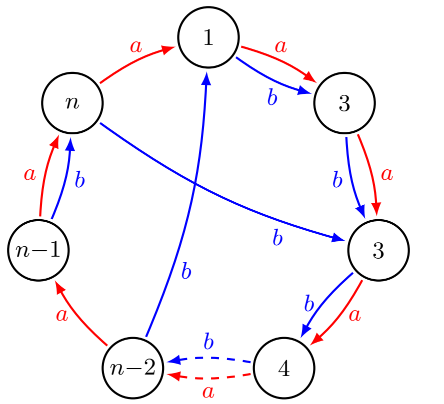

Figure 2.9.17: Automaton $\mathcal{G}_n$, n odd

The automaton $\mathcal{H}_n$ [10], represented in Figure 2.9.18, is defined for each integer $n > 3$ as the automaton with state set $Q = \{0, 1, \ldots, n-1\}$, alphabet $A_{\mathcal{H}_n} = \{a, b\}$ and transition function $\delta_{\mathcal{H}_n}$ such that, given $q \in Q$,

$$\delta_{\mathcal{H}_n}(q, a) = \begin{cases} q+1 & \text{if } q \notin \{n-2, n-1\}, \\ q+2 & \text{if } q \in \{n-2, n-1\}, \end{cases} \quad \delta_{\mathcal{H}_n}(q, b) = \begin{cases} q & \text{if } q \notin \{n-2, n-1\}, \\ n-1 & \text{if } q = n-2, \\ n-2 & \text{if } q = n-1. \end{cases}$$

Theorem 2.9.8 ([10]). *Given an integer $n > 2$, a shortest synchronizing word for $\mathcal{H}_n$ is $a(ba^{n-2})^{n-3}ba$, whose length is $n^2 - 4n + 6$.*

The automaton $\mathcal{I}_n$, represented in Figure 2.9.19, was found by the authors of [10] and is mentioned in that article, although not explicitly represented. It is defined for each

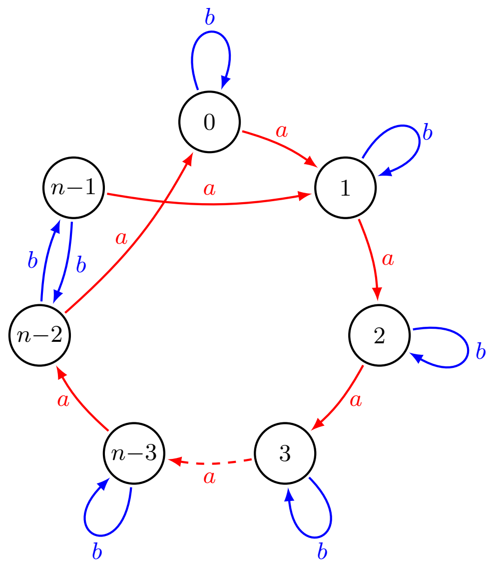

Figure 2.9.18: Automaton $\mathcal{H}_n$

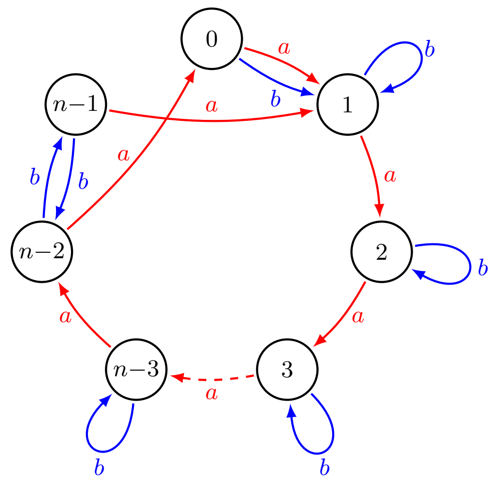

Figure 2.9.19: Automaton $\mathcal{I}_n$

integer $n > 3$ as the automaton with state set $Q = \{0, 1, \ldots, n-1\}$, alphabet $A_{\mathcal{I}_n} = \{a, b\}$ and transition function $\delta_{\mathcal{I}_n}$ such that, given $q \in Q$,

$$\delta_{\mathcal{I}_n}(q, a) = \begin{cases} q+1 & \text{if } q \notin \{n-2, n-1\}, \\ \underline{q+2} & \text{if } q \in \{n-2, n-1\}, \end{cases} \quad \delta_{\mathcal{I}_n}(q, b) = \begin{cases} q & \text{if } q \notin \{0, n-2, n-1\}, \\ q+1 & \text{if } q \in \{0, n-2\}, \\ n-2 & \text{if } q = n-1. \end{cases}$$

In [10] the authors state that the length of a shortest synchronizing word for $\mathcal{I}_n$ is $n^2 - 4n + 6$. It is easy to check that $aba(a^{n-2}b)^{n-3}$ is a synchronizing word for $\mathcal{I}_n$.

2.10 The road coloring problem

The digraph G with constant outdegree k is said to be *synchronizing* if there is a suitable labeling for which the resulting automaton $\mathcal{G} = (Q, A, \delta)$ is synchronizing. In [1] the authors conjectured that every strongly connected digraph G with n vertices, constant outdegree k, and such that the greatest common divisor of all its cycle lengths is 1, is synchronizing. They also proved that the condition on the greatest common divisor is necessary. This conjecture, known as the road coloring problem, remained open for many years. In 2009, Trahtman [44], using previous contributions from [15, 20, 23], proved the following result.

Theorem 2.10.1 ([44])**.** *The strongly connected digraph G with constant outdegree has a synchronizing labeling if and only if the greatest common divisor of the lengths of all* *cycles of* G *is* 1.

It is important to note that Trahtman's proof is constructive, that is, it actually provides a way to obtain a synchronizing labeling of the digraph G.

Chapter 3

Synchronizing digraphs

3.1 Preliminaries

We say that the digraph G with constant outdegree k is *totally synchronizing* if each of its suitable labelings leads to a synchronizing automaton. Given such a digraph, a *universal synchronizing word* is a word $w \in A^*$, such that w is a synchronizing word for every automaton that can be obtained from G, using the alphabet A with k letters.

Given a totally synchronizing digraph G with constant outdegree k and a word $w \in A^*$, where A represents an alphabet with k letters, we say that w has *rank* r with respect to G if r is the maximum rank of w for every automaton $\mathcal{G} = (Q, A, \delta)$, obtained from G by suitably labeling its arcs. The *rank* of the graph G is the minimum rank of all words in A^*; in other words, it is the maximum rank of all the automata obtained from G by suitably labeling its arcs.

We say that a digraph G with constant outdegree k is *monotonic* (respectively, *generalized monotonic*, *aperiodic*) if every automaton $\mathcal{G} = (Q, A, \delta)$ obtained from G by suitably labeling its arcs is monotonic (respectively, generalized monotonic, aperiodic). In this chapter, we solve the rank problem for monotonic digraphs. We also present a solution of that problem for generalized monotonic digraphs and aperiodic digraphs, by showing that those classes of digraphs are equal to the class of acyclic digraphs.

Given a digraph G with n vertices and constant outdegree k, denote by $\mathrm{len}(G)$ the length of a shortest universal synchronizing word for G. Naturally, $\mathrm{len}(G)$ will depend on the outdegree k. Thus, either we compute this length as a function of both n and k or, in order to make the problem more similar to the Černý Conjecture, we impose an appropriate restriction on k, so that the length of the shortest universal synchronizing word depends only on the number of vertices of the digraph.

A vital concept when trying to synchronize a digraph is that of reachability: to send all the vertices to the same vertex, the latter must be accessible from every vertex. Of course, that is not all that matters, but still we can assume that there is some vertex in the digraph such that all the arcs leaving that vertex have distinct destinations, without losing

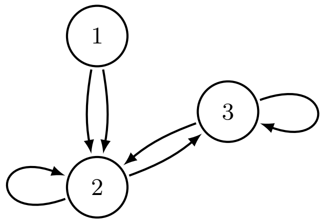

Figure 3.1.1: A digraph and its function-like diagram.

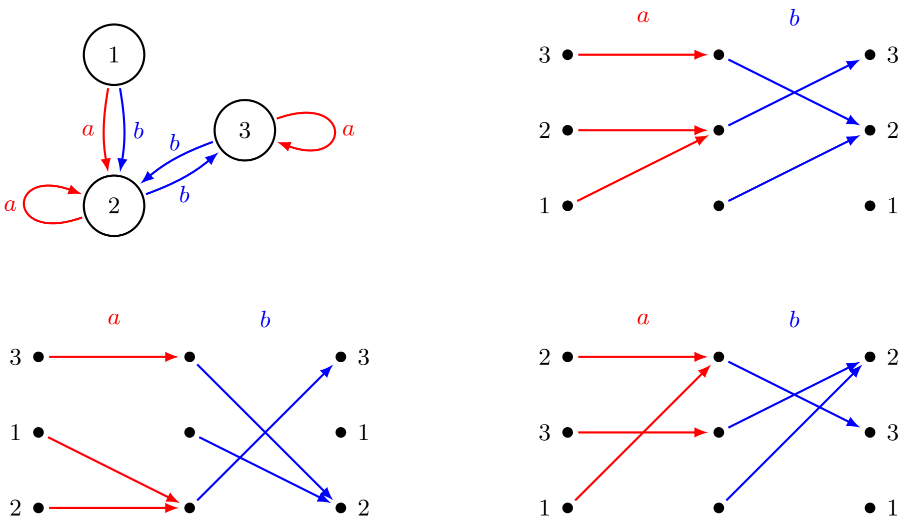

Figure 3.1.2: Function-like diagrams of an automaton obtained by suitably labeling the arcs from the digraph in Figure 3.1.1.

anything in terms of reachability. In the museum example given in the Introduction, this assumption is not a real restriction because there is not much to gain by making several paths share the same start point and also the same end point. Unless of course we are doing that to make the outdegree constant, but even in that case, there should be at least one intersection for which all the paths leaving it have different destinations. Given a digraph G with constant outdegree k, a vertex of G for which all k outgoing arcs have distinct destinations will be called *special*. We will denote the set of destinations of the arcs with origin in the vertex p by $N^+(p)$. Thus, for a special vertex p, we have $|N^+(p)| = k$.

As is shown in Figure 3.1.1, to represent digraphs we will use function-like diagrams, in which we have two columns, each one with a copy of the vertices represented in the same order, and arrows going from the first to the second column. An arrow connecting i on the left column to j on the right column indicates that there is a directed arc in the digraph going from the vertex i to the vertex j. We place labels on top of certain arcs to represent their multiplicity and arcs without label have multiplicity 1. To represent *simple paths*, that is, paths that do not include loops, we use dashed arrows. We will denote such paths using double parentheses, thus if we write $(\!(p,s)\!)$, we are referring to a simple path that starts in p and finishes in s.

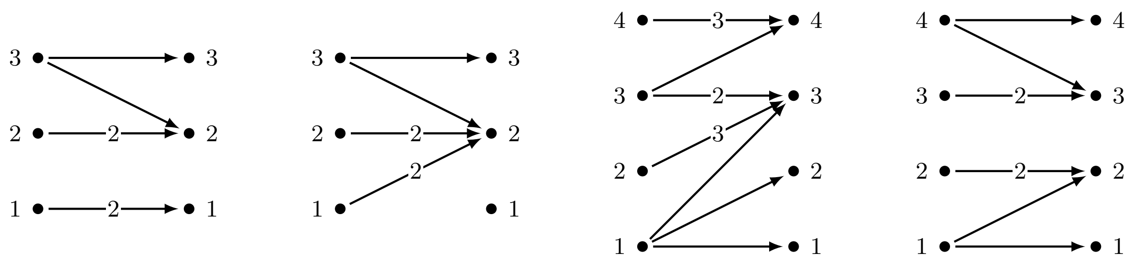

Figure 3.1.3: Examples of monotonic digraphs.

When considering automata, the function-like diagram will be drawn by dividing the arcs between several columns, according to their label, which will be indicated at the top of its column. This way, a digraph is monotonic if and only if for every automaton resulting from it, there is an order on the state set, such that there are no crosses between arrows in the same column of the function-like diagram. As we can see in Figure 3.1.2, the digraph from Figure 3.1.1 is not monotonic.

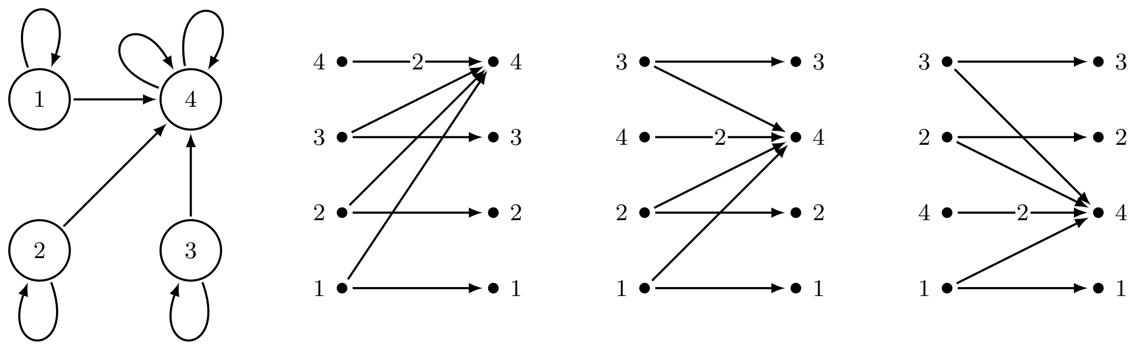

Figure 3.1.4: Digraph G'

If for a digraph G with constant outdegree, there is an order on its vertex set such that there are no crosses between the arrows in its function-like diagram, then G is monotonic. Examples of such monotonic digraphs can be seen in Figure 3.1.3. The converse statement is false; a counterexample for it was found by an anonymous referee of a submission of this work and can be seen in Figure 3.1.4. The digraph G' represented is monotonic, yet for every order considered on the vertex set $\{1,2,3,4\}$ there is some cross between the arrows of the function-like diagram. Indeed, since every permutation of the subset of vertices $\{1,2,3\}$ is an isomorphism over G it is enough to consider the position of the

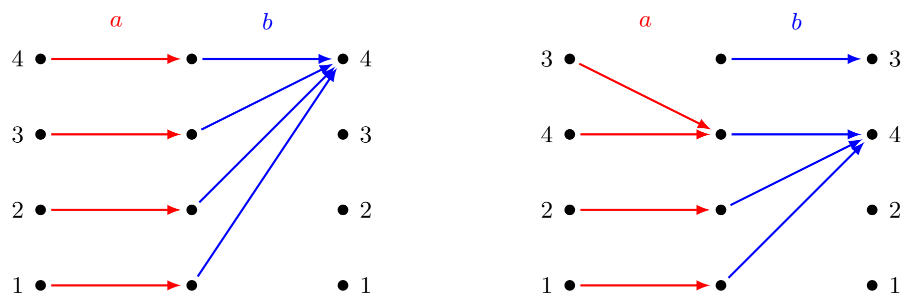

Figure 3.1.5: Automata obtained from the digraph G' represented in Figure 3.1.4.

vertex 4 in the linear order, and the function-like diagrams represented in Figure 3.1.4 show that there is always some cross. The same argument can be used to show that up to isomorphism there are only two distinct automata that can be obtained from G'. Function-like diagrams of these automata are represented in Figure 3.1.5, showing that they are both monotonic.

3.2 Strongly connected digraphs and digraphs with a sink

In this section, we provide an adaptation of Theorem 2.4.2 for digraphs. Given a digraph G and a subgraph H of G, the *quotient* G/H is the graph which is obtained from G by identifying all the vertices in H.In case H is a strongly connected special subgraph of G, the quotient G/H is called a *special quotient*.

Lemma 3.2.1. *Let G be a totally synchronizing digraph with constant outdegree and let $\mathcal{G}_1 = (Q, A, \delta_{\mathcal{G}_1})$ and $\mathcal{G}_2 = (Q, A, \delta_{\mathcal{G}_2})$ be two automata obtained by suitably labeling the edges in G. For $\mathcal{G} \in \{\mathcal{G}_1, \mathcal{G}_2\}$ denote by $S_{\mathcal{G}}$ the set of vertices of G to which $\mathcal{G}$ can be synchronized. Then $S_{\mathcal{G}_1} = S_{\mathcal{G}_2}$.*

Proof. It is enough to prove that $S_{\mathcal{G}_1} \subseteq S_{\mathcal{G}_2}$, since the reverse inclusion can be established in the same way. Consider a state $s \in S_{\mathcal{G}_1}$, let $w_{\mathcal{G}_2}$ be a synchronizing word for the automaton $\mathcal{G}_2$ and let $t \in S_{\mathcal{G}_2}$ be such that $\delta_{\mathcal{G}_2}(Q, w_{\mathcal{G}_2}) = t$. Since $\mathcal{G}_1$ can be synchronized in the state s, there is a path in G from t to s, hence there is a word w_s^t such that $\delta_{\mathcal{G}_2}(t, w_s^t) = s$. This implies that $\delta_{\mathcal{G}_2}(Q, w_{\mathcal{G}_2} w_s^t) = \delta_{\mathcal{G}_2}(t, w_s^t) = s$, hence $\mathcal{G}_2$ can be synchronized to the state s and $s \in S_{\mathcal{G}_2}$. $\square$

Theorem 3.2.2. *Let $\mathbf{C}$ be a class of totally synchronizing digraphs closed for special subgraphs and special quotients. Denote by $\mathbf{C}_n$ the class of all digraphs in $\mathbf{C}$ with n*

vertices. Consider a function $f : \mathbb{Z}^+ \longrightarrow \mathbb{N}$ *such that, for all integers* n, m *with* $n \geq m \geq 1$,

$$f(n) \geq f(n - m + 1) + f(m).$$

Suppose that for every positive integer n *and for every digraph* H *in* $\mathbf{C}_n$ *which either is strongly connected or has a sink,* $\mathrm{len}(H) \leq f(n)$*. Then, for every digraph* G *in* $\mathbf{C}_n$*,* $\mathrm{len}(G) \leq f(n)$*.*

Proof. Let G be a totally synchronizing digraph in $\mathbf{C}_n$. According to Lemma 3.2.1, we can consider the set S of all vertices in G to which each automaton obtained from G can be synchronized. For every vertex q in Q, if there is some vertex s in S such that the edge (s, q) belongs to G, then $q \in S$, because after synchronizing any automaton $\mathcal{G}$ obtained from G to the state s we would only have to use the label of (s, q) in $\mathcal{G}$ to synchronize it to q. Hence, we can consider the special subgraph H of G generated by S, that is, the special subgraph whose vertex set is S and whose arcs are the ones with origin (and, according to what we saw, destination) in S.

By definition of S, we know that for every $s, p \in S$, there is a path in G from s to p, hence H is strongly connected. But $\mathbf{C}$ is closed under taking special subgraphs and special quotients, therefore, $H, G/H \in \mathbf{C}$. Actually, if $|S| = m$, we have $H \in \mathbf{C}_m$ and $G/H \in \mathbf{C}_{n-m+1}$.

Since H is strongly connected and totally synchronizing, it has a universal synchronizing word of length $f(m)$. As for G/H, it has a sink, the class of vertices of G that belong to S, and it is totally synchronizing, therefore it has a universal synchronizing word of size $f(n - m + 1)$.

If we use a universal synchronizing word for G/H in G, its image set is a subset of S, hence, composing that word with a universal synchronizing word for H, we obtain a universal synchronizing word of G. Therefore, there is a universal synchronizing word for G of size $f(n - m + 1) + f(m) \leq f(n)$. □

3.3 Generalized monotonic, aperiodic and acyclic digraphs

In this section, we establish relations between the classes of digraphs that are being considered.

Lemma 3.3.1. *Every monotonic digraph is acyclic.*

Proof. Let G be a monotonic digraph with n vertices ($n > 1$). If G is not acyclic, then it has some nontrivial cycle. Let C be such a cycle of minimum length (so that it is simple) and suppose that it has the form $t_1 \longrightarrow t_2 \longrightarrow \cdots \longrightarrow t_m \longrightarrow t_1$, with $m > 1$. Clearly, there is a suitable transition function δ, such that every arc in C has the same label a. By the definition of monotonic digraph, we know that $t_i \leq t_{i+1}$ implies $\delta(t_i, a) \leq \delta(t_{i+1}, a)$, hence $t_i \leq t_{i+1}$ implies $t_{i+1} \leq t_{i+2}$, for $i \in \{1, 2, \ldots, m-2\}$, and equally $t_{m-1} \leq t_m$ implies $t_m \leq t_1$. This way, if $t_1 \leq t_2$ then we have $t_1 \leq t_2 \leq t_3 \leq \cdots \leq t_{m-1} \leq t_m \leq t_1$, so $t_1 = t_2 = \cdots = t_m$, which is absurd. A similar argument can be used for the case $t_1 \geq t_2$. Therefore G is acyclic. □

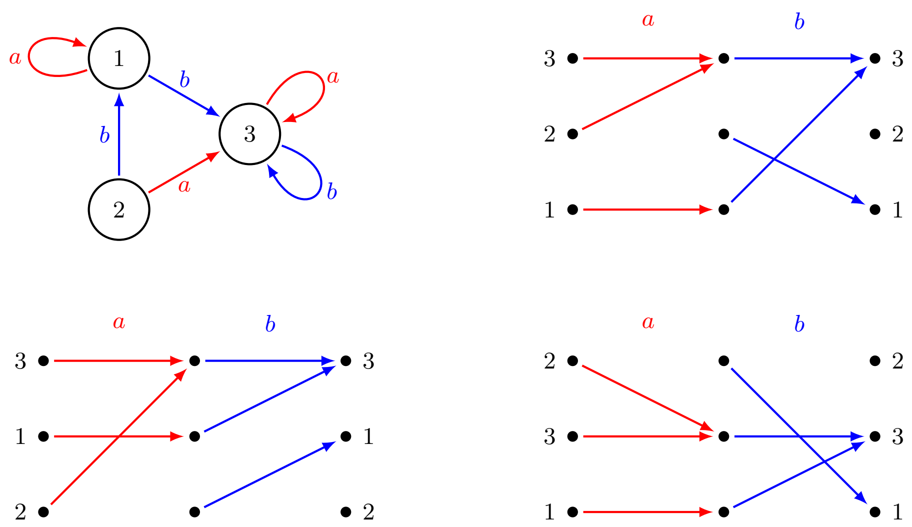

Figure 3.3.1: Automaton $\mathcal{G}''$

A counterexample to the reverse implication of Lemma 3.3.1 can be found in Figure 3.3.1. The automaton $\mathcal{G}''$ represented there is not monotonic even though its underlying digraph is acyclic.

Proposition 3.3.2. *For a finite digraph G with constant outdegree, the following conditions are equivalent:*

1. *G is aperiodic;*
2. *G is generalized monotonic;*
3. *G is acyclic.*

Proof. (1) $\Rightarrow$ (3). We prove the contrapositive. Suppose that G has some nontrivial directed cycle. Let C be such a cycle of minimum length (so that it is simple). Consider a suitable labeling of the arcs in G such that every arc in C has the same label $a \in A$. Let $\mathcal{G}$ be the resulting automaton. If $m > 1$ is the length of C, then a acts as a permutation of order m on the vertices of C, thus there can be no $l \in \mathbb{N}$ such that $a^l = a^{l+1}$ in the transition semigroup of $\mathcal{G}$, which implies that $\mathcal{G}$ and G are not aperiodic.

(3) $\Rightarrow$ (1). We establish the contrapositive. Suppose that G is not aperiodic, then some automaton $\mathcal{G} = (Q, A, \delta)$ obtained from G by suitably labeling its arcs is not aperiodic, and we may choose that automaton in such a way that there is some letter $a \in A$ such that $a^l \neq a^{l+1}$ for every $l \in \mathbb{N}$. On the other hand, since Q is finite, there are $i, j \in \mathbb{N}$ such that $j > i$ and $a^i = a^j$. Given $q \in Q$, let $p = \delta(q, a^i) = \delta(q, a^j)$. We have $\delta(p, a^{j-i}) = \delta(\delta(q, a^i), a^{j-i}) = \delta(q, a^i a^{j-i}) = \delta(q, a^j) = p$, that is, a^{j-i} labels a directed cycle containing p. But this means that a^{j-i} labels some nontrivial directed cycle in $\mathcal{G}$, because if all such cycles involved only one vertex, we would have $\delta(p, a^i) = \delta(p, a^{i+1}) = \cdots = \delta(p, a^j)$ for every $p \in Q$, which is absurd, since $a^l \neq a^{l+1}$ for every $l \in \mathbb{N}$. Thus, G is not acyclic.

(2) $\Rightarrow$ (3). Once more, we prove the contrapositive. Suppose that C is a nontrivial directed cycle of G with minimum length $m > 1$. Consider a suitable labeling of the arcs in G such that every arc in C has the same label $a \in A$ and let $\mathcal{G} = (Q, A, \delta)$ be the resulting automaton. For every congruence ρ on Q, if $(p, q) \in \rho$ with $p \neq q$ states in C, then either every vertex in C is in $[p]_\rho$ or the number of vertices of C that belong to $[p]_\rho$ is a proper divisor $d \neq 1$ of m. This way, when trying to build a chain of congruences that makes $\mathcal{G}$ generalized monotonic, either we collapse the entire cycle C at once or we do it in several steps. In the latter case, we start by joining d_1 vertices in the same class, where $d_1 \neq 1$ is a proper divisor of m, and obtain in the quotient automaton a cycle with m/d_1 elements. After i steps, we collapse d_{i+1} vertices of the remaining cycle, where $d_{i+1} \neq 1$ is a divisor of $m/(d_1 d_2 \ldots d_i)$ and obtain in the quotient automaton a cycle with $m/(d_1 \ldots d_i d_{i+1})$ elements. But at some point, since m is finite a congruence ρ_{j+1} will collapse an entire nontrivial cycle, that is, $d_{j+1} = m/(d_1 d_2 \ldots d_j) \neq 1$.

Now, let $\mathcal{H}$ be the subautomaton of $\mathcal{G}/\rho_j$ consisting only of the nontrivial cycle that is collapsed by ρ_{j+1}. Note that it is indeed a subautomaton since its states are those of the cycle and it has the single letter a which labels the arcs in the cycle. If $\mathcal{G}/\rho_j$ is ρ_{j+1}/ρ_j-monotonic, then $\mathcal{H}$ is monotonic and its underlying digraph H is also monotonic (it has only one possible suitable labeling). But this is absurd, because Lemma 3.3.1 establishes that every monotonic digraph is acyclic. Hence, $\mathcal{G}/\rho_j$ is not ρ_{j+1}/ρ_j-monotonic and G is not generalized monotonic.

(3) $\Rightarrow$ (2). Suppose that G is acyclic and let Q be the set of vertices of G. If G has no arcs, then it is obviously monotonic, hence we may assume that G has constant outdegree greater than 0. The digraph G must have at least one fixed point, since it is finite and acyclic. We define inductively a sequence of subsets of Q as follows. Let $F_1 \subseteq Q$ be the

set of fixed points of G. If $F_1 = Q$, then G is obviously generalized monotonic, actually it is monotonic. Suppose that $F_1 \subsetneq Q$, that we have already defined the sets $F_1 \subsetneq F_2 \subsetneq \cdots \subsetneq F_{i-1} \subsetneq Q$ and they are such that $|F_{j+1} - F_j| = 1$, for every $j \in \{1, 2, \ldots, i-1\}$. Since G is finite and acyclic, there is some vertex in $G - F_{i-1}$ such that all its outgoing arcs end in F_{i-1}. Let p be such a vertex and let $F_i = F_{i-1} \cup \{p\}$. Since Q is finite and the sequence $F_1, F_2, \ldots, F_{i-1}, F_i, \ldots$ is strictly increasing, there must be some l such that $F_l = Q$.

Define for every $j \in \{1, 2, \ldots, l\}$ the equivalence relation ρ_j on Q such that for every $q \in Q$,

$$[q]_{\rho_j} = \begin{cases} F_j & \text{if } q \in F_j, \\ \{q\} & \text{if } q \notin F_j. \end{cases}$$

Given an automaton $\mathcal{G}$ obtained from G by suitably labeling its arcs, ρ_j is a congruence on $\mathcal{G}$, because the only ρ_j-class that is not a singleton is an invariant set. If we consider the equality relation ρ_0, we have $\rho_0 \subsetneq \rho_1 \subsetneq \cdots \subsetneq \rho_l$, with ρ_l the universal relation on Q. Since the only ρ_1-class that is not a singleton is the set of fixed points of Q, $\mathcal{G}$ is ρ_1-monotonic. Also, because $|F_{j+1} - F_j| = 1$, $\mathcal{G}/\rho_j$ is ρ_{j+1}/ρ_j-monotonic for every $j \in \{1, 2, \ldots, l\}$. We conclude that $\mathcal{G}$ is generalized monotonic of level l and, since $\mathcal{G}$ was any automaton obtained from G by suitably labeling its arcs, G is generalized monotonic. □

Using Proposition 3.3.2, in order to solve the rank problem for aperiodic digraphs and generalized monotonic digraphs, all we have to do is solve it for acyclic digraphs, which is what is presented in the next section.

3.4 Synchronizing acyclic digraphs

In this section, we start by providing an alternative characterization of acyclic digraphs of a given rank r, thus obtaining a similar characterization of totally synchronizing acyclic digraphs. Then we establish some results that ultimately solve the rank problem for this class of digraphs.

Proposition 3.4.1. *Let G be an acyclic digraph with n vertices ($n > 1$) and constant outdegree k ($1 \leq k \leq n$). Then the following conditions are equivalent:*

1. *every automaton $\mathcal{G} = (Q, A, \delta)$ obtained from G by suitably labeling its arcs has rank r;*
2. *G has rank r;*
3. *G has precisely r fixed points.*

Proof. (1) $\Rightarrow$ (2). Obvious from the definitions.

(2) $\Rightarrow$ (3). Consider a suitable labeling of the arcs in G such that the resulting automaton $\mathcal{G} = (Q, A, \delta)$ has rank r. Let $w \in A^*$ be a word of rank r with respect to $\mathcal{G}$ and let $s \in \delta(Q, w)$. If $\delta(s, a) = t$ for $t \in Q$ and $a \in A$, then $\delta(s, aw) = \delta(t, w) \in \delta(Q, w)$, hence aw acts as a permutation on the elements of $\delta(Q, w)$. This means that aw must be the identity, otherwise it would label one or more directed cycles involving distinct vertices of G. But if aw is the identity, then it labels a directed cycle passing through s and t, thus $s = t$. Hence, s is fixed by every letter $a \in A$, which means that it is a fixed point of G.

On the other hand, if s is a fixed point of G, then it is necessarily fixed by every letter in A and therefore it is fixed by the word w, which means that it belongs to $\delta(Q, w)$.

(3) $\Rightarrow$ (1). Assume $\mathcal{G} = (Q, A, \delta)$ is an automaton resulting from a suitable labeling of the arcs in G. We already know from the proof of the previous implication that for a word w of minimum rank with respect to $\mathcal{G}$, the r fixed points from G belong to $\delta(Q, w)$. We also know that any other element in this set would be a fixed point for G, hence w has rank r. $\square$

Corollary 3.4.2. *Let G be an acyclic digraph with n vertices ($n > 1$) and constant outdegree k ($1 \leq k \leq n$). Then the following conditions are equivalent:*

1. *G is totally synchronizing;*
2. *G is synchronizing;*
3. *G has a sink.*

The next result contains the key argument for our solution of the rank problem for acyclic and monotonic digraphs.

Lemma 3.4.3. *Let G be an acyclic digraph with n vertices ($n > 1$) and constant outdegree k ($1 \leq k \leq n$). Let us use the alphabet $A = \{a_1, a_2, \ldots, a_k\}$ to form suitable labelings of the arcs in G.*

For a nonnegative integer l, consider a set $P = \{p_1, p_2, \ldots, p_l\}$ of vertices of G and positive integers $\alpha_1, \alpha_2, \ldots, \alpha_l \leq k$ such that, for every suitable transition function δ, and every word $w_i \in A^*$ with length α_i whose letters are all distinct, $\delta(p_i, w_i) \neq p_i$. Let α and β be nonnegative integers such that $\alpha_1 + \alpha_2 + \cdots + \alpha_l = \beta k + \alpha$ and $\alpha < k$.

Suppose that, given any vertex q of G, if s is a fixed point to which q is connected by a path, the simple path $(\!(q, s)\!)$ contains at most m distinct vertices that do not belong to $P \cup \{q\}$. Then $\delta(q, (a_1 a_2 \ldots a_k)^{m+\beta} a_1 a_2 \ldots a_\alpha)$ is a fixed point, for every suitable transition function δ.

Proof. Let δ be a suitable transition function. Since G is acyclic, given a vertex t and a word v with k distinct letters, either $\delta(t, v) \neq t$ or t is a fixed point.

Given any suitable labeling of the arcs in G, if we start in q and follow some word, after each block with k distinct letters either we reach a new vertex (in the sense that we have not passed it before) or we are already in a fixed point. But if at some point we reach the vertex p_i, the next block of α_i distinct letters will take us to a new vertex. Since G is acyclic, even if some path from q to s contains all the vertices in P, in order to go from q to a fixed point, we need at most m blocks of k distinct letters plus the blocks with α_i distinct letters for each $i = 1, 2, \ldots, l$. Hence, any word with $km+\alpha_1+\alpha_2+\cdots+\alpha_l = k(m+\beta)+\alpha$ letters, such that independently from where we start reading it, the next k letters of the word (if they exist) are all distinct, must necessarily take the vertex q to a fixed point. Since the word $(a_1a_2\ldots a_k)^{m+\beta}a_1a_2\ldots a_\alpha$ is in these conditions, we obtain the desired result. $\square$

The following theorem provides a word that has minimum rank for every acyclic digraph with n vertices, constant outdegree k, rank r and at least one special vertex.

Theorem 3.4.4. *Let G be an acyclic digraph with n vertices ($n > 1$) and constant outdegree k ($1 \leq k \leq n$). Assume that G has at least one special vertex and let us use the alphabet $A = \{a_1, a_2, \ldots, a_k\}$ to form suitable labelings of the arcs in G. If G has rank r, then*

$$ {}^{n}_{k}\bar{w}_r = \begin{cases} (a_1a_2\ldots a_k)^{n-r-1}a_1a_2 & \text{if } k > 1, \\ a_1^{n-r} & \text{if } k = 1 \end{cases} $$

is a minimum rank word for G.

Proof. Let δ be a suitable transition function for G using the letters in A. Let p be a special vertex of G. If $k > 1$, then given any two distinct letters x_i and x_j, we necessarily have $\delta(p, x_ix_j) \neq p$, because for each suitable labeling considered, only one letter may fix p.

According to Lemma 3.4.1, there are r fixed points in G. Hence, given a vertex q and any fixed point s, the simple path $(\!(q, s)\!)$ contains at most $n-r-1$ vertices that do not belong to $\{p, q\}$. For $k > 2$, using Lemma 3.4.3 with $l = 1, P = \{p\}, \alpha_1 = 2 = \alpha, \beta = 0$ and $m = n-r-1$ we conclude that $\delta(q, (a_1a_2\ldots a_k)^{n-r-1}a_1a_2)$ is a fixed point. Since this is true for any vertex q, the word ${}^{n}_{k}\bar{w}_r$ has rank r.

For $k \in \{1, 2\}$, we may use Lemma 3.4.3 with $l = \beta = \alpha = 0$ and $m = n-r$ to conclude that $\delta(q, {}^{n}_{k}\bar{w}_r)$ is a fixed point, for any vertex q, hence the word ${}^{n}_{k}\bar{w}_r$ has rank r. $\square$

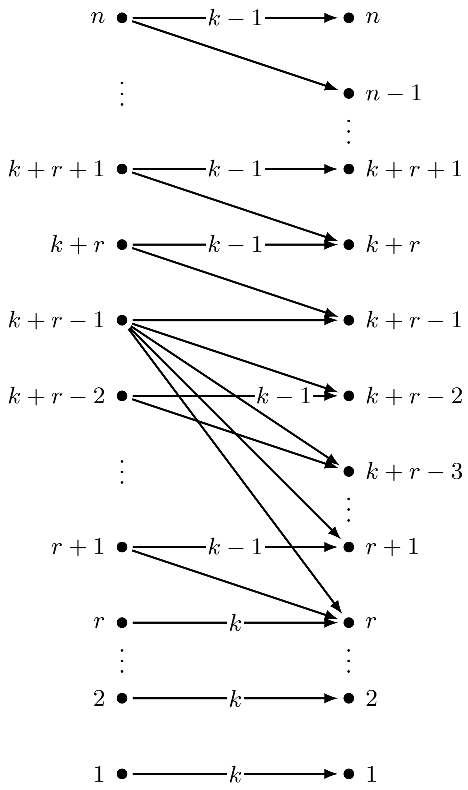

Figure 3.4.1: Digraph ${}^n_k\bar{G}_r$

For each $n > 1$ and $1 \le k \le n$, consider the acyclic digraph ${}^n_k\bar{G}_r$ represented by the diagram in Figure 3.4.1. The word ${}^n_k\bar{w}_r$ in Theorem 3.4.4 is a shortest minimum rank word for this digraph. Indeed, consider for each $i \in \{1, 2, \dots, k\}$, a suitable labeling of ${}^n_k\bar{G}_r$ with transition function δ_i, such that for $j \in \{k + r, n\}$, $\delta_i(j, x_i) = j - 1$ and $\delta_i(j, x_l) = j$ when $l \ne i$. Since for every word $\bar{w}$, $\delta_i(Q, \bar{w}) \subseteq \{1, 2, \dots, k\}$ implies that there are at least $n - k - r + 1$ occurrences of x_i in $\bar{w}$, we conclude that a word that takes all the vertices in ${}^n_k\bar{G}_r$ to $\{r, r + 1, \dots, k + r - 1\}$, independently of the suitable labeling considered, must have at least $n-k-r+1$ occurrences of each letter in A. After this, we need 2 distinct letters to make sure that the vertex $k + r - 1$ goes to some vertex in the subset $\{r, r + 1, \dots, k - r - 2\}$, since the first letter will fix k in some labelings. Finally, using the same argument as above, we need a word with $k - 2$ occurrences of each letter in A to take $\{r + 1, r + 2, \dots, k + r - 2\}$ to $\{r\}$ independently of the labeling.

The next result is a direct consequence of Theorem 3.4.4 and provides a totally synchronizing word for every totally synchronizing acyclic digraph with n vertices and constant outdegree k that has a special vertex.

Corollary 3.4.5. *Let G be an acyclic digraph with n vertices ($n > 1$) and constant outdegree k ($1 \le k \le n$). Assume that there is some special vertex in G. If G is totally* *synchronizing, then*

$$ {}^n_k\bar{w} = \begin{cases} (a_1a_2\dots a_k)^{n-2}a_1a_2 & \text{if } k > 1, \\ a_1^{n-1} & \text{if } k = 1 \end{cases} $$

is a universal synchronizing word for G.

From the above discussion concerning the digraph ${}^n_k\bar{G}_r$, represented in Figure 3.4.1, it is obvious that for $r = 1$ the word ${}^n_k\bar{w}$ is a shortest universal synchronizing word for this digraph.

Finally we are able to establish a bound on the length of shortest minimum rank words for acyclic digraphs with a special vertex, based on the number of vertices and the rank.

Corollary 3.4.6. *Let G be an acyclic digraph with n vertices ($n > 1$) and constant outdegree. Assume that there is some special vertex in G. If G has rank $r \geq 1$, then G has a rank r word of length $n(n-r-1)+2$ and this bound is tight.*

Proof. Let k ($1 \leq k \leq n$) be the constant outdegree of G. We know that G has a rank r word of length $k(n-r-1) + \min\{2, k\}$ and that this bound is tight, according to Theorem 3.4.4 and Figure 3.4.1, respectively. Hence to finish the proof, it is enough to observe that $k(n-r-1) + \min\{2, k\}$ is maximum and equal to $n(n-r-1)+2$ when $k = n$. □

From Corollary 3.4.6 we easily obtain a bound on the length of shortest totally synchronizing words for totally synchronizing acyclic digraphs with a special vertex, based on the number of vertices.

Corollary 3.4.7. *Let G be an acyclic digraph with n vertices ($n > 1$) and constant outdegree. Assume that there is some special vertex in G. If G is totally synchronizing, then it has a universal synchronizing word of length $n(n-2)+2$ and this bound is tight.*

Note that in the museum example considered earlier in this chapter it makes sense to assume that the digraph is acyclic, since people usually want to visit each attraction a single time, as long as the exit and the entrance are not the same. Moreover, if the exit is considered to be a sink in that digraph, then we may construct universal synchronizing words which would lead all visitors to the exit. Although it is not guaranteed that following such set of directions would make a visitor see all the attractions, it would still be useful as a way for lost people to find the exit. It could also be used to direct everyone to the exit at closing time.

The following result can be obtained from the proof of Theorem 3.4.4 and shows what happens in the general case, where we have an acyclic digraph with outdegree k and we do not know if there is some special vertex.

Corollary 3.4.8. *Let G be an acyclic digraph with n vertices ($n > 1$), constant outdegree k and rank r. If we consider the alphabet $A = \{a_1, a_2, \ldots, a_k\}$, then*

$$ {}^{n}_{k}\hat{w}_r = (a_1 a_2 \ldots a_k)^{n-r}, $$

is a rank r word for G.

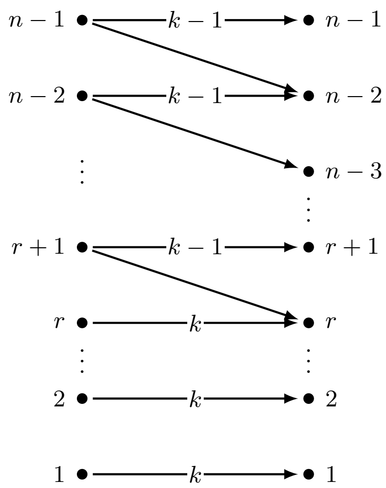

Figure 3.4.2: Digraph ${}^{n}_{k}\dot{G}_r$

For the digraph ${}^{n}_{k}\dot{G}_r$ in Figure 3.4.2 the word ${}^{n}_{k}\hat{w}_r$ from Corollary 3.4.8 is a shortest minimum rank word.

3.5 Synchronizing monotonic digraphs

We begin this section with a few technical results that will be necessary near the end, where we solve the rank problem for monotonic digraphs with constant outdegree.

We will often use the following result concerning a graph with a simple path such that all its arcs have the same label.

Lemma 3.5.1. *Let G be a monotonic digraph with n vertices ($n > 1$). Suppose that p and q are vertices and that there is a simple path from p to q (respectively, q to p) in G. Consider a suitable labeling of the arcs in G, such that all the arcs in that path have the same label, and a perfect order for that labeling. Assume that $p < q$ for that order. Then every vertex t in the path from p to q (respectively, q to p) is such that $p \leq t \leq q$.*

Proof. Let $((p,q))$ be the simple path from p to q. We only consider this case, because the other one, in which there is a simple path from q to p, is then obtained by applying this one to the reverse order.

Aiming for a contradiction, assume that there is a vertex t in $((p,q))$ such that $t < p$. Let $\bar{t} \in ((p,q))$ be the first vertex with this property and $\bar{p}$ be the vertex immediately before $\bar{t}$ in $((p,q))$. Let $\bar{q}$ be the first vertex in $((p,q))$ after $\bar{t}$ such that $\bar{q} > \bar{t}$ (it exists because $q > \bar{t}$) and let $\bar{s}$ be the vertex immediately before $\bar{q}$ in the path $((p,q))$. This way, we have $\bar{s} \leq \bar{t} < p \leq \bar{p}$ and $\bar{q} > \bar{t}$, which means there is a cross between the arcs $(\bar{p},\bar{t})$ and $(\bar{s},\bar{q})$. But this is absurd because they have the same label and we considered a perfect order for this labeling.

If we assume that $t > q$ for some vertex t in $((p,q))$, then similar arguments lead to a contradiction. □

The next lemma establishes conditions that we will need to apply Lemma 3.4.3 in order to solve the rank problem for monotonic digraphs with a special vertex. It concerns the case where the special vertex is connected to a single fixed point. We will need the notion of monotonic digraph with not necessarily constant outdegree. The idea is that given a suitable labeling of the such a digraph, the incomplete (in the sense that the action of a letter on a state may not be defined) automaton obtained is monotonic, that is, given states p, q and a letter a, if $\delta(p,a)$ and $\delta(q,a)$ are both defined and $p \leq q$, then $\delta(p,a) \leq \delta(q,a)$.

Lemma 3.5.2. *Let G be a monotonic digraph with n vertices ($n > 1$) and not necessarily constant outdegree. Suppose that the outdegree of each vertex is at least 1. Let p be a special vertex of G. Suppose that there is a single fixed point $\bar{s}$ in G such that p is connected to it by a path. Then, there can only be loops at most in one vertex of $N^+(p) - \{p\}$.*

Proof. We may assume that $|N^+(p)| > 1$, because the result is trivial otherwise. Aiming towards a contradiction, suppose that $t, \bar{t} \in N^+(p) - \{p\}$ are such that the arcs (t,t) and $(\bar{t},\bar{t})$ are in G. Consider a suitable labeling of the arcs in G such that $(p,t), (\bar{t},\bar{t})$ have label $a \in A$ and $(p,\bar{t}), (t,t)$ have label $b \in A - \{a\}$. There are two possibilities:

1. we have a simple path in G from one of the vertices in $N^+(p)$ with loops to another and we assume, without loss of generality, that that path is $((t,\bar{t}))$;
2. there are no paths of the forms $((t,\bar{t}))$, $((\bar{t},t))$.

In Case 1, consider the label a in every arc of the simple path $((t,\bar{t}))$ (that path cannot contain p, since G is acyclic). So, we have the diagram in Figure 3.5.1 (recall that we use dashed arrows to represent simple paths). Assuming that $p > t$, and using Lemma 3.5.1,

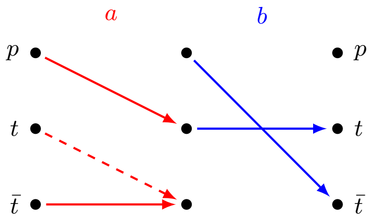

Figure 3.5.1

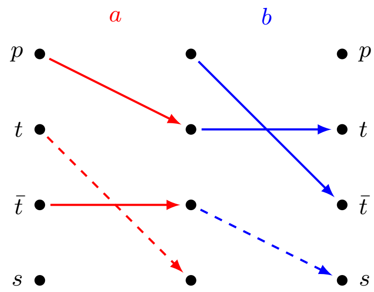

Figure 3.5.2

we must have $t > \bar{t}$. But this means we have a cross between the arcs $(p, \bar{t})$ and (t, t), both with label b and that is absurd.

In Case 2, since the outdegree of each vertex is at least 1 and $\bar{s}$ is the single fixed point such that p is connected to it by a path, the vertices t and $\bar{t}$ are connected by simple paths to $\bar{s}$. Thus, there is a vertex $s \neq t, \bar{t}$ for which there are disjoint (in the sense of sharing no arcs) simple paths $((t, s))$, $((\bar{t}, s))$. Consider the label a in every arc of the simple path $((t, s))$ (that path cannot contain the vertex p, since G is acyclic, and it also cannot contain the vertex $\bar{t}$, because there is no path from t to $\bar{t}$). For similar reasons we may label every arc of the path $((\bar{t}, s))$ with b, since it is disjoint from the path $((t, s))$. This way, we have the diagram in Figure 3.5.2. Assuming that $p > t$ and using Lemma 3.5.1, we must have $t > s$. According to the same result, $s < \bar{t} < p$, because we have a path from p to s passing through $\bar{t}$ and with all arcs having the same label. Now, if $t < \bar{t} < p$ there is a cross between (p, t) and $(\bar{t}, \bar{t})$, hence $s < \bar{t} < t$. But then $(p, \bar{t})$ crosses (t, t), which is absurd. $\square$

The following result is the counterpart of Lemma 3.5.2 for the case where the special vertex may be connected to more than one fixed point.

Lemma 3.5.3. *Let G be a monotonic digraph with n vertices ($n > 1$) and not necessarily constant outdegree. Suppose that the outdegree of each vertex is at least 1. Let p be a special vertex of G. Then, there can only be loops at most in two vertices of $N^+(p) - \{p\}$. Also, if there are two vertices in $N^+(p) - \{p\}$ that have loops, there can be no path connecting one of them to the other.*

Proof. Since G is monotonic, there can only be paths connecting p to at most two fixed points s_1 and s_2, because if p were connected to a third fixed point s_3, then the path from p to some s_i would necessarily cross the loops of some other fixed point s_j.

Given a fixed point s of G, consider the induced subgraph G_s whose vertex set is the subset Q_s of all the vertices for which there is a path connecting them to s. Note that this subgraph is monotonic, because given any suitable labeling of the arcs in G_s, it can be extended to a suitable labeling of the arcs in G and that extended labeling respects some order in the vertices in G, which we can restrict to an order over the vertices in G_s. Obviously the graph G_s has a single fixed point, s. Finally, since each vertex in G_s is connected by a path to s, we know that each vertex in G_s has outdegree at least 1.

For $i = 1, 2$ if $N_i = N^+(p) \cap Q_{s_i}$, we are in the conditions of Lemma 3.5.2 and we know that at most one vertex in $N_i - \{p\}$ has loops. But p is only connected to s_1 and s_2, therefore $N^+(p) = N_1 \cup N_2$ and there can only be loops at two vertices in $N^+(p) - \{p\}$.

To finish the proof it is enough to see that if $t, \bar{t}$ are vertices in $N^+(p) - \{p\}$ such that (t, t) and $(\bar{t}, \bar{t})$ are in G then we cannot have both t and $\bar{t}$ in the same subgraph G_{s_l}, because it would contradict Lemma 3.5.2, therefore there can be no paths of the forms $((t, \bar{t}))$ or $((\bar{t}, t))$ in G. $\square$

The next lemma will also provide conditions necessary to use Lemma 3.4.3 to its full potential when solving the rank problem for monotonic digraphs with a special vertex.

Lemma 3.5.4. *Let G be a monotonic digraph with n vertices ($n > 1$) and constant outdegree $k \geq 1$. Let p be a special vertex of G. Then, there is no path in G passing through more than two vertices in $N^+(p) - \{p\}$.*

Proof. We may assume that $k \geq 3$, because otherwise $|N^+(p)| \leq 2$ and the result is trivial. Aiming towards a contradiction, let $t, \bar{t}, \tilde{t} \in N^+(p) - \{p\}$ be three distinct vertices such that there is a path from t to $\tilde{t}$ passing through $\bar{t}$, that is, the simple paths $((t, \bar{t}))$ and $\left((\bar{t}, \tilde{t})\right)$ are in G. We consider a suitable labeling in the arcs of G such that (p, t) has label $a \in A$, $(p, \bar{t})$ has label $b \in A$ and $(p, \tilde{t})$ has label $c \in A$. There are two possibilities:

1. there is an arc $(\bar{t}, \tilde{t})$ in G;
2. the simple path $\left((\bar{t}, \tilde{t})\right)$ has at least two arcs and, in this case we consider a vertex q such that the path $((\bar{t}, q))$ and the arc $(q, \tilde{t})$ are in G.

In Case 1, label $(\bar{t}, \tilde{t})$ with c and every arc in $((t, \bar{t}))$ with a (p is not in that path). Since G has outdegree $k \geq 3$, there must be some arc leaving t besides the one that belongs to the path $((t, \bar{t}))$. Let $(t, \bar{q})$ be that arc and label it c. Given a perfect order for this labeling, we may assume that $p < t$ and according to Lemma 3.5.1, $t < \bar{t}$. If $\tilde{t} < \bar{q}$, then $(t, \bar{q})$ crosses $(\bar{t}, \tilde{t})$, as we can observe in Figure 3.5.3. If $\bar{q} < \tilde{t}$, then $(t, \bar{q})$ crosses $(p, \tilde{t})$. Since all these arcs have label c, we must have $\bar{q} = \tilde{t}$.

Now, consider in $(\bar{t}, \tilde{t})$ the label c, in $(t, \tilde{t})$ the label b and in every arc of the simple path $((t, \bar{t}))$ the label c, this can be done, since p is not in that path. Considering a perfect order for this labeling, we may assume that $t < \bar{t}$. Lemma 3.5.1 allows us to conclude

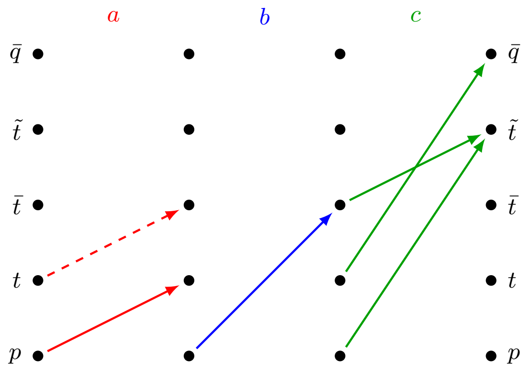

Figure 3.5.3

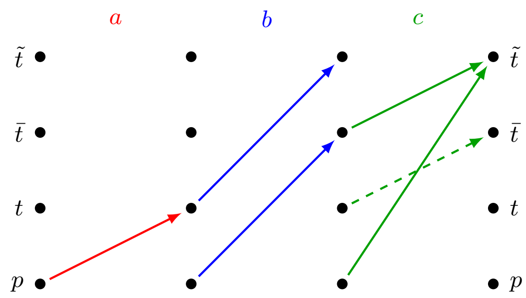

Figure 3.5.4

that $\bar{t} < \tilde{t}$. Now, if $t < p$, $(p, \bar{t})$ crosses $(t, \tilde{t})$ and they have the same label b, so this is absurd. Hence, $p < t$ and we are in the situation of Figure 3.5.4. But then, using Lemma 3.5.1, we conclude that the arcs in the path $((t, \bar{t}))$ cross $(p, \tilde{t})$, since they have the same label c, this is absurd. Therefore, Case 1 is not possible.

In Case 2, let $(q, \tilde{t})$ have label c, let the arcs in the path $((\bar{t}, q))$ have label b and let the arcs in the path $((t, \bar{t}))$ have label a (p is not in those paths). Since G has outdegree $k \geq 3$, there must be some arc leaving t besides the one that belongs to the path $((t, \bar{t}))$. Let $(t, \tilde{q})$ be that arc and label it c. Given a perfect order for this labeling, we may assume that $p < t$ and, according to Lemma 3.5.1, $p < t < \bar{t} < q$, because the vertex t belongs to the path $p, \bar{t}$, which has label a, and the vertex $\tilde{t}$ belongs to the path $((p, q))$, which has label b. If $\tilde{t} < \tilde{q}$, then $(t, \tilde{q})$ and $(q, \tilde{t})$ cross each other, as we can see in Figure 3.5.5. If $\tilde{q} < \tilde{t}$, then $(t, \tilde{q})$ and $(p, \tilde{t})$ cross each other. Since all these arcs have label c, we must have $\tilde{q} = \tilde{t}$.

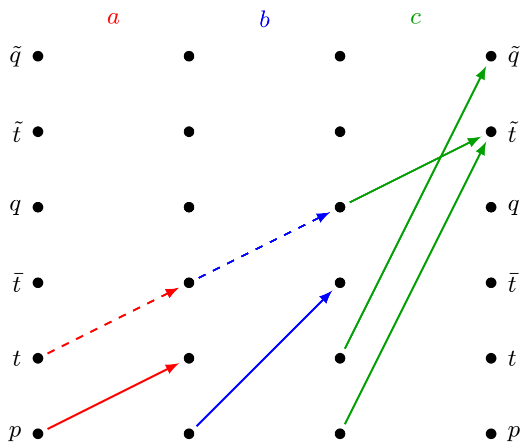

Figure 3.5.5

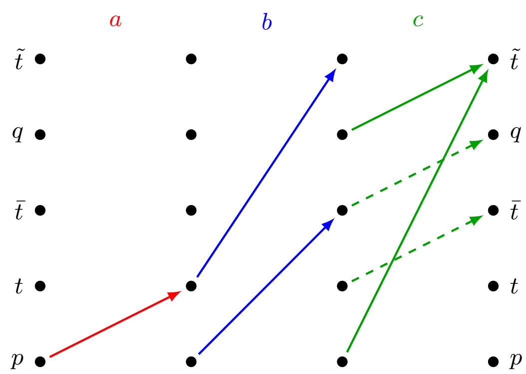

Figure 3.5.6

Now, consider in $(t, \tilde{t})$ the label b, in the arcs of the path $((t, \bar{t}))$ the label c (p is not in that path), in the arcs of the path $((\bar{t}, q))$ the label c (p is not in that path, neither is any of the vertices in the path $((t, \bar{t}))$) and in $(q, \tilde{t})$ label c also. Considering a perfect order for this labeling, we may assume that $t < \bar{t}$. Lemma 3.5.1 allows us to conclude that $\bar{t} < q < \tilde{t}$. Now, if $t < p$, then $(p, \bar{t})$ crosses $(t, \tilde{t})$ and they have the same label b, so this is absurd. Hence, $p < t$ and we are in the situation of Figure 3.5.6. But then, using Lemma 3.5.1, we conclude that the arcs in the path $(\!(t, \bar{t})\!)$ cross $(p, \tilde{t})$, since they have the same label c, this is absurd. Therefore, Case 2 is also impossible and we have reached the desired contradiction. □

The next theorem supplies a minimum rank word for all monotonic digraphs with n vertices, constant outdegree k and rank r that have a special vertex, which is connected to a single fixed point.

Theorem 3.5.5. *Let G be a monotonic digraph with n vertices ($n > 1$) and constant outdegree k ($1 \leq k \leq n$). Suppose that G has rank $r \geq 1$ and a special vertex p. Suppose also that if $k > 2$, then there is a single fixed point $\bar{s}$ such that p is connected to $\bar{s}$ by a path. If we use the alphabet $A = \{a_1, a_2, \ldots, a_k\}$ to form suitable labelings of the arcs in G, then*

$$ {}^{n}_{k}w_r = \begin{cases} (a_1 a_2 \ldots a_k)^{n-k-r+1} a_1 a_2 a_3 & \text{if } k > 2, \\ (a_1 a_2 \ldots a_k)^{n-r} & \text{if } k \leq 2 \end{cases} $$

is a minimum rank word for G.

Proof. Let Q be the vertex set of G and consider a vertex $q \in Q$. If q is not a fixed point, then we know that there is a simple path $(\!(q, s)\!)$ from q to some fixed point s of G. That path cannot contain any other fixed point of G, which means that there are $r - 1$ distinct vertices that do not belong to $(\!(q, s)\!)$, since according to Lemma 3.3.1 and Proposition 3.4.1 G has r fixed points.

Suppose for now that $k > 2$. Using Lemma 3.5.4, we know that the path $(\!(q, s)\!)$ contains at most two vertices of $N^+(p) - \{p\}$. According to Lemma 3.5.2, there is at most one vertex in $N^+(p) - \{p\}$ that has loops, hence, there is at most one fixed point in $N^+(p) - \{p\}$. However, we know that p and therefore every vertex in $N^+(p)$ is connected to a single fixed point. Hence, if some vertex in $N^+(p) - \{p\}$ is a fixed point, then that vertex is $\bar{s}$. In that case, either the path $(\!(q, s)\!)$ contains no vertex in $N^+(p) \cup \{p\}$, or $s = \bar{s}$. Either way, besides the $r - 1$ fixed points, there are at least $k - 3$ distinct vertices that do not belong to $(\!(q, s)\!)$, since p may belong to $N^+(p)$. So, in total, there are at most $n - (r-1) - (k-3) = n - k - r + 4$ distinct vertices that belong to $(\!(q, s)\!)$, one of them being p and two others belonging to $N^+(p) - \{p\}$. Let us denote the two possible vertices in $N^+(p) - \{p\}$ that belong to $(\!(q, s)\!)$ by t and $\bar{t}$ and suppose that $\bar{t}$ is the only one that may have loops. Then, there are at most $n - k - r + 1$ vertices in $(\!(q, s)\!)$ that do not belong to $\{q, p, t\}$.

Let δ be a suitable transition function for G using the letters in A. The vertex p has at most one loop, hence $\delta(p, a_i a_j) \neq p$, for every distinct $a_i, a_j \in A$. Also, since t has no loops, we have $\delta(t, a_i) \neq t$, for every $a_i \in A$. Thus, we may use Lemma 3.4.3 with $l = 2, P = \{p, t\}, \alpha_1 = 2, \alpha_2 = 1$, and $m = n-k-r+1$ to conclude that $\delta(q, (a_1 a_2 \ldots a_k)^{n-k-r+1} a_1 a_2 a_3)$ is a fixed point. Since this is true for any vertex q, the word ${}^n_k w_r$ has rank r.

For $k \in \{1, 2\}$, there are at most $n-(r-1) = n-r+1$ distinct vertices in the path $(\!(q, s)\!)$, hence we may use Lemma 3.4.3 with $l = \beta = \alpha = 0$ and $m = n - r$ to conclude that $\delta(q, (a_1 \ldots a_k)^{n-r})$ is a fixed point, for any vertex q, hence the word ${}^n_k w_r$ has rank r. □

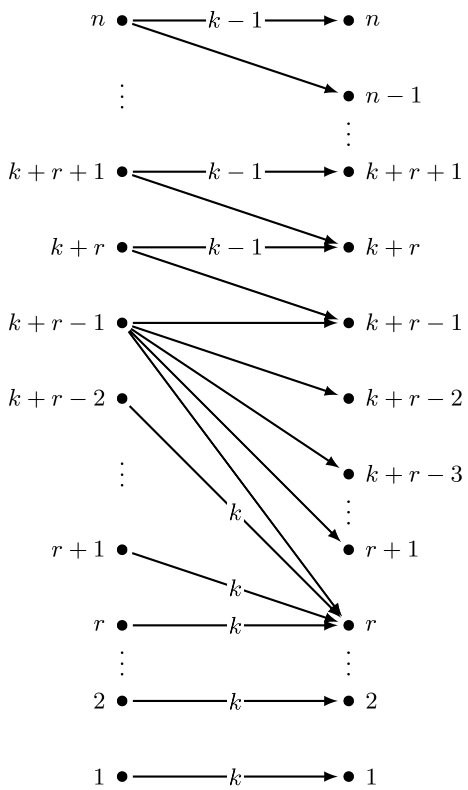

Figure 3.5.7: Digraph ${}^n_k G_r$

For each $n > 1$, $1 \leq k \leq n$ and $1 \leq r < n$ such that $k + r \leq n + 1$, consider the digraph ${}^n_k G_r$ represented by the diagram in Figure 3.5.7. This digraph is monotonic and the word ${}^n_k w_r$ in Theorem 3.5.5 is a shortest rank r word for this digraph. Indeed, consider for each $i \in \{1, 2, \ldots, k\}$, a suitable labeling of ${}^n_k G_r$ with transition function δ_i, such that for $j > k + r - 1$, $\delta_i(j, a_i) = j - 1$ and $\delta_i(j, a_l) = j$ when $l \neq i$. Since $\delta_i(Q, w') \subseteq \{1, 2, \ldots, k + r - 1\}$ implies that there are at least $n - k - r + 1$ occurrences of a_i in w', we conclude that a word that takes all the vertices in ${}^n_k G$ to $\{1, 2, \ldots, k + r - 1\}$, no matter what suitable labeling is considered, must have at least $n - k - r + 1$ occurrences of the letter a_i, for each $i \in \{1, 2, \ldots, k\}$. Finally, we need $\min\{3, k\}$ distinct letters to take $\{1, 2, \ldots, k+r-1\}$ to $\{1, 2, \ldots, r\}$ independently of the labeling. To see this, observe that if $k > 1$ for some labelings the first letter fixes the vertex $k + r - 1$ and the second letter sends it to a vertex j such that $r \leq j < k + r - 1$; if $k > 2$ we can have $j > r$ and the third letter is necessary to send j to r.

From Theorem 3.5.5, we obtain the following result that provides a totally synchronizing word for every totally synchronizing monotonic digraph with n vertices and constant outdegree k.

Corollary 3.5.6. *Let G be a monotonic digraph with n vertices ($n > 1$) and constant outdegree k ($1 \leq k \leq n$). Suppose that G is totally synchronizing and let p be a special vertex. Then*

$$ {}^{n}_{k}w = \begin{cases} (a_1 a_2 \ldots a_k)^{n-k} a_1 a_2 a_3 & \text{if } k > 2, \\ (a_1 a_2 \ldots a_k)^{n-1} & \text{if } k \leq 2 \end{cases} $$

is a universal synchronizing word for G.

Proof. Since G is totally synchronizing, according to Lemma 3.3.1 and Corollary 3.4.2, it has a unique fixed point, hence we are in the conditions of Theorem 3.5.5 and the result is obtained by noting that ${}^{n}_{k}w = {}^{n}_{k}w_1$. □

The next result is the counterpart of Theorem 3.5.5 for the case where the special vertex may be connected to more than one fixed point.

Theorem 3.5.7. *Let G be a monotonic digraph with n vertices ($n > 2$) and constant outdegree k ($2 < k \leq n$). Suppose that G has rank $r > 1$. Let p be a special vertex and suppose there are two fixed points s_1 and s_2 such that p is connected to them by paths. If we use the alphabet $A = \{a_1, a_2, \ldots, a_k\}$ to form suitable labelings of the arcs in G, then*

$$ {}^{n}_{k}\tilde{w}_r = \begin{cases} (a_1 a_2 \ldots a_k)^{n-k-r+2} a_1 a_2 a_3 & \text{if } k > 3, \\ (a_1 a_2 \ldots a_k)^{n-k-r+2} a_1 a_2 & \text{if } k = 3 \end{cases} $$

is a minimum rank word for G.

Proof. Let Q be the vertex set of G and consider a vertex $q \in Q$. If q is not a fixed point, then we know that there is a simple path $(\!(q, s)\!)$ from q to some fixed point s of G. That path cannot contain any other fixed point of G, which means that there are $r - 1$ distinct vertices that do not belong to $(\!(q, s)\!)$ since, according to Lemma 3.3.1 and Proposition 3.4.1, G has r fixed points.

Suppose for now that $k > 3$. Using Lemma 3.5.4, we know that the path $(\!(q, s)\!)$ contains at most two vertices of $N^+(p) - \{p\}$. According to Lemma 3.5.3, there are at most two vertices in $N^+(p) - \{p\}$ that have loops, hence, there are at most two fixed points in $N^+(p) - \{p\}$. Since p is only connected to the fixed points s_1 and s_2, $N^+(p) - \{p\}$ can only contain these fixed points. Thus, if s_1 or s_2 belong to $N^+(p) - \{p\}$, either the path $(\!(q, s)\!)$ contains no vertex in $N^+(p) \cup \{p\}$, or $s = s_i$, for some $i = 1, 2$. Either way, besides the $r - 1$ fixed points, there are at least $k - 4$ distinct vertices that do not belong to $(\!(q, s)\!)$, since p may belong to $N^+(p)$. So in total, there are at most $n - (r - 1) - (k - 4) = n - k - r + 5$ distinct vertices that belong to $(\!(q, s)\!)$, one of them being p and two others belonging to $N^+(p) - \{p\}$. Let us denote the two possible vertices in $N^+(p) - \{p\}$ that belong to $(\!(q, s)\!)$ by t and $\bar{t}$. According to Lemma 3.5.3 only one of them may have loops, suppose that it is $\bar{t}$. Then, there are at most $n - k - r + 2$ vertices in $(\!(q, s)\!)$ that do not belong do to $\{q, p, t\}$.

Let δ be a suitable transition function for G using the letters in A. The vertex p has at most one loop, hence given distinct letters a_i and a_j, we have $\delta(p, a_i a_j) \neq p$. Also, since t has no loops, we have $\delta(t, a_i) \neq t$, for every $a_i \in A$. Thus, if we use Lemma 3.4.3 with $l = 2, P = \{p, t\}, \alpha_1 = 2, \alpha_2 = 1$ and $m = n - k - r + 2$, we conclude that $\delta(q, (a_1 a_2 \dots a_k)^{n-k-r+2} a_1 a_2 a_3)$ is a fixed point. Since this is true for any vertex q, the word ${}^n_k w_r$ has rank r.

If $k = 3$, then we know that there are at most $n - (r - 1) = n - k - r + 4$ distinct vertices in the path $(\!(q, s)\!)$, one of them being p and two others, t and $\bar{t}$, belonging to $N^+(p) - \{p\}$. We need to consider two cases:

1. the vertex p belongs to $N^+(p)$;
2. the vertex p does not belong to $N^+(p)$.

In Case 1, the vertex p has a single loop, so $\delta(p, a_i a_j) \neq p$ for every $a_i, a_j \in A$. Since besides q and p there are at most $n - k - r + 2$ distinct vertices in $(\!(q, s)\!)$, if we use Lemma 3.4.3 with $l = 1, P = \{p\}, \alpha_1 = 2 = \alpha, \beta = 0$ and $m = n - k - r + 2$, we necessarily have $\delta(q, (a_1 a_2 \dots a_k)^{n-k-r+2} a_1 a_2) = s$.

In Case 2, the vertex p has no loops and according to Lemma 3.5.3 only one of the vertices in $N^+(p)$ that belong to the path $(\!(q, s)\!)$ may have loops. As above, suppose that $\bar{t}$ is the only one that may have loops. Hence we have $\delta(p, a_i) \neq p$ and $\delta(t, a_i) \neq t$, for every $a_i \in A$. Since besides q, p and t there are at most $n - k - r + 1$ distinct vertices in $(\!(q, s)\!)$, if we use Lemma 3.4.3 with $l = 2, P = \{p, t\}, \alpha_1 = \alpha_2 = 1, \alpha = 2, \beta = 0$ and $m = n - k - r + 1$, we have $\delta(q, (a_1 a_2 \dots a_k)^{n-k-r+1} a_1 a_2) = s$.

In all cases, ${}^n_k \tilde{w}_r$ is a word of minimum rank for G. $\square$

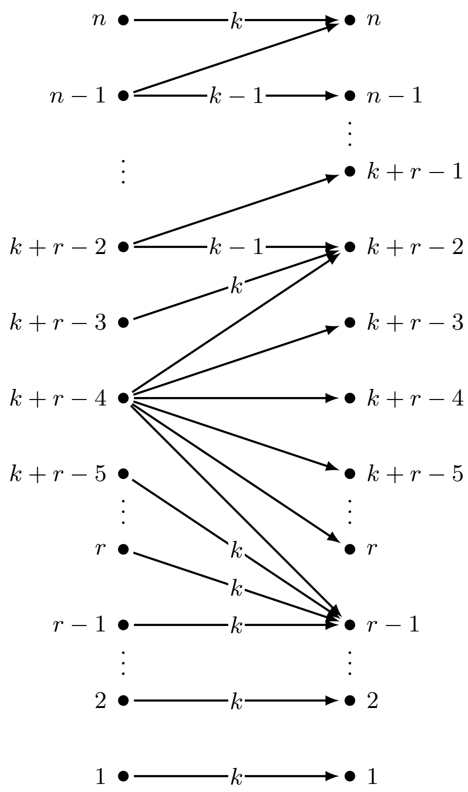

Figure 3.5.8: Digraph ${}^n_k\tilde{G}_r$

For each $n > 2$, $2 < k \leq n$ and $1 \leq r < n$ such that $k+r \leq n+2$, consider the digraph ${}^n_k\tilde{G}_r$ represented by the diagram in Figure 3.5.8. The word ${}^n_k\tilde{w}_r$ in Theorem 3.5.7 is a shortest minimum rank r word for this digraph. Indeed, consider for each $i, l, m \in \{1, 2, \ldots, k\}$ a suitable labeling of ${}^n_k\tilde{G}_r$ with transition function ${}_m^l\delta_i$. For $j \in \{k+r-2, k+r-3, \ldots, n-1\}$, let ${}_m^l\delta_i(j, a_i) = j+1$ and ${}_m^l\delta_i(j, a_{\bar{i}}) = j$ when $\bar{i} \neq i$. Let ${}_m^l\delta_i(k+r-4, a_m) = k+r-4$, and ${}_m^l\delta_i(k+r-4, a_l) = k+r-3$. Clearly, to make sure that the vertex $k+r-4$ is sent to some other vertex independently of the labeling considered we will need to use a word with two distinct letters a_m and a_l. Now ${}_m^l\delta_i(k+r-4, a_m a_l) = k+r-3$, so, if $k > 3$ a third letter is necessary to send $k+r-3$ to $k+r-2$. For $k = 3$, the digraph ${}^n_3\tilde{G}_r$ is such that the vertex $k+r-4$ is connected to itself, $k+r-5$ and $k+r-3$. So in general we need $\min\{3, k-1\}$ distinct letters to make sure that $k+r-4$ is either sent to $k+r-2$ or the fixed point $r-1$, depending on the labeling considered. Finally, since ${}_m^l\delta_i(\{k+r-2, k+r-1, \ldots, n\}, w') \subseteq \{n\}$ implies that there are at least $n-k-r+2$ occurrences of a_i in w', we conclude that a word that takes all the vertices in $\{k+r-2, k+r-1, \ldots, n\}$ to n, no matter which suitable labeling is considered, must have at least $n-k-r+2$ occurrences of the letter a_i, for each $i \in \{1, 2, \ldots, k\}$.

The next result is a consequence of Theorems 3.5.5 and 3.5.7. It supplies a bound on the length of shortest minimum rank words for monotonic digraphs with a special vertex, based on the number of vertices and the rank.

Corollary 3.5.8. *Let G be a monotonic digraph with n vertices ($n > 1$) and constant outdegree k ($1 \leq k \leq n$). Suppose that G has rank r ($1 \leq r < n$) and that there is some special vertex in G. Then, for $n - r = 1, 2, 3, 4$ there are rank r words of lengths* $2, 5, 8, 11$ *respectively. If $n - r \geq 5$, there is a rank r word for G of length*

$$\left\lfloor \frac{n-r+2}{2} \right\rfloor \left\lceil \frac{n-r+2}{2} \right\rceil + 3.$$

All these bounds are tight.

Proof. For $k \in \{1, 2\}$, let

$$\xi(n, r, k) = k(n - r)$$

be the function that associates with each triple (n, r, k) such that $n > 1$, $r > 1$ and $k+r \leq n+1$, the length of the word ${}^{n}_{k}w_r$ in Theorem 3.5.5. For $k \geq 3$, let

$$\xi(n, r, k) = k(n - k - r + 2) + \min\{3, k - 1\}$$

be the function that associates with each triple (n, r, k) such that $n > 1$, $r > 1$ and $k+r \leq n+2$, the length of the word ${}^{n}_{k}\tilde{w}_r$ in Theorem 3.5.7. Also let

$$\psi(n, r) = \max_{k}\{\xi(n, r, k)\}.$$

For each triple (n, r, k) in the conditions above, the digraphs ${}^{n}_{k}G_r$ and ${}^{n}_{k}\tilde{G}_r$ from Figures 3.5.7 and 3.5.8, respectively, show that the upper bounds $\xi(n, r, k)$ from Theorems 3.5.5 and 3.5.7, respectively, are tight. Hence, to finish the proof, all we need to do is to compute $\psi(n, r)$.

Since $\xi(n, r, 2) = 2(n - r) > n - r = \xi(n, r, 1)$, we have $\psi(n, r) \geq \xi(n, r, 2)$ for every n, r and so we may assume that $k > 1$.

For $k = 3$, we have $\xi(n, r, k) = k(n - k - r + 2) + k - 1 = 3(n - r) - 1$. For $k > 3$, we have $\min\{3, k - 1\} = 3$ and so $\xi(n, r, k) = k(n - k - r + 2) + 3$. For each $n, r \geq 3$, the maximum of $k(n - k - r + 2) + 3$ is obtained when $k = \lfloor (n - r + 2)/2 \rfloor$. If $n - r \leq 5$, $\lfloor (n - r + 2)/2 \rfloor \leq 3$, hence we need to study these cases separately. But when $n - r > 5$, $\lfloor (n - r + 2)/2 \rfloor > 3$ and

$$\psi(n, r) = \left\lfloor \frac{n-r+2}{2} \right\rfloor \left\lceil \frac{n-r+2}{2} \right\rceil + 3,$$

because

$$\left\lfloor \frac{n-r+2}{2} \right\rfloor \left\lceil \frac{n-r+2}{2} \right\rceil + 3 > 3(n - r) - 1 > 2(n - r),$$

for all n, r in these conditions.

Finally, observing the following table

$n-r$	1	1	2	2	2	3	3	3	3	4	4	4	4	5	5	5	5
k	2	3	2	3	4	2	3	4	5	2	3	4	5	2	3	4	5
$\psi(n,r)$	2	2	4	5	3	6	8	7	3	8	11	11	8	10	14	15	13

allows us to conclude that

$n-r$	1	2	3	4	5
$\psi(n,r)$	2	5	8	11	15

Observe that for $n-r=5$, $\psi(n,r) = 15 = \lfloor (n-r+2)/2 \rfloor \lceil (n-r+2)/2 \rceil + 3$. □

The following Corollary is obtained as a direct consequence of Corollary 3.5.8 and establishes a bound on the length of shortest totally synchronizing words for totally synchronizing monotonic digraphs with a special vertex.

Corollary 3.5.9. *Let G be a monotonic digraph with n vertices ($n > 1$) and constant outdegree k ($1 < k \leq n$). Suppose that G is totally synchronizing and that there is some special vertex in G. Then, for $n = 2,3,4,5$ there are universal synchronizing words of lengths $2,5,8,11$, respectively. If $n \geq 6$, then there is a universal synchronizing word for G of length*

$$\left\lfloor \frac{n+1}{2} \right\rfloor \left\lceil \frac{n+1}{2} \right\rceil + 3.$$

All these bounds are tight.

Since the digraph ${}^n_k\dot{G}_r$ in Figure 3.4.2 is monotonic, in the general case, where we have a monotonic digraph with outdegree k and we do not know if there is some special vertex, we cannot further improve the result from Corollary 3.4.8.

Chapter 4

Weakly monotonic automata with large level

4.1 A sequence of automata

For each positive integer n, consider the complete deterministic finite automaton $\mathcal{A}_n = (Q_n, A_n, \delta_n)$, with set of states $Q_n = \{0, 1, \ldots, n-1\}$, alphabet $A_n = \{a_0, a_1, \ldots, a_{n-1}\}$ and transition function δ_n such that:

- for each $i \in 0, 1, \ldots, n-2$ and each $q \in Q_n$,

$$\delta_n(q, a_i) = \begin{cases} i & \text{if } q < n-i-1 \text{ or } q = n-i-1 \geq \left\lceil \frac{n}{2} \right\rceil \\ i+1 & \text{if } q \geq n-i \text{ or } q = n-i-1 < \left\lceil \frac{n}{2} \right\rceil; \end{cases}$$

- for every $q \in Q_n$,

$$\delta_n(q, a_{n-1}) = \begin{cases} n-q-1 & \text{if } q < \left\lceil \frac{n}{2} \right\rceil \\ n-q & \text{if } q \geq \left\lceil \frac{n}{2} \right\rceil. \end{cases}$$

Note that

$$\text{for every } n > 1 \text{ and every } a \in A_n,\ \delta_n\left(\left\lceil \frac{n}{2} \right\rceil, a\right) = \delta_n\left(\left\lceil \frac{n}{2} \right\rceil - 1, a\right). \tag{4.1.1}$$

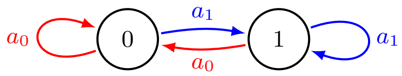

Figure 4.1.1: Automaton $\mathcal{A}_2$

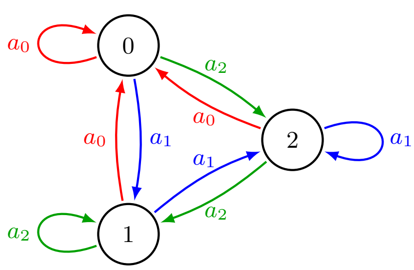

Figure 4.1.2: Automaton $\mathcal{A}_3$

The automata $\mathcal{A}_2, \mathcal{A}_3, \mathcal{A}_4$ and $\mathcal{A}_5$ are represented in Figures 4.1.1, 4.1.2, 4.1.3 and 4.1.4, respectively.

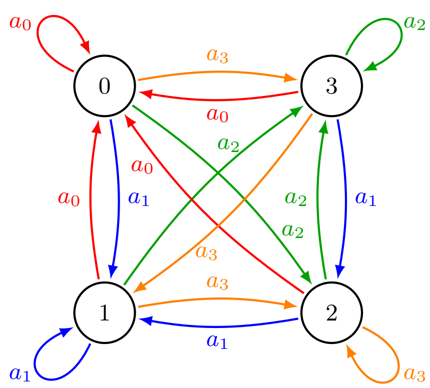

Figure 4.1.3: Automaton $\mathcal{A}_4$

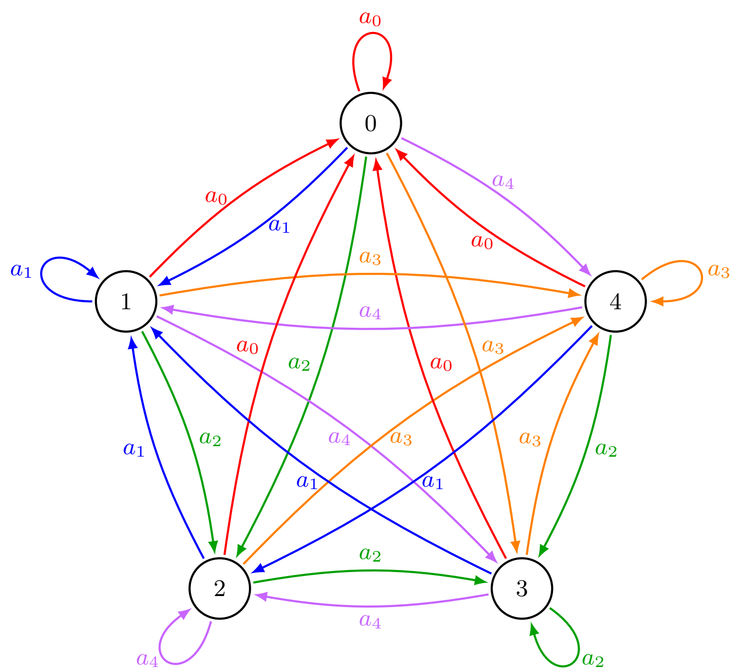

Figure 4.1.4: Automaton $\mathcal{A}_5$

4.2 Weak monotonicity

Let us begin with some results that will help to establish that for every positive integer n, the automaton $\mathcal{A}_n$ is weakly monotonic of level $n-1$.

Lemma 4.2.1. *Let ρ be a stable and transitive binary relation on $\mathcal{A}_n$. Suppose that $(s,t) \in \rho$ with $s \neq t$ and that there is a nonempty set I_t^s of consecutive elements of $\{0, 1, \dots, n-2\}$ such that for each $i \in I_t^s$, $\delta_n(s, a_i) = i$ and $\delta_n(t, a_i) = i+1$. Suppose also that for $p = \min I_t^s$ and $q = \max I_t^s + 1$, $\delta_n(s, a_{n-1}) = q$ and $\delta_n(t, a_{n-1}) = p$. Then the relation ρ cannot be antisymmetric.*

Proof. We know that for every $i \in I_t^s$, $\delta_n(s, a_i) = i$ and $\delta_n(t, a_i) = i+1$, therefore

$$\delta_n(s, a_p) = p \text{ and } \delta_n(t, a_p) = p+1,$$

$$\delta_n(s, a_{p+1}) = p+1 \text{ and } \delta_n(t, a_{p+1}) = p+2,$$

$$\vdots$$

$$\delta_n(s, a_{q-1}) = q-1 \text{ and } \delta_n(t, a_{q-1}) = q.$$

Since ρ is stable and $(s,t) \in \rho$, we have $(p, p+1), (p+1, p+2), \dots, (q-1, q) \in \rho$. Using the transitivity of ρ, we conclude that $(p,q) \in \rho$. But we also have $(q,p) \in \rho$, because $\delta_n(s, a_{n-1}) = q$ and $\delta_n(t, a_{n-1}) = p$ and ρ is stable. Thus, since $p \neq q$ because I_t^s is nonempty, ρ cannot be antisymmetric. $\square$

Lemma 4.2.2. *Let π_n^0 be the equality relation on $\mathcal{A}_n$. The only stable partial orders on $\mathcal{A}_n$ are π_n^0, $\rho_n^1 = \pi_n^0 \cup \{(\lceil n/2\rceil - 1, \lceil n/2\rceil)\}$ and $\bar{\rho}_n^1 = \pi_n^0 \cup \{(\lceil n/2\rceil, \lceil n/2\rceil - 1)\}$.*

Proof. Let ρ be a stable and transitive binary relation on $\mathcal{A}_n$ and suppose that $(s,t) \in \rho$ with $s \neq t$ and $\{s,t\} \neq \{\lceil n/2\rceil - 1, \lceil n/2\rceil\}$. We can assume without loss of generality that $s < t$ for the usual order on $\mathbb{N}$, otherwise it would be enough to consider the reverse order of ρ. Since $\{s,t\} \neq \{\lceil n/2\rceil - 1, \lceil n/2\rceil\}$, we have the following possibilities:

1. $s < t < \lceil n/2\rceil$;
2. $\lceil n/2\rceil < s < t$;
3. $s < \lceil n/2\rceil < t$;
4. $s = \lceil n/2\rceil < t$;
5. $s < \lceil n/2\rceil = t$.

In Case 1, note that the set $I_t^s = \{i \in \{0,1,\ldots,n-2\} : n-t-1 \leq i < n-s-1\}$ is nonempty. For each $i \in I_t^s$, we have $s < n-i-1 \leq t$, hence $\delta_n(s,a_i) = i$ and $\delta_n(t,a_i) = i+1$. We also have $\delta_n(s,a_{n-1}) = n-s-1$ and $\delta_n(t,a_{n-1}) = n-t-1$. Hence, we are in the conditions of Lemma 4.2.1 and ρ cannot be antisymmetric, which means that it is not a partial order.

In Case 2, we put $I_t^s = \{i \in \{0,1,\ldots,n-2\} : n-t \leq i < n-s\}$, which is again a nonempty set. For each $i \in I_t^s$, we have $s < n-i \leq t$, hence $\delta_n(s,a_i) = i$ and $\delta_n(t,a_i) = i+1$. We also have $\delta_n(s,a_{n-1}) = n-s$ and $\delta_n(t,a_{n-1}) = n-t$. Thus, we are in the conditions of Lemma 4.2.1 and ρ cannot be antisymmetric, which means that it is not a partial order.

In Case 3, $s < t-1$ and so the set $I_t^s = \{i \in \{0,1,\ldots,n-2\} : n-t \leq i < n-s-1\}$ is nonempty. For each $i \in I_t^s$, we have $s < n-i-1 < t$, hence $\delta_n(s,a_i) = i$ and $\delta_n(t,a_i) = i+1$. We also have $\delta_n(s,a_{n-1}) = n-s-1$ and $\delta_n(t,a_{n-1}) = n-t$. Hence, we are in the conditions of Lemma 4.2.1 and ρ cannot be antisymmetric, which means that it is not a partial order.

In Case 4, we have $(\lceil n/2\rceil, t) \in \rho$, with $t > \lceil n/2\rceil$. Since $\delta_n(\lceil n/2\rceil, a_{n-t}) = n-t$ and $\delta_n(t, a_{n-t}) = n-t+1$, so that $(n-t, n-t+1) \in \rho$, we fall again in Case 1 unless n is even and $t = n/2+1$, in which case we have $(n-t, n-t+1) = (n/2-1, n/2) \in \rho$ and also $(n/2, n/2+1) \in \rho$. But $\delta_n(n/2, a_{n-1}) = n - n/2 = n/2$ and $\delta_n(n/2+1, a_{n-1}) = n-(n/2+1) = n/2-1$, so that $(n/2, n/2-1) \in \rho$, since ρ is stable. This proves that ρ cannot be antisymmetric because both $(n/2, n/2-1)$ and $(n/2-1, n/2)$ belong to ρ.

In Case 5, since $\{s,t\} \neq \{\lceil n/2\rceil - 1, \lceil n/2\rceil\}$, we must have $s < \lceil n/2\rceil - 1$ and $t = \lceil n/2\rceil$, with $(s,t) \in \rho$. Since $\delta_n(s, a_{n-\lceil n/2\rceil}) = n - \lceil n/2\rceil$ and $\delta_n(t, a_{n-\lceil n/2\rceil}) = n - \lceil n/2\rceil + 1$, we deduce that $(n-\lceil n/2\rceil, n-\lceil n/2\rceil + 1) \in \rho$, which falls in Cases 3 or 4, that we have already treated.

To finish the proof, it is enough to verify that ρ_n^1 is a stable partial order on $\mathcal{A}_n$, since $\bar{\rho}_n^1$ is the reverse order of ρ_n^1. In view of (4.1.1), we deduce that ρ_n^1 is stable and it is trivial to check that it is reflexive, transitive and antisymmetric. □

Given a positive integer n, consider the automaton $\mathcal{B}_n = (Q_n, A_n \uplus \{b\}, \bar{\delta}_n)$, where $\bar{\delta}_n$ is such that

$$\bar{\delta}_n|_{Q_n \times A_n} = \delta_n \text{ and, for every } q \in Q_n,\ \bar{\delta}_n(q,b) = \lceil n/2 \rceil - 1.$$

Lemma 4.2.3. *Consider the stable equivalence relation*

$$\pi_n^1 = \pi_n^0 \cup \{(\lceil n/2 \rceil - 1, \lceil n/2 \rceil), (\lceil n/2 \rceil, \lceil n/2 \rceil - 1)\}$$

on $\mathcal{A}_n$. Then, for every $n \geq 2$,

$$\mathcal{A}_n/\pi_n^1 \simeq \mathcal{B}_{n-1}.$$

Proof. Consider the functions

$$\begin{aligned} \xi : Q_n/\pi_n^1 &\longrightarrow Q_{n-1} \\ [q] &\longmapsto \begin{cases} q & \text{if } q < \lceil \frac{n}{2} \rceil \\ q-1 & \text{if } q \geq \lceil \frac{n}{2} \rceil \end{cases} \end{aligned} \qquad \begin{aligned} \psi : A_n &\longrightarrow A_{n-1} \cup \{b\} \\ a_i &\longmapsto \begin{cases} a_i & \text{if } i < \lceil \frac{n}{2} \rceil - 1 \\ b & \text{if } i = \lceil \frac{n}{2} \rceil - 1 \\ a_{i-1} & \text{if } i > \lceil \frac{n}{2} \rceil - 1. \end{cases} \end{aligned}$$

Note that ξ is well defined, because the only nontrivial class is $\{\lceil \frac{n}{2} \rceil - 1, \lceil \frac{n}{2} \rceil\}$. For the same reason, ξ is bijective and it is obvious that ψ is also a bijection. Hence, to finish the proof all we need to check is that the pair (ξ, ψ) defines a morphism between the automata $\mathcal{A}_n/\pi_n^1$ and $\mathcal{B}_{n-1}$, that is, for every $[q] \in Q_n/\pi_n^1$ and every $a_i \in A_n$,

$$\bar{\delta}_{n-1}(\xi([q]), \psi(a_i)) = \xi(\delta_n([q], a_i)). \tag{4.2.1}$$

We have the following possibilities:

1. $i = \lceil n/2 \rceil - 1$;
2. $i < \lceil n/2 \rceil - 1$ and $q \leq \lceil n/2 \rceil$;
3. $i < \lceil n/2 \rceil - 1$ and $q > \lceil n/2 \rceil$;
4. $\lceil n/2 \rceil - 1 < i < n - 1$ and $q \leq \lceil n/2 \rceil$;
5. $\lceil n/2 \rceil - 1 < i < n - 1$ and $q > \lceil n/2 \rceil$;
6. $i = n - 1$.

In Case 1, $\psi(a_i) = b$ and $\bar{\delta}_{n-1}(p, b) = \lceil n/2 \rceil - 1$, for all $p \in Q_{n-1}$, hence

$$\bar{\delta}_{n-1}(\xi([q]), \psi(a_i)) = \left\lceil \frac{n}{2} \right\rceil - 1, \text{ for every } [q] \in Q_n/\pi_n^1.$$

On the other hand,

$$\delta_n([q], a_i) = \begin{cases} [i] & \text{if } q < n-i-1 \text{ or } q = n-i-1 \geq \lceil n/2 \rceil \\ [i+1] & \text{if } q \geq n-i \text{ or } q = n-i-1 < \lceil n/2 \rceil. \end{cases}$$

Since $[i] = \{i, i+1\} = [i+1]$ and $\xi([i]) = \lceil n/2 \rceil - 1$, we have

$$\xi(\delta_n([q], a_i)) = \left\lceil \frac{n}{2} \right\rceil - 1, \text{ for every } [q] \in Q_n/\pi_n^1.$$

Therefore, the equality (4.2.1) holds in this case.

In Case 2, $\psi(a_i) = a_i$ and $\xi([q]) = q$, for $q < \lceil n/2 \rceil$. For $q = \lceil n/2 \rceil$, $[q] = [\lceil n/2 \rceil - 1]$, so it is enough to consider $q < \lceil n/2 \rceil$. It follows that

$$\begin{aligned} \bar{\delta}_{n-1}(\xi([q]), \psi(a_i)) &= \bar{\delta}_{n-1}(q, a_i) = \delta_{n-1}(q, a_i) \\ &= \begin{cases} i & \text{if } q < n-i-2 \text{ or } q = n-i-2 \geq \lceil \frac{n-1}{2} \rceil \\ i+1 & \text{if } q \geq n-i-1 \text{ or } q = n-i-2 < \lceil \frac{n-1}{2} \rceil. \end{cases} \end{aligned}$$

But $i < \lceil n/2 \rceil - 1$ implies $n-i-2 \geq \lceil (n-1)/2 \rceil$, therefore the condition $q = n-i-2 < \lceil (n-1)/2 \rceil$ is impossible and

$$\bar{\delta}_{n-1}(\xi([q]), \psi(a_i)) = \begin{cases} i & \text{if } q < n-i-1 \\ i+1 & \text{if } q \geq n-i-1. \end{cases}$$

On the other hand,

$$\xi(\delta_n([q], a_i)) = \begin{cases} \xi([i]) & \text{if } q < n-i-1 \\ \xi([i+1]) & \text{if } q \geq n-i-1 \end{cases} = \begin{cases} i & \text{if } q < n-i-1 \\ i+1 & \text{if } q \geq n-i-1, \end{cases}$$

because

$$i < \left\lceil \frac{n}{2} \right\rceil - 1 \text{ implies } \Big(\xi([i]) = i \text{ and } \xi([i+1]) = i+1\Big). \tag{4.2.2}$$

Thus, the equality (4.2.1) holds in this case.

In Case 3, $\psi(a_i) = a_i$, $\xi([q]) = q-1$ and $q-1 \geq \lceil n/2 \rceil \geq \lceil (n-1)/2 \rceil$. Hence

$$\begin{aligned} \bar{\delta}_{n-1}(\xi([q]), \psi(a_i)) &= \bar{\delta}_{n-1}(q-1, a_i) = \delta_{n-1}(q-1, a_i) \\ &= \begin{cases} i & \text{if } q-1 < n-i-1 \\ i+1 & \text{if } q-1 \geq n-i-1 \end{cases} = \begin{cases} i & \text{if } q < n-i \\ i+1 & \text{if } q \geq n-i. \end{cases} \end{aligned}$$

On the other hand, in view of (4.2.2), we have

$$\xi(\delta_n([q], a_i)) = \begin{cases} \xi([i]) & \text{if } q < n - i \\ \xi([i+1]) & \text{if } q \geq n - i \end{cases} = \begin{cases} i & \text{if } q < n - i \\ i+1 & \text{if } q \geq n - i. \end{cases}$$

Thus, the equality (4.2.1) holds in this case.

In Case 4, $\psi(a_i) = a_{i-1}$ and $\xi([q]) = q$, for $q < \lceil n/2 \rceil$. For $q = \lceil n/2 \rceil$, $[q] = [\lceil n/2 \rceil - 1]$, so it is enough to consider $q < \lceil n/2 \rceil$. It follows that

$$\begin{aligned} \bar{\delta}_{n-1}(\xi([q]), \psi(a_i)) &= \bar{\delta}_{n-1}(q, a_{i-1}) = \delta_{n-1}(q, a_{i-1}) \\ &= \begin{cases} i-1 & \text{if } q < n-i-1 \text{ or } q = n-i-1 \geq \lceil \frac{n-1}{2} \rceil \\ i & \text{if } q \geq n-i \text{ or } q = n-i-1 < \lceil \frac{n-1}{2} \rceil. \end{cases} \end{aligned}$$

But

$$i > \left\lceil \frac{n}{2} \right\rceil - 1 \text{ implies } n - i - 1 < \left\lceil \frac{n-1}{2} \right\rceil \leq \left\lceil \frac{n}{2} \right\rceil, \tag{4.2.3}$$

therefore the condition $q = n - i - 1 \geq \lceil (n-1)/2 \rceil$ is impossible and

$$\bar{\delta}_{n-1}(\xi([q]), \psi(a_i)) = \begin{cases} i-1 & \text{if } q < n-i-1 \\ i & \text{if } q \geq n-i-1. \end{cases}$$

On the other hand,

$$\xi(\delta_n([q], a_i)) = \begin{cases} \xi([i]) & \text{if } q < n-i-1 \\ \xi([i+1]) & \text{if } q \geq n-i-1 \end{cases} = \begin{cases} i-1 & \text{if } q < n-i-1 \\ i & \text{if } q \geq n-i-1, \end{cases}$$

because

$$i \geq \left\lceil \frac{n}{2} \right\rceil \text{ implies } \Big(\xi([i]) = i-1 \text{ and } \xi([i+1]) = i \Big). \tag{4.2.4}$$

Thus, the equality (4.2.1) holds in this case.

In Case 5, $\psi(a_i) = a_{i-1}$, $\xi([q]) = q - 1$ and $q - 1 \geq \lceil n/2 \rceil \geq \lceil (n-1)/2 \rceil$. Hence

$$\begin{aligned} \bar{\delta}_{n-1}(\xi([q]), \psi(a_i)) &= \bar{\delta}_{n-1}(q-1, a_{i-1}) = \delta_{n-1}(q-1, a_{i-1}) \\ &= \begin{cases} i-1 & \text{if } q-1 \leq n-1-(i-1)-1 \\ i & \text{if } q-1 > n-1-(i-1)-1 \end{cases} = \begin{cases} i-1 & \text{if } q \leq n-i \\ i & \text{if } q > n-i. \end{cases} \end{aligned}$$

On the other hand, in view of (4.2.4) and since $q > \lceil n/2 \rceil$, we have

$$\xi(\delta_n([q], a_i)) = \begin{cases} \xi([i]) & \text{if } q \leq n-i-1 \\ \xi([i+1]) & \text{if } q > n-i-1 \end{cases} = \begin{cases} i-1 & \text{if } q \leq n-i-1 \\ i & \text{if } q > n-i-1. \end{cases}$$

If $q = n - i$, then $q \leq n - \lceil n/2 \rceil$, because $i \geq \lceil n/2 \rceil$. Hence, we obtain $q \leq \lceil n/2 \rceil$, which is absurd since $q > \lceil n/2 \rceil$. Thus, equality (4.2.1) holds in this case.

In Case 6, $\psi(a_n) = a_{n-2}$, hence

$$\bar{\delta}_{n-1}(\xi([q]), \psi(a_{n-1}))$$

$$= \begin{cases} \bar{\delta}_{n-1}(q, a_{n-2}) & \text{if } q < \lceil \frac{n}{2} \rceil \\ \bar{\delta}_{n-1}(q-1, a_{n-2}) & \text{if } q \geq \lceil \frac{n}{2} \rceil \end{cases} = \begin{cases} n-1-q-1 & \text{if } q < \lceil \frac{n}{2} \rceil \text{ and } q < \lceil \frac{n-1}{2} \rceil \\ n-1-q & \text{if } q < \lceil \frac{n}{2} \rceil \text{ and } q \geq \lceil \frac{n-1}{2} \rceil \\ n-1-(q-1)-1 & \text{if } q \geq \lceil \frac{n}{2} \rceil \text{ and } q-1 < \lceil \frac{n-1}{2} \rceil \\ n-1-(q-1) & \text{if } q \geq \lceil \frac{n}{2} \rceil \text{ and } q-1 \geq \lceil \frac{n-1}{2} \rceil \end{cases}$$

$$= \begin{cases} n-q-2 & \text{if } q < \lceil \frac{n-1}{2} \rceil \\ n-q-1 & \text{if } q = \lceil \frac{n-1}{2} \rceil \\ n-q & \text{if } q \geq \lceil \frac{n-1}{2} \rceil. \end{cases}$$

On the other hand,

$$\xi(\delta_n([q], a_{n-1}))$$

$$= \begin{cases} \xi([n-q-1]) & \text{if } q < \lceil \frac{n}{2} \rceil \\ \xi([n-q]) & \text{if } q \geq \lceil \frac{n}{2} \rceil \end{cases} = \begin{cases} n-q-2 & \text{if } q < \lceil \frac{n}{2} \rceil \text{ and } n-q-1 \geq \lceil \frac{n}{2} \rceil \\ n-q-1 & \text{if } q < \lceil \frac{n}{2} \rceil \text{ and } n-q-1 < \lceil \frac{n}{2} \rceil \\ n-q-1 & \text{if } q \geq \lceil \frac{n}{2} \rceil \text{ and } n-q \geq \lceil \frac{n}{2} \rceil \\ n-q & \text{if } q \geq \lceil \frac{n}{2} \rceil \text{ and } n-q < \lceil \frac{n}{2} \rceil \end{cases}$$

$$= \begin{cases} n-q-2 & \text{if } q < \lceil \frac{n-1}{2} \rceil \\ n-q-1 & \text{if } q = \lceil \frac{n-1}{2} \rceil \\ n-q & \text{if } q \geq \lceil \frac{n-1}{2} \rceil, \end{cases}$$

because if $n - q = \lceil n/2 \rceil$, then $q = n - \lceil n/2 \rceil = \lfloor n/2 \rfloor = \lceil (n-1)/2 \rceil$. Thus, the equality (4.2.1) holds in this case as well, concluding our proof. □

Lemma 4.2.4. *Let $\mathcal{A} = (Q, A, \delta)$ be a complete deterministic finite automaton and consider the automaton $\mathcal{B} = (Q, A \uplus \{b\}, \bar{\delta})$, where $\bar{\delta}|_{Q \times A} = \delta$ and there is $\bar{q} \in Q$ such that, for all $q \in Q$, $\bar{\delta}(q, b) = \bar{q}$. Then for every natural number $l \in \mathbb{N}$, $\mathcal{A}$ is weakly monotonic of level l if and only if $\mathcal{B}$ is weakly monotonic of level l.*

Proof. Suppose that $\mathcal{A}$ is weakly monotonic of level l for some natural number l. Then there is a strictly increasing chain of stable binary relations $\rho^0 \subsetneq \rho^1 \subsetneq \cdots \subsetneq \rho^l$ on $\mathcal{A}$ such that:

1. ρ^0 is the equality relation $\{(q, q) : q \in Q\}$;

2. for each $i \in \{1, 2, \dots, l\}$, $\pi^{i-1} = \mathrm{Eq}_{\mathcal{A}}(\rho^{i-1}) \subsetneq \rho^i$ and ρ^i/π^{i-1} is a partial order on Q/π^{i-1};
3. $\pi^l = \mathrm{Eq}_{\mathcal{A}}(\rho^l)$ is the universal relation on Q.

It is clear that $\rho^0 \subsetneq \rho^1 \subsetneq \cdots \subsetneq \rho^l$ is a strictly increasing chain of stable binary relations on $\mathcal{B}$, since the state set is the same in both automata, the only letter present in $\mathcal{B}$ that is not in $\mathcal{A}$ acts as a constant, and all these relations contain the equality relation. Trivially, Condition 1 holds in $\mathcal{B}$. Condition 2 is also verified, because $\mathrm{Eq}_{\mathcal{A}}(\rho) = \mathrm{Eq}_{\mathcal{B}}(\rho)$ for any binary relation on these automata. Finally, condition 3 holds for the same reason. Which means that $\mathcal{B}$ is weakly monotonic of level l. The converse is proved in the same way. □

Theorem 4.2.5. *For every positive integer n, the automaton $\mathcal{A}_n$ is weakly monotonic of level $n-1$.*

Proof. We use induction on n to prove that $\mathcal{A}_n$ is weakly monotonic of level $n-1$. Clearly $\mathcal{A}_1$ is weakly monotonic of level 0. Suppose that for some integer $n \geq 2$, $\mathcal{A}_{n-1}$ is weakly monotonic of level $n-2$.

According to Lemma 4.2.2, the only stable partial orders on $\mathcal{A}_n$ are the equality relation, $\rho_n^1 = \pi_n^0 \cup \{(\lceil n/2 \rceil - 1, \lceil n/2 \rceil)\}$ and $\bar{\rho}_n^1 = \pi_n^0 \cup \{(\lceil n/2 \rceil, \lceil n/2 \rceil - 1)\}$. Now using Lemmas 4.2.3 and 4.2.4, we know that $\mathcal{A}_n/\pi_n^1$ and $\mathcal{A}_{n-1}$ have the same level, where $\pi_n^1 = \mathrm{Eq}(\rho_n^1) = \mathrm{Eq}(\bar{\rho}_n^1)$. But if the level of $\mathcal{A}_n/\pi_n^1$ is $n-2$ and π_n^1 is the only stable equivalence relation obtained from a stable partial order in $\mathcal{A}_n$ that is not the equality relation, then $\mathcal{A}_n$ is weakly monotonic of level $n-2+1 = n-1$.

We have established that for every positive integer n, $\mathcal{A}_n$ is a strongly connected weakly monotonic automaton of level $n-1$. □

4.3 Aperiodicity

We already know from Proposition 2.8.1 that every aperiodic automaton is weakly monotonic. But we also know from Corollary 2.8.3 that not all weakly monotonic automata are aperiodic. Let us see that the sequence of automata $\mathcal{A}_n$ is aperiodic.

Theorem 4.3.1. *For every positive integer n, the automaton $\mathcal{A}_n$ is aperiodic.*

Proof. Let T_n be the transformation monoid of the automaton $\mathcal{A}_n$ and consider the associated function $\zeta_n : A_n^* \longrightarrow T_n$. To see that $\mathcal{A}_n$ is aperiodic, we will use induction on n. The automaton $\mathcal{A}_1$ is clearly aperiodic. Moreover, for every idempotent $e \in T_1$ and every word $w \in \zeta_1^{-1}(e)$, we have $|\delta_1(Q_1, w)| = 1$, that is w is a synchronizing word. Suppose that, for some integer $n \geq 2$, $\mathcal{A}_{n-1}$ is aperiodic and, for every idempotent $\bar{e} \in T_{n-1}$ and every word $\bar{w} \in \zeta_{n-1}^{-1}(\bar{e})$, we have $|\delta_{n-1}(Q_{n-1}, \bar{w})| = 1$.

Consider the functions

$$\begin{aligned} \xi : Q_n &\longrightarrow Q_{n-1} & \theta : A_n &\longrightarrow A_{n-1}^* \\ s &\longmapsto \begin{cases} s & \text{if } s < \lceil \frac{n}{2} \rceil \\ s-1 & \text{if } s \geq \lceil \frac{n}{2} \rceil \end{cases} & a_i &\longmapsto \begin{cases} a_i & \text{if } i < \lceil \frac{n}{2} \rceil - 1 \\ a_0 a_{\lceil n/2 \rceil - 1} & \text{if } i = \lceil \frac{n}{2} \rceil - 1 \\ a_{i-1} & \text{if } i > \lceil \frac{n}{2} \rceil - 1. \end{cases} \end{aligned}$$

In the proof of Lemma 4.2.3, we presented an isomorphism $\mathcal{A}_n/\pi_n^1 \longrightarrow \mathcal{B}_{n-1}$ that was obtained from functions $\xi : Q_n/\pi_n^1 \longrightarrow Q_{n-1}$ and $\psi : A_n \longrightarrow A_{n-1} \cup \{b\}$, where π_n^1 is the kernel of the mapping ξ. Thus the pair (ξ, θ) is obtained by composing the quotient morphism $\mathcal{A}_n \longrightarrow \mathcal{A}_n/\pi_n^1$ with the isomorphism $(\xi, \psi) : \mathcal{A}_n/\pi_n^1 \longrightarrow \mathcal{B}_{n-1}$ and finally with the morphism $\mathcal{B}_{n-1} \longrightarrow \mathcal{A}_{n-1}$ that fixes the states and the letters a_i and maps the letter b to $a_0 a_{\lceil n/2 \rceil - 1}$. Hence (ξ, θ) is a morphism of automata. Now, using θ, we can define a morphism $\Theta : T_n \longrightarrow T_{n-1}$, by putting the image of an element of T_n written as a product of letters in A_n, to be the value in T_{n-1} of the product of the images of those letters by θ. All we need to check is that Θ is well defined, that is, if α and β represent the same element of T_n, then $\Theta(\alpha)$ and $\Theta(\beta)$ represent the same element of T_{n-1}. But if α and β represent the same element of T_n, then $\delta_n(q, \alpha) = \delta_n(q, \beta)$, for every $q \in Q_n$. This implies that $\delta_{n-1}(\xi(q), \theta(\alpha)) = \delta_{n-1}(\xi(q), \theta(\beta))$, for every $q \in Q_n$. Or equivalently $\delta_{n-1}(p, \theta(\alpha)) = \delta_{n-1}(p, \theta(\beta))$, for every $p \in Q_{n-1}$, because ξ is surjective. But this means that $\Theta(\alpha)$ and $\Theta(\beta)$ represent the same element of T_{n-1}.

Now, consider an idempotent $e \in T_n - \{1\}$, since Θ is a monoid morphism, we know that $\Theta(e)$ is an idempotent of $T_{n-1} - \{1\}$. Thus, according to the induction hypothesis, for $w \in \zeta_n^{-1}(e)$, we have $|\xi(\delta_n(Q_n), w))| = |\delta_{n-1}(\xi(Q_n), \theta(w))| = 1$, because $\theta(w) \in \zeta_{n-1}^{-1}(\Theta(e))$. If $|\delta_n(Q_n, w)| \neq 1$, then $\delta_n(Q_n, w) = \{\lceil n/2 \rceil - 1, \lceil n/2 \rceil\}$, because these are the only two distinct elements in Q_n that have the same image under the function ξ. Since e is an idempotent, for all $q \in Q_n$ we have $\delta_n(\delta_n(q, w), w) = \delta_n(q, w^2) = \delta_n(q, w)$, that is, w fixes all the elements in $\delta_n(Q_n, w)$. But we know that for every $a \in A$, $\delta_n(\lceil n/2 \rceil - 1, a) = \delta_n(\lceil n/2 \rceil, a)$, therefore there is no $w \in \zeta_n^{-1}(e)$ such that $\delta_n(Q_n, w) = \{\lceil n/2 \rceil - 1, \lceil n/2 \rceil\}$. Which means that $|\delta_n(Q_n, w)| = 1$.

We proved that, for every word w in A_n^* such that $\zeta_n(w)$ is an idempotent of $T_n - \{1\}$, w is a synchronizing word. Now suppose that $x \in T_n$ and $m > 1$ are such that $x^m = x$. Then x^{m-1} is an idempotent, thus every word $w \in \zeta_n^{-1}(x^{m-1})$ is a synchronizing word in the automaton $\mathcal{A}_n$. Consider the word $v \in \zeta_n^{-1}(x)$. Then wv is still a synchronizing word and it belongs to $\zeta_n^{-1}(x^{m-1}x) = \zeta_n^{-1}(x^m) = \zeta_n^{-1}(x)$, therefore x is an idempotent because for each $s \in Q_n$, $\delta_n(s, (wv)^2) = \delta_n(s, wv)$. But this means that if $x^m = x$ and $m > 1$, then $x^2 = x$, that is, T_n is aperiodic, whence $\mathcal{A}_n$ is aperiodic. $\square$

Corollary 4.3.2. *For every positive integer n, the automaton $\mathcal{A}_n$ is strongly connected, aperiodic and weakly monotonic of level $n-1$.*

Proof. It is clear that $\mathcal{A}_n$ is strongly connected for every positive integer n, because given $q \in Q_n$, $\delta_n(q, a_0) = 0$, $\delta_n(0, a_q) = q$.

The other two properties are the content of Theorems 4.3.1 and 4.2.5, respectively. $\square$

We found a family of strongly connected aperiodic automata whose level of weak monotonicity increases with the number of states. Of course, higher levels do not correspond necessarily to bigger synchronizing words. Indeed, adding a letter that acts as a constant function has no effect on the level of weak monotonicity of an automaton, while it makes synchronization quite trivial.

Note that we actually proved in Theorem 4.3.1 that the transformation monoid of each $\mathcal{A}_n$ is a nilpotent extension of a right zero semigroup with an identity element adjoined.

Chapter 5

Synchronizing subsets of states

5.1 Preliminaries

Given a synchronizing automaton $\mathcal{G} = (Q, A, \delta)$ and a subset S of Q, we denote by $\text{len}(\mathcal{G}, S)$ the length of the shortest word $w \in A^*$ that synchronizes S. Let $\text{len}(\mathcal{G}, m)$ be the maximum value of $\text{len}(\mathcal{G}, S)$, for any subset S of Q with m elements. Also, let $\text{len}(n, m)$ be the maximum value of $\text{len}(\mathcal{G}, S)$ where $\mathcal{G}$ is a synchronizing automaton with n states and S is a subset of states of $\mathcal{G}$ with m elements. The main problem in this chapter is to compute $\text{len}(n, m)$, for all positive integers n, m such that $m \leq n$. In this sense, we propose the following generalization of Černý's Conjecture.

Conjecture 5.1.1. *Given a synchronizing automaton $\mathcal{G} = (Q, A, \delta)$ with n states and a subset S of Q with m elements, there is a synchronizing word $w \in A^*$ for S, whose length is at most*

$$f(n, m) = (n-1)^2 - \left\lceil \frac{n-m}{m} \right\rceil \left(2n - m \left\lceil \frac{n}{m} \right\rceil - 1\right).$$

Note that for $m = n$, we obtain $\text{len}(n, n) = (n-1)^2$, which is the Černý Conjecture.

Given an automaton $\mathcal{G} = (Q, A, \delta)$ with n states, a cyclic order $q_0, q_1, \ldots, q_{n-1}, q_0$ on the set of states Q and a subset S of Q, a *gap* of S is an interval of $Q - S$ that is not strictly contained in any other interval of $Q - S$. Consider the set $\Omega(S)$ of all gaps of S. We denote by $\Gamma(S) \in \{0, 1, \ldots, n-1\}$ the largest size of a gap of $\Omega(S)$ and by $G(S)$ the number of gaps of size $\Gamma(S)$ in $\Omega(S)$. Note that we may consider gaps of size 0, thus between two consecutive elements of a subset S there is always a gap, eventually an empty one, and so $\Omega(S)$ has m elements.

5.2 The Černý automaton

In this section, we prove that

$$\text{len}(n, m) \geq (n-1)^2 - \left\lceil \frac{n-m}{m} \right\rceil \left(2n - m \left\lceil \frac{n}{m} \right\rceil - 1\right).$$

To do that we use similar ideas to those that allowed Černý to prove that $\mathrm{len}(n) \geq (n-1)^2$. Since the original paper by Černý [13] is only available in Slovak, our understanding of what is done there comes from [49]. Let us begin with a useful lemma.

Lemma 5.2.1. *Consider the automaton $\mathcal{G} = (Q, A, \delta)$ with n states and the cyclic order $q_0, q_1, \ldots, q_{n-1}, q_0$ on the set of states Q. Let S be a subset of Q with $|S| = m \leq n = |Q|$. If $\Gamma(S)$ is minimum among all subsets of Q with m elements, then $\Gamma(S) = \lceil n/m \rceil - 1$. If we assume additionally that $G(S)$ is the minimum value of $G(T)$ for all subsets T with m elements and minimum $\Gamma(T)$, then there are $G(S) = n - m\Gamma(S)$ gaps of size $\Gamma(S)$, and all the other gaps of S have size $\Gamma(S) - 1$.*

Proof. Since there are $n - m$ states to distribute in m gaps and we want $\Gamma(S)$ to be minimum, we have

$$\Gamma(S) = \left\lceil \frac{n-m}{m} \right\rceil = \left\lceil \frac{n}{m} \right\rceil - 1.$$

We also want to guarantee that $G(S)$ is minimum, thus the states of $Q - S$ must be distributed in the gaps of S as equitably as possible. So, if x is the quotient and y is the remainder of the division of $n - m$ by m, then there are y gaps of size $x + 1$ and all the others have size x. Hence all gaps of S have size $\Gamma(S)$ or $\Gamma(S) - 1$. Let $H(S)$ represent the number of gaps of size $\Gamma(S) - 1$. Then $G(S)\Gamma(S) + H(S)(\Gamma(S) - 1) = n - m$ and $G(S) + H(S) = m$. Thus, for $\Gamma(S)$ minimum, the minimum value of $G(S)$ is equal to $n - m\Gamma(S)$. □

To facilitate the presentation, throughout the rest of the chapter let $\gamma = \lceil n/m \rceil - 1$ and $g = n - m\gamma$. Let us see that the Černý automaton satisfies Conjecture 5.1.1.

Theorem 5.2.2. *Given a subset S of states of the Černý automaton $\mathcal{C}_n = (Q, A_{\mathcal{C}_n}, \delta_{\mathcal{C}_n})$, such that $|S| = m$, there is a word $w \in A_{\mathcal{C}_n}^*$ such that $|\delta_{\mathcal{C}_n}(S, w)| = 1$ and*

$$|w| \leq f(n, m) = (n-1)^2 - \left\lceil \frac{n-m}{m} \right\rceil \left(2n - m \left\lceil \frac{n}{m} \right\rceil - 1 \right).$$

Proof. Consider the cyclic order $0, 1, \ldots, n-1, 0$ on the state set Q of $\mathcal{C}_n$. Given a subset P of Q, such that $\Gamma(P) < n - 1$, there is a word $v \in A^*$, such that $|v| \leq n$ and $\Gamma(\delta_{\mathcal{C}_n}(P, v)) = \Gamma(P) + 1$. Indeed, if $[q, q + \Gamma(P) - 1]$ is a gap of P of size $\Gamma(P)$, then there is some $k \in \{0, 1, \ldots, n-1\}$ such that $\delta_{\mathcal{C}_n}([q, q+\Gamma(P)-1], a^k) = [n-\Gamma(P)-1, n-2]$, because a acts as a cyclic permutation of size n on Q. Hence the word $v = a^k b$ satisfies the desired condition, since $\delta_{\mathcal{C}_n}(P, v) \subseteq \delta_{\mathcal{C}_n}(Q - [n - \Gamma(P) - 1, n - 2], b) = \delta_{\mathcal{C}_n}([n - 1, n - 2 - \Gamma(P)], b) = [0, n - 2 - \Gamma(P)]$ has size $n - \Gamma(P) - 1$, thus $\delta_{\mathcal{C}_n}(P, v)$ has the gap $[n - \Gamma(P) - 1, n - 1]$ of size $\Gamma(P) + 1$.

Using this, we know that there is some word $w \in A_{\mathcal{C}_n}^*$ such that $|w| \leq n(n - \Gamma(S) - 1)$ and $\Gamma(\delta_{\mathcal{C}_n}(S, w)) = n - 1$, that is, w synchronizes S, as intended. According to Lemma 5.2.1, we have $\Gamma(S) \geq \gamma$. If $\Gamma(S) > \gamma$, then $|w| \leq n(n-\Gamma(S)-1) \leq n(n-\gamma-2) = (n-1)^2-\gamma n-1 < f(n,m)$, because $f(n,m)-((n-1)^2-\gamma n-1) = \gamma(-n+m\lceil n/m\rceil+1)+1 \geq \gamma + 1 > 0$.

To finish the proof we only need to consider the case where $\Gamma(S) = \gamma$. Using Lemma 5.2.1, we know that there are at least g gaps of size γ in S, which we will call *large gaps*. Let us see that at least one of those gaps has its first state in the interval $[(g-2)\gamma+g-1, n-\gamma-1]$. Indeed, before and after each large gap, there is at least one state of S; hence, in the interval $[n-\gamma, (g-2)\gamma+g-2]$, whose size is $(g-1)\gamma+g-1$, we can fit at most $g-1$ large gaps. Consider a gap $I = [q, q+\gamma-1]$ of S with $q \in [(g-2)\gamma+g-1, n-\gamma-1]$. There is some $k \in \{0, 1, \ldots, n-(g-1)\gamma-g\}$ such that $\delta_{\mathcal{C}_n}(I, a^k) = [n-\gamma-1, n-2]$, because $n-\gamma-1-((g-2)\gamma+g-1) = n-(g-1)\gamma-g$. Hence for the word $v = a^k b$, we have $\Gamma(\delta_{\mathcal{C}_n}(S, v)) = \gamma+1$ and $|v| \leq n-(g-1)\gamma-g+1$. Using this together with what we saw in the first paragraph of this proof, we deduce that there is a synchronizing word w for S whose size is at most $n(n-\gamma-2)+n-(g-1)\gamma-g+1$ and a simple calculation shows that this is equal to $f(n,m)$. $\square$

Now that we have shown that the Černý automaton satisfies Conjecture 5.1.1, let us see that, for some subsets of states of this automaton, that bound is the best that can be achieved.

Theorem 5.2.3. *For all positive integers n, m such that $n > 1$ and $m \leq n$, there is a subset $S_{\mathcal{C}_n}$ of the state set $Q = \{0, 1, \ldots, n-1\}$ of the Černý automaton $\mathcal{C}_n$, such that $|S_{\mathcal{C}_n}| = m$ and the shortest word $w \in A_{\mathcal{C}_n}^*$ for which $|\delta_{\mathcal{C}_n}(S_{\mathcal{C}_n}, w)| = 1$ has length equal to*

$$f(n,m) = (n-1)^2 - \left\lceil \frac{n-m}{m} \right\rceil \left(2n - m \left\lceil \frac{n}{m} \right\rceil - 1\right).$$

Proof. For $n = m$, this result simply states that the length of a shortest synchronizing word for the Černý automaton $\mathcal{C}_n$ is $(n-1)^2$. Since that was established in [13], from now on we will assume $m < n$.

Given positive integers n, m such that $n > 1$ and $m < n$, consider the set given by

$$S_{\mathcal{C}_n} = \big\{0, \gamma+1, 2\gamma+2, \ldots, (g-1)\gamma+g-1, g\gamma+g-1, (g+1)\gamma+g-1, \ldots, (m-1)\gamma+g-1\big\}.$$

Note that $S_{\mathcal{C}_n}$ is a subset of Q by the choice of γ and g.

Clearly $|S_{\mathcal{C}_n}| = m$ and we will show that it takes at least $f(n,m)$ letters to synchronize this subset. If we consider the cyclic order $0, 1, \ldots, n-1, 0$ on the state set Q of $\mathcal{C}_n$, then it is easy to see from the definition of $S_{\mathcal{C}_n}$ that $\Gamma(S_{\mathcal{C}_n}) = \gamma$. There are g gaps of size γ in $S_{\mathcal{C}_n}$, which we again call *large gaps*. Also, since $m < n$, we have $\gamma \geq 1$ and there are $h = m - g$ gaps of size $\gamma - 1$ in $S_{\mathcal{C}_n}$, which we call *small gaps*.

Let $w = a_1 a_2 \cdots a_l$, with $a_i \in A_{\mathcal{C}_n} = \{a, b\}$ for each $i \in \{1, 2, \ldots, l\}$, be a shortest word such that $|\delta_{\mathcal{C}_n}(S_{\mathcal{C}_n}, w)| = 1$ and consider the subsets of Q given by $S_i = \delta_{\mathcal{C}_n}(S_{\mathcal{C}_n}, a_1 a_2 \cdots a_i)$. If we make $S_0 = S_{\mathcal{C}_n}$, then $\delta_{\mathcal{C}_n}(S_{i-1}, a_i) = S_i$ for every $i \in \{1, 2, \ldots, l\}$. Since w synchronizes $S_{\mathcal{C}_n}$, $|S_l| = |\delta_{\mathcal{C}_n}(S_{\mathcal{C}_n}, w)| = 1$, which means that $\Gamma(S_l) = n - 1$. For every $j \in \{\gamma, \gamma + 1, \ldots, n - 1\}$, let

$$T_j = S_{\min\{i=0,1,\ldots,l \ | \ \Gamma(S_i)=j\}}.$$

That is, T_j is the first set S_i for which a record value of Γ is achieved among these subsets. Note that each T_j is well defined. Indeed, since the letter b fixes every state except $n - 1$ which is sent to 0, given any subset P, $\Gamma(\delta_{\mathcal{C}_n}(P, b))$ is either $\Gamma(P)$, $\Gamma(P) + 1$ or $\Gamma(P) - 1$. Also $\Gamma(\delta_{\mathcal{C}_n}(P, a))$ is always equal to $\Gamma(P)$, since a acts as a cyclic permutation of length n. Therefore, for every $j \in \{\gamma, \gamma + 1, \ldots, n - 1\}$, there is some $i \in \{0, 1, \ldots, l\}$ such that $\Gamma(S_i) = j$.

In order to compute the length l of w, we must determine how many letters are necessary to go from T_{j-1} to T_j. That is, for each $j \in \{\gamma + 1, \gamma + 2, \ldots, n - 1\}$ we want to calculate

$$\alpha_j = \min\{i = 0, 1, \ldots, l \mid \Gamma(S_i) = j\} - \min\{i = 0, 1, \ldots, l \mid \Gamma(S_i) = j - 1\}.$$

Suppose that the subset P of Q has a gap of size $\bar{\gamma} \geq 1$ and that it is possible to increase that gap using only one letter. Then that gap must be the interval $[n - \bar{\gamma} - 1, n - 2]$. Therefore, the subset $\delta_{\mathcal{C}_n}(P, b)$ has the gap $[n - \bar{\gamma} - 1, n - 1]$ of size $\bar{\gamma} + 1$. For every $j \in \{\gamma + 1, \gamma + 2, \ldots, n - 1\}$, the subset T_j has the interval $[n - j, n - 1]$ as its only gap of size j. This allows us to conclude that for $j \in \{\gamma + 1, \gamma + 2, \ldots, n - 2\}$, $\alpha_{j+1} = n$, because we must use $n - 1$ copies of the letter a to take T_j to a subset whose largest gap is $[n - j - 1, n - 2]$ and then use the letter b to obtain the subset T_{j+1} whose largest gap is $[n - j - 1, n - 1]$.

Let us compute $\alpha_{\gamma+1}$. We know that $S_{\mathcal{C}_n}$ has g large gaps of size γ and h small gaps of size $\gamma - 1$. If we used some word to increase one of the small gaps and then increase that gap to obtain a subset with a gap of size $\gamma + 1$, we would need more than n letters, according to what we saw above. However, to increase one of the large gaps of $S_{\mathcal{C}_n}$, all we need to do is to use enough copies of a to take $S_{\mathcal{C}_n}$ to a subset with $[n - \gamma - 1, n - 2]$ as a largest gap and then use the letter b. To place the gap $[(g-2)\gamma + g - 1, (g-1)\gamma + g - 2]$ of $S_{\mathcal{C}_n}$ in the desired position we need $n - 2 - ((g-1)\gamma + g - 2) = n - (g-1)\gamma - g$ copies of a, and all the other large gaps would take more copies of a. Hence, we have $\alpha_{\gamma+1} = n - (g-1)\gamma - g + 1 \leq n$.

To finish the proof, we need to show that $\alpha_{\gamma+1} + \alpha_{\gamma+2} + \cdots + \alpha_{n-1} = f(n, m)$, which is a simple calculation. □

With this result we have established a lower bound on the length of shortest synchronizing words for subsets of synchronizing automata. The next sections are mainly devoted to finding upper bounds of such length for certain classes of synchronizing automata.

5.3 Automata with a sink

The next proposition is a generalization of Theorem 2.4.1. It provides an upper bound on the length of synchronizing words for subsets of automata with a sink.

Proposition 5.3.1. *Suppose that the synchronizing automaton $\mathcal{G} = (Q, A, \delta)$ with n states has a sink s. Then given a nonempty subset S of Q with m elements, there is a synchronizing word w for S of length at most*

$$f_s(n, m) = nm - \frac{m(m+1)}{2}. \tag{5.3.1}$$

Proof. Let T be a nonempty subset of Q and suppose that $v \in A^*$ is a shortest word that takes some element t of T to the sink s. The path from t to s labelled by the word v contains no elements from T other than t, otherwise there would be some word shorter than v taking a state of T to s. For the same reason, the referred path does not visit any given state more than once. Therefore, the length of the word v is at most $n - |T|$.

Iterating the application of the previous paragraph, starting with $T = \delta(S, u) - \{s\}$ for some word $u \in A^*$, we can obtain a sequence with at most m words $v_m, v_{m-1}, \ldots, v_1$ such that for each i, $|v_i| \leq n - i$ and $\delta(p_i, v_i) = s$ for some $p_i \in S_i$, where $S_i = \delta(S, v_m v_{m-1} \cdots v_{i+1}) - \{s\}$ and $S_m = S - \{s\}$.

Since s is fixed by every letter in A, the word $w = v_m v_{m-1} \ldots v_1$ sends every state in S to s. Also, the length of w is at most

$$\sum_{i=m}^{1} (n - i) = nm - \frac{m(m+1)}{2},$$

which means that this word satisfies the desired conditions. □

Our next result shows that the bound given by Proposition 5.3.1 is tight whenever $m > 1$. Obviously, for $m = 1$ the empty word can be taken as a synchronizing word for S and its length is $0 < nm - \frac{m(m+1)}{2} = n - 1$. For $m > 1$, we will use the Rystsov automaton $\mathcal{R}_n$, as well as an adaptation of Rystsov's argument, to show that $nm - \frac{m(m+1)}{2}$ is a lower bound on the length of shortest words that synchronize subsets of automata with a sink.

Proposition 5.3.2. *For all positive integers n, m such that $n > 1$ and $1 < m \leq n$, there is a subset $S_{\mathcal{R}_n}$ of the state set $Q = \{0, 1, \ldots, n-1\}$ of the Rystsov automaton $\mathcal{R}_n$, such that the shortest word $w \in A_{\mathcal{R}_n}$ for which $|\delta_{\mathcal{R}_n}(S_{\mathcal{R}_n}, w)| = 1$ has length $f_s(n, m) = nm - \frac{m(m+1)}{2}$.*

Proof. Consider the subset $S_{\mathcal{R}_n} = \{n - m, n - m + 1, \ldots, n - 1\}$ of the state set Q of $\mathcal{R}_n$. The only way to synchronize $S_{\mathcal{R}_n}$ is to send every state in it to 0, because 0 is a sink and the only state such that $|\delta_{\mathcal{R}_n}^{-1}(0, a)| > 1$ for some letter a. Given any subset T of Q, let $\mathrm{sum}(T)$ be the integer sum of all the elements of T. Then, for every $a \in A_{\mathcal{R}_n}$, we have $\mathrm{sum}(\delta(T, a)) \geq \mathrm{sum}(T) - 1$, because there is at most one state t in T such that $\delta(t, a) < t$ and in that case we have $\delta(t, a) = t - 1$. By induction, for every word v with l letters we have $\mathrm{sum}(\delta(T, v)) \geq \mathrm{sum}(T) - l$. Now, suppose that the word w of length l synchronizes $S_{\mathcal{R}_n}$, then we have $0 = \mathrm{sum}(\delta_{\mathcal{R}_n}(S_{\mathcal{R}_n}, w)) \geq \mathrm{sum}(S_{\mathcal{R}_n}) - l$, which is equivalent to $l \geq \mathrm{sum}(S_{\mathcal{R}_n})$. Since

$$\mathrm{sum}(S_{\mathcal{R}_n}) = \sum_{i=n-m}^{n-1} i = nm - \frac{m(m+1)}{2},$$

using Proposition 5.3.1, it is clear that we need exactly $nm - \frac{m(m+1)}{2}$ letters to synchronize $S_{\mathcal{R}_n}$. □

We have a tight upper bound for the length of shortest words that synchronize subsets of states of automata with a sink. But in order to see that this class of automata satisfies Conjecture 5.1.1 we need to check that for every n, m satisfying the appropriate conditions $f_s(n, m) \leq f(n, m)$. That is the content of the final lemma in this section. But before that, let us establish a technical result that will be useful to deal with the ceilings of quotients in $f(n, m)$.

Lemma 5.3.3. *Given positive integers x, y, we have $y \left\lceil \frac{x}{y} \right\rceil = x + y - \varepsilon$ for a unique $\varepsilon \in \{1, 2, \ldots, y\}$.*

Proof. Let us write $x = yq + \bar{\varepsilon}$, with q an nonnegative integer and $\bar{\varepsilon} \in \{0, 1, \ldots, y - 1\}$. Then,

$$y \left\lceil \frac{x}{y} \right\rceil = y \left\lceil \frac{yq + \bar{\varepsilon}}{y} \right\rceil = yq + y \left\lceil \frac{\bar{\varepsilon}}{y} \right\rceil =$$
$$= \begin{cases} yq + y & \text{if } \bar{\varepsilon} > 0 \\ yq & \text{if } \bar{\varepsilon} = 0 \end{cases} = \begin{cases} x + y - \bar{\varepsilon} & \text{if } \bar{\varepsilon} > 0 \\ x + y - y & \text{if } \bar{\varepsilon} = 0. \end{cases}$$

If we make

$$\varepsilon = \begin{cases} \bar{\varepsilon} & \text{if } \bar{\varepsilon} > 0 \\ y & \text{if } \bar{\varepsilon} = 0 \end{cases}$$

we have the desired result. □

We will also need the following result whose proof is elementary.

Lemma 5.3.4. *Consider the function $\hat{f}(x) = x(x - m - 1)$ where x is a real number. We have* $\min\{\hat{f}(x) : 1 \leq x \leq m\} = \hat{f}\left(\frac{m+1}{2}\right) = -\left(\frac{m+1}{2}\right)^2$ *and* $\max\{\hat{f}(x) : 1 \leq x \leq m\} = \hat{f}(1) = \hat{f}(m) = -m$.

Lemma 5.3.5. *For every pair of integers (n, m) such that $n > 1$ and $1 < m \leq n$, the inequality*

$$nm - \frac{m(m+1)}{2} \leq (n-1)^2 - \left\lceil \frac{n-m}{m} \right\rceil \left(2n - m\left\lceil \frac{n}{m} \right\rceil - 1\right) \qquad (5.3.2)$$

holds.

Proof. For $m = n$ we have $f_s(n, m) = \frac{n(n-1)}{2}$ and $f(n, m) = (n-1)^2$, so (5.3.2) is equivalent to $(n-1)(n-1-n/2) \geq 0$, which is obviously true since $n \geq 2$. Note also that for $n = 3$ and $m = 2$ we have $f(n, m) = 3 = f_s(n, m)$. So, from now on we assume that $1 < m < n$ and $n > 3$.

Since $m > 0$, by multiplying by $2m$, inequality (5.3.2) is equivalent to

$$2m(n-1)^2 - 2\left(m\left\lceil \frac{n}{m} \right\rceil - m\right)\left(2n - m\left\lceil \frac{n}{m} \right\rceil - 1\right) - 2nm^2 + m^2(m+1) \geq 0.$$

Using Lemma 5.3.3, we may write $m\left\lceil \frac{n}{m} \right\rceil = n + m - \varepsilon$, for some $\varepsilon \in \{1, 2, \ldots, m\}$. Therefore, it is enough to prove that

$$2m(n-1)^2 - 2(n + m - \varepsilon - m)(2n - n - m + \varepsilon - 1) - 2nm^2 + m^2(m+1) \geq 0,$$

or expanding,

$$2n^2m - 2n^2 - 2nm^2 - 2nm + 2n + m^3 + m^2 + 2m + 2\varepsilon^2 - 2m\varepsilon - 2\varepsilon \geq 0,$$

for every $\varepsilon \in \{1, 2, \ldots, m\}$.

According to Lemma 5.3.4 the minimum of $\hat{f}(\varepsilon)$, for $1 \leq \varepsilon \leq m$, is $-\left(\frac{m+1}{2}\right)^2$. Therefore, the minimum of $2\varepsilon^2 - 2m\varepsilon - 2\varepsilon = 2\hat{f}(\varepsilon)$ is $-\frac{(m+1)^2}{2}$ and defining

$$P(n, m) = 2n^2m - 2n^2 - 2nm^2 - 2nm + 2n + m^3 + m^2 + 2m - \frac{(m+1)^2}{2},$$

in order to obtain (5.3.2), we can simply establish the inequality $P(n,m) \geq 0$, which we will do using induction on n.

Let us start with the case $n = 4$. We have $P(4,2) = 7/2$ and $P(4,3) = 10$, therefore $P(4,m) > 0$ for every $1 < m < 4$. Suppose now that $P(n,m) \geq 0$ for some n and every $1 < m < n$. We have $P(n+1,m) = P(n,m) + 4n(m-1) - 2m^2$. Since $n > m$, $4n(m-1) - 2m^2 \geq 4(m+1)(m-1) - 2m^2 = 2(m^2 - 2)$, which is non negative for every $m > 1$. Thus $P(n+1,m) \geq 0$ for every $1 < m < n$. □

From Proposition 5.3.1 and Lemma 5.3.5 the following result is obtained directly.

Corollary 5.3.6. *Automata with a sink satisfy Conjecture 5.1.1.*

This result will be useful in the next section.

5.4 Strongly connected automata

One of the objectives of this section is to show that if Conjecture 5.1.1 is established for strongly connected automata, then the general case is solved as well. The following result was inspired by Proposition 2.4.2.

Proposition 5.4.1. *Let* $\mathbf{C}$ *be a class of synchronizing automata closed for subautomata and quotients. Denote by* $\mathbf{C}_n$ *the class of all automata in* $\mathbf{C}$ *with* n *states. Consider a function* $f : \mathbb{Z}^+ \times \mathbb{Z}^+ \longrightarrow \mathbb{N}$ *such that, for all integers* n, m, k, l *with* $n > 1$*,* $1 \leq m, k \leq n$ *and* $\max\{0, m-n+k\} \leq l < \min\{m, k+1\}$,

$$f(n,m) \geq f(n-k+1, m-l) + f(k, \min\{m,k\}) \tag{5.4.1}$$

Suppose that for every positive integer n *and for every automaton* $\mathcal{G} = (Q, A, \delta)$ *in* $\mathbf{C}_n$ *which either is strongly connected or has a sink* $\operatorname{len}(\mathcal{G}, m) \leq f(n,m)$*. Then given any automaton* $\mathcal{G} = (Q, A, \delta)$ *in* $\mathbf{C}_n$*, we have* $\operatorname{len}(\mathcal{G}, m) \leq f(n,m)$*.*

Proof. Let $\mathcal{G} = (Q, A, \delta)$ be any automaton in $\mathbf{C}_n$. Suppose that the subset S of Q has $m \geq 1$ elements and consider the subset T of Q of all states in which the automaton $\mathcal{G}$ can be synchronized. Let $k = |T| \geq 1$ and $l = |T \cap S|$. Note that this implies that $0 \leq l \leq k$, since $T \cap S \subseteq T$, and that $m - l \leq n - k$, since $S - T \subseteq Q - T$.

If we restrict the transition function δ to T, we obtain a subautomaton of $\mathcal{G}$, because if $s \in T$ there is some word w such that $\delta(Q, w) = s$, but given $a \in A$, wa is also a synchronizing word, which means that $\delta(s, a) \in T$. The subautomaton (T, A, δ) is synchronizing, strongly connected and belongs to $\mathbf{C}_n$, therefore any subset P of T such that $|P| = \min\{m,k\}$ can be synchronized by a word v of size $f(k, \min\{m,k\})$. Note that if $l = m$ then the subset S is contained in T, thus it can be synchronized by a word w of size $f(k,m)$ and we have the desired result since $f(n,m) \geq f(k,m)$. Hence we will assume $l < m$.

We may consider a congruence ρ of the automaton $\mathcal{G}$ given by the $n-k+1$ classes consisting of T and the singletons of $Q-T$. Then, the automaton $\mathcal{G}/\rho$ is a synchronizing automaton with a sink (the class T) that belongs to $\mathbf{C}_n$. Thus, there is a word u of length $f(n-k+1, m-l)$ that synchronizes the subset $(S-T)/\rho$ of Q/ρ.

Let $\delta(S,u) = P$, then P is a subset of T with at most $\min\{m,k\}$ elements, therefore it can be synchronized by a word v of size $f(k, \min\{m,k\})$. Thus, the word $w = uv \in A^*$ has length $f(n-k+1, m-l) + f(k, \min\{m,k\}) \leq f(n,m)$ and synchronizes the set S. $\square$

The next lemma is necessary in order to proceed.

Lemma 5.4.2. *For each positive integer n, the function $\bar{f}$, that to $m \leq n$ associates*

$$\bar{f}(m) = (n-1)^2 - \left\lceil \frac{n-m}{m} \right\rceil \left(2n - m\left\lceil \frac{n}{m} \right\rceil - 1\right),$$

is nondecreasing.

Proof. Suppose that m_1 and m_2 are positive integers such that $m_1 \leq m_2 \leq n$. Consider the Černý automaton $\mathcal{C}_n$ with n states. Using Theorem 5.2.3, let S_1 be a subset of states of $\mathcal{C}_n$ such that $|S_1| = m_1$ and the shortest synchronizing word for S_1 has length $\bar{f}(m_1)$. Consider a subset of states S_2 such that $S_1 \subseteq S_2$ and $|S_2| = m_2$. According to Theorem 5.2.2, there is a word w_2 of length at most $\bar{f}(m_2)$ such that $|\delta(S_2, w_2)| = 1$. Since $S_1 \subseteq S_2$, we have $|\delta(S_1, w_2)| = 1$. But the length of the shortest synchronizing word for S_1 is $\bar{f}(m_1)$, thus we have $\bar{f}(m_1) \leq |w_2| \leq \bar{f}(m_2)$. $\square$

To apply Proposition 5.4.1 to the class of all synchronizing automata and the bound from Conjecture 5.1.1, we need the following result.

Lemma 5.4.3. *For all integers n, m, k, l with $n > 1$, $1 \leq m, k \leq n$ and $0, m-n+k \leq l < m, k+1$, the function*

$$f(n,m) = (n-1)^2 - \left\lceil \frac{n-m}{m} \right\rceil \left(2n - m\left\lceil \frac{n}{m} \right\rceil - 1\right)$$

satisfies condition (5.4.1).

Proof. From Lemma 5.4.2, we know that $f(n-k+1, m-l) \le f(n-k+1, m)$ for every $l \in \{0, 1, \dots, m-1\}$. Thus we only need to consider the case $l = 0$. Also, we will assume $1 < m, k < n$ because the result is trivial otherwise.

Using Lemma 5.3.3, let $\varepsilon_1, \varepsilon_2, \varepsilon_3 \in \{1, 2, \dots, m\}$ be such that $m\left\lceil \frac{n}{m} \right\rceil = n+m-\varepsilon_1$, $m\left\lceil \frac{n-k+1}{m} \right\rceil = n-k+1+m-\varepsilon_2$ and $m\left\lceil \frac{k}{m} \right\rceil = k+m-\varepsilon_3$.

For $k \le m$, we want to prove that

$$f(n,m) - f(n-k+1,m) - f(k,k) \ge 0, \tag{5.4.2}$$

which is equivalent to showing that

$$m\big(f(n,m) - f(n-k+1,m) - f(k,k)\big) \ge 0. \tag{5.4.3}$$

Using the definition of the function f as well as the equalities from the previous paragraph, we may write (5.4.3) in the form

$$m\big((n-1)^2-(n-k)^2-(k-1)^2\big)-(n-\varepsilon_1)(n-m+\varepsilon_1-1)+(n-k-\varepsilon_2+1)(n-m-k+\varepsilon_2) \ge 0.$$

Some simple computations lead us to the equivalent inequality

$$m(2nk-2k^2-2n+2k)-n(n-m-1)+(n-k+1)(n-m-k)+\varepsilon_1(\varepsilon_1-m-1)-\varepsilon_2(\varepsilon_2-m-1) \ge 0. \tag{5.4.4}$$

According to Lemma 5.3.4, we have $\varepsilon_1(\varepsilon_1-m-1) \ge -\left(\frac{m+1}{2}\right)^2$ and $\varepsilon_2(\varepsilon_2-m-1) \le -m$. Hence to prove that (5.4.4) holds it is enough to establish the inequality

$$m(2nk-2k^2-2n+2k) - n(n-m-1) + (n-k+1)(n-m-k) - \left(\frac{m+1}{2}\right)^2 + m \ge 0,$$

which is equivalent to

$$2n - 2nm - \left(\frac{m+1}{2}\right)^2 - (2m-1)k^2 + (2nm-2n+3m-1)k \ge 0. \tag{5.4.5}$$

Consider the function $\tilde{f}(x) = -(2m-1)x^2 + (2nm-2n+3m-1)x$, where x is a real number. Since $-(2m-1) < 0$, for every $m > 1$, this is a quadratic function whose graph is concave down, hence $\min\{\tilde{f}(x) : 2 \le x \le m\} = \min\{\tilde{f}(2), \tilde{f}(m)\} \ge \min\{\tilde{f}(3/2), \tilde{f}(m)\}$. The roots of $\tilde{f}$ are $x_1 = 0$ and $x_2 = \frac{2nm-2n+3m-1}{2m-1}$ and we will see that $x_1 < 3/2 \le m < x_2$. Indeed, we have

$$x_2 - m = \frac{2nm-2n-2m^2+4m-1}{2m-1},$$

thus in order to prove that $x_2 > m$, it is enough to check that $2nm-2n-2m^2+4m-1 > 0$. This is equivalent to $2n(m-1) - 2m(m-2) - 1 > 0$, which is easy to see using $n > m$. In order to show that $\tilde{f}(3/2) < \tilde{f}(m)$, we will prove that $x_2 - m > 3/2 - x_1$. We have

$$x_2 - m - \frac{3}{2} = \frac{4n(m-1) - 2m(2m-1) + 1}{4m-2},$$

therefore it suffices to establish that $4n(m-1) - 2m(2m-1) + 1 > 0$, which is easy to do using $n \geq m+1$. This allows us to conclude that $\min\{\tilde{f}(x) : 2 \leq x \leq m\} \geq \tilde{f}(3/2) = 3nm - 3n + 3/4$. Hence, to obtain (5.4.5), all we need to do is to establish the inequality

$$2n - 2nm - \left(\frac{m+1}{2}\right)^2 + 3nm - 3n + 3/4 \geq 0,$$

which is equivalent to

$$n(m-1) - \left(\frac{m+1}{2}\right)^2 + 3/4 \geq 0. \tag{5.4.6}$$

Finally all that is left to observe is that

$$0 < \frac{m+1}{2} \leq m-1 < n, \text{ as long as } 3 \leq m < n. \tag{5.4.7}$$

For $m = 2$, n must be at least 3 and, by direct calculation, we see that (5.4.6) is valid in this case. Hence, condition (5.4.6) is satisfied for all values of n, m such that $1 < m < n$, which means that the inequality (5.4.2) holds.

For $k > m$, we must have $n > m+1$, since $n > k > m$, and we want to prove that

$$f(n,m) - f(n-k+1,m) - f(k,m) \geq 0, \tag{5.4.8}$$

which is equivalent to showing that

$$m\big(f(n,m) - f(n-k+1,m) - f(k,m)\big) \geq 0. \tag{5.4.9}$$

Using the definition of the function f as well as the equalities from the second paragraph of this proof, we see that (5.4.9) is equivalent to

$$\begin{aligned} m\big((n-1)^2 - (n-k)^2 - (k-1)^2\big) - (n-\varepsilon_1)(n-m+\varepsilon_1-1) \\ +(n-k-\varepsilon_2+1)(n-m-k+\varepsilon_2) + (k-\varepsilon_3)(k-m+\varepsilon_3-1) \geq 0. \end{aligned}$$

Some simple computations lead us to the equivalent inequality

$$\begin{aligned} m(2nk - 2k^2 - 2n + 2k) - n(n-m-1) + (n-k+1)(n-m-k) \\ +k(k-m-1) + \varepsilon_1(\varepsilon_1 - m - 1) - \varepsilon_2(\varepsilon_2 - m - 1) - \varepsilon_3(\varepsilon_3 - m - 1) \geq 0. \end{aligned} \tag{5.4.10}$$

Using what we saw above for the function $\tilde{f}$ we see that in order to obtain (5.4.10) it is enough to establish the inequality

$$2nmk - 2mk^2 - 2nm + 2mk + 2n - 2nk + mk + 2k^2 - m - 2k - \left(\frac{m+1}{2}\right)^2 + m + m \geq 0,$$

which is equivalent to

$$2n - 2nm + m - \left(\frac{m+1}{2}\right)^2 - 2(m-1)k^2 + 2(nm - n + m - 1)k \geq 0. \tag{5.4.11}$$

Consider the function $\hat{f}(x) = -2(m-1)x^2 + 2(nm - n + m - 1)x$, where x is a real number. Since $-2(m-1) < 0$, for every $m > 1$, this is a quadratic function whose graph is concave down, hence $\min\{\hat{f}(x) : m+1 \leq x \leq n-1\} = \min\{\hat{f}(m+1), \hat{f}(n-1)\}$. The roots of $\hat{f}$ are $x_1 = 0$ and $x_2 = \frac{nm-n+m-1}{m-1} = n+1$, with $x_1 < m+1 \leq n-1 < x_2$. Plus, we have $m + 1 - x_1 \geq 3 > 2 = x_2 - (n-1)$. Therefore, using the symmetry of the quadratic function we see that $\min\{\hat{f}(x) : m+1 \leq x \leq n-1\} = \hat{f}(n-1) = 4nm - 4m - 4n + 4$. So, to obtain (5.4.11), all we need to do is to establish the inequality

$$2n - 2nm + m - \left(\frac{m+1}{2}\right)^2 + 4nm - 4m - 4n + 4 \geq 0,$$

which is equivalent to

$$(2n-3)(m-1) - \left(\frac{m+1}{2}\right)^2 + 1 \geq 0. \tag{5.4.12}$$

Finally, using the inequalities in (5.4.7) as well as $m - 1 \leq 2n - 3$, we obtain the desired result for $3 \leq m < n$. For $m = 2$, n must be at least 4 and it is easy to see that (5.4.12) is valid. Hence, condition (5.4.12) is satisfied for all n, m such that $1 < m < n$, which implies that the inequality (5.4.8) holds. □

Now we can establish the main result in this section.

Theorem 5.4.4. *Suppose that Conjecture 5.1.1 is valid for all strongly connected automata. Then it holds for all automata.*

Proof. Using Proposition 5.4.1 together with Lemma 5.4.3, we obtain that in order to establish Conjecture 5.1.1 in the general case, it is enough to do so for strongly connected automata and automata with a sink. From Corollary 5.3.6, we know that automata with a sink satisfy Conjecture 5.1.1, therefore strongly connected automata are all that is left to study. □

In the following sections, we take a closer look at some classes of strongly connected automata that contain known families of automata which are hard to synchronize.

5.5 Circular automata

In this section, we use Theorem 2.5.1 to provide an upper bound on the length of synchronizing words for subsets of synchronizing circular automata with n states. Recall that when dealing with circular automata, the letter a always acts as a circular permutation.

Theorem 5.5.1. *Let $\mathcal{G} = (Q, A, \delta)$ be a synchronizing circular automaton with n states. Then for every nonempty subset S of Q with m elements, there is a word $w \in A^*$ such that $|\delta(S, w)| = 1$ and $|w|$ is at most*

$$f_c(n, m) = (n-1)^2 - \left\lceil \frac{n-m}{m} \right\rceil (n-m).$$

Proof. Note that since the automaton $\mathcal{G}$ is synchronizing, there must be some state $s \in Q$ and some letter $b \in A$ such that $|\delta^{-1}(\{s\}, b)| \geq 2$. Using this together with Theorem 2.5.1, we know that for every $k \in \{0, 1, \ldots, n-2\}$ there is some word $v_k \in A^*$ such that $|\delta^{-1}(\{s\}, v_k)| \geq n-k$ and $|v_k| \leq 1 + n(n-2-k)$. The case $k = 0$ was used by Dubuc to obtain Theorem 2.5.2 which is the same as our result for $m = n$.

For $m < n$, consider the subset $T = \delta^{-1}(\{s\}, v_\gamma)$ of Q. Then, we have $|Q - T| \leq n - (n - \gamma) = \gamma$. For each $i \in \{0, 1, \ldots, n-1\}$, let $T_i = \delta^{-1}(T, a^i)$. Since a cyclically permutes all states in Q, a^i acts as a bijection on Q. Thus, we have $|T_i| = |T|$ and so $|Q - T_i| \leq \gamma$ for every i.

For every $i \in \{0, 1, \ldots, n-1\}$ such that $S \nsubseteq T_i$, we have $S \cap (Q - \delta^{-1}(T, a^i)) \neq \varnothing$, whence there are states $s_i, q_i \in Q$ such that $s_i \in S$, $q_i \notin T$ and $\delta^{-1}(\{q_i\}, a^i) = \{s_i\}$. Suppose that $i, j \in \{0, 1, \ldots, n-1\}$ are such that $i \neq j$, $S \nsubseteq T_i$ and $S \nsubseteq T_j$. Suppose also that $q \in S$ and $q_i, q_j \in Q$ are such that $\delta^{-1}(\{q_i\}, a^i) = \{q\} = \delta^{-1}(\{q_j\}, a^j)$. Clearly, since $i \neq j$ and $i, j \in \{0, 1, \ldots, n-1\}$, we must have $q_i \neq q_j$. Thus, the function that to each $i \in \{0, 1, \ldots, n-1\}$ such that $S \nsubseteq T_i$ associates the pair (s_i, q_i) is injective. This implies that there are at most $|S| \cdot |Q - T| = m\gamma$ indices $i \in \{0, 1, \ldots, n-1\}$ such that $S \nsubseteq T_i$.

According to Lemma 5.3.3, we have $m\gamma = n - \varepsilon$ for some $\varepsilon \in \{1, 2, \ldots, m\}$. Therefore $m\gamma \leq n-1$ and so there must be some $j \in \{0, 1, \ldots, n-1\}$ such that $S \subseteq T_j$ and $j \leq m\gamma$. Let $w = a^j v_\gamma$, then $\delta^{-1}(s, w) = \delta^{-1}(\delta^{-1}(s, v_\gamma), a^j) = \delta^{-1}(T, a^j) = T_j \supseteq S$ and so $|\delta(S, w)| = 1$. Also, $|w| \leq 1 + n(n-2-\gamma) + m\gamma = (n-1)^2 - \left\lceil \frac{n-m}{m} \right\rceil (n-m)$ and our result is proved. $\square$

Let us compare the bound from the previous theorem with the one from Conjecture 5.1.1.

We have

$$f_c(n,m) - f(n,m) = \gamma\left(n - m\left(\left\lceil \frac{n}{m}\right\rceil - 1\right) - 1\right) = \gamma\left(n - m\gamma - 1\right).$$

Using Lemma 5.3.3, we may write $m\gamma = n - \varepsilon$, for some $\varepsilon \in \{1, 2, \dots, m\}$, hence $0 \leq f_c(n,m) - f(n,m) = \gamma(\varepsilon - 1) \leq \gamma(m-1) \leq n - \gamma - 1$. Thus, the bound in Conjecture 5.1.1 is never greater than the bound we just obtained for circular automata (although the difference between them is at most a linear function of n). This means that Theorem 5.5.1 does not quite establish Conjecture 5.1.1 for the class of circular automata. In the following section, we introduce a further condition which allows us to prove Conjecture 5.1.1 in Section 5.7 for a special class of circular automata.

5.6 Weakly oriented automata

In this section, we establish the Černý Conjecture for weakly oriented automata, that is, we obtain a generalization of Theorem 2.6.2, with a much simpler proof.

Recall that, given an integer α, we denote by $\underline{\alpha} \in \{0, 1, \dots, n-1\}$ the remainder of the integer division of α by n.

Given a cyclic order, if $\delta^{-1}(I, b)$ is an interval for every letter $b \in A$ and every interval I of Q, then we say that the automaton $\mathcal{G} = (Q, A, \delta)$ is *weakly oriented*, that the intervals are *preserved* by δ^{-1}, and that the cyclic order is *weakly preserved*. Note that this definition is equivalent to saying that for every interval I and every word $w \in A^*$, $\delta^{-1}(I, w)$ is an interval. Lemma 2.6.1 states that every oriented automaton is weakly oriented.

To show that the reverse implication is not true, we claim that for each natural $n \geq 3$, the automaton $\mathcal{WO}_n = (Q, \{b\}, \delta_{\mathcal{WO}_n})$, represented in Figure 5.6.1, such that $Q = \{0, 1, \dots, n-1\}$ and $\delta_{\mathcal{WO}_n}(p, b) = \underline{n - p + 2}$, is weakly oriented but not oriented. Note that given $q \in Q$, we have $\delta^{-1}_{\mathcal{WO}_n}(q, b) = \underline{n - q + 2}$.

Consider the abelian group of integers $\mathbb{Z}$ under addition. Equipped with its natural linear order, it is a linearly ordered group, in the sense that the order is preserved by addition. We may think of Q as the cyclic group $\mathbb{Z}/n\mathbb{Z}$. Together with the cyclic order $0, 1, \dots, n-1, 0$ induced by the linear order of $\mathbb{Z}$, we obtain a cyclically ordered group. Given $\alpha, \hat{\alpha}, \tilde{\alpha} \in \mathbb{Z}$, in Q we have $\langle \underline{\alpha}, \underline{\hat{\alpha}}, \underline{\tilde{\alpha}} \rangle$ if and only if one of the following conditions is verified:

(i) $\underline{\alpha} \leq \underline{\hat{\alpha}} \leq \underline{\tilde{\alpha}}$;
(ii) $\underline{\tilde{\alpha}} \leq \underline{\alpha} \leq \underline{\hat{\alpha}}$;
(iii) $\underline{\hat{\alpha}} \leq \underline{\tilde{\alpha}} \leq \underline{\alpha}$.

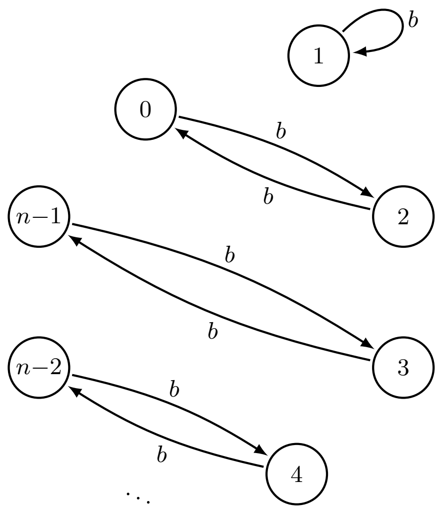

Figure 5.6.1: Automaton $\mathcal{WO}_n$

We will assume that we are in Case (i), because the other cases are analogous. Since the linear order in $\mathbb{Z}$ is preserved by addition, we have $n-\underline{\tilde{\alpha}}+2 < n-\underline{\hat{\alpha}}+2 < n-\underline{\alpha}+2$. Hence in Q, we have $\langle \underline{n-\tilde{\alpha}+2}, \underline{n-\hat{\alpha}+2}, \underline{n-\alpha+2} \rangle$, that is, $\langle \delta^{-1}_{\mathcal{WO}_n}(\underline{\tilde{\alpha}}, b), \delta^{-1}_{\mathcal{WO}_n}(\underline{\hat{\alpha}}, b), \delta^{-1}_{\mathcal{WO}_n}(\underline{\alpha}, b) \rangle$.

Given an interval $I = [p, \bar{p}] \subseteq Q$, we have $\delta^{-1}_{\mathcal{WO}_n}(I, b) = \{\delta^{-1}_{\mathcal{WO}_n}(q, b) : \langle p, q, \bar{p} \rangle\}$. According to what we saw above $\langle p, q, \bar{p} \rangle$ is equivalent to $\langle \delta^{-1}_{\mathcal{WO}_n}(\bar{p}, b), \delta^{-1}_{\mathcal{WO}_n}(q, b), \delta^{-1}_{\mathcal{WO}_n}(p, b) \rangle$, thus $\delta^{-1}_{\mathcal{WO}_n}(I, b)$ is equal to the interval $[\delta^{-1}_{\mathcal{WO}_n}(\bar{p}, b), \delta^{-1}_{\mathcal{WO}_n}(p, b)]$ and $\mathcal{WO}_n$ is weakly oriented.

Now consider any cyclic order in Q. Since it is a total order, we must have $\langle 0, 1, 2 \rangle$ or $\langle 2, 1, 0 \rangle$. Let us assume the latter, since they are analogous. If the cyclic order were preserved by the transition function $\delta_{\mathcal{WO}_n}$, then we would have $\langle \delta_{\mathcal{WO}_n}(0, b), \delta_{\mathcal{WO}_n}(1, b), \delta_{\mathcal{WO}_n}(2, b) \rangle$, that is $\langle 2, 1, 0 \rangle$, which contradicts the asymmetry condition. Thus $\mathcal{WO}_n$ is not oriented.

Theorem 5.6.1. *Given a weakly oriented synchronizing automaton $\mathcal{G} = (Q, A, \delta)$ with n states, the shortest synchronizing word for $\mathcal{G}$ has at most $(n-1)^2$ letters.*

Proof. Let $w = a_1 a_2 \dots a_l$ be a shortest synchronizing word for $\mathcal{G}$ and consider the state $s \in Q$ such that $\delta(Q, w) = \{s\}$. We will consider the sets $I_i = \delta^{-1}(\{s\}, a_i a_{i+1} \dots a_l)$. Since $\mathcal{G}$ is weakly oriented and $\{s\} = [s, s]$ is an interval, each I_i is an interval as well. Also, we have $I_1 = Q$, since the word w synchronizes the state set Q in s.

Given $i, j \in \{1, 2, \dots, l\}$ if $i \neq j$, then $I_i \neq I_j$. Otherwise, assuming without loss of generality that $i < j$, the word $v = a_1 a_2 \dots a_{i-1} a_j a_{j+1} \dots a_l$ is shorter than w and yet

$$\delta^{-1}(\{s\}, v) = \delta^{-1}(\delta^{-1}(\{s\}, a_j a_{j+1} \dots a_l), a_1 a_2 \dots a_{i-1})$$
$$= \delta^{-1}(I_j, a_1 a_2 \dots a_{i-1}) = \delta^{-1}(I_i, a_1 a_2 \dots a_{i-1}) = Q,$$

that is, v synchronizes the automaton $\mathcal{G}$, which is absurd, since the word w is a shortest synchronizing word. For the same reason, in the sequence $I_1, I_2, \ldots, I_l$ only the interval $I_1 = Q$ has n elements and no interval has size 1.

Now, an interval $I = [p, q]$ is completely determined by its size and its *first element* p. Thus, for each $m \in \{2, 3, \ldots, n-1\}$, there are n distinct intervals of size m. Therefore, the sequence $I_1, I_2, \ldots, I_l$ has at most n intervals of each size $m \in \{2, 3, \ldots, n-1\}$ plus one element of size n. That is, we have $l \leq n(n-2) + 1 = (n-1)^2$. □

M. V. Volkov has brought to the author's attention that Černý's Conjecture was established for weakly oriented automata in [7]. Indeed, in that article, the notion of weakly monotonic is used to refer to automata such that the action of any given letter either preserves or reverses some fixed cyclic order. The authors prove that such automata satisfy the Černý Conjecture, by closely following the arguments used by Eppstein to obtain the same result for oriented automata. Therefore our result establishing the Černý Conjecture for weakly oriented automata is not new. However, the proof is new and simpler than those of Eppstein or Ananichev and Volkov. Let us see that given a weakly oriented automaton, the action of each letter either preserves or reverses a fixed cyclic order. The reverse implication was proved in [7]. Therefore these notions of weakly oriented are one and the same.

Lemma 5.6.2. *Consider a weakly oriented automaton $\mathcal{G} = (Q, A, \delta)$, two states $p, q \in Q$ and a letter $a \in A$, such that the sets $\delta^{-1}(\{p\}, a)$, $\delta^{-1}(\{q\}, a)$ are nonempty. Then there are states $\bar{p}$ and $\bar{q} \in Q$ such that $\delta(\bar{p}, a) = p$, $\delta(\bar{q}, a) = q$ and $\delta^{-1}([p, q], a) = [\bar{p}, \bar{q}]$ or $\delta^{-1}([p, q], a) = [\bar{q}, \bar{p}]$.*

Proof. We use induction on the number of states m in $[p, q]$.

If $m = 1$, then $p = q$ and since $\delta^{-1}(\{p\}, a)$ is an interval, there are states $\tilde{p}, \hat{p} \in Q$ such that $\delta^{-1}(\{p\}, a) = [\tilde{p}, \hat{p}]$. Thus our result is established for $\bar{p} = \tilde{p}$ and $\bar{q} = \hat{p}$.

Now suppose that the result is valid for intervals with $m-1$ states. Then $\delta^{-1}([p, \underline{q-1}], a) = [\bar{p}, \overline{\underline{q-1}}]$ or $\delta^{-1}([p, \underline{q-1}], a) = [\overline{\underline{q-1}}, \bar{p}]$ for some $\bar{p}, \overline{\underline{q-1}} \in Q$ such that $\delta(\bar{p}, a) = p$ and $\delta(\overline{\underline{q-1}}) = \underline{q-1}$. Let $\delta^{-1}(\{q\}, a) = [\tilde{q}, \hat{q}]$. If $\delta^{-1}([p, \underline{q-1}], a) = [\bar{p}, \overline{\underline{q-1}}]$, then since $\delta^{-1}([\underline{q-1}, q], a)$ is an interval and $\underline{\overline{\underline{q-1}} - 1} \notin \delta^{-1}(\{q\}, a)$, we have $\delta^{-1}([\underline{q-1}, q], a) = [\widetilde{\underline{q-1}}, \hat{q}]$ for some $\widetilde{\underline{q-1}} \in \delta^{-1}(\{\underline{q-1}\}, a)$. Therefore, we obtain $\delta^{-1}([p, q], a) = [\bar{p}, \hat{q}]$ and our result is established for $\bar{q} = \hat{q}$. Similarly, if $\delta^{-1}([p, \underline{q-1}], a) = [\overline{\underline{q-1}}, \bar{p}]$, then we have $\delta^{-1}([p, q], a) = [\tilde{q}, \bar{p}]$ and our result is established for $\bar{q} = \tilde{q}$. □

Proposition 5.6.3. *Given a weakly oriented automaton $\mathcal{G} = (Q, A, \delta)$ with n states, there is a cyclic order on the state set Q, such that given any letter in A its action either* *preserves or reverses this cyclic order.*

Proof. Since $\mathcal{G}$ is weakly oriented, we may assume without loss of generality that the cyclic order $0, 1, \ldots, n-1, 0$ is weakly preserved, that is, given an interval I of Q for this order, $\delta^{-1}(I, a)$ is an interval for every $a \in A$. Our objective is to prove that either $\delta(0, a), \delta(1, a), \ldots, \delta(n-1, a), \delta(0, a)$ is a subsequence of $0, 1, \ldots, n-1, 0$ or $\delta(n-1, a), \delta(n-2, a), \ldots, \delta(0, a), \delta(n-1, a)$ is a subsequence of $0, 1, \ldots, n-1, 0$. Let us assume that this is not the case. Then there are distinct states $i, j, k, l \in Q$ such that i, j, k, l is a subsequence of $0, 1, \ldots, n-1, 0$ and the distinct states $\delta(i, a), \delta(j, a), \delta(l, a), \delta(k, a)$ form a subsequence of $0, 1, \ldots, n-1, 0$.

According to Lemma 5.6.2, there are states $\bar{i}, \bar{k}$ such that $\delta(\bar{i}, a) = \delta(i, a)$, $\delta(\bar{k}, a) = \delta(k, a)$ and either $\delta^{-1}([\delta(i, a), \delta(k, a)], a) = [\bar{i}, \bar{k}]$ or $\delta^{-1}([\delta(i, a), \delta(k, a)], a) = [\bar{k}, \bar{i}]$. Since $\delta(i, a), \delta(j, a), \delta(k, a)$ is a subsequence of $0, 1, \ldots, n-1, 0$, then $\delta(j, a) \in [\delta(i, a), \delta(k, a)]$, thus $j \in \delta^{-1}([\delta(i, a), \delta(k, a)], a)$. But i, j, k is also a subsequence of $0, 1, \ldots, n-1, 0$, therefore we must have $j \in [i, k] \subseteq \delta^{-1}([\delta(i, a), \delta(k, a)], a) = [\bar{i}, \bar{k}]$.

Since $\delta(i, a), \delta(l, a), \delta(k, a)$ is a subsequence of $0, 1, \ldots, n-1, 0$, we know that $\delta(l, a) \in [\delta(i, a), \delta(k, a)]$, that is, $l \in \delta^{-1}([\delta(i, a), \delta(k, a)], a) = [\bar{i}, \bar{k}]$. Therefore, eliminating eventual repetitions ($\bar{i}$ may be equal to i and $\bar{k}$ may be equal to k), $\bar{i}, i, l, k, \bar{k}$ is a subsequence of $0, 1, \ldots, n-1, 0$, which contradicts the hypothesis that i, k, l is a subsequence of $0, 1, \ldots, n-1$. □

Whether Conjecture 5.1.1 is valid for all weakly oriented automata or not, remains unknown. But we were able to establish it for a subclass of weakly oriented automata, as is detailed in the following section.

5.7 Weakly oriented circular automata

Let us begin with a result that will help to better deal with weakly oriented circular automata.

Lemma 5.7.1. *Consider the weakly oriented circular automaton $\mathcal{G} = (Q, A, \delta)$, where $Q = \{0, 1, \ldots, n-1\}$ and the order $0, 1, \ldots, n-1, 0$ is weakly preserved. Then there is some $\lambda \in \{1, 2, \ldots, n-1\}$ such that $\delta(i, a) = \underline{i + \lambda}$ for every $i \in Q$. Also λ and n are relatively prime.*

Proof. Since a acts as a cycle of length n on Q, given any subset T of Q, we have $\delta(T, a) = \delta^{-1}(T, a^{n-1})$, hence $\delta(I, a)$ is an interval for every interval I. Thus, for $\lambda \in \{1, 2, \ldots, n-1\}$

such that $\delta(0, a) = \lambda$, we are in one of the following situations:

(a) $\delta(1, a) = \underline{-1 + \lambda}$;
(b) $\delta(1, a) = \underline{1 + \lambda}$.

We will use two step induction on i to prove that in Case (a), $\delta(i, a) = \underline{-i + \lambda}$, for all $i \in \{0, 1, \ldots, n-1\}$. We know that $\delta(0, a) = \lambda = \underline{\lambda}$ and that, since we are in Case (a), $\delta(1, a) = \underline{-1 + \lambda}$. That is, we already have our formula established for $i = 0$ and $i = 1$. We will now assume that it has been verified for some $i-2$ and $i-1$ and prove that it also holds for i. We have $\delta(i-2, a) = \underline{-i + 2 + \lambda}$ and $\delta(i-1, a) = \underline{-i + 1 + \lambda}$, plus we know that $\delta([i-1, i], a)$ is an interval, hence we must have $\delta(i, a) = \underline{-i + \lambda}$. In particular, $\delta(\lambda, a) = 0$, which is absurd for $n > 2$. For $n \leq 2$, this lemma is quite trivial and there is nothing to prove, so we have ruled out Case (a).

Let us turn our attention to Case (b). Using similar arguments to those from Case (a), one can prove that $\delta(i, a) = \underline{i + \lambda}$, for all $i \in \{0, 1, \ldots, n-1\}$.

Suppose that l is the greatest common divisor of λ and n. Then we have $\delta(0, a^{n/l}) = \underline{\lambda \cdot n/l} = \underline{n \cdot \lambda/l} = 0$, because n divides $n \cdot \lambda/l$. Hence a has a cycle of length n/l on Q, which implies that $l = 1$, because a acts as a circular permutation on Q, that is, its unique cycle has length n. $\square$

Given a weakly oriented circular automaton $\mathcal{G} = (Q, A, \delta)$ with n states, we will assume without loss of generality that we are in the conditions of Lemma 5.7.1 and that $n \geq 2$. Recall that we define the *jump* of $\mathcal{G}$ as the integer $\lambda \in \{1, 2, \ldots, n-1\}$ such that $\delta(i, a) = \underline{i + \lambda}$ for every $i \in Q$.

The next four lemmas are concerned with the existence of a letter of rank $n-1$ on a weakly oriented automaton.

Lemma 5.7.2. *Let $\mathcal{G} = (Q, A, \delta)$ be a weakly oriented automaton with $Q = \{0, 1, \ldots, n-1\}$ and suppose that the letter $b \in A$ has rank $n-1$. Then there are unique states $p, s \in Q$ for which $\delta^{-1}(\{p\}, b) = \varnothing$ and $\delta^{-1}(\{s\}, b) = \{q_1, q_2\}$, with $q_1, q_2 \in Q$ such that $q_2 = \underline{q_1 + 1}$.*

Moreover, if p and s are adjacent states then, up to reversal of the order, we may assume that $p = \underline{s - 1}$ and there are two possibilities:

1. *for every $q \in Q - \{p, s\}$, $\delta^{-1}(\{q\}, b) = \{\underline{q_2 + q - s}\}$;*
2. *for every $q \in Q - \{p, s\}$, $\delta^{-1}(\{q\}, b) = \{\underline{q_1 - q + s}\}$.*

Proof. Since b has rank $n-1$, that is, $|\delta(Q, b)| = n-1$, there must be distinct states q_1, q_2 such that $\delta(q_1, b) = \delta(q_2, b) = s$ for some $s \in Q$. We also know that given $q \in Q$, $\delta(q, b)$ is a single state, that is, the automaton $\mathcal{G}$ is deterministic, hence, there must be a single state $p \in Q$ such that $\delta^{-1}(\{p\}, b) = \varnothing$, because there are two states with the same image by $\delta(\cdot, b)$.

Since $\mathcal{G}$ is weakly oriented and $\{s\}$ is an interval, $\delta^{-1}(\{s\}, b)$ must be an interval, that is, q_1 and q_2 must be adjacent and we may assume without loss of generality that $q_2 = \underline{q_1 + 1}$.

The rest of this proof is quite similar to that of Lemma 5.7.1. We will use two step induction to obtain the desired results.

If p and s are adjacent then either $p = \underline{s-1}$ or $p = \underline{s+1}$. If $p = \underline{s+1}$, then we may relabel the states of Q by replacing q with $n - q$, for every $q \in Q$, and consider the reverse order. The automaton obtained is weakly oriented for this order and thus satisfies all the requirements of our lemma and is such that $p = \underline{s-1}$. Thus we may assume that $p = \underline{s-1}$. Since $\mathcal{G}$ is weakly oriented and $\delta^{-1}(\{s\}, b) = \{q_1, q_2\}$, $\delta^{-1}(\{\underline{s+1}\}, b)$ is either $\{\underline{q_2+1}\}$ or $\{\underline{q_1-1}\}$.

If $\delta^{-1}(\{\underline{s+1}\}, b) = \{\underline{q_2+1}\}$, then $\delta^{-1}(\{\underline{s+2}\}, b) = \{\underline{q_2+2}\}$. Moreover, if we assume that $\delta^{-1}(\{\underline{s+j}\}, b) = \{\underline{q_2+j}\}$ and $\delta^{-1}(\{\underline{s+j+1}\}, b) = \{\underline{q_2+j+1}\}$ for some $j \in \{1, 2, \ldots, n-4\}$, then $\delta^{-1}(\{\underline{s+j+2}\}, b) = \{\underline{q_2+j+2}\}$. This way, using two step induction on $j \in \{1, 2, \ldots, n-2\}$, we have $\delta^{-1}(\{\underline{s+j}\}, b) = \{q_2 + j\}$. Given $q \in Q - \{\underline{s-1}, s\}$ we may write $q = \underline{s+q-s}$, with $\underline{q-s} \in \{1, 2, \ldots, n-2\}$, thus we are in Case 1 and we have $\delta^{-1}(\{q\}, b) = \{\underline{q_2+q-s}\}$ for every $q \in Q - \{p, s\}$.

If $\delta^{-1}(\{\underline{s+1}\}, b) = \{\underline{q_1-1}\}$, then $\delta^{-1}(\{\underline{s+2}\}, b) = \{\underline{q_1-2}\}$. Moreover, if we assume that $\delta^{-1}(\{\underline{s+j}\}, b) = \{\underline{q_1-j}\}$ and $\delta^{-1}(\{\underline{s+j+1}\}, b) = \{\underline{q_1-j-1}\}$ for some $j \in \{1, 2, \ldots, n-4\}$, then $\delta^{-1}(\{\underline{s+j+2}\}, b) = \{\underline{q_1-j-2}\}$. This way, using two step induction on $j \in \{1, 2, \ldots, n-2\}$, we have $\delta^{-1}(\{\underline{s+j}\}, b) = \{\underline{q_1-j}\}$. Given $q \in Q - \{\underline{s-1}, s\}$ we may write $q = \underline{s+q-s}$, with $\underline{q-s} \in \{1, 2, \ldots, n-2\}$, thus we are in Case 2 and we have $\delta^{-1}(\{q\}, b) = \{\underline{q_1-q+s}\}$ for every $q \in Q - \{p, s\}$. □

Given a weakly oriented circular automaton $\mathcal{G} = (Q, A, \delta)$ with n states and an interval I of Q, we denote by I_j the interval $\delta^{-1}(I, a^j)$ for every $j \in \{0, 1, 2, \ldots, n-1\}$.

Lemma 5.7.3. *Let $\mathcal{G} = (Q, A, \delta)$ be a weakly oriented circular automaton with n states and suppose that the letter $b \in A$ has rank $n-1$. Then, given a nonempty proper interval I of Q there is some $j \in \{0, 1, 2, \ldots, n-1\}$ for which the word $u = ba^j$ is such that $|\delta^{-1}(I, u)| = |I| + 1$ and u has at most n letters. Moreover, if I is such that $\delta^{-1}(I, b) \neq I$, $\delta^{-1}(I, b) \neq \delta^{-1}(I, a)$ and $|\delta^{-1}(I, b)| \geq |I|$, then there is a word u with at most $n-1$ letters such that $|\delta^{-1}(I, u)| = |I| + 1$.*

Proof. Since a acts as a circular permutation and $\mathcal{G}$ is weakly oriented, the set $\mathcal{I} = \{I_i = \delta^{-1}(I, a^i) : i \in \{0, 1, 2, \ldots, n-1\}\}$ contains all intervals of Q with $|I|$ states. In particular, there is some $j \in \{0, 1, 2, \ldots, n-1\}$ such that I_j contains s and not p. This implies that $|\delta^{-1}(I_j, b)| = |I| + 1$, thus $|\delta^{-1}(I, ba^j)| = |I| + 1$.

If $j \leq n-2$ the word $u = ba^j$ satisfies the requirements of the second part of the lemma. Otherwise, since $|\delta^{-1}(I, b)| \geq |I|$ and b has rank $n-1$, then either $|\delta^{-1}(I, b)| = |I| + 1$ and our result is established for $u = b$, or $|\delta^{-1}(I, b)| = |I|$ and so $\delta^{-1}(I, b) = \delta^{-1}(I, a^j)$ for some $j \in \{2, 3, \ldots, n-1\}$. Thus, there is some $k \in \{0, 1, \ldots, n-3\}$ for which the word $u = ba^k b$ is such that $|\delta^{-1}(I, u)| = |I| + 1$. Since u has at most $n-1$ the proof is complete. $\square$

Lemma 5.7.4. *Let $\mathcal{G} = (Q, A, \delta)$ be a weakly oriented circular automaton with n states and jump $\lambda \in \{2, 3, \ldots, n-2\}$. Suppose that $A = \{a, b\}$ and that the letter b has rank $n-1$ and let I^1 be a singleton subset. For each $l \in \{2, 3, \ldots, n-2\}$, there is a shortest word u_{l-1} such that $I^l = \delta^{-1}(I^{l-1}, u_{l-1})$ has l states. Moreover, if n is odd, then there is at most one $\bar{l} \in \{2, 3, \ldots, n-2\}$, for which $u_{\bar{l}}$ has n letters. For every other $l \in \{2, 3, \ldots, n-2\} - \{\bar{l}\}$, u_l has at most $n-1$ letters. If n is even, then for every $l \in \{2, 3, \ldots, n-2\}$, u_l has at most $n-1$ letters.*

Proof. As we saw in Lemma 5.7.2, there are unique states $p, s \in Q$ for which $\delta^{-1}(\{p\}, b) = \varnothing$ and $\delta^{-1}(\{s\}, b) = \{q_1, q_2\}$, with $q_1, q_2 \in Q$ such that $q_2 = \underline{q_1 + 1}$. Also, given $q \in Q - \{p, s\}$, $\delta^{-1}(\{q\}, b)$ is a singleton set.

By Lemma 5.7.3, given an interval $I \subsetneq Q$, there is a minimum $j(I) \in \{0, 1, \ldots, n-1\}$ such that $|\delta^{-1}(I_{j(I)}, b)| = |I| + 1$, thus $|\delta^{-1}(I, ba^{j(I)})| = |I| + 1$. If for every $I \in \{I^2, I^3, \ldots, I^{n-2}\}$ we have $j(I) < n-1$, then our result is established. Otherwise, the only interval that contains s but not p is I^l_{n-1}. Hence, p and s must be adjacent, since for $l < n-1$ there are always at least two intervals of size l that contain s but not p if they are not adjacent. Thus, we may assume that the conditions of the second part of Lemma 5.7.2 hold. From hereon, when we refer to Cases 1 and 2 we mean those from that lemma.

Since a acts as a circular permutation and u_{l-1} is a shortest word such that $\delta^{-1}(I^{l-1}, u_{l-1}) = I^l$ for some interval I^{l-1} with $l-1$ states, the first letter of u_{l-1} is necessarily b and we may write $u_{l-1} = b\tilde{u}_{l-1}$. Also, the interval $K = \delta^{-1}(I^{l-1}, \tilde{u}_{l-1})$ must have $l-1$ states and since $\delta^{-1}(K, b)$ has l states, K must contain s and not p.

We have $p = \underline{s-1}$ thus

$$I^l_{n-1} = [s, \underline{s+l-1}]. \tag{5.7.1}$$

Also, since $I^l_{n-1} = \delta(I^l, a)$ and a has jump λ, then

$$I^l = [\underline{s-\lambda}, \underline{s-\lambda+l-1}]. \tag{5.7.2}$$

As for K it must be equal to $[s, \underline{s+l-2}]$. We also have $\delta^{-1}(K,b) = I^l$, that is,

$$\delta^{-1}([s, \underline{s+l-2}], b) = [\underline{s-\lambda}, \underline{s-\lambda+l-1}]. \tag{5.7.3}$$

In Case 1, using (5.7.3) we have $\delta^{-1}(K,b) = \delta^{-1}(\{s\} \cup [\underline{s+1}, \underline{s+l-2}], b) = \{q_1, q_2\} \cup [\underline{q_2+1}, \underline{q_2+l-2}] = [q_1, \underline{q_1+l-1}] = [\underline{s-\lambda}, \underline{s-\lambda+l-1}]$. Hence, we conclude that $q_1 = \underline{s-\lambda}$. Which yields $\delta^{-1}(\{q\}, b) = \{\underline{q-\lambda+1}\}$, for every $q \in Q - \{p,s\}$, and $\delta^{-1}(\{p,s\}, b) = \{\underline{s-\lambda}, \underline{s-\lambda+1}\} = \{\underline{p-\lambda+1}, \underline{s-\lambda+1}\}$.

Suppose that I^l is such that either $p, s \in I^l$ or $p, s \notin I^l$. Note that in this case, given a nonempty proper interval I of Q, we have $\delta^{-1}(I,b) \neq I$, $\delta^{-1}(I,b) \neq \delta^{-1}(I,a)$ and $|\delta^{-1}(I,b)| = |I|$. Thus we are in the conditions of Lemma 5.7.3 and our result is established.

Now suppose that $p \in I^l$ and $s \notin I^l$. It follows that $I^l = [\underline{s-l}, \underline{s-1}]$, whence $l = \lambda$, according to (5.7.2). This implies that in this case the value of l is fixed, hence there is at most one $\bar{l} \in \{2, 3, \ldots, n-1\}$ for which $u_{\bar{l}}$ has n letters. Since $I_1^l = \delta^{-1}(I^l, a) \neq I^l$ and $I_1^l \neq I_{n-1}^l$, either $p, s \in I_1^l$ or $p, s \notin I_1^l$. Using (5.7.2), we obtain $\tilde{I} = \delta^{-1}(I_1^l, b) = \delta^{-1}(I^l, ba) = \delta^{-1}([\underline{s-2\lambda}, \underline{s-\lambda-1}], b) = [\underline{s-3\lambda+1}, \underline{s-2\lambda}]$. We have $\tilde{I} \neq I_1^l$, because otherwise we would have $\underline{s-2\lambda} = \underline{s-\lambda-1}$, that is, $\lambda = 1$, which contradicts the hypothesis that $\lambda > 1$. Also, we have $\tilde{I} \neq I_2^l = \delta^{-1}(I_1^l, a)$, because otherwise we would have $\underline{s-2\lambda} = \underline{s-2\lambda-1}$, that is, $0 = \underline{-1}$, which is absurd as well. If $\tilde{I} = I^l$, then $\underline{s-2\lambda} = \underline{s-1}$, that is, $\underline{2\lambda-1} = 0$ and n must be odd.

For n even, we have $\tilde{I} \notin \{I^l, I_1^l, I_2^l\}$ and $|\tilde{I}| = l$, whence $\tilde{I} = I_j^l$ for some $j \in \{3, 4, \ldots, n-1\}$ and there is some $k \in \{0, 1, \ldots, n-4\}$ such that $|\delta^{-1}(I^l, ba^kba)| = l+1$. Since ba^kba has at most $n-1$ letters so does u_l.

In Case 2, using (5.7.3) we have $\delta^{-1}(K,b) = \delta^{-1}(\{s\} \cup [\underline{s+1}, \underline{s+l-2}], b) = \{q_1, q_2\} \cup [\underline{q_1-l+2}, \underline{q_1-1}] = [\underline{q_2-l+1}, q_2] = [\underline{s-\lambda}, \underline{s-\lambda+l-1}]$. Hence, we conclude that

$$q_2 = \underline{s-\lambda+l-1}, \tag{5.7.4}$$

hence $l = \underline{q_2+1+\lambda-s}$. Since l is fixed, there is at most one $\bar{l} \in \{2, 3, \ldots, n-1\}$ for which $u_{\bar{l}}$ has n letters. Therefore our proof is concluded for n odd and we may assume that n is even. We have three possibilities:

2a. $s = q_2$;
2b. $p = q_2$;
2c. $s \neq q_2 \neq p$.

In Case 2a, we have $s = q_2 = \underline{s-\lambda+l-1}$, hence $\lambda = l-1$. Also, $q_1 = \underline{s-1} = p$, $\delta^{-1}(\{s\}, b) = \{p, s\}$ and $\delta^{-1}(\{q\}, b) = \{\underline{2s-q-1}\}$, for every $q \in Q - \{p, s\}$. Since $\lambda >$

1, then $l > 2$. Thus, according to (5.7.2) we have $I^l = [\underline{s-\lambda}, s]$ and $\delta^{-1}(I^l, b) = [\underline{s-1}, \underline{s+\lambda-1}] \neq I^l$. Also, $\delta^{-1}(I^l, b) \neq \delta^{-1}(I^l, a) = [\underline{s-2\lambda}, \underline{s-\lambda}]$ because n is even. Thus, we are in the conditions of Lemma 5.7.3 and our result is obtained.

In Case 2b, we have $\underline{s-1} = q_2 = \underline{s-\lambda+l-1}$, thus $\lambda = l$ and $\delta^{-1}(\{q\}, b) = \{\underline{2s-q-2}\}$, for every $q \in Q - \{p, s\}$. Let $\hat{I} = [\underline{s-\lambda-1}, \underline{s-2}]$. If $\hat{I} = I^l_{n-2}$, then $\delta^{-1}(\hat{I}, a) = I^l_{n-1}$ and, using (5.7.1), it follows that $[\underline{s-2\lambda-1}, \underline{s-\lambda-2}] = [s, \underline{s+\lambda-1}]$. This implies that $\underline{2\lambda+1} = 0$, which is absurd for n even. Thus, there is some $j \in \{0, 1, \ldots, n-3, n-1\}$ such that $\hat{I} = I^l_j$. Since $l < n-1$, then $p, s \notin \hat{I}$ and $\hat{I} \neq I^l_{n-1}$ and so $j \leq n-3$. Thus, we have $\delta^{-1}(\hat{I}, b) = [s, \underline{s+\lambda-1}] = I^l_{n-1}$, which implies that $|\delta^{-1}(\hat{I}, b^2)| = l+1$. The word b^2a^j has at most $n-1$ letters and, therefore, so does u_l.

Suppose that we are in Case 2c and that $p \in I^l$ and $s \notin I^l$. Then $I^l = [\underline{s-l}, \underline{s-1}]$, which means that $l = \lambda$, according to (5.7.2). Thus, using (5.7.4), we deduce that $q_2 = \underline{s-1}$, contrary to the assumption. Therefore either $p, s \in I^l$ or $p, s \notin I^l$, which implies that $|\delta^{-1}(I^l, b)| = l$. From (5.7.4), we obtain $q_1 = \underline{s-\lambda+l-2}$. Thus, for every $q \in Q - \{p, s\}$, $\delta^{-1}(\{q\}, b) = \{\underline{q_1-q+s}\} = \{\underline{2s-q-\lambda+l-2}\}$. Also $\delta^{-1}(\{p, s\}, b) = \{\underline{s-\lambda+l-2}, \underline{s-\lambda+l-1}\} = \{\underline{2s-s-\lambda+l-2}, \underline{2s-p-\lambda+l-2}\}$. Using (5.7.2), we conclude that $\delta^{-1}(I^l, b) = \delta^{-1}([\underline{s-\lambda}, \underline{s-\lambda+l-1}], b) = [\underline{s-1}, \underline{s+l-2}]$. Since $\lambda > 1$, it follows that $\delta^{-1}(I^l, b) \neq I^l$. Using (5.7.2) once again, we obtain $\delta^{-1}(I^l, a) = [\underline{s-2\lambda}, \underline{s-2\lambda+l-1}]$. Hence, since n is even, we must have $\delta^{-1}(I^l, b) \neq \delta^{-1}(I^l, a)$. This means that we are in the conditions of Lemma 5.7.3, which completes the proof for this last case. $\square$

Lemma 5.7.5. *Let $\mathcal{G} = (Q, A, \delta)$ be a weakly oriented circular automaton with n states and jump $\lambda \in \{2, 3, \ldots, n-2\}$. Suppose that the letter $b \in A$ has rank $n-1$. Then $\mathcal{G}$ is synchronizing. Also, if n is odd, given $l \in \{2, 3, \ldots, n-2\}$ there are a state $s \in Q$ and a word v_l with at most $2+(n-1)(l-2)$ letters such that $|\delta^{-1}(\{s\}, v_l)| = l$. If n is even, given $l \in \{2, 3, \ldots, n-2\}$ there are a state $s \in Q$ and a word v_l with at most $1+(n-1)(l-2)$ letters such that $|\delta^{-1}(\{s\}, v_l)| = l$.*

Proof. We may apply Lemma 5.7.4 to the automaton $\mathcal{G} = (Q, \{a, b\}, \delta)$ and the interval $I^1 = \{s\}$ to obtain a sequence of shortest words $u_1, u_2, \ldots, u_{n-2}$ such that, for each $l = 2, 3, \ldots, n-2$, the interval $\delta^{-1}(I^1, u_1u_2\ldots u_{l-1})$ has l states. Since $|\delta^{-1}(\{s\}, b)| = 2$, then u_1 is a letter. Also, for n odd, there is at most one $\bar{l} \in \{2, 3, \ldots, n-2\}$ for which $u_{\bar{l}}$ has at most n letters. For every other $l \in \{2, 3, \ldots, n-2\} - \{\bar{l}\}$, u_l has at most $n-1$ letters. For n even, the word u_l has at most $n-1$ letters for every $l \in \{2, 3, \ldots, n-2\}$. The word $v_l = u_1u_2\ldots u_{l-1}$ is in the desired conditions. $\square$

We need two more lemmas before we establish some upper bounds on the length of shortest synchronizing words of subsets of states of weakly oriented circular automata.

Lemma 5.7.6. *Consider the weakly oriented circular automaton* $\mathcal{G} = (Q, \{a\}, \delta)$ *of jump* $\lambda \in \{1, n-1\}$ *and let* S *be a subset of* Q*. Suppose that the interval* T *of* Q *is such that* $|T| \geq n - \Gamma(S)$*. Then the inclusion* $S \subseteq \delta^{-1}(T, a^l)$ *holds for some* $l \in \{0, 1, \ldots, n - (G(S)-1)\Gamma(S) - G(S)\}$*.*

Proof. If $\lambda = n-1$, then we may relabel the states of $\mathcal{G}$ in such a way that q becomes $n-q$ for every $q \in Q$. The automaton obtained is a weakly oriented automaton of jump 1. Therefore, we may assume $\lambda = 1$.

Since $\Gamma(S)$ is the size of the largest gap of S and a cyclically permutes Q, there is some $j \in \{0, 1, \ldots, n-1\}$ such that $S \subseteq \delta^{-1}(T, a^j)$. Let l be the minimum j with this property. We want to see that $l \leq n - (G(S)-1)\Gamma(S) - G(S)$.

Let $[p_1, q_1], [p_2, q_2], \ldots, [p_{G(S)}, q_{G(S)}]$ be the $G(S)$ gaps of size $\Gamma(S)$ of S, with $\langle p_i, p_{i+1}, p_{i+2}\rangle$, for every $i \in \{1, 2, \ldots, G(S)-2\}$, and $\langle p_{G(S)-1}, p_{G(S)}, p_1\rangle$. Also, denote by $[p, q]$ the only non trivial gap of T. We want to compute the smallest number l such that $\delta^{-1}([p,q], a^l) \subseteq [p_i, q_i]$, that is, $[\underline{p-l}, \underline{q-l}] \subseteq [p_i, q_i]$, for some $i \in \{1, 2, \ldots, G(S)\}$. Clearly it is enough to search for the smallest l such that $\underline{p-l} = p_i$, for some $i \in \{1, 2, \ldots, G(S)\}$.

In the worst case, we have $p = \underline{p_1 - 1}$ and between two consecutive large gaps there is a single element of S, that is, $p_i = \underline{p_{i-1} + \Gamma(S) + 1}$, for every $i \in \{2, 3, \ldots, G(S)\}$. This means that $p_{G(S)} = \underline{p_1 + (G(S)-1)(\Gamma(S)+1)} = \underline{p + (G(S)-1)\Gamma(S) + G(S)}$. Thus, if we make $l = n - (G(S)-1)\Gamma(S) - G(S)$, we have $\underline{p-l} = p_{G(S)}$. $\square$

In the general case of weakly oriented circular automata of jump λ, for $\lambda \in \{1, 2, \ldots, n-1\}$ such that λ and n are relatively prime, we can obtain the following result.

Lemma 5.7.7. *Consider the weakly oriented circular automaton* $\mathcal{G} = (Q, \{a\}, \delta)$ *and let* S *be a subset of* Q*. Suppose that the interval* T *of* Q *is such that* $|T| \geq n - \Gamma(S)$*. Then the inclusion* $S \subseteq \delta^{-1}(T, a^l)$ *holds for some* $l \in \{0, 1, \ldots, n - G(S)\}$*.*

Proof. Since $\Gamma(S)$ is the size of the largest gap of S, $G(S)$ is the number of gaps of size $\Gamma(S)$ in S and a cyclically permutes Q, there are $G(S)$ elements $i \in \{0, 1, \ldots, n-1\}$ such that $S \subseteq \delta^{-1}(T, a^i)$. Hence, the minimum i with this property is at most $n - G(S)$. $\square$

Note that if S is strictly contained in Q, the bound $n - (G(S)-1)\Gamma(S) - G(S)$ obtained in Lemma 5.7.6 is smaller than the bound $n - G(S)$ obtained in Lemma 5.7.7 whenever $G(S) > 1$, because the difference between them is $(G(S)-1)\Gamma(S)$. Since $(G(S) -$

$1)\Gamma(S)$ is the total number of states in $G(S)-1$ gaps of size $\Gamma(S)$, it is at most $n-m-\Gamma(S)$, because there are $G(S)$ gaps of size $\Gamma(S)$ and m states in S.

To see that the upper bound obtained in Lemma 5.7.7 is tight for $\lambda \in \{2, 3, \ldots, n-2\}$, consider the automaton $\mathcal{T} = (Q, \{a\}, \delta)$, where $|Q| = n \geq 7$ is odd and $\delta(i, a) = \underline{i+2}$, and the subsets $S = Q - \{2, 4, 6\}$ and $T = Q - \{0\}$. We have $G(S) = 3$, thus $n - G(S) = n - 3$. Also, for $l \in \{0, 1, \ldots, n-1\}$, $\delta^{-1}(T, a^l) = Q - \delta^{-1}(0, a^l) = Q - \{\underline{-2l}\} = Q - \{\underline{2n-2l}\}$, therefore $S \subseteq \delta^{-1}(T, a^l)$ if and only if $\underline{2n-2l} \in \{2, 4, 6\}$, that is, $l \in \{n-1, n-2, n-3\}$.

Theorem 5.7.8. *Let $\mathcal{G} = (Q, A, \delta)$ be a synchronizing weakly oriented circular automaton with n states such that at least one of the following conditions is verified:*

1. *$\mathcal{G}$ has jump 1 or $n-1$;*
2. *there is a letter $b \in A$ of rank $n-1$.*

Then for every subset S of Q with m elements, there is a word $w \in A^*$ such that $|\delta(S, w)| = 1$ and

$$|w| \leq (n-1)^2 - \left\lceil \frac{n-m}{m} \right\rceil \left(2n - m \left\lceil \frac{n}{m} \right\rceil - 1\right).$$

Proof. If $S = Q$, then the result is a corollary of Theorem 2.5.2. Thus, from hereon we assume that S is a proper subset of Q, which implies that $\Gamma(S), G(S) \geq 1$.

Using Theorem 2.5.1 and proceeding as in the proof of Theorem 5.5.1, we know that there are a state $s \in Q$ and a word $v \in A^*$ such that $|\delta^{-1}(s, v)| \geq n - \Gamma(S)$ and $|v| \leq 1 + n(n-2-\Gamma(S))$. We know that the subset $T = \delta^{-1}(s, v)$ of Q is an interval, because $\mathcal{G}$ is weakly oriented. Since $\Gamma(S)$ is the size of the largest gap of S, there is some $i \in \{0, 1, \ldots, n-1\}$ such that $\delta^{-1}(T, a^i) \supseteq S$. Let l be the minimum such i. The word $w = a^l v$ obviously synchronizes S. All that remains to be shown is that its size is at most $f(n, m)$.

If S is such that $\Gamma(S) > \gamma = \left\lceil \frac{n-m}{m} \right\rceil$, then $|w| \leq 1 + n(n-2-\gamma-1) + n - 1 = (n-1)^2 - \gamma n - 1$. Using Lemma 5.3.3, let $\varepsilon \in \{1, 2, \ldots, m\}$ be such that $m \left\lceil \frac{n}{m} \right\rceil = n + m - \varepsilon$. We have

$$\begin{aligned} &(n-1)^2 - \gamma\left(2n - m\left\lceil \frac{n}{m} \right\rceil - 1\right) - ((n-1)^2 - \gamma n - 1) \\ &= \gamma(-2n + (n + m - \varepsilon) + 1 + n) + 1 = \gamma(m - \varepsilon + 1) + 1 \\ &\geq \gamma(m - m + 1) + 1 = \gamma + 1 > 0. \end{aligned}$$

Thus, $|w| \leq f(n, m)$ and our result is proved in this case, independently of whether $\mathcal{G}$ verifies the Conditions 1 or 2. Moreover, according to Lemma 5.2.1, we know that $\Gamma(S) \geq \gamma$, therefore we only have to verify the case when $\Gamma(S) = \gamma$.

Suppose that Condition 1 is satisfied. Then, using Lemma 5.7.6 we know that $|w| \leq 1 + n(n-2-\gamma) + n - (G(S)-1)\gamma - G(S)$ and we want to compute $G(S)$ such that this bound is maximum. That means that we want to compute the minimum value of $G(S)$, which is $g = n-m\gamma$ according to Lemma 5.2.1. We have $|w| \leq 1+n(n-2-\gamma)+n-(g-1)\gamma-g$ and some simple computations show that the right hand side of the inequality coincides with $f(n,m)$.

Now suppose that Condition 1 is not satisfied. Then we have a weakly oriented circular automaton with jump $\lambda \in \{2,3,\ldots,n-2\}$, which implies that $n > 3$. Also, Condition 2 must be satisfied, therefore we are in the conditions of Lemma 5.7.5. Thus, for n odd, we have a word $v \in A^*$ of length at most $2+(n-1)(n-2-\gamma)$ such that the interval $T = \delta^{-1}(\{s\}, v)$ has $n-\gamma$ states. Using Lemma 5.7.7, we know that there is some $k \in \{0,1,\ldots,n-G(S)\}$ such that $S \subseteq \delta^{-1}(T, a^k)$. The word $w = a^k v$ is a synchronizing word for S and its length is at most $2+(n-1)(n-2-\gamma)+n-G(S)$, which is maximum for $G(S) = g = n-m\gamma$. Hence, we have $|w| \leq 2+(n-1)(n-2-\gamma)+n-g = 1+n(n-2-\gamma)-(n-2-\gamma)+n-g+1 = 1+n(n-2-\gamma)-(n-3-\gamma)+n-g$. Since n is odd, if $m=2$ then we have $g=1$, $\gamma \geq 2$ because n is odd and greater than 3, thus $\gamma+m = n-(\gamma-1) \leq n-1 = n-(g-1)\gamma-g$. It follows that $|w| \leq 1+n(n-2-\gamma)+\gamma+2 = 1+n(n-2-\gamma)+\gamma+m \leq 1+n(n-2-\gamma)+n-(g-1)\gamma-g = f(n,m)$. For $m \geq 3$, according to the observation made after Lemma 5.7.7, we have $(g-1)\gamma \leq n-3-\gamma$, because there at least 3 states in S. Therefore, we have $|w| \leq 1+n(n-2-\gamma)+n-(n-3-\gamma)-g \leq 1+n(n-2-\gamma)+n-(g-1)\gamma-g = f(n,m)$.

For n even, we have a word $v \in A^*$ of length at most $1+(n-1)(n-2-\gamma)$ such that the interval $T = \delta^{-1}(\{s\}, v)$ has $n-\gamma$ states. Using Lemma 5.7.7, we know that there is some $l \in \{0,1,\ldots,n-G(S)\}$ such that $S \subseteq \delta^{-1}(T, a^l)$. The word $w = a^l v$ is a synchronizing word for S and its length is at most $1+(n-1)(n-2-\gamma)+n-G(S)$, which is maximum for $G(S) = g = n-m\gamma$. Hence we have $|w| \leq 1+(n-1)(n-2-\gamma)+n-g = 1+n(n-2-\gamma)+n-(n-2-\gamma)-g$. According to the observation made after Lemma 5.7.7, we have $(g-1)\gamma \leq n-2-\gamma$, because there at least 2 states in S. Therefore, we have $|w| \leq 1+n(n-2-\gamma)+n-(g-1)\gamma-g = f(n,m)$. □

In the general case, when the Conditions 1 and 2 from Theorem 5.7.8 are not verified, we have the following result. That the general bound it establishes is not quite as good as the one from Conjecture 5.1.1 is the result of the observation made after Lemma 5.7.7.

Theorem 5.7.9. *Let $\mathcal{G} = (Q, A, \delta)$ be a synchronizing weakly oriented circular automaton with n states. Then for every subset S of Q with m elements, there is a word $w \in A^*$ such that $|\delta(S,w)| = 1$ and*

$$|w| \leq (n-1)^2 - \left\lceil \frac{n-m}{m} \right\rceil (n-m).$$

Proof. The proof is the same as in Theorem 5.7.8, including the fact that for S such that $\Gamma(S) > \gamma = \left\lceil \frac{n-m}{m} \right\rceil$, we have a synchronizing word w with length $|w| \leq 1 + n(n - 2 - \gamma - 1) + n - 1 = (n-1)^2 - \gamma n - 1 \leq f(n,m) \leq (n-1)^2 - \left\lceil \frac{n-m}{m} \right\rceil (n-m)$.

If S is such that $\Gamma(S) = \gamma$, then using Lemma 5.7.7 and proceeding as in the proof of Theorem 5.7.8 for Case 1, we have a synchronizing word w with length $|w| \leq 1 + n(n - 2 - \gamma) + n - G(S)$, which is maximum for $g = n - m\gamma$, according to Lemma 5.2.1.

We have $|w| \leq 1 + n(n-2-\gamma) + n - g$ and some simple computations show that this is equal to $(n-1)^2 - \left\lceil \frac{n-m}{m} \right\rceil (n-m)$. □

5.8 Slowly synchronizing automata

In Chapter 2, we mentioned some small examples of extreme synchronizing automata as well as some sequences of slowly synchronizing automata. In this section, we use these examples as further evidence towards Conjecture 5.1.1.

To verify that the automata $\mathcal{X}_3^1, \mathcal{X}_3^2, \mathcal{X}_3^3, \mathcal{X}_4^1, \mathcal{X}_4^2, \mathcal{X}_4^3, \mathcal{X}_5$ and $\mathcal{X}_6$ satisfy Conjecture 5.1.1 one may use the power automaton construction. In fact, for $\mathcal{X}_3^1, \mathcal{X}_3^2, \mathcal{X}_3^3, \mathcal{X}_4^1, \mathcal{X}_4^2$ and $\mathcal{X}_4^3$ the bound given by $f(n,m)$ is tight, that is for each of these automata there is a subset with m states such that its shortest synchronizing word has length $f(n,m)$. However, for the Roman automaton $\mathcal{X}_5$ and the Kari automaton $\mathcal{X}_6$ this is not the case. Indeed, for $\mathcal{X}_5$, we have $n = 5$ and for $m = 2, f(n,m) = 10$, however, one can easily verify, through the power automaton construction, that all subsets with 2 states can be synchronized with at most 9 letters. For $\mathcal{X}_6$, we have $n = 6$ and:

- for $m = 2, f(n,m) = 15$, yet all subsets with 2 states can be synchronized with at most 11 letters;
- for $m = 3, f(n,m) = 20$, yet all subsets with 3 states can be synchronized with at most 17 letters.

One may wonder whether Conjecture 5.1.1 is a consequence of the Černý Conjecture. That is, if it is possible to obtain a result that states that if the automaton $\mathcal{G}$ satisfies the Černý Conjecture, then it also satisfies Conjecture 5.1.1. One way to do this would be to prove that given synchronizing automata $\mathcal{G}$ and $\mathcal{H}$ with n states, if $\mathrm{len}(\mathcal{G}) = \mathrm{len}(\mathcal{H})$, then for every $1 \leq m \leq n, \mathrm{len}(\mathcal{G}, m) = \mathrm{len}(\mathcal{H}, m)$. Clearly the automata $\mathcal{X}_5$ and $\mathcal{X}_6$ are counterexamples for this statement, because for $n \in \{5, 6\}$, we have $\mathrm{len}(\mathcal{X}_n) = \mathrm{len}(\mathcal{C}_n)$ and yet $\mathrm{len}(\mathcal{X}_n, 2) < \mathrm{len}(\mathcal{C}_n, 2)$.

Besides the Černý automaton $\mathcal{C}_n$, the automata $\mathcal{D}'_n$ and $\mathcal{W}_n$ are weakly oriented circular automata of jump 1. Therefore, according to Theorem 5.7.8, they satisfy Conjecture 5.1.1. The automata $\mathcal{F}_n$ and $\mathcal{J}_n$ are weakly oriented circular automata of jump $\frac{n-1}{2} > 1$ and have a letter b of rank $n-1$. Thus, according to Theorem 5.7.8, they also satisfy Conjecture 5.1.1.

Proposition 5.8.1. *For each odd integer $n > 3$, the automaton $\mathcal{B}_n$ satisfies Conjecture 5.1.1.*

Proof. The automaton $\mathcal{B}_n$ is a weakly oriented circular automaton of rank jump $\frac{n-1}{2} > 1$. It has no letter of rank $n-1$, however the action of b in $\mathcal{B}_n$ is very similar to that of b in $\mathcal{F}_n$. To see that $\mathcal{B}_n$ satisfies Conjecture 5.1.1, it is enough to consider proper subsets S of Q, since Theorem 2.5.2 provides the result for $S = Q$. Let $s = \frac{n+1}{2}$, we have $\delta_{\mathcal{B}_n}^{-1}(\{s\}, b) = [s, \underline{s+1}]$. Given $l \in \{2, 3, \ldots, n-2\}$, we have $\delta_{\mathcal{B}_n}^{-1}([\underline{s-l+2}, \underline{s+1}], a^{n-2}) = [\underline{s-l+1}, s]$ and, if $\underline{s-l+1} \neq 1$, that is, if $l \neq s$, then $\delta_{\mathcal{B}_n}^{-1}([\underline{s-l+1}, s], b) = [\underline{s-l+1}, \underline{s+1}]$ has $l+1$ elements (if $\underline{s-l+1} = 1$, then $\delta_{\mathcal{B}_n}^{-1}(\{\underline{s-l+1}\}) = \varnothing$). For $l = s$, we have $\delta_{\mathcal{B}_n}^{-1}([\underline{s-l+2}, \underline{s+1}], a^{n-3}) = \delta_{\mathcal{B}_n}^{-1}([2, \underline{s+1}], a^{n-3}) = [s, 0]$ and $\delta_{\mathcal{B}_n}^{-1}([s, 0], b) = [s, 1]$ has $s+1$ elements. Also, $\delta_{\mathcal{B}_n}^{-1}([s, 1], (ba^{n-2})^k) = [\underline{s-k}, 1]$ has $s+k+1$ elements for every $k \in \{1, 2, \ldots, n-s-1\}$.

Thus, for $l \in \{2, 3, \ldots, n-1\}$ there is a word v_l with at most $1 + (n-1)(l-2)$ letters such that $\delta_{\mathcal{B}_n}^{-1}(\{s\}, v_l)$ has l elements. This means that the automaton $\mathcal{B}_n$ satisfies Lemma 5.7.5, hence we may proceed as in the proof of Theorem 5.7.8 to see that $\mathcal{B}_n$ satisfies Conjecture 5.1.1. $\square$

For $Q = \{0, 1, \ldots, n-1\}$, let $C = \{0, 1, \ldots, n-2\}$. In the automata $\mathcal{D}''_n$, $\mathcal{E}_n$, $\mathcal{H}_n$ and $\mathcal{I}_n$, the letter a acts as a circular permutation on C and sends $n-1$ to a state from C. We may consider the circular order $0, 1, \ldots, n-2, 0$ on C and so obtain intervals of C as intervals of Q, for the usual circular order, intersected with C. For $\delta \in \{\delta_{\mathcal{D}''_n}, \delta_{\mathcal{E}_n}, \delta_{\mathcal{H}_n}, \delta_{\mathcal{I}_n}\}$, denote by $q_0 \in C$ the state such that $\delta(q_0, a) = \delta(n-1, a)$. Since q_0 must be adjacent to $n-1$, it is either $n-2$ or 0. Indeed, it is $n-2$ for $\mathcal{D}''_n$, $\mathcal{E}_n$ and it is 0 for $\mathcal{H}_n$, $\mathcal{I}_n$.

Lemma 5.8.2. *Let $\mathcal{G} = (Q, A, \delta)$ be an automaton in $\{\mathcal{D}''_n, \mathcal{E}_n, \mathcal{H}_n, \mathcal{I}_n\}$ and consider the subset $C = \{0, 1, \ldots, n-2\}$ of Q. Given $l \in \{2, 3, \ldots, n-1\}$ there is a state $s \in C$ and a word v_l, with at most $3 + n(l-2)$ letters, for which $T = \delta^{-1}(\{s\}, v_l)$ is an interval of Q, with l states in C, such that $n-1 \in T$ if and only if $q_0 \in T$.*

Proof. For $\mathcal{D}''_n$, the word $v_l = a(ba^{n-1})^{l-2}ba$ and the state $s = 0$ are in the desired conditions. Indeed,

$$\begin{aligned}
&\delta^{-1}_{\mathcal{D}''_n}(\{0\}, a(ba^{n-1})^{l-2}ba) = \delta^{-1}_{\mathcal{D}''_n}(\{n-2, n-1\}, a(ba^{n-1})^{l-2}b) \\
&= \delta^{-1}_{\mathcal{D}''_n}(\{n-3, n-2\}, a(ba^{n-1})^{l-2}) = \delta^{-1}_{\mathcal{D}''_n}(\{n-3, n-2, n-1\}, a(ba^{n-1})^{l-3}b) \\
&= \delta^{-1}_{\mathcal{D}''_n}(\{n-4, n-3, n-2\}, a(ba^{n-1})^{l-3}) = \cdots = \delta^{-1}_{\mathcal{D}''_n}(\{n-1-l, n-l, \ldots, n-2\}, a) \\
&= \{n-2-l, n-1-l, \ldots, n-3\}.
\end{aligned}$$

For $\mathcal{E}_n$, the word $v_l = (b^2a^{n-2})^{l-2}b^2$ and the state $s = 0$ are in the desired conditions. Indeed,

$$\begin{aligned}
&\delta^{-1}_{\mathcal{E}_n}(\{0\}, (b^2a^{n-2})^{l-2}b^2) = \delta^{-1}_{\mathcal{E}_n}(\{n-1, 0\}, (b^2a^{n-2})^{l-2}b) \\
&= \delta^{-1}_{\mathcal{E}_n}(\{n-2, n-1, 0\}, (b^2a^{n-2})^{l-2}) = \delta^{-1}_{\mathcal{E}_n}(\{0, 1\}, (b^2a^{n-2})^{l-3}b^2) \\
&= \delta^{-1}_{\mathcal{E}_n}(\{n-2, n-1, 0, 1\}, (b^2a^{n-2})^{l-3}) = \cdots = \{n-2, n-1, 0, \ldots, l-2\}.
\end{aligned}$$

For $\mathcal{H}_n$, the word $v_l = a(ba^{n-2})^{l-2}ba$ and the state $s = 1$ are in the desired conditions. Indeed, for $l = 2$, we have

$$\delta^{-1}_{\mathcal{H}_n}(\{1\}, aba) = \delta^{-1}_{\mathcal{H}_n}(\{n-1, 0\}, ab) = \delta^{-1}_{\mathcal{H}_n}(\{n-2, 0\}, a) = \{n-3, n-2\}.$$

For $l > 2$, we have

$$\begin{aligned}
&\delta^{-1}_{\mathcal{H}_n}(\{1\}, a(ba^{n-2})^{l-2}ba) = \delta^{-1}_{\mathcal{H}_n}(\{n-1, 0\}, a(ba^{n-2})^{l-2}b) \\
&= \delta^{-1}_{\mathcal{H}_n}(\{n-2, 0\}, a(ba^{n-2})^{l-2}) = \delta^{-1}_{\mathcal{H}_n}(\{n-1, 0, 1\}, a(ba^{n-2})^{l-3}b) \\
&= \delta^{-1}_{\mathcal{H}_n}(\{n-2, 0, 1\}, a(ba^{n-2})^{l-3}) = \cdots = \delta^{-1}_{\mathcal{H}_n}(\{n-2, 0, 1, \ldots, l-2\}, a) \\
&= \{n-3, n-2, \ldots, l-3\}.
\end{aligned}$$

For $\mathcal{I}_n$, the word $v_l = a(ba^{n-2})^{l-2}b$ and the state $s = 1$ are in the desired conditions. Indeed,

$$\begin{aligned}
&\delta^{-1}_{\mathcal{I}_n}(\{1\}, a(ba^{n-2})^{l-2}b) = \delta^{-1}_{\mathcal{I}_n}(\{0, 1\}, a(ba^{n-2})^{l-2}) = \delta^{-1}_{\mathcal{I}_n}(\{1, 2\}, a(ba^{n-2})^{l-3}b) \\
&= \delta^{-1}_{\mathcal{I}_n}(\{0, 1, 2\}, (aba^{n-2})^{l-3}) = \cdots = \delta^{-1}_{\mathcal{I}_n}(\{1, 2, \ldots, l-1\}, ab) \\
&= \delta^{-1}_{\mathcal{I}_n}(\{0, 1, \ldots, l-1\}, a) = \{n-2, n-1, 0, \ldots, l-2\}. \quad \square
\end{aligned}$$

Given a subset S of Q such that $|S| = m$, consider the subset $\tilde{S}$ defined by

$$\tilde{S} = \begin{cases} S \cup \{q_0\} & \text{if } n-1 \in S \text{ and } q_0 \notin S, \\ S & \text{otherwise.} \end{cases}$$

Let $\tilde{\Omega}(S)$ denote the set of all gaps of $\tilde{S} \cap C$ in the cycle C with the restricted order. We denote the largest size of an element of $\tilde{\Omega}(S)$ by $\tilde{\Gamma}(S)$. Note that $\tilde{S}$ must have at least one element in C, hence we have $\tilde{\Gamma}(S) \in \{0, 1, \ldots, n-2\}$. Let $\tilde{G}(S)$ denote the number of gaps of size $\tilde{\Gamma}(S)$ in $\tilde{\Omega}(S)$. The next two lemmas are related to $\tilde{S}$ and will be used to prove that the automata $\mathcal{D}''_n$, $\mathcal{E}_n$, $\mathcal{H}_n$ and $\mathcal{I}_n$ satisfy Conjecture 5.1.1.

Lemma 5.8.3. *Consider the weakly monotonic automaton $\mathcal{G} = (Q, \{a\}, \delta)$ with n states. Suppose that the letter a acts as a circular permutation on the subset $C = \{0, 1, \ldots, n-2\}$ of Q and sends $n-1$ to a state of C. Then given a subset S of Q, we have $\tilde{\Gamma}(S) \geq \Gamma(S)-1$.*

Proof. If $n-1 \notin S$, then $\tilde{S} = S$ and given $X \in \Omega(S)$, either $X \subseteq C$ and so $X \in \tilde{\Omega}(S)$, or $n-1 \in X$ and so $X - \{n-1\} \in \tilde{\Omega}(S)$. Thus $\tilde{\Gamma}(S) \geq \Gamma(S) - 1$.

If $n-1 \in S$ then $\tilde{S} = S \cup \{q_0\}$ and given $X \in \Omega(S)$, we have $X \subseteq C$. If $q_0 \notin X$, then $X \in \tilde{\Omega}(S)$. Otherwise, if $q_0 \in X$, since $n-1$ and q_0 are adjacent and $n-1 \notin X$, then $X - \{q_0\}$ is an interval of Q, therefore an interval of C, which means it belongs to $\tilde{\Omega}(S)$. Either way, we have $\tilde{\Gamma}(S) \geq \Gamma(S) - 1$. □

Lemma 5.8.4. *Consider the weakly monotonic automaton $\mathcal{G} = (Q, \{a\}, \delta)$ with n states. Suppose that the letter a acts as a circular permutation on the subset $C = \{0, 1, \ldots, n-2\}$ of Q and sends $n-1$ to a state of C. Let S be a subset of Q and k be a nonnegative integer. Suppose that the interval T of Q has l states, for some positive integer l, and is such that $n-1 \in T$ if and only if $q_0 \in T$. Let $\tilde{\delta}$ represent the restriction of δ to C. If $\tilde{S} \cap C \subseteq \tilde{\delta}^{-1}(T \cap C, a^k)$, then $S \subseteq \delta^{-1}(T, a^k)$.*

Proof. For $k = 0$, we are simply stating that if $\tilde{S} \cap C \subseteq T \cap C$, then $S \subseteq T$. If $n-1 \notin S$, then $S = \tilde{S} = \tilde{S} \cap C \subseteq T \cap C \subseteq T$. Otherwise, if $n-1 \in S$, then $q_0 \in \tilde{S}$, thus $q_0 \in T$ and according to our hypothesis on T, we have $n-1 \in T$. Hence, $S \subseteq (\tilde{S} \cap C) \cup \{n-1\} \subseteq (T \cap C) \cup \{n-1\} \subseteq T$.

Now let us assume $k > 0$. If $n-1 \notin S$, then $S = \tilde{S} \cap C \subseteq \tilde{\delta}^{-1}(T \cap C, a^k) \subseteq \delta^{-1}(T \cap C, a^k) \subseteq \delta^{-1}(T, a^k)$. If $n-1 \in S$, then $q_0 \in \tilde{\delta}^{-1}(T \cap C, a^k)$, therefore $n-1 \in \delta^{-1}(T \cap C, a^k)$, because $\delta(n-1, a) = \delta(q_0, a)$, hence $S \subseteq (\tilde{S} \cap C) \cup \{n-1\} \subseteq \delta^{-1}(T \cap C, a^k) \subseteq \delta^{-1}(T, a^k)$. □

Proposition 5.8.5. *Let $\mathcal{G} = (Q, A, \delta)$ be an automaton in $\{\mathcal{D}''_n, \mathcal{E}_n, \mathcal{H}_n, \mathcal{I}_n\}$. Then $\mathcal{G}$ satisfies Conjecture 5.1.1.*

Proof. Using Lemma 5.8.2, consider the state $s \in C$ and the word $v_{n-1-\tilde{\Gamma}(S)} \in A^*$, whose length is at most $3 + n(n - \tilde{\Gamma}(S) - 3)$ and for which $T = \delta^{-1}(\{s\}, v_{n-1-\tilde{\Gamma}(S)})$ is an interval of Q with $n - 1 - \tilde{\Gamma}(S)$ states in C, such that $n-1 \in T$ if and only if $q_0 \in T$.

Considering the automaton $\tilde{\mathcal{G}} = (C, \{a\}, \tilde{\delta})$ and the subsets $\tilde{S} \cap C$ and $T \cap C$ of C, we know from Lemma 5.7.6 that there is some $k \in \{0, 1, \ldots, n-1-(\tilde{G}(S)-1)\tilde{\Gamma}(S) - \tilde{G}(S)\}$ such that $\tilde{S} \cap C \subseteq \tilde{\delta}^{-1}(T \cap C, a^k)$. According to Lemma 5.8.4, this implies that $S \subseteq \delta^{-1}(T, a^k)$.

The word $w = a^k v_{n-1-\tilde{\Gamma}(S)}$ is such that $|\delta(S, w)| = 1$ and $|w| \leq 3 + n(n - \tilde{\Gamma}(S) - 3) + n - 1 - (\tilde{G}(S) - 1)\tilde{\Gamma}(S) - \tilde{G}(S) = (n-1)^2 + 1 - (n + \tilde{G}(S) - 1)\tilde{\Gamma}(S) - \tilde{G}(S)$.

The length of w is maximum if S is such that $\tilde{\Gamma}(S)$ is minimum among all subsets with m elements and $\tilde{G}(S)$ is minimum among all subsets P with m elements and minimum $\tilde{\Gamma}(P)$.

According to Lemma 5.8.3, we have $\tilde{\Gamma}(S) \geq \Gamma(S) - 1$. Hence, using Lemma 5.2.1, the minimum value of $\tilde{\Gamma}(S)$ is $\gamma - 1$.

By definition there is at most one $X \in \tilde{\Omega}(S)$ such that $X \notin \Omega(S)$. Hence, if $\tilde{\Gamma}(S) \geq \Gamma(S)$, we have $\tilde{G}(S) \geq G(S) - 1$. Otherwise, assuming that $\tilde{\Gamma}(S)$ is minimum and, therefore, so is $\Gamma(S)$, according to Lemma 5.2.1, we have $\Gamma(S) = \gamma$, $G(S) = g$ and all other gaps of S have size $\gamma - 1 = \tilde{\Gamma}(S)$. Thus, if $\tilde{\Gamma}(S) = \Gamma(S) - 1$, then $\tilde{G}(S) = m$.

Using these lower bounds on $\tilde{\Gamma}(S)$ and $\tilde{G}(S)$, we have

$$|w| \leq (n-1)^2 + 1 - (n + g - 2)\gamma - (g - 1),$$

if $\Gamma(\tilde{S}) = \gamma$ and $\tilde{G}(S) = g - 1$, or

$$|w| \leq (n-1)^2 + 1 - (n + m - 1)(\gamma - 1) - m = (n-1)^2 + n - (n + m - 1)\gamma,$$

if $\Gamma(\tilde{S}) = \gamma - 1$ and $\tilde{G}(S) = m$.

Since $m \geq g$, we have $n - (n + m - 1)\gamma \geq 1 - (n + g - 2)\gamma - (g - 1)$. It follows that $|w| \leq (n-1)^2 + n - (n + m - 1)\gamma$.

Since $f(n, m) = (n-1)^2 + n - (g-1)\gamma - g$, to finish the proof it suffices to check that $(n-1)^2 + n - (g-1)\gamma - g \geq (n-1)^2 + n - (n + m - 1)\gamma$, that is, $(g-1)\gamma + g \leq (n + m - 1)\gamma = (m - 1)\gamma + n\gamma$. This is obvious, since $g \leq m \leq n\gamma$. □

5.9 Experimental Evidence

Early in our work on subset synchronization, some experiments were conducted to verify our conjecture for specific automata. First we checked all the known examples of extreme and slowly synchronizing automata (in the last case up to a certain number of states). Then we considered all synchronizing automata with a small number of states and a small alphabet, namely all automata with at most 4 states and 4 letters, as well as those with 5 states and 2 letters. Larger automata were being verified thoroughly but that work was interrupted, because finding shortest synchronizing words for all subsets is computationally very expensive.

Marek Szykuła heard about this work from M. V. Volkov and, at his request, conducted some more comprehensive experiments, concluding that our conjecture holds for the following cases:

- all automata with at most 5 states;
- all automata with 6 states and at most 4 letters;
- all automata with 7 states and 3 letters;
- all automata with at most 10 states and 2 letters.

Up to 9 states, M. Szykuła's work included non synchronizing automata, so for these small examples, a more general version of our conjecture holds. However, as was proved in [25, 38, 48] and referred in the Introduction, this is not true in general.

These computational results provide further evidence in favor of the bound we propose for the length of shortest subset synchronizing words.

Chapter 6

Conclusion

In Chapter 3, we have obtained tight upper bounds on the length of shortest universal synchronizing words for monotonic digraphs, generalized monotonic digraphs, aperiodic digraphs and acyclic digraphs. We have also shown that in order to obtain a general upper bound for all totally synchronizing digraphs, one may focus on the classes of strongly connected digraphs and digraphs with a sink.

The problem of computing the length of shortest universal synchronizing words for strongly connected digraphs and for digraphs with a sink remains open. The case of digraphs with a sink is probably easier to approach. For once, it is a simpler case for automata synchronization. Also note that if a digraph has a sink, then it is necessarily synchronizing, since all automata with a sink are synchronizing (see, for example [35]). As for strongly connected digraphs, a set of conditions that guarantee total synchronization remains unknown. Besides the fact that it is likely a simpler problem, digraphs with a sink have another advantage: the final state of each automaton after synchronization is always the same, namely the graph's sink state. In the general case, the state to which a totally synchronizing word takes an automaton depends on the automaton. That is not quite so useful, since one of the applications for total synchronization is not knowing the labeling of the digraph that describes the machine we want to reset.

In Chapter 4, we have exhibited a family of strongly connected aperiodic automata whose level of weak monotonicity grows with the number of states. This undermines any attempt to further improve the best known upper bound [47] on the length of shortest synchronizing words for strongly connected aperiodic automata, by using low levels of weak monotonicity. However, as stated in [47], the lower bound on the length of shortest synchronizing words for this class of automata is a linear function of the number of states, while the upper bound remains a quadratic function on the number of states. Hence, the problem of establishing a tight bound for this class of automata remains open.

In Chapter 5, a generalization of Černý's Conjecture for synchronizing subsets of states was presented. Using the Černý automaton we showed that the proposed upper bound is a lower bound. We established our conjecture for automata with a sink, which allowed us to show that if it is satisfied by strongly connected automata, then it is satisfied by all automata. We also proved our conjecture for a subclass of strongly connected automata, namely weakly oriented circular automata of jump 1 or with a letter of rank $n-1$. An upper bound was obtained for circular automata, but it is not quite as good as the one conjectured. All known examples of extreme and slowly synchronizing automata were shown to satisfy our conjecture. Also Marek Szykuła has verified computationally the bound we propose for all automata up to a certain size, which provides further evidence towards the conjecture. We further presented a simpler proof of Černý's Conjecture for weakly oriented automata, which was obtained in [7].

Whether our conjecture is true remains an open problem. Also, one may try to obtain a generalization of the Rank Conjecture for subsets. Such a conjecture would generalize all known open problems on the length of shortest words of a certain rank for automata.

References

[1] R. L. Adler, L. W. Goodwyn, and B. Weiss, *Equivalence of topological Markov shifts*, Israel J. Math. **27** (1977), no. 1, 48–63. (Cited on pages 13, 14, and 34.)

[2] R. L. Adler and B. Weiss, *Similarity of automorphisms of the torus*, Memoirs of the American Mathematical Society, No. 98, American Mathematical Society, Providence, R.I., 1970. (Cited on pages 13 and 14.)

[3] J. Almeida and A. Cardoso, *A sequence of weakly monotonic automata with increasing level*, Int. J. Algebra **7** (2013), no. 1-4, 91–100. (Cited on page 16.)

[4] J. Almeida, S. W. Margolis, B. Steinberg, and M. V. Volkov, *Representation theory of finite semigroups, semigroup radicals and formal language theory*, Trans. Amer. Math. Soc. **361** (2009), 1429–1461. (Cited on pages 13 and 14.)

[5] J. Almeida and B. Steinberg, *Matrix mortality and the Černý-Pin conjecture*, Developments in language theory, Lecture Notes in Comput. Sci., vol. 5583, Springer, Berlin, 2009, pp. 67–80. (Cited on pages 13 and 14.)

[6] D. S. Ananichev and M. V. Volkov, *Collapsing words vs. synchronizing words*, Developments in language theory (Vienna, 2001), Lecture Notes in Comput. Sci., vol. 2295, Springer, Berlin, 2002, pp. 166–174. (Cited on page 15.)

[7] ______, *Some results on Černý type problems for transformation semigroups*, Proceedings of the Workshop Semigroups and Languages (Singapore) (I. M. Araújo, M. J. J. Branco, V. H. Fernandes, and G. M. S. Gomes, eds.), World Scientific, 2004, pp. 23–42. (Cited on pages 13, 17, 86, and 104.)

[8] ______, *Synchronizing monotonic automata*, Theor. Comp. Sci. **327** (2004), 225–239. (Cited on pages 22, 23, and 26.)

[9] ______, *Synchronizing generalized monotonic automata*, Theor. Comp. Sci. **330** (2005), 3–13. (Cited on pages 13, 22, and 23.)

[10] D. S. Ananichev, M. V. Volkov, and V. V. Gusev, *Primitive digraphs with large exponents and slowly synchronizing automata*, Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI) **402** (2012), no. Kombinatorika i Teoriya Grafov. IV, 9–39, 218. (Cited on pages 29, 30, 31, 32, 33, and 34.)

[11] D. S. Ananichev, M. V. Volkov, and Y. I. Zaks, *Synchronizing automata with a letter of deficiency 2*, Theor. Comp. Sci. **376** (2007), 30–41. (Cited on pages 13, 29, and 31.)

[12] F. Arnold and B. Steinberg, *Synchronizing groups and automata*, Theor. Comp. Sci. **359** (2006), 101–110. (Cited on page 13.)

[13] J. Černý, *Poznámka k homogénnym eksperimentom s konecnými automatami (A note on homogeneous experiments with finite automata)*, Mat.-Fyz. Cas. Solvensk. Akad. Vied. **14** (1964), 208–216. (Cited on pages 13, 16, 20, 21, 72, and 73.)

[14] J. Černý, A. Pirická, and B. Rosenauerová, *On directable automata*, Kybernetika (Prague) **7** (1971), 289–298. (Cited on page 28.)

[15] K. Culik, II, J. Karhumäki, and J. Kari, *A note on synchronized automata and road coloring problem*, Developments in language theory (Vienna, 2001), Lecture Notes in Comput. Sci., vol. 2295, Springer, Berlin, 2002, pp. 175–185. (Cited on page 34.)

[16] L. Dubuc, *Sur les automates circulaires et la conjecture de Černý*, Theoret. Informatics Appl. **32** (1998), 21–34. (Cited on pages 13 and 25.)

[17] D. Eppstein, *Reset sequences for monotonic automata*, SIAM J. Comput. **19** (1990), 500–510. (Cited on pages 13, 17, and 26.)

[18] M. A. Fischler and M. Tannenbaum, *Synchronizing and representation problems for sequential machines with masked outputs*, Proc. 11th Annual Symp. Foundations Comput. Sci. (1970), 97–103. (Cited on page 13.)

[19] P. Frankl, *An extremal problem for two families of sets*, European J. Combin. **3** (1982), 125–127. (Cited on page 13.)

[20] J. Friedman, *On the road coloring problem*, Proc. Amer. Math. Soc. **110** (1990), no. 4, 1133–1135. (Cited on page 34.)

[21] M. Grech and A. Kisielewicz, *The Černý conjecture for automata respecting intervals of a directed graph*, Discrete Math. Theor. Comput. Sci. **15** (2013), no. 3, 61–72. (Cited on page 13.)

[22] J. Kari, *A counter example to a conjecture concerning synchronizing words in finite automata*, Bull. Eur. Assoc. Theor. Comput. Sci. EATCS (2001), no. 73, 146. (Cited on pages 13 and 21.)

[23] ———, *Synchronizing finite automata on Eulerian digraphs*, Theoret. Comput. Sci. **295** (2003), no. 1-3, 223–232, Mathematical foundations of computer science (Mariánské Lázně, 2001). (Cited on pages 13 and 34.)

[24] A. A. Klyachko, I. K. Rystsov, and M. A. Spivak, *An extremal combinatorial problem associated with the bound of the length of a synchronizing word in an automaton.*, Cybernet. Systems Anal. **23** (1987), no. 2, 165–171. (Cited on page 13.)

[25] D. Lee and M. Yannakakis, *Testing finite-state machines: state identification and verification*, IEEE Trans. Comput. **43** (1994), no. 3, 306–320. (Cited on pages 16 and 101.)

[26] S. W. Margolis, J.-E. Pin, and M. V. Volkov, *Words guaranteeing minimum image*, Internat. J. Found. Comput. Sci. **15** (2004), no. 2, 259–276. (Cited on page 15.)

[27] B. K. Natarajan, *An algorithmic approach to the automated design of parts orienters*, Proceedings of the 27th Annual Symposium on Foundations of Computer Science (Washington, DC, USA), SFCS '86, IEEE Computer Society, 1986, pp. 132–142. (Cited on page 16.)

[28] C. Nicaud, *Fast synchronization of random automata*, CoRR **abs/1404.6962** (2014). (Cited on page 29.)

[29] J.-E. Pin, *Sur un cas particulier de la conjecture de Černý*, 5th ICALP (Berlin), Lect. Notes Comput. Sci., vol. 62, Springer, 1978, pp. 345–352. (Cited on pages 13 and 25.)

[30] ______, *Le problème de la synchronisation et la conjecture de Černý*, Noncommutative structures in algebra and geometric combinatorics (Naples, 1978), Quad. "Ricerca Sci.", vol. 109, CNR, Rome, 1981, pp. 37–48. (Cited on pages 13 and 21.)

[31] ______, *On two combinatorial problems arising from automata theory*, Annals Discrete Math. **17** (1983), 535–548. (Cited on pages 13, 22, and 28.)

[32] A. Roman, *A note on Černý conjecture for automata over 3-letter alphabet*, Journal of Automata, Languages and Combinatorics **13** (2008), no. 2, 141–143. (Cited on page 28.)

[33] I. K. Rystsov, *On the rank of a finite automaton*, Kibernet. Sistem. Anal. (1992), no. 3, 3–10, 187. (Cited on page 13.)

[34] ______, *Quasioptimal bound for the length of reset words for regular automata*, Acta Cybernet. **12** (1995), no. 2, 145–152. (Cited on page 13.)

[35] ______, *Reset words for commutative and solvable automata*, Theor. Comp. Sci. **172** (1997), 273–279. (Cited on pages 13, 23, and 103.)

[36] ______, *On the length of reset words for automata with simple idempotents*, Kibernet. Sistem. Anal. (2000), no. 3, 32–39, 187. (Cited on page 13.)

[37] ———, *On the height of a finite automaton*, Kibernet. Sistem. Anal. **40** (2004), no. 4, 3–16, 188. (Cited on page 13.)

[38] A. Salomaa, *Composition sequences for functions over a finite domain*, Theoret. Comput. Sci. **292** (2003), no. 1, 263–281, Selected papers in honor of Jean Berstel. (Cited on pages 16 and 101.)

[39] S. Sandberg, *Homing and synchronizing sequences*, Model-Based Testing of Reactive Systems, Lecture Notes in Comput. Sci., vol. 3472, 2005, pp. 5–33. (Cited on page 16.)

[40] B. Steinberg, *Černý's conjecture and group representation theory*, J. Algebraic Combin. **31** (2010), no. 1, 83–109. (Cited on page 13.)

[41] ———, *The Černý conjecture for one-cluster automata with prime length cycle*, Theoret. Comput. Sci. **412** (2011), no. 39, 5487–5491. (Cited on page 13.)

[42] A. N. Trahtman, *An efficient algorithm finds noticeable trends and examples concerning the Černy conjecture*, Mathematical foundations of computer science 2006, Lecture Notes in Computer Science, vol. 4162, Springer, Berlin, 2006, pp. 789–800. (Cited on page 13.)

[43] ———, *The Černý conjecture for aperiodic automata*, Discrete Math. Theor. Comput. Sci. **9** (2007), 3–10 (electronic). (Cited on pages 13 and 26.)

[44] ———, *The road coloring problem*, Israel J. Math. **172** (2009), 51–60. (Cited on pages 14 and 34.)

[45] ———, *Modifying the upper bound on the length of minimal synchronizing word*, Fundamentals of computation theory, Lecture Notes in Comput. Sci., vol. 6914, Springer, Heidelberg, 2011, pp. 173–180. (Cited on pages 13 and 29.)

[46] M. V. Volkov, *Synchronizing automata and the Černý conjecture*, Language and Automata: Theory and Aplications. LATA 2008 (Berlin-Heidelberg-N.Y.) (C. Martín-Vide, F. Otto, and H. Fernau, eds.), Lect. Notes Comp. Sci., no. 5196, Springer-Verlag, 2008, pp. 11–27. (Cited on pages 13 and 27.)

[47] ———, *Synchronizing automata preserving a chain of partial orders*, Theor. Comp. Sci. **410** (2009), 3513 – 3519. (Cited on pages 13, 16, 23, 24, 27, and 103.)

[48] V. Vorel, *Subset Synchronization of Transitive Automata*, 2014, arXiv:1403.3972 [cs.FL]. (Cited on pages 16, 17, and 101.)

[49] P. J. Walker, *Synchronising automata and a conjecture of Černý*, Master's thesis, University of Manchester, United Kingdom, 2008. (Cited on page 72.)

List of Figures

Index