Radboud University Nijmegen

Faculty of Science

Synchronizing automata and their reset words

The expected length of a reset word

Master thesis Mathematics

Author:
A.M.M. van Hoorn BSc
s4760387

Supervisor:
Dr. ir. H. Don

Second reader:
Dr. W. Bosma

June 2022

Content

Chapter 1

Introduction

Fresh carrots come out of the ground with green leaves attached, called haulm. However, before the carrots are sold in the supermarket, the haulm is in most cases removed. The haulm can be cut off for every carrot individually, but it would be faster if all carrots lie side by side with the haulm of each carrot pointing the same way. It is under these circumstances possible for a machine to cut off the haulm of all the carrots at once. The use of a machine for this process is more beneficial in comparison to manual labour, because it is cheaper in the long term. For such a machine to function efficiently, all haulms have to be aligned in the same direction. In Figure 1.1 we see different phases of this process. First all carrots are in disorder, in the next phase they are all aligned with the haulm pointing to the right. The end product consists of carrots without their haulm.

Figure 1.1: Phases of removing the haulm.

The step to achieve the correct alignment is executed by a machine, that performs a series of actions. The starting position of a carrot has no impact on the end result, since the haulms of all carrots are pointing in the same direction when the process of the machine has ended. In mathematics the necessary actions to achieve this and the possible positions are schematically visualised as an automaton.
The starting position of a carrot can be simplified to four possibilities. If we look from above, the haulm can point up (U), down (D), left (L) and right (R). We call (U), (D), (L) and (R) the four states of a carrot.

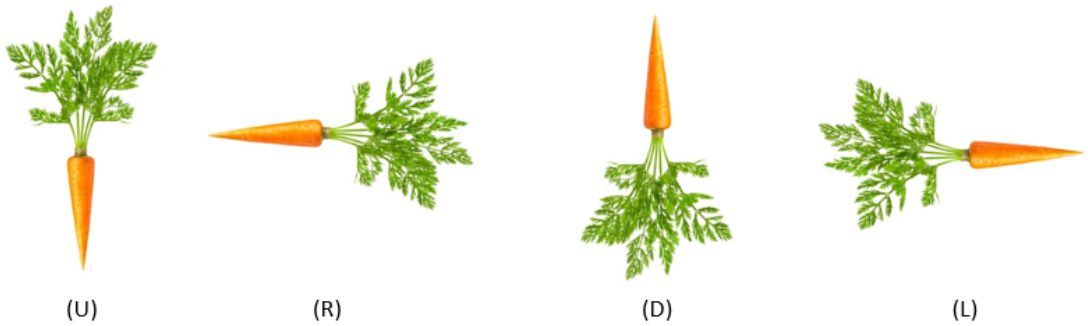

Figure 1.2: The four different states of a carrot.

All carrots, no matter the state they are in, are processed in the machine simultaneously. The machine has two possible actions for moving carrots. Option one consists of turning all the carrots clockwise. Option two consists of turning only the carrots which are in state (U). The carrots in state (R),(D) and (L) stay in their same state, when option two is applied.
The question is, with which sequence of actions we can go from carrots in all possible states ((U), (D), (L) and (R)) to all carrots in the same state (R)? For financial reasons, it is of importance that the machine is as efficient as possible. The question is now, what is the shortest sequence of actions that accomplishes our goal (all carrots in the same state (R))?
This we can research with the use of mathematics. As stated before, the machine to align the carrots is perceived as an automaton $\mathcal{A} = (Q, \Sigma, \delta)$, with a finite amount of states Q, a alphabet Σ and a transition function δ. In our carrot example, Q consists of the four states (U), (R), (D) and (L). The alphabet represents the different actions we can perform. In our carrot example, there are two possible action and thus two letters. In the introduction of this thesis letter a stands for action two and letter b for action one. The transition function $\delta : Q \times \Sigma \to Q$, tells us what a letter does on the current state (of for instance our carrots). For example, in our machine, letter b turns the carrots a quarter clockwise. Thus a carrot in state (R) goes to state (D) after "reading" letter b ($\delta((\text{R}), b) = (\text{D})$).
Schematically this looks like shown below.

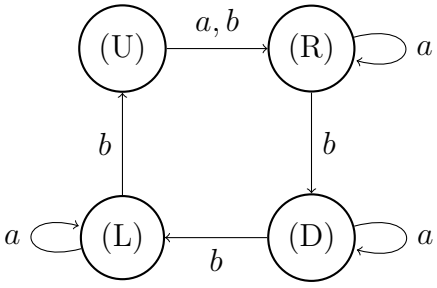

Figure 1.3: Diagram of the carrot automaton.

A sequence of letters that causes all carrots to end in the same state, for instance state (R), is called a reset word. An automaton which has a reset word is called a synchronizing automaton. There are many different reset words, but with the shortest reset word, our machine performs as efficient as possible. For that reason we search for the shortest reset word, in this case this is word $w = abbbabbba$ (see Theorem 3.3).

There are many more objects for which an automaton with its shortest reset word is required to sort and orientate the objects. For instance, cutting mushrooms stems at the same length, or sticking an etiquette at a certain surface of an object. This raises the following questions: Which synchronizing automaton has the largest shortest reset word, and what is the length of that word?

In 1964, J. Černý, a Slovak computer scientist, first explicitly mentioned a synchronizing automaton, although he called such automaton differently at the time. The name 'synchronizing' in this context was probably introduced by F.C. Hennie in the same year. The year 1964 was also the year that J. Černý came with the still not proven Černý conjecture, claiming that considering all synchronizing automata with $n \in \mathbb{N}$ states, the length of the largest shortest reset word is $(n-1)^2$. Throughout time, different mathematicians found different upper bounds for the length of the largest shortest reset word. We will discuss Černý's conjecture and several upper bounds in Chapter 3.

Most studies in the literature are written about the length of the shortest reset word when we can choose the sequence of the letters ourselves. However, there are less publications about this subject in case we can't choose the sequence of the letters. In that case we get a letter $\sigma \in \Sigma$ with a certain probability (the sum of those probabilities must be equal to one). Since we are working with probabilities we can only look at the expected length of a reset word. This raises the following questions: Which synchronizing automaton has the largest expected length of a reset word? Considering all synchronizing automata with $n \in \mathbb{N}$ states, what is the largest expected length of a reset word? Does the automaton with the largest shortest reset word also have the largest expected length of a reset word?

In this thesis we will discuss two problems, namely what is the length of the largest shortest reset word and what is the value of the largest expected length of a reset word.
To make these problems more clear and abstract, we first provide some preliminaries and definitions in Chapter 2. Then in Chapter 3 we discuss the first problem, what is the length of the largest shortest reset word. This is mostly done by literature research. In the fourth Chapter we discuss how to calculate the expected length of a reset word of a certain automaton and we use this knowledge to look which automaton has the largest expected length of a reset word. Finally, in the same chapter, we prove that the value of the largest expected length of a reset word is bounded by some upper and lower bound. We end this thesis with a conclusion about the findings and suggest further related research topics.

Chapter 2

Preliminaries and definitions

Before we can start with the research, we need some definitions.[9][5][8][4]
Normally when we talk about languages we talk about English, Dutch, Spanish, etc. In mathematics we can also talk about languages, here we form words from a given alphabet.

Definition 2.1. A *alphabet* is a finite set of symbols and/or letters. We denote a alphabet with Σ.

Example 2.2. Examples of alphabets are:

- $\Sigma = \mathbb{N} = \{1, 2, \dots\}$
- $\Sigma = \{a, b\}$
- $\Sigma = \{a, b, c, \dots, x, y, z\}$ (Dutch alphabet)
- $\Sigma = \{$yellow, orange, red, green, blue, purple$\}$ (The colors of a rainbow)
- $\Sigma = \{\alpha, \beta, \gamma, \dots, \omega\}$ (Greek alphabet)

Remark. In this thesis, the set of natural number is: $\mathbb{N} = \{1, 2, \dots\}$.

Definition 2.3. A *word* is a finite sequence of letters/symbols from an alphabet Σ. We define λ to be the empty word.
We say a word w is of length m when the number of symbols forming this word w is m. Notation: length$(w) := |w| = m$
$|w|_\sigma$ is the number of times symbol $\sigma \in \Sigma$ occurs in word w.
Let $\sigma \in \Sigma$ and $j \in \mathbb{N}$, then we denote with σ^j the word of j times the letter σ. Thus, $\sigma^j = \underbrace{\sigma\sigma\sigma\cdots\sigma}_{j}$

Example 2.4. Let $\Sigma = \{a, b\}$, then $w = (ab^3)^2a = abbbabbba$ is a possible word. This word w is of length 9 ($|w| = 9$) and has $|w|_a = 3$ and $|w|_b = 6$.

Definition 2.5. With Σ^* we denote the set of all finite words over Σ. So this is the set of all words that we can make with our alphabet Σ.

Remark. Clearly a single symbol/letter is also a word, therefore $\Sigma \subseteq \Sigma^*$.
Since $\lambda \in \Sigma^*$ for all alphabets, we have $\Sigma^* \neq \emptyset$. In addition if $\Sigma \neq \emptyset$, then $|\Sigma^*| = \infty$.

Example 2.6. Let $\Sigma = \{a, b\}$, then $\Sigma^* = \{\lambda, a, b, aa, bb, ab, ba, aaa, \dots, abbbabbba, \dots\}$.

Definition 2.7. Suppose $v, w \in \Sigma^*$, then we denote the *concatenation* of the words v and w by $v \cdot w$ ($\in \Sigma^*$). Often we drop $\cdot$, so we write vw for $v \cdot w$.

Example 2.8. Let $v = aba$ and $w = bb$, then $vw = ababb$.

Remark. Let $v, w \in \Sigma^*$ and $\sigma \in \Sigma$, then $|vw| = |v| + |w|$ and $|vw|_\sigma = |v|_\sigma + |w|_\sigma$. The concatenation isn't commutative. Look for instance at Example 2.8, here is $vw = ababb$, but $wv = bbaba \neq vw$.

Definition 2.9. Let $i \in \mathbb{N}$, then we have the following notations.
$\Sigma^i := \{w \in \Sigma^* \mid |w| = i\}$, so Σ^i is the collection of words with length equal to i.
$\Sigma^{\leq i} := \{w \in \Sigma^* \mid |w| \leq i\}$, so $\Sigma^{\leq i}$ is the collection of words with length less or equal then i.

Remark. We have $\Sigma^i \subseteq \Sigma^{\leq i}$.

Now we have defined words, we want to define a machine that can process these words.

Definition 2.10. A *deterministic finite automaton (DFA)* $\mathcal{A}$ is a 3-tuple (Q, Σ, δ), where

- Q is a finite set of states.
- Σ is an alphabet.
- δ is a (transition) function: $\delta : Q \times \Sigma \to Q$. Let $q \in Q$ a state and $l \in \Sigma$ a letter from our alphabet, then $\delta(q, l) = q' \in Q$. The delta function gives you a (different) state given a state and a letter from our alphabet.

In this thesis we often call a DFA an automaton.
We can expand the definition of the delta function to a function that processes words not only symbols/letters from our alphabet.

Definition 2.11. Let $w \in \Sigma^*$ ($w \neq \lambda$), which we can write as $w = ul$ with $u \in \Sigma^*$ and $l \in \Sigma$. Let $q \in Q$. We define the function $\delta : Q \times \Sigma^* \to Q$ as
$\delta(q, w) := \delta(\delta(q, u), l)$. It holds that $\delta(q, \lambda) := q$.

Example 2.12. In Figure 2.1 we see a example of a deterministic finite automaton (DFA). Here we have:

$Q := \{q_0, q_1, q_2\}$ $\qquad$ $\Sigma := \{a, b\}$
$\delta(q_0, a) = q_1$ $\qquad$ $\delta(q_0, b) = q_1$
$\delta(q_1, a) = q_2$ $\qquad$ $\delta(q_1, b) = q_0$
$\delta(q_2, a) = q_1$ $\qquad$ $\delta(q_2, b) = q_2$

$$\begin{aligned}\delta(q_0, aaba) = \delta(\delta(q_0, aab), a) = \delta(\delta(\delta(q_0, aa), b), a) = \delta(\delta(\delta(\delta(q_0, a), a), b), a)\\ = \delta(\delta(\delta(q_1, a), b), a) = \delta(\delta(q_2, b), a) = \delta(q_2, a) = q_1\end{aligned}$$

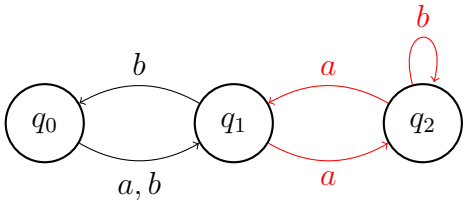

Figure 2.1: A deterministic finite automaton.

Definition 2.13. The power automaton $\mathcal{P}_\mathcal{A}$ of a given DFA $\mathcal{A} = (Q, \Sigma, \delta)$ is a 3-tuple $(\hat{Q}, \Sigma, \delta)$ with:

- $\hat{Q} = \mathcal{P}(Q)\backslash\emptyset$
- The function δ is an expansion of our already seen delta function, defined as follows.
  $\delta : \mathcal{P}(Q)\backslash\emptyset \times \Sigma^* \to \mathcal{P}(Q)\backslash\emptyset$
  We have $\delta(H, w) := \cup_{q\in H}\delta(q, w)$, with $H \in \hat{Q}$ and $w \in \Sigma^*$ a word.

Example 2.14. The power automaton of the DFA in Example 2.12 is given in Figure 2.2.

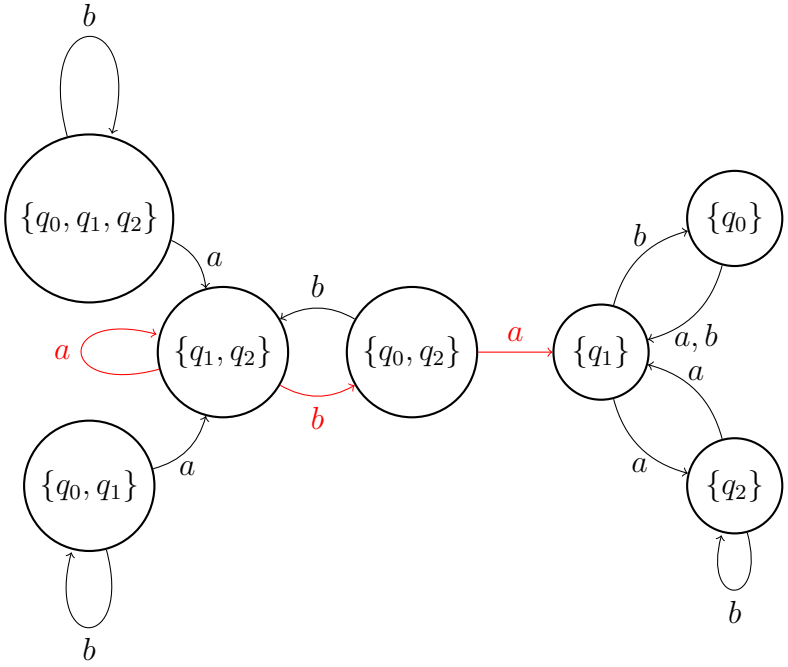

Figure 2.2: The power automaton of the DFA in Figure 2.1

Definition 2.15. A automaton is called *synchronizing* when there exist a $w \in \Sigma^*$ and a state $q \in Q$ such that, $\forall q' \in Q$, $\delta(q', w) = q$. The word $w \in \Sigma^*$ is then called a *reset (or synchronizing) word.*
Let $p, q \in Q$, then we call $w \in \Sigma^*$ a *reset word for p and q* if $\delta(p, w) = \delta(q, w)$.
Let $S \subseteq Q$, then we call $w \in \Sigma^*$ a *reset word for S* if $\delta(p, w) = \delta(q, w)$ for all $p, q \in S$.

Remark. Not every automaton is synchronizing. When an automaton is synchronizing, there are multiple reset words. Thus, reset words aren't unique.
In addition, the largest reset word for a synchronizing automaton $\mathcal{A}$ is infinitely long. If $w \in \Sigma^*$ is a reset word, then it is still a reset word after we add (infinitely many) letters at the end of word w.

Definition 2.16. Let $q \in Q$ be a state, $S \subseteq Q$ and $w \in \Sigma^*$ a word. Then we use the following notation: $q \circ w := \delta(q, w)$.
We also write $S \circ w := \delta(S, w) = \{q \circ w \mid q \in S\}$.
$S \circ w^{-1}$ is *the preimage* of S, thus $S \circ w^{-1} = \{q \in Q \mid q \circ w \in S\}$.
When S is a singleton, let's say $S = \{q\}$, then we write
$q \circ w^{-1} = \{q\} \circ w^{-1} = \{p \in Q \mid q = p \circ w\}$.

Definition 2.17. Let w be a word and $0 \leq k \leq |w|$ an integer. Then $w_{[k]}$ is the word consisting of the first k letters of word w. For $1 \leq k \leq |w|$, w_k is the k^{th} letter of word w .

Example 2.18. Let $w = abba$. Then $w_{[0]} = \lambda$ (the empty word), $w_{[1]} = a$, $w_{[2]} = ab$, $w_{[3]} = abb$ and $w_{[4]} = abba = w$. We also have $w_1 = w_4 = a$ and $w_2 = w_3 = b$.

Definition 2.19. Let $\mathcal{A}$ be a DFA. A path in $\mathcal{A}$ indicated by a word $w \in \Sigma^*$, starting in some state $q \in Q$, is the path composed of the arrows in $\mathcal{A}$ you follow, indicated by the letters of word w.
Analogue, a path in $\mathcal{P}_\mathcal{A}$ indicated by a word $w \in \Sigma^*$, starting in some state
$\emptyset \neq S \subseteq Q$, is the path composed of the arrows in $\mathcal{P}_\mathcal{A}$ you follow, indicated by the letters of word w.

Example 2.20. Let $\mathcal{A}$ be the DFA in Figure 2.1, then $\mathcal{P}_\mathcal{A}$ is given in Figure 2.2. Let $w = aba$.
The path in $\mathcal{A}$ indicated by word w, with starting state q_1, is indicated in red in Figure 2.1. This path starts in state q_1, goes to state q_2, goes through a self loop and ends in state q_2.
The path in $\mathcal{P}_\mathcal{A}$ indicated by word w, with starting state $\{q_1, q_2\}$, is indicated in red in Figure 2.2. This path starts in state $\{q_1, q_2\}$, goes through a self loop, then goes to state $\{q_0, q_2\}$ and ends in state $\{q_1\}$.

Observation 2.21. A DFA $\mathcal{A}$ is synchronizing if and only if there exist a path from Q to a singleton ($\{\cdot\} \subset Q$) in the corresponding power automaton $\mathcal{P}_\mathcal{A}$.

We can modify this observation to a proposition about when a word $w \in \Sigma^*$ is a reset word or not.

Proposition 2.22. *A word $w \in \Sigma^*$ is a reset word for DFA $\mathcal{A}$ if and only if w indicates a path from Q to a singleton ($\{\cdot\} \subset Q$) in the corresponding power automaton $\mathcal{P}_\mathcal{A}$.*

Let's look at some examples.

Example 2.23. The word $v = aba$ is a reset word for the DFA in Figure 2.1. This reset word leads every state to state q_1. However, then every word w, with the subword aba in it, is a reset word (but then perhaps to a different state). So $u = abab$ is a reset word to state q_2 and $z = abaa$ is a reset word to state q_2.

Example 2.24. In Figure 2.3 we see a DFA $\mathcal{A}$ with 4 states. The corresponding power automaton is given in Figure 2.4. To find a reset word for this automaton we try to find a path from $Q = \{1, 2, 3, 4\}$ to a singleton ($\{1\}$, $\{2\}$ or $\{3\}$, $\{4\}$). We can see in Figure 2.4, that the word $v = abbababbba$ indicates such a path (to $\{1\}$). However, we can see that the word $u = abbbabbba$ is also a reset word. Note that in word v every time we could have the possibility to get $|\delta(S, l)| < |S|$, we choose our next letter to be that letter l. However, this did not lead to the shortest reset word in this automaton.

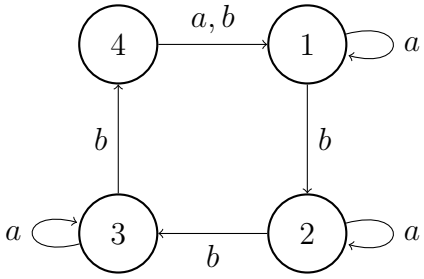

Figure 2.3: The Černý automaton with 4 states.

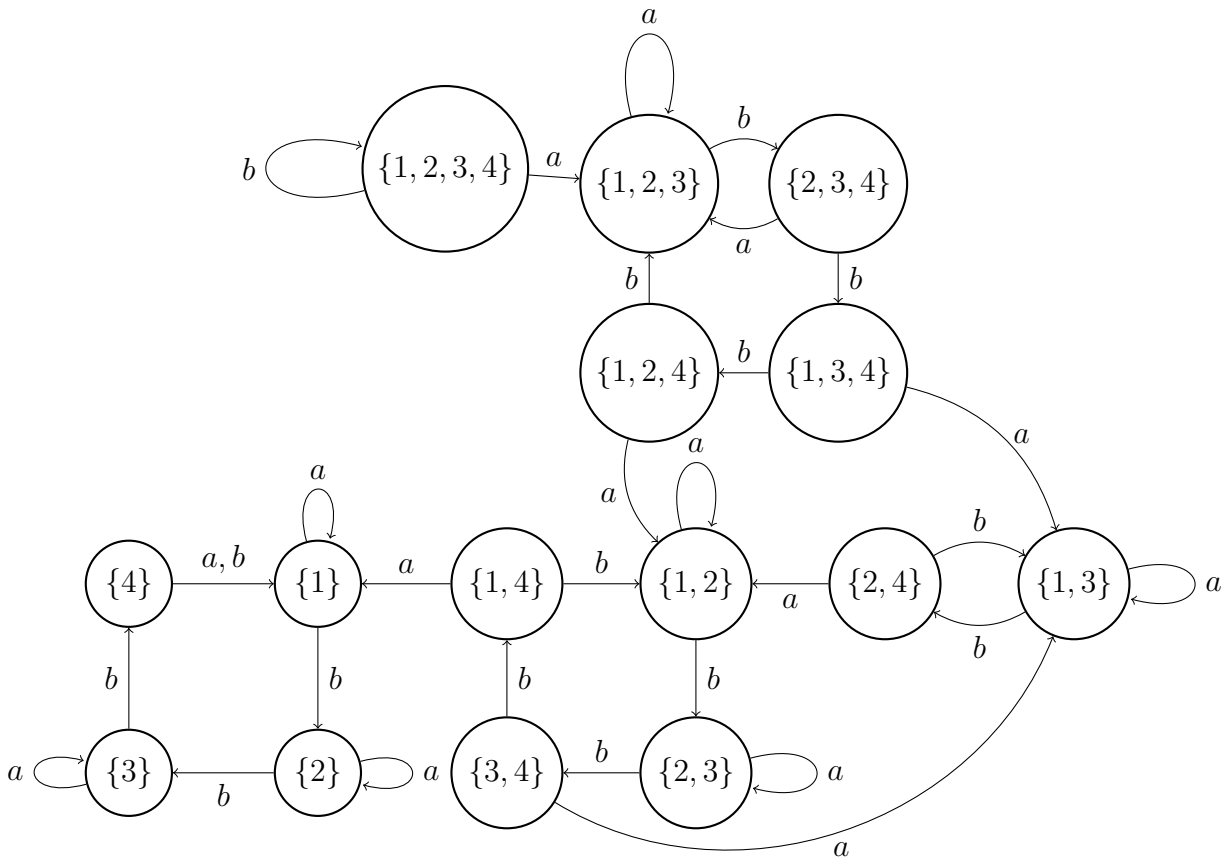

Figure 2.4: The power automaton of Figure 2.3

Chapter 3

Černý's conjecture

In practice, we always look for the shortest reset word, by using that word we are faster to a singleton.
Let $\mathcal{A}$ be a DFA with n states and w the shortest reset word for $\mathcal{A}$. Then we define $l(\mathcal{A})$ to be the length of this shortest word ($l(\mathcal{A}) = |w|$).

For every DFA $\mathcal{A}$, with $n \in \mathbb{N}$ states, we are interested in the length of the shortest reset word. There are several different DFA's $\mathcal{A}$ with n states. We are interested in the maximal length of the shortest reset word considering all DFA's $\mathcal{A}$ with n states.

Definition 3.1. $C(n) := \max\{l(\mathcal{A}) \mid \mathcal{A}$ is a synchronizing DFA with n states$\}$.

In 1964, Ján Černý came up with the conjecture that $C(n) = (n-1)^2$ [4]. This is called the *Černý's conjecture* and is still an unsolved problem.

Černý's conjecture: $C(n) = (n-1)^2$

In 1969, Ján Černý showed a construction of a automaton with n states for which the shortest reset word has length $(n-1)^2$. This automaton is called the *Černý automaton*, which will be discussed in Subsection 3.1. This automaton shows that $C(n) \geq (n-1)^2$, but proving $C(n) \leq (n-1)^2$ has so far not been successful. We do have other upper bounds about $C(n)$ that are proven, these will be discussed in Subsection 3.2.

3.1 The Černý automaton

Definition 3.2. The *Černý automaton* with n states ($Q = \{1, 2, \ldots, n\}$), is a DFA with $\Sigma = \{a, b\}$ and the following transition function.

$$\delta : Q \times \Sigma^* \to Q : \begin{cases} \delta(i,a) = i & \text{for } i = 1, \ldots, n-1 \\ \delta(i,b) = i+1 \bmod n & \text{for } i = 1, \ldots, n-1 \\ \delta(n,a) = \delta(n,b) = 1 & \end{cases}$$

We denote the Černý automaton with n states by $\mathcal{C}_n$.

In Figure 2.3, we see the Černý automaton with 4 states, $\mathcal{C}_4$. We have already seen that $w = abbbabbba$ is a reset word for this automaton ($\mathcal{C}_4$). $w = (ab^{n-1})^{n-2}a$ is a reset for $\mathcal{C}_n$. This we can check as follows. Observe that $\delta(n, ab^{n-1}) = n$ and that for all $k \in \{1, \ldots, n-1\}$ it holds that $\delta(k, ab^{n-1}) = k - 1$. This means that for all $k \in \{1, \ldots, n-2\}$ we get $\delta(k, (ab^{n-1})^{n-2}) = n$. We also have $\delta(n, (ab^{n-1})^{n-2}) = n$ and $\delta(n-1, (ab^{n-1})^{n-2}) = 1$. Since $\delta(n, a) = \delta(1, a) = 1$, we then get that $w = (ab^{n-1})^{n-2}a$ is a reset word for $\mathcal{C}_n$.

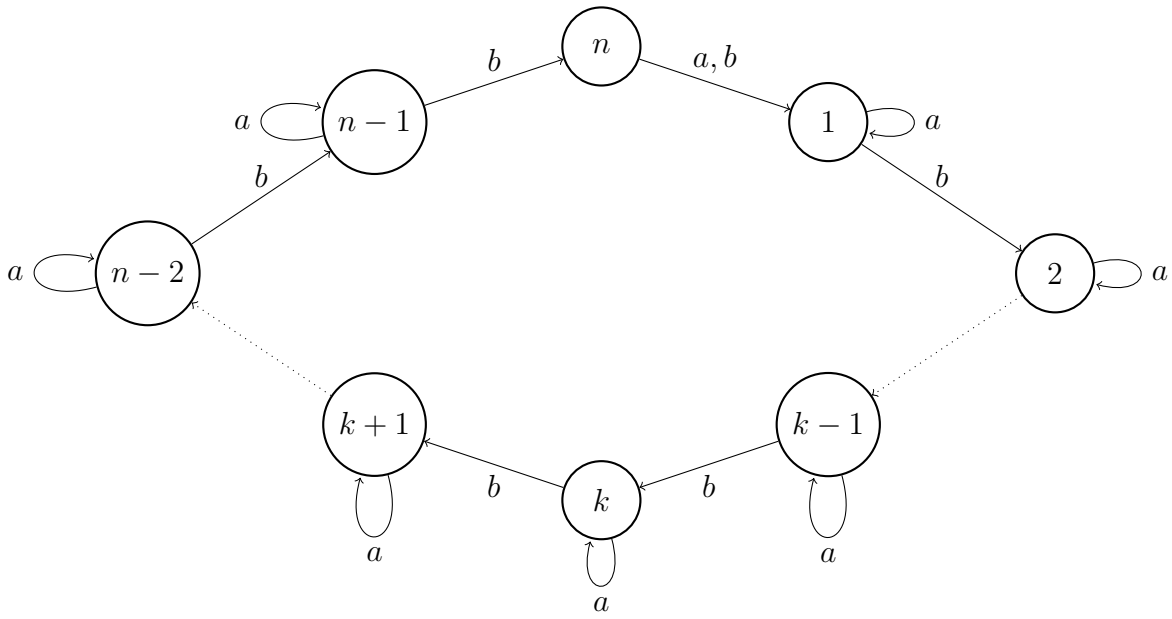

Figure 3.1: The Černý automaton with n states ($\mathcal{C}_n$).

Now we like to prove that this is also the shortest possible reset word for $\mathcal{C}_n$.

Theorem 3.3. *Let $\mathcal{C}_n$ be the Černý automaton with n states an w the shortest reset word of $\mathcal{C}_n$. Then $|w| = (n-1)^2$.[4]*

Proof. ([11]) We give an informal prove. The situation we describe is analogue to the situation we will describe in the proof of Theorem 4.15. In subsection 4.2.3 we will give more formal definitions.

Let w be the shortest reset word for $\mathcal{C}_n$. We set a certain situation. We have n pawns: $\{1, \ldots, n\}$.
Consider the situation that we start with a pawn on each state, let say pawn k starts at state k, where $k = 1, \ldots, n$.

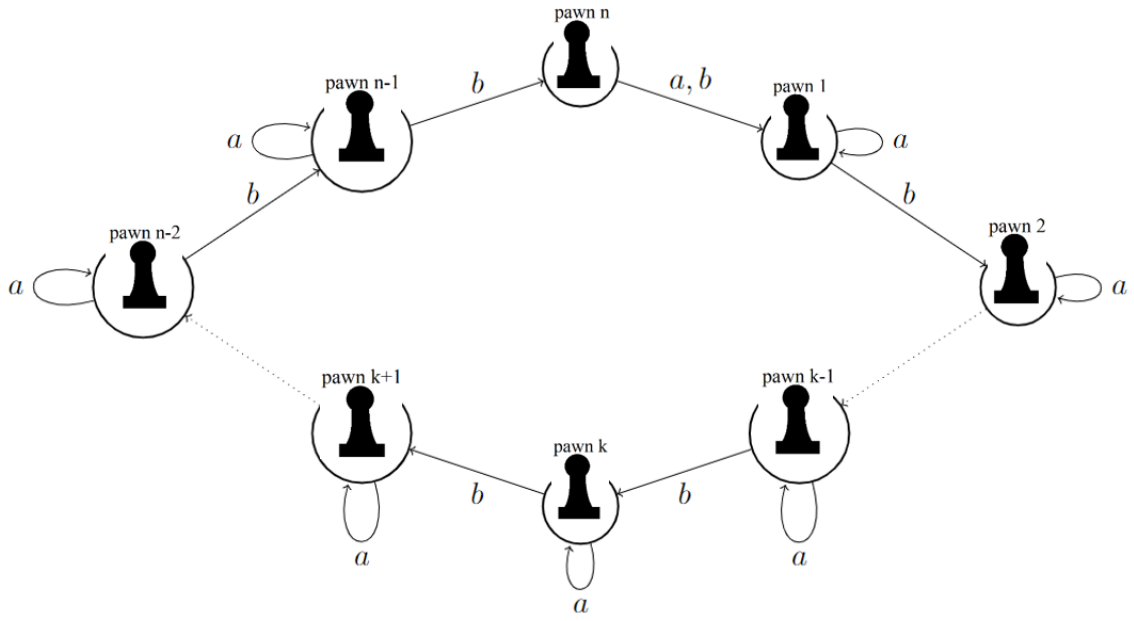

Figure 3.2: Starting situation: pawn k on state k.

If we read the letter b, starting in the starting position, then all pawns move one state forward. So, pawn n will be on state 1 and pawn k will be on state $k+1$, for all $k = 1, \ldots, n-1$.

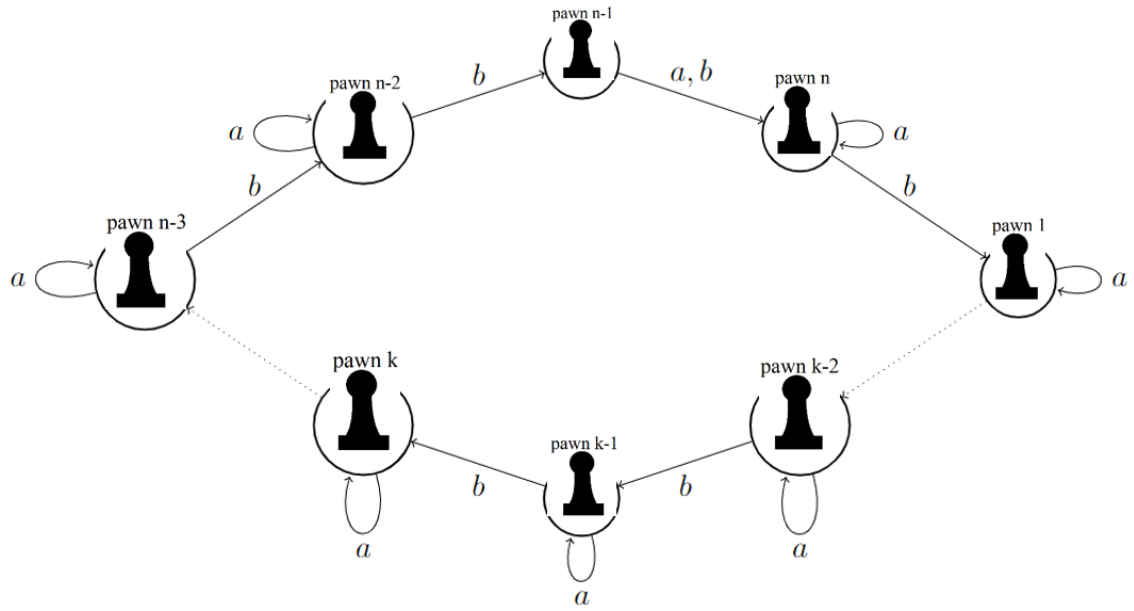

Figure 3.3: Situation after reading letter b.

If we read the letter a, starting in the starting position, then pawn k stays at state k for all $k = 1, \ldots, n-1$. Pawn n will go to state 1 after reading the letter a. In

this situation, pawn n catches up with pawn 1. Pawn n and 1 now follow the same path, thus will always be on the same state together.

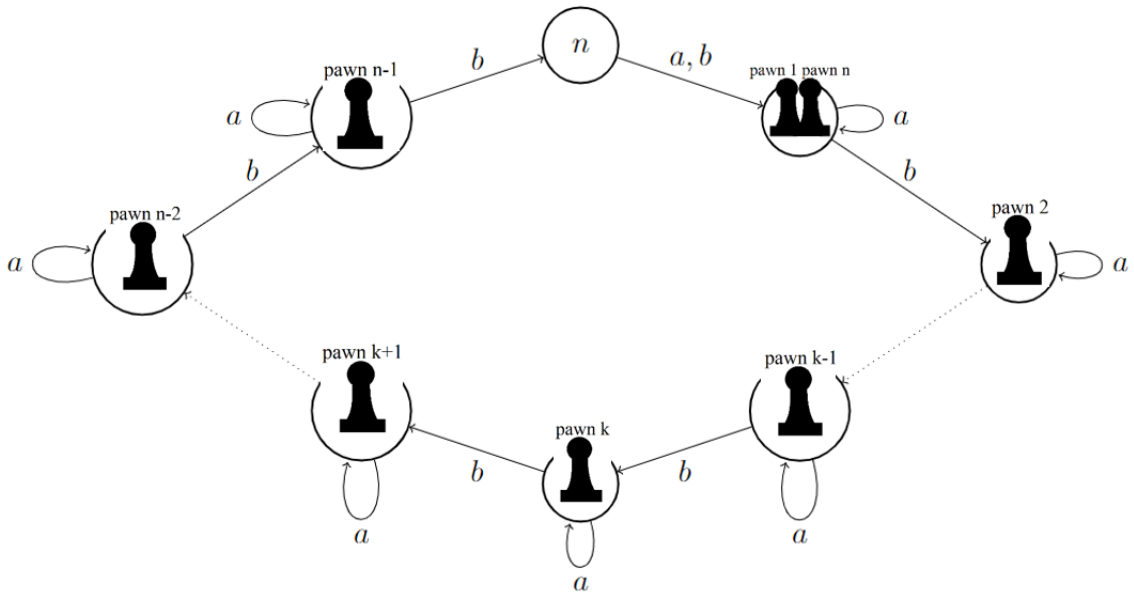

Figure 3.4: Situation after reading letter a.

Because of how the Černý automaton on n states is defined all pawns can only walk circles in a clockwise direction. If $w \in \Sigma^*$ is a reset word, then after reading w all pawns must end at the same state. This means that there must be a $k \in \{1, \ldots, n\}$ such that pawn k catches up with pawn $k-1$ (without pawn $k-1$ catching up to pawn k).
It also holds that once we have a $k \in \{1, \ldots, n\}$, such that pawn k catches up with pawn $k-1$ (without pawn $k-1$ catching up to pawn k), we have a reset word. Because once a pawn catches up to another pawn they, from that point on, follow the same path. For pawn k to catch up to pawn $k-1$, pawn k first has to catch up to all other pawns, since all pawns only can walk clockwise circles.

So in order to prove the theorem, we need to show that the shortest word that bring all these pawns to one state $w \in \Sigma^*$ has length $(n-1)^2$. The question now reads, "How many letters do we need for pawn k to catch up with pawn $k-1$?"

Suppose we look at pawn $k \in \{1, \ldots, n\}$, starting at state k. Then we want to know how many letters we at least need (in a word), for pawn k to catch up with pawn $k-1$.
The only place in our automaton for pawn k to gain on pawn $k-1$ is when pawn k is standing on state n. If pawn k is standing on any other state the amount of states between pawn k and pawn $k-1$ remains the same or even increase no matter the letter (a or b) that is read.
We count the number of states between pawns clockwise (in the same direction that the pawns walk). In our starting situation there are $n-2$ states in between pawn

k and pawn $k-1$. For pawn k to catch up with pawn $k-1$, pawn k has to stand at least $n-1$ times on state n.

We want to know the length of the shortest reset word. First we must have $n-k$ b's to get pawn k to state n. If we have an a in between these b's, our word would only become longer without pawn k catching up with any other pawn. Each time pawn k stands on state n we choose an a. This way pawn k still moves clockwise while the other pawn stand still, that is how pawn k catches up with the other pawns one by one. Then we chose $n-1$ b's, to get again to state n as fast as possible. By same argument as before there is no point of adding a's in between. This we must repeat until pawn k comes together with pawn $k-1$. Each time we have an a, pawn k could catch up with one other pawn, so we need $n-1$ a's. This means that our word consist of at least: $n-k$ b's, $n-2$ times: one a followed by $n-1$ b's, one a. This word has length $\geq n-k+(n-2)(1+n-1)+1 = (n-1)^2+n-k$.

Let $w \in \Sigma^*$ be a reset word for $\mathcal{C}_n$, then by the construction above we know that $|w| \geq \min\{(n-1)^2+n-k \mid 1 \leq k \leq n\}$.
$(n-1)^2+n-k$ is minimal for $k=n$, which implies that
$\min\{(n-1)^2+n-k \mid 1 \leq k \leq n\} = (n-1)^2$. This all together gives that, if $w \in \Sigma^*$ is a reset word $\mathcal{C}_n$, then $|w| \geq (n-1)^2$.

We already saw that $v = (ab^{n-1})^{n-2}a$ a reset word is for $\mathcal{C}_n$.
$|ab^{n-1}| = 1+1\cdot(n-1) = n$, so we have $|v| = n(n-2)+1 = n^2-2n+1 = (n-1)^2$
Which means that $|w| \leq (n-1)^2$, for $w \in \Sigma^*$ the shortest reset word of $\mathcal{C}_n$.
Combining these two inequalities gives that for $w \in \Sigma^*$ the shortest reset word of $\mathcal{C}_n$, it must hold that $|w| = (n-1)^2$. □

3.2 Upper bounds

We have seen that $C(n) \geq (n-1)^2$, but the Černý's conjecture ($C(n) = (n-1)^2$) remains unproven. However, over time different upper bounds of $C(n)$ have been proven, each time (slightly) better than the already known upper bound.
In 1964 Černý himself came up with the following upper bound [4].

Lemma 3.4. *Let $n \in \mathbb{N}$. Then it holds that $C(n) \leq 2^n - n - 1$.*

Proof. Let $\mathcal{A}$ be a synchronizing DFA with n states ($|Q| = n$) and $\mathcal{P}_\mathcal{A}$ the corresponding power automaton. Then we know from Proposition 2.22 that a word $w \in \Sigma^*$ is a reset word for DFA $\mathcal{A}$ if and only if w indicates a path from Q to a singleton ($\{\cdot\} \subset Q$) in the corresponding power automaton $\mathcal{P}_\mathcal{A}$.
There are 2^n subsets of Q, so there are 2^n-1 elements in $\hat{Q} = \mathcal{P}(Q)\backslash\emptyset$. The longest path, without going through the same state more then once, from Q to a singleton in $\mathcal{P}_\mathcal{A}$ is the path that goes through all states in $\hat{Q}$ except the singletons, since when we reach a singleton our path ends. We have n states, so we have n singletons. Then the longest path, without going through the same state more then once, from Q to a singleton in $\mathcal{P}_\mathcal{A}$ goes through 2^n-1-n states (in $\mathcal{P}_\mathcal{A}$). This gives that for the shortest reset word $w \in \Sigma^*$ of $\mathcal{A}$ holds: $|w| \leq 2^n-n-1$. Thus, $C(n) \leq 2^n-n-1$. □

In 1966, Starke came with a better upper bound [4]:

$$C(n) \leq 1 + \frac{n(n-1)(n-2)}{2}$$

Lemma 3.5. *Let $n \in \mathbb{N}$. Then it holds that $C(n) \leq 1 + \frac{n(n-1)(n-2)}{2}$.*

Proof. Let $\mathcal{A}$ be a synchronizing DFA with n states and $\mathcal{P}_\mathcal{A}$ the corresponding power automaton.
Take $S \subset Q$, with $|S| \geq 2$ arbitrary. Take a $p, q \in Q$ with $p, q \in S$ and $p \neq q$. We claim the following. There exists a word $w \in \Sigma^*$ which is a reset word for p and q with $|w| \leq \binom{n}{2}$.

To prove this claim we look at the power automaton $\mathcal{P}_\mathcal{A}$. If we search for a reset word $w \in \Sigma^*$ for p and q, we look for a path from the state $\{p, q\}$ to a singleton in $\mathcal{P}_\mathcal{A}$. In $\mathcal{P}_\mathcal{A}$ we can't go from a state $S \subseteq Q$ with $|S| = 2$ to a state $V \subseteq Q$ with $|V| \geq 3$.
Thus, the longest of such paths, without going through the same state more then once, goes through all states $\{r, s\}$ $(r, s \in Q,\ r \neq s)$ and then ends in a singleton. There are in total $\binom{n}{2}$ different states of the form $\{r, s\}$ $(r, s \in Q,\ r \neq s)$. This gives $|w| \leq \binom{n}{2}$.

If $w \in \Sigma^*$ is a reset word for $\mathcal{A}$, then w indicates a path from Q to a singleton in $\mathcal{P}_\mathcal{A}$. We are trying to find a upper bound for $C(n)$.

Let's start at Q. It takes a word $w \in \Sigma^*$ with only one letter to get form Q to some set $S \subset Q$ with $|S| < |Q| = n$. If all letters in our alphabet sent Q back to Q in $\mathcal{P}_\mathcal{A}$ then our automaton $\mathcal{A}$ isn't synchronizing. This is in contradiction with our assumption that $\mathcal{A}$ is synchronizing.
Now we have a subset $S \subset Q$, with $|S| \leq n - 1$.
If $|S| = 1$, then we found our shortest reset word $w \in \Sigma^*$ for $\mathcal{A}$ $(|w| = 1)$.
If $|S| \geq 2$, then we can pick a $p, q \in S$ with $p \neq q$. We know that there exist a reset word $w \in \Sigma^*$ for p and q with $|w| \leq \binom{n}{2}$. Thus, for $S_w := \delta(S, w) \subset Q$ it holds that $|S_w| < |S|$.
We repeat the same steps for $S_w \subset Q$ until we reach a singleton. The concatenation of all the found words (in chronological order) gives a path from Q to a singleton, so is a reset word for $\mathcal{A}$.

In the worst case we have $|S_w| = |S| - 1$, each time we apply the case $|S| \geq 2$. This means we have to apply the case $|S| \geq 2$ at least $n - 2$ times (for $S \subset Q$ with $|S| = n - 1, n - 2, ..., 2$). Then our found reset word $w \in \Sigma^*$ has length $|w| \leq 1 + (n-2)\binom{n}{2} = 1 + \frac{(n-2)(n-1)n}{2}$.
This implies that there exist a reset word $w \in \Sigma^*$ for $\mathcal{A}$ with $|w| \leq 1 + \frac{n(n-1)(n-2)}{2}$, which proves our lemma. □

There is a special class of automatons, namely the automatons with a sink state.

Definition 3.6. We call a state $q \in Q$ a *sink state* if there are no outgoing transition except self-loops. In other words, $q \in Q$ is called a sink state if $q = q \circ l$ for all $l \in \Sigma$.

Remark. Any automaton with more then one sink state isn't synchronizing.
Additionally a synchronizing automaton with a sink state always synchronizes in the sink state. In other words, if $q \in Q$ is the sink state, then for every reset word $w \in \Sigma^*$ we have $Q \circ w = q$.

For a automaton with a sink state we have the following upper bound [3].

Proposition 3.7. *Let $\mathcal{A} = (Q, \Sigma, \delta)$ be a synchronizing n-state DFA with a sink state. Let $w \in \Sigma^*$ the shortest reset word for this automaton $\mathcal{A}$. Then we have*

$$|w| \leq \frac{(n-1)\,n}{2}$$

Proof. Let $q \in Q$ be the sink state and let $\{q\} \subset T \subseteq Q$. There always exists a state unequal to q in T, $p \in T$ $p \neq q$, for which there exists a word $w \in \Sigma^*$ with $p \circ w = q$ and $w \leq n - |T|$.
With this word $w \in \Sigma^*$, we have $|T \circ w| < |T|$, since $q \circ v = q$ for all words $v \in \Sigma^*$ and thus also for $v = w$.
This gives that there exist a reset word $w \in \Sigma^*$ of length:

$$\begin{aligned} |w| &\leq \sum_{i=n}^{1} n - i \\ &= \sum_{i=0}^{n-1} i \\ &= \frac{1}{2}\,(n-1)\,n \end{aligned}$$

Thus, for every automaton $\mathcal{A}$ with a sink state the following must hold.

$$|w| \leq \frac{(n-1)\,n}{2}$$

here is $w \in \Sigma^*$ the shortest reset word of the automaton $\mathcal{A}$. □

Proposition 3.8. *The upper bound, in Proposition 3.7 for automatons with a sink state, is tight.*

Proof. We are going to proof this by showing an automaton with a sink state which has a shortest reset word of length $\frac{(n-1)n}{2}$.

Consider the following automaton $\mathcal{A} = (Q, \Sigma, \delta)$. Where $Q = \{1, \ldots, n\}$,
$\Sigma = \{a_1, \ldots, a_{n-1}\}$ and the transition function is determined as shown in Figure 3.5.

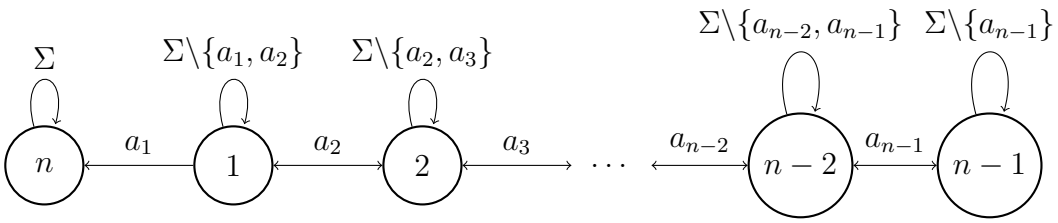

Figure 3.5: Automaton with sink state. [7]

State n the sink state. Lets again consider the situation where we start with a pawn on each state, let say pawn k starts on state k ($k = 1, \ldots, n$). Then the shortest word for pawn k to get to state n is $v = a_k a_{k-1} \ldots a_1$ ($|v| = k$). By definition of our transition function we have $q \circ v = q$ for all $k < q < n - 1$. But observe that $q \circ v = q + 1$ for all $1 < q < k$, since $q \circ a_k a_{k-1} \ldots a_{q+2} = q$, then letter a_{q+1} takes pawn q to state $q + 1$ and then by definition of the transition function $q + 1 \circ a_q a_{q-1} \ldots a_1 = q + 1$.
This gives that the shortest reset word the following is.

$$w = a_1 a_2 a_1 a_3 a_2 a_1 a_4 a_3 a_2 a_1 \ldots a_{n-1} a_{n-2} \ldots a_2 a_1$$

Note that we indeed first take pawn 1 to state n, then pawn 2, then pawn 3, etc. If we first should take pawn k, with $k \neq 1$, to state n, it would take a longer word to take pawn 1 to state n, since it is now standing on state 2. So, then we would get a reset word which is longer than w.
By calculating $|w|$, our prove is concluded.

$$|w| = \sum_{i=1}^{n-1} i = \frac{1}{2}(n-1)\, n$$

□

This upper bound for automatons with a sink state is of order $\mathcal{O}(n^2)$, which is much better then all other general (until now) found upper bounds of $C(n)$, which are of order $\mathcal{O}(n^3)$.

In 1982 J.-E Pin and P. Frankl came with the following upper bound [4].

$$C(n) \leq \frac{n^3 - n}{6}$$

This was then the best found upper bound.
Marek Szykuła was later able to improve this by the factor $\frac{85059}{85184}$ [8].
We are going to discuss the found upper bound by Marek Szykuła further in the next subsection. Here we are going to use slightly more accurate numbers, since we don't approximate the decimal numbers with a rational number. All statements and proofs in Subsection 3.2.1 are inspired by the paper written by Marek Szykuła [8].

3.2.1 Upper bound by Marek Szykuła

In this subsection we deal with a DFA $\mathcal{A} = (Q, \Sigma, \delta)$, with $n := |Q|$. We assume $Q = \{1, \ldots, n\}$.

Definition 3.9. Let $\mathcal{A} = (Q, \Sigma, \delta)$ be a automaton, $w \in \Sigma^*$ a word and $q \in Q$ a state. Then we say that word w is *avoiding for a state* q, if after reading word w, the automaton cannot be in q, no matter in which state you started.
In other notation, word w is *avoiding for a state* q if $q \notin Q \circ w$.

Definition 3.10. Let $w \in \Sigma^*$ be a word. Then we define the *rank* of word w to be $|Q \circ w|$. In other words the *rank* of word w is the cardinality of the image of Q under the action of word w.

Remark. A reset word has rank 1.

Definition 3.11. We say that $w \in \Sigma^*$ is *a shortest reset word* if w is a reset word and if for all words $v \in \Sigma^{\leq |w|-1}$ it holds that v isn't a reset word.

Definition 3.12. Let $S \subseteq Q$ and $q \in Q$ a state. Then we say that a word $w \in \Sigma^*$ *compresses* the subset S, if $|S \circ w| < |S|$.
Furthermore we say that $w \in \Sigma^*$ *avoids state* q if $q \notin Q \circ w$. A state q is *avoidable* if there exists a word $w \in \Sigma^*$ such that $q \notin Q \circ w$. In other words, a state that admits an avoiding word is avoidable.
We also say that a state q is avoidable from subset S, if there exists a word $w \in \Sigma^*$ such that $q \notin S \circ w$.

Remark. Generally, avoiding words do not necessarily exists. But in case of a synchronizing automaton there always exists an avoiding word, unless there is a sink state. The sink state can not be avoided.

Since we are looking for a general upper bound, we only have to look at the worst cases. That is why we can discard the automatons with a sink state. We already have seen that, in that case, we have a upper bounds of order $\mathcal{O}(n^2)$, so all upper bound of order $\mathcal{O}(n^3)$ also hold for an automaton with a sink state for large enough n.

From now on (in this subsection) we assume that $\mathcal{A}$ is a DFA without a sink state.

We are going to show that for every state $q \in Q$ and subset $S \subseteq Q$, there either exists a short avoiding word for q from S, or that there exists a short compressing word for S.

Definition 3.13. Let $v \in \mathbb{R}^n$ a vector and $i \in \{1, \ldots, n\}$. With $v(i)$ we denote the value of the i^{th} position of vector v. Let $S \subseteq Q$ a subset of Q. We define $[S] \in \mathbb{R}^{1 \times n}$ to be the characteristic row vector of S.

$$\begin{cases} [S](i) = 1 & \text{if } i \in S \\ [S](i) = 0 & \text{otherwise} \end{cases}$$

For a word $w \in \Sigma^*$ we denote the $n \times n$ matrix of the transformation of w by $[w]$.

$$\begin{cases} [w](i,j) = 1 & \text{if } i \circ w = j \\ [w](i,j) = 0 & \text{otherwise} \end{cases}$$

Remark. The $n \times n$ matrix $[w]$ has exactly one 1 in each row. The matrix $[w]$ indicates all transformation of the states when word w is applied.
That is why $|S| = \sum_{i \in Q} [S](i) = \sum_{i \in Q} [S][w](i)$ holds for all $S \subseteq Q$ and $w \in \Sigma^*$.
For all $v, u \in \Sigma^*$ it also holds that $[uv] = [u][v]$.

Property 3.14. Let $S \subseteq Q$, $u \in \Sigma^*$ and $1 \leq i \leq n$. Then we define $[S][u] \in \mathbb{R}^{1 \times n}$ as the vector for which the i^{th}-value gives how many states from S go to state i, after applying word u. Thus, $([S][u])(i) = |\{q \in S \mid q \circ u = i\}|$.

Remark. By definition of $[S][u]$ and $[S \circ u]$, we have that the following holds. $([S][u])(i) \geq 1$ if and only if $[S \circ u](i) = 1$.

Definition 3.15. Let $V \subseteq \mathbb{R}^n$. Then we denote with $\text{Span}(V)$ the linear subspace spanned by the vectors in V.

Definition 3.16. Let $L \subseteq \mathbb{R}^n$ a linear subspace and M an $n \times n$ matrix. The dimension of L, we denote with $\text{Dim}(L)$. We define $LM = \{v \cdot M \mid v \in L\}$ as the linear subspace mapped by M.

First we prove that by a short (linear) word we can either avoid a state from the current subset or compress the current subset. We make this more precise in the following lemma.

Lemma 3.17. *Let $\mathcal{A} = (Q, \Sigma, \delta)$ be a synchronizing n-state automaton, $\emptyset \neq S \subseteq Q$ and $\emptyset \neq A \subset S$. Suppose there is a word $w \in \Sigma^*$ such that $A \not\subseteq S \circ w$.*
Then there exists a word $w \in \Sigma^*$ with $|w| \leq n - |A|$ satisfying either

1. *$A \not\subseteq S \circ w$ or,*
2. *$|S \circ w| < |S|$*

Proof. Define the linear subspaces $L_i := \text{Span}\left(\left\{[S][w] \mid w \in \Sigma^{\leq i}\right\}\right)$ for $i = 0, 1, 2, \ldots$.
By definition of L_i we have a increasing sequence of sets:

$$L_0 \subseteq L_1 \subseteq L_2 \subseteq L_3 \subseteq \ldots$$

Since the sequence $(L_i)_i$ is an increasing sequence and $L_i \subseteq \mathbb{R}^n$ for all $i = 0, 1, 2, \ldots$.
We have that $\text{Dim}(L_i) \leq n$ for all $i = 0, 1, 2, \ldots$ and

$$\text{Dim}(L_0) \leq \text{Dim}(L_1) \leq \text{Dim}(L_2) \leq \text{Dim}(L_3) \leq \ldots$$

This implies that there must exists a k such that $L_k = L_{k+1}$. So $(L_i)_i$ satisfies the ascending chain condition.

Now we are going to make this even stronger by proving that there exists a k such that $L_k = L_{k+1} = L_{k+2} = \ldots$.

To do this we are going to prove that if $L_k = L_{k+1}$, then $L_{k+1} = L_{k+2}$.

First observe that $L_{i+1} = L_i \cup \text{Span}\left(\{[S][w] \mid w \in \Sigma^* \text{ with } |w| = i+1\}\right)$, by definition of L_i. With this observation we are going to show that $L_{i+1} = \text{Span}\left(L_i \cup \bigcup_{a\in\Sigma} L_i[a]\right)$.

Let $w \in \Sigma^*$ with $|w| = i+1$, then there is a letter $a \in \Sigma$ and a word $v \in \Sigma^*$ with $|v| = i$ such that $w = va$. This gives us the following.

$$\begin{aligned}[S][w] &= [S][va] \\ &= [S][v][a]\end{aligned}$$

$[S][v] \in L_i$ by definition of L_i. Thus,
$\text{Span}\left(\{[S][w] \mid w \in \Sigma^* \text{ with } |w| = i+1\}\right) \subseteq \bigcup_{a\in\Sigma} L_i[a]$.
This implies $L_{i+1} \subseteq L_i \cup \bigcup_{a\in\Sigma} L_i[a]$.

Let $u \in \left(L_i \cup \bigcup_{a\in\Sigma} L_i[a]\right)$ arbitrary. By definition we can then write $u = l \cdot [a]$ for some $l \in L_i$. By definition of L_i we can write l as a linear combination of vectors in the set $\{[S][w] \mid w \in \Sigma^{\leq i}\}$.
Therefore, if we can proof that for all elements $([S][w])$ in $\left\{[S][w] \mid w \in \Sigma^{\leq i}\right\}$ it holds that $[S][w][a] \in L_{i+1}$ (for $a \in \Sigma$ arbitrary), then u must also be an element of L_{i+1}. Which would give us that $L_{i+1} \supseteq L_i \cup \bigcup_{a\in\Sigma} L_i[a]$.

Take $v \in \Sigma^{\leq i}$ and $a \in \Sigma$ arbitrary, then $va \in \Sigma^{\leq i+1}$. So,
$[S][v][a] = [S][va] \in \{[S][w] \mid w \in \Sigma^{\leq i+1}\} \subseteq L_{i+1}$.

Both inclusions together gives that $\forall i \geq 0$:

$$L_{i+1} = \text{Span}\left(L_i \cup \bigcup_{a\in\Sigma} L_i[a]\right)$$

Suppose there is a $k \geq 0$ such that $L_k = L_{k+1}$, then we have for $i = k$ the following

$$\begin{aligned}L_k &= L_{k+1} \\ &= \text{Span}\left(L_k \cup \bigcup_{a\in\Sigma} L_k[a]\right) \\ &= \text{Span}\left(L_{k+1} \cup \bigcup_{a\in\Sigma} L_{k+1}[a]\right) \\ &= L_{k+2}\end{aligned}$$

Applying this iteratively gives $L_k = L_{k+i}$ for all $i \geq 0$.
Let i be the smallest integer such that $L_i = L_{i+1}$, then for all $j \geq i$ we have $L_i = L_j$.
We define $m := \text{Dim}\left(L_i\right)$.

By definition we know $L_0 = \{c \cdot [S] \mid c \in \mathbb{R}\}$, so $\text{Dim}\left(L_0\right) = 1$. Since $L_j \subset L_{j+1}$ for all $j < i$ we have that the dimensions grow by at least 1 up to m. This gives

$m \geq \text{Dim}\,(L_k) \geq \min\{m, k+1\}$ for all k.
This implies for $k = n - |A|$ that we have

$$m \geq \text{Dim}\left(L_{n-|A|}\right) \geq \min\{m, n-|A|+1\}$$

Take $w \in \Sigma^*$ arbitrary. Define $z := [S][w]$.
If $z\,(q) = 0$ for some $q \in A$, then $q \notin S \circ w$. So we have case 1.
If there exists a $q \in A$ such that $z\,(q) \geq 2$, then a pair of states form S is compressed by word w to state q. So we have case 2.

In order to prove this lemma we have to prove that there exists a z in the spanning set of $L_{n-|A|}$, so $z \in \left\{[S][w] \mid w \in \Sigma^{\leq n-|A|}\right\}$, such that either

- $\exists q \in A$ such that $z\,(q) = 0$, or
- $\exists q \in A$ such that $z\,(q) \geq 2$

(Since this implies that there exists a word $w \in \Sigma^{n-|A|}$ satisfying case 1 or case 2.)

Suppose this is not the case, then for all $z \in \left\{[S][w] \mid w \in \Sigma^{\leq n-|A|}\right\}$ it must hold that $z\,(q) = 1\ \forall q \in A$.

Let $v \in L_k$, then v is a linear combination of vectors $v_1, v_2, \ldots$ from the spanning set of L_k. Let $v = a_1 \cdot v_1 + a_2 \cdot v_2 + \ldots$, where $v_1, v_2, \cdots \in \left\{[S][w] \mid w \in \Sigma^{\leq k}\right\}$ and $a_1, a_2, \cdots \in \mathbb{R}$.

Define $c = \sum_i a_i$.
Let $k = n - |A|$. Because of our contradiction assumption we have that every vector $v_j = [S][w]$ in the spanning set of $L_{n-|A|}$ has $[S][w]\,(q) = 1$ for all $q \in A$. We also know $\sum_{i=1}^{n} ([S][w])\,(i) = |S|$. This gives

$$\begin{aligned}
\sum_i v\,(i) &= \sum_j \sum_i a_j v_j\,(i) \\
&= \sum_j a_j \sum_i v_j\,(i) \\
&= |S| \cdot \sum_j a_j \\
&= c|S|
\end{aligned}$$

for $q \in A$ we have

$$\begin{aligned}
v\,(q) &= a_1 v_1\,(q) + a_2 v_2\,(q) + \ldots \\
&= a_1 \cdot 1 + a_2 \cdot 1 + \ldots \\
&= \sum_i a_i = c
\end{aligned}$$

Together this gives that the sum of entries at positions corresponding to the states in $Q\backslash A$ is equal to $c|S| - c|A| = c\,(|S| - |A|)$.

$$\begin{aligned}\sum_{p' \in Q\backslash A} v\,(p') &= \sum_{p \in Q} v\,(p) - \sum_{p \in A} v\,(p) \\ &= c|S| - \sum_{p \in A} c \\ &= c|S| - c|A| = c\,(|S| - |A|)\end{aligned}$$

Thus, for all $q \in A$ we have the following.

$$\begin{aligned}v\,(q) &= c \\ &= \frac{1}{|S| - |A|} \cdot c\,(|S| - |A|) \\ &= \frac{1}{|S| - |A|} \sum_{p \in Q\backslash A} v\,(p)\end{aligned}$$

The values at the positions corresponding to $q \in A$ are completely determined by the values from the other positions (corresponding to $p \in Q\backslash A$). $Q\backslash A$ had $n - |A|$ elements. This gives that $\mathrm{Dim}\left(L_{n-|A|}\right) \leq n - |A|$.
This together with the fact $m \geq \mathrm{Dim}\left(L_{n-|A|}\right) \geq \min\{m, n - |A| + 1\}$, gives us that $\mathrm{Dim}\left(L_{n-|A|}\right) = m$

We assumed that there exists a word $w \in \Sigma^*$ that is an avoiding word for some state $q \in A$. Hence there is a $q \in A$ such that $q \notin S \circ w$.
Then there always exist a word $w \in \Sigma^*$ for which $\forall q \in A : [S][w](q) = \frac{1}{|S|-|A|} \sum_{p \in Q\backslash A} [S][w](p)$ does not hold.
If A is singleton (let's say $A = \{q\}$), then we know that there exists a word $w \in \Sigma^*$ such that there is a $q \in A$ with $q \notin S \circ w$. So $[S][w](q) = 0$, but $\sum_{p \in Q\backslash A} [S][w](p)$ isn't equal to zero. So $[S][w](q) = \frac{1}{|S|-|A|} \sum_{p \in Q\backslash A} [S][w](p)$ doesn't hold for $q \in A$.
If $|A| \geq 2$, then we know that there exists a word $w \in \Sigma^*$ such that there is a $q \in A$ with $q \notin S \circ w$. Now we have two possible cases, either $S \circ w \subset A$ or $S \circ w \not\subset A$. If $S \circ w \subset A$, then we have $\sum_{p \in Q\backslash A} [S][w](p) = 0$ but there exist also a $q' \in S \circ w \subset A$, so we have also $[S][w](q') \neq 0$. So also in this case $\forall q \in A : [S][w](q) = \frac{1}{|S|-|A|} \sum_{p \in Q\backslash A} [S][w](p)$ does not hold. If $S \circ w \not\subset A$ then $\sum_{p \in Q\backslash A} [S][w](p) \neq 0$, but $[S][w](q) = 0$. So, also in this case,
$\forall q \in A : [S][w](q) = \frac{1}{|S|-|A|} \sum_{p \in Q\backslash A} [S][w](p)$ does not hold.

We know that for all $v \in L_{n-|A|}$ the following must hold $\forall q \in A : v(q) = \frac{1}{|S|-|A|} \sum_{p \in Q\backslash A} v(p)$.
But we have also that there exist a word $w \in \Sigma$, such that
$\forall q \in A : [S][w](q) = \frac{1}{|S|-|A|} \sum_{p \in Q\backslash A} [S][w](p)$ doesn't hold. This implies that $[S][w] \notin L_{n-|A|}$, which indicates that the dimension of $L_{n-|A|}$ is not maximal. In other words, $\mathrm{Dim}\left(L_{n-|A|}\right) \neq m$. This gives us a contradiction.
With this we have shown that there exist a z in the spanning set of $L_{n-|A|}$ such that, either there exist a $q \in A$ such that $z(q) = 0$, or there exist a $q \in A$ such that $z(q) \geq 2$. With this we have proven our lemma. □

Lemma 3.18. *Let $\mathcal{A} = (Q, \Sigma, \delta)$ be a n-state automaton, $\emptyset \neq S \subseteq Q$, $\emptyset \neq A \subset S$ and $k \geq 1$ an integer. Suppose there exists a word $w \in \Sigma^*$ such that $A \not\subseteq S \circ w$. Then there exists a word $w \in \Sigma^*$ with $|w| \leq k\,(n - |A|)$ satisfying either*

1. *$A \not\subseteq S \circ w$ or,*
2. *$|S \circ w| \leq |S| - k$*

Proof. If case 1 holds for some $w \in \Sigma^{\leq k(n-|A|)}$, then we are done. So suppose this is not the case.
We are going to iteratively apply Lemma 3.17 (k times) for subset A, starting in set S.
For $i = 0, \ldots, k-1$ apply Lemma 3.17 for subset $S \circ w_1 \cdots w_i$, where $w_i \in \Sigma^{\leq n-|A|}$ is the word obtained in the i^{th} iteration.

After applying Lemma 3.17 k times we obtain a word $w_1 \cdots w_k$, with length $|w_1 \cdots w_k| \leq k\,(n - |A|)$.

In each iteration we must have case 2 (of Lemma 3.17), otherwise there exists an $i \in \{1, \ldots, k-1\}$ such that $A \not\subseteq S \circ w_1 \cdots w_i$. This gives a contradiction with our assumption that case 1 doesn't hold, since $|w_1 \cdots w_i| \leq i\,(n - |A|) \leq k\,(n - |A|)$ for all $i = 1, \ldots, k-1$.
So it must hold that $|S \circ w_1| < |S|$, $|S \circ w_1 w_2| < |S \circ w_1|, \ldots,$
$|S \circ w_1 \cdots w_k| < |S \circ w_1 \cdots w_{k-1}|$. This means that

$$|S \circ w_1 \cdots w_k| \leq |S \circ w_1 \cdots w_{k-1}| - 1 \leq \cdots \leq |S \circ w_1| - (k-1) \leq |S| - k$$

Thus case 2 of our lemma holds.

However we can't just apply Lemma 3.17 k times, since it is not given that each time the assumptions of Lemma 3.17 are satisfied. Therefore, the last thing we have to do in this proof, is that we need to prove that the conditions of Lemma 3.17 are satisfied in each iteration.

That there exists a word $w \in \Sigma^*$ such that $A \not\subseteq S \circ w$ is already given in the assumptions of this lemma. So we only have to prove that $A \subset S \circ w_1 \cdots w_i$ for all $i = 0, \ldots, k-1$. This is already given for $i = 0$, since in this lemma is given that $A \subset S$.
Let $i \geq 1$. Since in each iteration case 2 of lemma 3.17 must hold, we already have $A \subseteq S \circ w_1 \cdots w_i$ for all $i = 1, \ldots, k-1$. We have left to prove that $A \neq S \circ w_1 \cdots w_i$ for all $i = 1, \ldots, k-1$.

Suppose $A = S \circ w_1 \cdots w_i$, for some $i = 1, \ldots, k-1$. We know that for all $M \subseteq Q$ and $a \in \Sigma$ it must hold that $|M \circ a| \leq |M|$ (the number of states only decreases). Since $A = S \circ w_1 \cdots w_i$ and case 1 of this lemma doesn't hold, we get $A = S \circ w_1 \cdots w_i a$ for all $a \in \Sigma$. This gives that $A \circ a = A$ for all $a \in \Sigma$, which is in contradiction with the fact that there exist a word $w \in \Sigma^*$ such that $A \not\subseteq S \circ w$.
Thus, if $A = S \circ w_1 \cdots w_i$ for some $i = 1, \ldots, k-1$, then there must exists a letter

$a \in \Sigma$ such that $A \not\subseteq S \circ w_1 \cdots w_i a$. This is again in contradiction with our assumption that case 1 doesn't hold, since $|w_1 \cdots w_i a| \leq i\,(n - |A|) + 1 \leq k\,(n - |A|)$ for $i \in \{1, \ldots, k-1\}$ ($(n - |A|) \geq 1$ because $A \subset S \subseteq Q$).
So, we have proven that $A \subset S \circ w_1 \cdots w_i$ for all $i = 0, \ldots, k-1$.

With this we have checked that the conditions of Lemma 3.17 are satisfied. □

Lemma 3.19. *Let $\mathcal{A} = (Q, \Sigma, \delta)$ be a n-state automaton, $\emptyset \neq S \subseteq Q$ and $\emptyset \neq A \subseteq S$. If there exists a word $w \in \Sigma^*$ such that $A \not\subseteq S \circ w$. Then there exists a word $w \in \Sigma^*$, with length $|w| \leq (|S| - |A|)\,(n - |A|) + 1$, such that $A \not\subseteq S \circ w$.*

Proof. Assume that there exists a word $w \in \Sigma^*$ such that $A \not\subseteq S \circ w$.
Again we iteratively apply Lemma 3.17 (at most $|S| - |A|$ times) for subset A, starting with set S. We stop this iteration if the conditions of Lemma 3.17 are not met, so in other words if $A = S \circ w_1 \cdots w_i$.
For all $i = 1, \ldots, |S| - |A|$ we have that in the i^{th} iteration we obtain a word w_i with $|w_i| \leq n - |A|$.

In the worst case we have that $|S \circ w_1 \cdots w_i| = |S \circ w_1 \cdots w_{i-1}| - 1$ for all $i = 1, \ldots, |S| - |A|$. Since the number of states in our set $S \circ w_1 \cdots w_i$ can only decrease in each iteration. Thus, in the worst case we have the following.

$$|S \circ w_1 \cdots w_{|S|-|A|}| = |S| - (|S| - |A|) = |A|$$

This means that there exist an $i \in \{0, \ldots, |S| - |A|\}$ such that either $A \not\subseteq S \circ w_1 \cdots w_i$ or $A = S \circ w_1 \cdots w_i$.

If there exists an $i \in \{1, \ldots, |S| - |A|\}$ such that $A \not\subseteq S \circ w_1 \cdots w_i$. Then we done, since $|w_1 \cdots w_i| \leq i\,(n - |A|) \leq (|S| - |A|)\,(n - |A|) \leq (|S| - |A|)\,(n - |A|) + 1$. So there exist word $w \in \Sigma^*$, with length $|w| \leq (|S| - |A|)\,(n - |A|) + 1$, such that $A \not\subseteq S \circ w$

If we have to stop our iteration at some point $i \in \{0, \ldots, |S| - |A|\}$ because we have $A = S \circ w_1 \cdots w_i$ for some i. Then just as shown in the proof of Lemma 3.18 there must exists a letter $a \in \Sigma$ such that $A \circ a \neq A$.
$|w_1 \cdots w_i a| \leq i\,(n - |A|) + 1 \leq (|S| - |A|)\,(n - |A|) + 1$ and $A \not\subseteq S \circ w_1 \cdots w_i a$ (shown in proof of lemma 3.18). So, there exist word $w \in \Sigma^*$, with length $|w| \leq (|S| - |A|)\,(n - |A|) + 1$, such that $A \not\subseteq S \circ w$

Thus in both cases there exists a word $w \in \Sigma^*$, with length $|w| \leq (|S| - |A|)\,(n - |A|) + 1$, such that $A \not\subseteq S \circ w$. □

Lemma 3.20. *Let $n \geq 2$ and $\mathcal{A} = (Q, \Sigma, \delta)$ be a n-state automaton. Assume that all $\emptyset \neq A \subset Q$ contain an avoidable state from Q (so for all $\emptyset \neq A \subset Q$: $\exists q \in A$ and $\exists w \in \Sigma^*$ such that $q \notin Q \circ w$). Then for all $\emptyset \neq A \subset Q$ there exists a word $w \in \Sigma^*$ avoiding a state from A (so $\exists w \in \Sigma^*$: $A \not\subseteq Q \circ w$), with length $|w| \leq (n - 1 - |A|)\,(n - |A|) + 2$.*

Proof. Let $\emptyset \neq A \subset Q$ an arbitrary subset. Since there exist an avoidable state in A, we know that there exist a $q \in A$ and a word $w \in \Sigma^*$ such that $q \notin Q \circ w$ ($A \not\subseteq Q \circ w$). This means that there exists a letter $a \in \Sigma$ such that $|Q \circ a| < n$.
If this was not the case ($\forall a \in \Sigma$: $|Q \circ a| = n$) then we have that $\forall a \in \Sigma$: $Q \circ a = Q$. This would mean that we could never get a word $w \in \Sigma^*$ such that $q \notin Q \circ w$, which gives us a contradiction.

If $A \not\subseteq Q \circ a$, then we have proven that there exists a word $w\,(= a)$ ($|w| = 1 \leq (n - 1 - |A|)\,(n - |A|) + 2$) that avoids a state from A.

Otherwise we have $A \subseteq Q \circ a$.
Define $S := Q \circ a$.
Apply Lemma 3.19 with subset $A \subseteq S = Q \circ a$. Then we know from this Lemma 3.19 that there exists a word $w \in \Sigma^*$, with $|w| \leq (|S| - |A|)\,(n - |A|) + 1$, such that $A \not\subseteq S \circ w = Q \circ aw$.
Note that $|aw| \leq (|Q \circ a| - |A|)\,(n - |A|) + 1 + 1 \leq (n - 1 - |A|)\,(n - |A|) + 2$.
So we have shown that there exists a word $v = aw$ with length at most $(n - 1 - |A|)\,(n - |A|) + 2$ such that $A \not\subseteq Q \circ v$.
Since we took $\emptyset \neq A \subset Q$ arbitrary, we have proven this for all $\emptyset \neq A \subset Q$. □

Let $q \in Q$. If we take $A = \{q\}$ in Lemma 3.20 then we get that for the shortest avoiding word w of state q it holds that $|w| \leq (n-2)(n-1) + 2$.

Lemma 3.21. *Let $w \in \Sigma^*$ and $g = min\{|q \circ w^{-1}| \mid q \in Q \circ w\}$ (The minimal number of states that go to some state q). There are at least $(g+1)\,|Q \circ w| - n$ states $q \in Q \circ w$ such that $|q \circ w^{-1}| = g$.*

Proof. Define $d := |\{q \in Q \circ w \mid |q \circ w^{-1}| = g\}|$. This lemma is proven, when we have shown that $d \geq (g+1)\,|Q \circ w| - n$.

By definition of d and g we know that there are $|Q \circ w| - d$ states with preimages of size at least $g+1$. In other words there are $|Q \circ w| - d$ states $q \in Q \circ w$ with $|q \circ w^{-1}| \geq g + 1$.

Note the following two things.
First $(Q \circ w) \circ w^{-1} = Q$ for all $w \in \Sigma^*$, by definition of the preimage of $Q \circ w$.
Second for $p, q \in Q$ with $p \neq q$ we have $p \circ w^{-1} \cap q \circ w^{-1} = \emptyset$. Because we look at a DFA automaton $\mathcal{A}$, there isn't a state $r \in Q$ that can go to both state p and state q after reading w.

With this we get the following

$$\begin{aligned} n &\geq \left|Q \circ w^{-1}\right| \\ &\geq dg + (g+1)\,(|Q \circ w| - d) \\ &= (g+1)\,|Q \circ w| - d \end{aligned}$$

This gives $d \geq (g+1)\,|Q \circ w| - n$. □

Remark. When $g = 1$, Lemma 3.21 gives that there are at least $2\,|Q \circ w| - n$ states in $Q \circ w$ with a unique preimage.

Lemma 3.22. *Let $w \in \Sigma^*$ be a word of rank r ($|Q \circ w| = r$), with $\left\lfloor \frac{n+1}{2} \right\rfloor \leq r \leq n-1$. Suppose that for some integer $k \geq 1$ and for all $A \subset Q$ with $1 \leq |A| \leq n-1$, there is a word $v_A \in \Sigma^{k(n-|A|)}$ such that $A \not\subseteq Q \circ v_A$.*
Then there exists a word $u \in \Sigma^*$ with $|Q \circ u| \leq \frac{n}{2}$ (rank of u is less of equal to $\frac{n}{2}$) and

$$|u| \leq |w| + k\frac{n^2 - (2n - 2r - 1)^2}{4}$$

Proof. We are going to prove this by giving such a word u. We are going to construct this word $u \in \Sigma^*$ inductively.

For $i = r, r-1, \ldots, \left\lfloor \frac{n}{2} \right\rfloor$ we inductively construct words w_i with
$|w_i| \leq |w| + k\,(r-i)\,(2n - r - i - 1)$ and rank $|Q \circ w_i| \leq i$.
In the end we see that $u = w_{\left\lfloor \frac{n}{2} \right\rfloor}$ is the wanted word.

First define $w_r := w$.

$$\begin{aligned} |w_r| &= |w| \\ &\leq |w| + k(r-r)(2n - r - r - 1) \end{aligned}$$

Given was $|Q \circ w| = r$, so also $|Q \circ w_r| \leq r$ holds.

Now let $i < r$ and suppose we have already found w_{i+1}. Because $|Q \circ w_{i+1}| \leq i + 1$ we have two cases: $|Q \circ w_{i+1}| \leq i$ and $|Q \circ w_{i+1}| = i + 1$.
If $|Q \circ w_{i+1}| \leq i$, then define $w_i = w_{i+1}$.

$$\begin{aligned} |w_i| &= |w_{i+1}| \\ &\leq |w| + k(r-i-1)(2n - r - i - 2) \\ &\leq |w| + k(r-i)(2n - r - i - 1) \end{aligned}$$

$|Q \circ w_{i+1}| = |Q \circ w_i| \leq i \leq i + 1$

If $|Q \circ w_{i+1}| = i + 1$, then we expand word w_{i+1} to get word w_i.
Since $\left\lfloor \frac{n}{2} \right\rfloor \leq i < r$ we get

$$\begin{aligned} i + 1 &\geq \left\lfloor \frac{n}{2} \right\rfloor + 1 \\ &\geq \frac{n}{2} - \frac{1}{2} + \frac{2}{2} \\ &= \frac{n+1}{2} \end{aligned}$$

This gives $|Q \circ w_{i+1}| = i + 1 \geq \frac{n+1}{2}$.
By Lemma 3.21 (and the remark after this lemma) there exists a set
$\emptyset \neq B \subseteq \{q \in Q \circ w_{i+1} \mid |q \circ w_{i+1}^{-1}| = 1\} \subseteq Q \circ w_{i+1}$ of size
$|B| \geq 2|Q \circ w_{i+1}| - n = 2i + 2 - n$.

Let $X \subseteq B$ be a subset of size $|X| = 2i + 2 - n$.

Define $Y := X \circ w_{i+1}^{-1}$. All states in X have an unique preimage (since $X \subseteq B$), thus we have that $|Y| = |X| = 2i + 2 - n$
Since $i \leq r - 1$ and $X \neq \emptyset$, we have $1 \leq |Y| \leq 2(r-1) + 2 - n = 2r - n < n$. So by the assumption of this lemma, then there exists a word $v_Y \in \Sigma^{k(n-|Y|)}$ with $Y \not\subseteq Q \circ v_Y$.
Now define $w_i := v_Y w_{i+1}$

Since $Y \not\subseteq Q \circ v_Y$, there exists a $p \in Y$ such that $p \notin Q \circ v_Y$.
Suppose $q = p \circ w_{i+1}$.
This gives that $q \notin Q \circ v_Y w_{i+1} = Q \circ w_i$, because $p \notin Q \circ v_Y$. w_{i+1} is a subword of word w_i and $|w_i| \geq |w_{i+1}|$, so $Q \circ w_i \subseteq Q \circ w_{i+1}$. Now we have a state $q \in Q \circ w_{i+1}$ with $q \notin Q \circ w_i$. This means that $Q \circ w_i \subset Q \circ w_{i+1}$. Which implies that $|Q \circ w_i| \leq |Q \circ w_{i+1}| - 1 = i + 1 - 1 = i$.
We know the following of the length of word w_i.

$$
\begin{aligned}
|w_i| &= |v_Y| + |w_{i+1}| \\
&\leq k(n - |Y|) + |w| + k(r - i - 1)(2n - r - i - 2) \\
&= k(n - 2i - 2 + n) + |w| + k(r - i - 1)(2n - r - i - 2) \\
&= 2k(n - i - 1) + |w| + k(r - i - 1)(2n - r - i - 2) \\
&= k(2(n - i - 1) - (r - i - 1) + (r - i - 1)(2n - r - i - 1)) + |w| \\
&= k(2n - r - i - 1 - (2n - r - i - 1) + (r - i)(2n - r - i - 1)) + |w| \\
&= k(r - i)(2n - r - i - 1) + |w|
\end{aligned}
$$

So, for our defined w_i, it holds that $|w_i| \leq k(r-i)(2n-r-i-1) + |w|$ and $|Q \circ w_i| \leq i$.

With this we have proven that we can construct words w_i with
$|w_i| \leq |w| + k(r-i)(2n-r-i-1)$ and rank $|Q \circ w_i| \leq i$, for $i = r, r-1, \ldots, \lfloor \frac{n}{2} \rfloor$.
If we know look at the word w_i for $i = \lfloor \frac{n}{2} \rfloor$, then we see that $|Q \circ w_{\lfloor \frac{n}{2} \rfloor}| \leq \lfloor \frac{n}{2} \rfloor \leq \frac{n}{2}$ and that we have the following restriction on $|w_{\lfloor \frac{n}{2} \rfloor}|$.

$$
\begin{aligned}
|w_{\lfloor \frac{n}{2} \rfloor}| &\leq |w| + k\left(r - \left\lfloor \frac{n}{2} \right\rfloor\right)\left(2n - r - \left\lfloor \frac{n}{2} \right\rfloor - 1\right) \\
&\leq |w| + k\left(r - \frac{n-1}{2}\right)\left(2n - r - \frac{n-1}{2} - 1\right) \\
&= |w| + k\left(2nr - r^2 - \frac{n-1}{2}r - r - n(n-1) + \frac{n-1}{2}r + \left(\frac{n-1}{2}\right)^2 + \frac{n-1}{2}\right) \\
&= |w| + k\left(2nr - r^2 - r - n^2 + n + \frac{n-1}{2} + \frac{n^2 - 2n + 1}{4}\right) \\
&= |w| + \frac{k}{4}\left(8nr - 4r^2 - 4r - 4n^2 + 4n + 2n - 2 + n^2 - 2n + 1\right)
\end{aligned}
$$

$$
\begin{aligned}
&= |w| + \frac{k}{4}\left(n^2 - \left(1 + 4n^2 - 4n - 8nr + 4r^2 + 4r\right)\right) \\
&= |w| + \frac{k}{4}\left(n^2 - (2n - 2r - 1)(2n - 2r - 1)\right) \\
&= |w| + k\frac{n - (2n - 2r - 1)^2}{4}
\end{aligned}
$$

So, we have found a word $u \in \Sigma^*$ with $|Q \circ u| \leq \frac{n}{2}$ and $|u| \leq |w| + k\frac{n^2-(2n-2r-1)^2}{4}$ (namely $u = w_{\lfloor \frac{n}{2} \rfloor}$). □

Definition 3.23. Let $\mathcal{A} = (Q, \Sigma, \delta)$ be a n-state synchronising automaton. We say that $\mathcal{A}$ is a strongly connected automaton if for all states $q_1, q_2 \in Q$ there is a word $w \in \Sigma^*$ such that $q_1 \circ w = q_2$.

Proposition 3.24 ([1],[2])**.** *Let $\mathcal{A} = (Q, \Sigma, \delta)$ be a n-state strongly connected synchronising automaton. Let $S \subseteq Q$ with $|S| \geq 2$. Then there exists a word $w \in \Sigma^*$ with $|w| \leq \frac{(n-|S|+2)(n-|S|+1)}{2}$ such that $|S \circ w| < |S|$.*

Definition 3.25. Let $1 \leq i < j \leq n$ be integers. Then we define the following number.

$$C(j, i) := \sum_{s=i+1}^{j} \frac{(n - s + 2)(n - s + 1)}{2}$$

Remark. $C(j, i)$ is an upperbound on the length of the shortest word compressing a subset of size j to a subset of size at most i. This you can see by starting with a subset $S \subseteq Q$ with $|S| = j$ and then iteratively applying Proposition 3.24.

Corollary 3.26. *Let $1 \leq i < j \leq n$ integers. Then*

$$C(j, i) = \frac{1}{2}(j - i)n^2 + \left((j - i) - \frac{1}{2}\left(j^2 - i^2\right)\right)n + \frac{1}{6}\left(j^3 - i^3\right) - \frac{1}{2}\left(j^2 - i^2\right) + \frac{1}{3}(j - i)$$

Proof. $C(j, i)$ is defined as a finite sum, thus we can rewrite this. Here we use, $\sum_{s=1}^{j} s = \frac{1}{2}j(j + 1)$ and $\sum_{s=1}^{j} s^2 = \frac{1}{6}j(j + 1)(2j + 1)$.

$$
\begin{aligned}
\sum_{s=i+1}^{j} \frac{(n - s + 2)(n - s + 1)}{2} &= \frac{1}{2}\sum_{s=i+1}^{j}\left(n^2 + 3n + 2 + s^2 - (2n + 3)s\right) \\
&= \frac{1}{2}\sum_{s=i+1}^{j}\left(n^2 + 3n + 2\right) + \frac{1}{2}\sum_{s=i+1}^{j}\left(s^2 - (2n + 3)s\right) \\
&= \frac{1}{2}\left(n^2 + 3n + 2\right)(j - i) + \frac{1}{2}\sum_{s=1}^{j}\left(s^2 - (2n + 3)s\right) \\
&\quad - \frac{1}{2}\sum_{s=1}^{i}\left(s^2 - (2n + 3)s\right)
\end{aligned}
$$

$$
\begin{aligned}
=&\frac{1}{2}\left(n^2+3n+2\right)(j-i)+\frac{1}{2}\cdot\frac{1}{6}j\,(j+1)\,(2j+1)\\
&-\frac{1}{2}\,(2n+3)\,\frac{1}{2}j\,(j+1)-\frac{1}{2}\cdot\frac{1}{6}i\,(i+1)\,(2i+1)\\
&+\frac{1}{2}\,(2n+3)\,\frac{1}{2}i\,(i+1)\\
=&\frac{1}{2}\left(n^2+3n+2\right)(j-i)+\frac{1}{12}\left(j\left(2j^2+j+2j+1\right)\right.\\
&\left.-i\left(2i^2+i+2i+1\right)\right)+\frac{1}{4}\,(2n+3)\left(i^2+i-j^2-j\right)\\
=&\frac{1}{2}\left(n^2+3n+2\right)(j-i)+\frac{1}{12}\left(2j^3+3j^2+j-\left(2i^3+3i^2+i\right)\right)\\
&+\frac{1}{4}\,(2n+3)\left(i^2-j^2+i-j\right)\\
=&\frac{1}{2}\,(j-i)\,n^2+\left(\frac{3}{2}\,(j-i)+\frac{1}{2}\left(i^2-j^2+i-j\right)\right)n+(j-i)\\
&+\frac{1}{12}\left(2\left(j^3-i^3\right)+3\left(j^2-i^2\right)+j-i\right)+\frac{3}{4}\left(i^2-j^2+i-j\right)\\
=&\frac{1}{2}\,(j-i)\,n^2+\left((j-i)-\frac{1}{2}\left(j^2-i^2\right)\right)n+(j-i)\\
&+\frac{1}{6}\left(j^3-i^3\right)+\frac{1}{4}\left(j^2-i^2\right)+\frac{1}{12}\,(j-i)-\frac{3}{4}\left(j^2-i^2\right)-\frac{3}{4}\,(j-i)\\
=&\frac{1}{2}\,(j-i)\,n^2+\left((j-i)-\frac{1}{2}\left(j^2-i^2\right)\right)n\\
&+\frac{1}{6}\left(j^3-i^3\right)-\frac{1}{2}\left(j^2-i^2\right)+\frac{1}{3}\,(j-i)
\end{aligned}
$$

□

Lemma 3.27. *Suppose that for some integer $1 \le k \le \frac{n}{8}$ and for all $A \subset Q$ with $1 \le |A| \le n-1$, there exists a word $v_A \in \Sigma^{k(n-|A|)}$ such that $A \not\subseteq Q \circ v_A$. Then there exists a word $w \in \Sigma^*$ such that $|Q \circ w| \le \frac{n}{2}$ and*

$$|w| \le k\frac{3n^2-64k^2+144k+13}{12}$$

Proof. In the proof of Lemma 3.22 we have seen that there exist a word $(v_Y \in \Sigma^{k(n-|Y|)})$ which reduces a subset $(Q \circ w_{i+1})$ of size $i+1$ to a subset $(Q \circ w_i)$ of size i. This word is of length at most $2k\,(n-i-1)$ (since $|Y| = 2i+2-n$). When we compare this to our other upper bound $C\,(i+1,i)$ we get the following.

$$
\begin{aligned}
2k\left(n-i-1\right) =& C\left(i+1,i\right)\\
=& \frac{1}{2}\left(i+1-i\right)n^2+\left(\left(i+1-i\right)-\frac{1}{2}\left(\left(i+1\right)^2-i^2\right)\right)n+\frac{1}{6}\left(\left(i+1\right)^3-i^3\right)\\
& -\frac{1}{2}\left(\left(i+1\right)^2-i^2\right)+\frac{1}{3}\left(i+1-i\right)\\
=& \frac{1}{2}n^2+\left(1-\frac{1}{2}\left(2i+1\right)\right)n+\frac{1}{6}\left(3i^2+3i+1\right)-\frac{1}{2}\left(2i+1\right)+\frac{1}{3}\\
=& \frac{1}{2}n^2+\left(\frac{1}{2}-i\right)n+\frac{1}{2}i^2-\frac{1}{2}i\\
=& \frac{1}{2}n^2+\frac{1}{2}n-\left(n+\frac{1}{2}\right)i+\frac{1}{2}i^2\\
0 =& \frac{1}{2}i^2-\left(n+\frac{1}{2}-2k\right)i+\frac{1}{2}n^2+\left(\frac{1}{2}-2k\right)n+2k
\end{aligned}
$$

The abc-formula gives two possible solutions (i_1 and i_2) for i.

$$
\begin{aligned}
i_1 :&= n+\frac{1}{2}-2k+\frac{1}{2}\sqrt{16k^2-24k+1}\\
&= n+\frac{1}{2}-2k+\frac{1}{2}\sqrt{\left(4k-1\right)^2-16k}\\
&\approx n+\frac{1}{2}-2k+\frac{1}{2}\sqrt{\left(4k-1\right)^2}\\
&= n+\frac{1}{2}-2k+\frac{1}{2}\left(4k-1\right)\\
&= n\\
i_2 :&= n+\frac{1}{2}-2k-\frac{1}{2}\sqrt{16k^2-24k+1}\\
&= n+\frac{1}{2}-2k-\frac{1}{2}\sqrt{\left(4k-1\right)^2-16k}\\
&\approx n+\frac{1}{2}-2k-\frac{1}{2}\sqrt{\left(4k-1\right)^2}\\
&= n+\frac{1}{2}-2k-\frac{1}{2}\left(4k-1\right)\\
&= n-4k+1
\end{aligned}
$$

It must hold that $i < n$, so we can disregard the solution i_1. Which leaves us with the solution i_2. Since we are interested in the case that n is large we define $i = n - 4k$ and $j = n$. Then we know that there exists a word $v \in \Sigma^*$ such that $|v| \leq C(j,i) = C(n, n-4k)$ and $|Q \circ v| \leq i = n - 4k < n$.

$$
\begin{aligned}
C(n, n-4k) &= \sum_{s=n-4k+1}^{n} \frac{(n-s+2)(n-s+1)}{2} \\
&= \frac{1}{2} \sum_{i=0}^{4k-1} (4k-i+1)(4k-i) \\
&= \frac{1}{2} \sum_{i=1}^{4k} i(i+1) \\
&= \frac{1}{2} \sum_{i=1}^{4k} i^2 + \frac{1}{2} \sum_{i=1}^{4k} i \\
&= \frac{1}{2} \cdot \frac{1}{6} 4k(4k+1)(8k+1) + \frac{1}{2} \cdot \frac{1}{2} 4k(4k+1) \\
&= 4k \left(\frac{1}{12} \left(32k^2 + 12k + 1\right) + \frac{1}{4}(4k+1) \right) \\
&= 4k \left(\frac{8}{3} k^2 + k + \frac{1}{12} + \frac{1}{4} + k \right) \\
&= \frac{4k(8k^2 + 6k + 1)}{3}
\end{aligned}
$$

If $|Q \circ v| > \frac{n}{2}$, then since $\left\lfloor \frac{n+1}{2} \right\rfloor = \begin{cases} \frac{n}{2} & \text{if } n \text{ even} \\ \frac{n+1}{2} & \text{if } n \text{ odd} \end{cases}$ we have $|Q \circ v| \geq \left\lfloor \frac{n+1}{2} \right\rfloor$. We can apply Lemma 3.22, this gives that there exists a word $w \in \Sigma^*$ such that $|Q \circ w| \leq \frac{n}{2}$ and:

$$
\begin{aligned}
|w| &\leq |v| + k \frac{n^2 - (2n - 2(n-4k) - 1)^2}{4} \\
&\leq \frac{4k(8k^2 + 6k + 1)}{3} + k \frac{n^2 - (8k-1)^2}{4} \\
&= k \frac{16(8k^2 + 6k + 1) + 3\left(n^2 - (8k-1)^2\right)}{12} \\
&= k \frac{3n^2 + 16(8k^2 + 6k + 1) - 3(64k^2 - 16k + 1)}{12} \\
&= k \frac{3n^2 - 64k^2 + 144k + 13}{12}
\end{aligned}
$$

If $|Q \circ v| \leq \frac{n}{2}$, then the already found word is the desired word (word v). This is because $k \frac{n^2 - (8k-1)^2}{4} \geq 0$ (since $k \leq \frac{n}{8}$), so $|v| \leq \frac{4k\left(8k^2+6k+1\right)}{3} \leq k \frac{3n^2 - 64k^2 + 144k + 13}{12}$ □

Suppose we meet all assumptions of Lemma 3.27. Then we like to see that the result of Lemma 3.27 is a better upper bound then the already known upper bound $C\left(n, \frac{n}{2}\right)$.

We have $1 \leq k \leq \frac{n}{8}$. Suppose $k := cn$, where $c \in \left[\frac{1}{n}, \frac{1}{8}\right]$. Lemma 3.27 gives then that there exists a word $w \in \Sigma^*$ with $|Q \circ w| \leq \frac{n}{2}$ and $|w| \leq cn\frac{3n^2-64(cn)^2+144cn+13}{12}$.

$$cn\frac{3n^2 - 64\left(cn\right)^2 + 144cn + 13}{12} = \frac{\left(3c - 64c^3\right)n^3 + 144cn + 13}{12}$$

We want to compare the coefficient before n^3 to the coefficient before n^3 in $C(n, \frac{n}{2})$

$$\begin{aligned}
C\left(n, \frac{n}{2}\right) &= \frac{1}{2} \cdot \frac{n}{2}n^2 + \left(\frac{n}{2} - \frac{1}{2}\left(n^2 - \left(\frac{n}{2}\right)^2\right)\right)n + \frac{1}{6}\left(n^3 - \left(\frac{n}{2}\right)^3\right) - \frac{1}{2}\left(n^2 - \left(\frac{n}{2}\right)^2\right) + \frac{1}{3} \cdot \frac{n}{2} \\
&= \frac{n^3}{4} + \left(\frac{n}{2} - \frac{1}{2} \cdot \frac{3n^2}{4}\right)n + \frac{1}{6} \cdot \frac{7n^3}{8} - \frac{1}{2} \cdot \frac{3n^2}{4} + \frac{n}{6} \\
&= \frac{n^3}{4} + \frac{n^2}{2} - \frac{3n^3}{8} + \frac{7n^3}{48} - \frac{3n^2}{8} + \frac{n}{6} \\
&= \frac{n^3}{48} + \frac{n^2}{8} + \frac{n}{6} \\
&= \frac{n^3 + 6n^2 + 8n}{48}
\end{aligned}$$

So if indeed the result of Lemma 3.27 is a better upper bound then the already known upper bound $C\left(n, \frac{n}{2}\right)$, we must have that $\frac{3c-64c^3}{12} \leq \frac{1}{48}$.

$$\begin{aligned}
\frac{\left(3c - 64c^3\right)}{12} &\leq \frac{1}{48} \\
3c - 64c^3 &\leq \frac{1}{4} \\
0 &\leq 64c^3 - 3c + \frac{1}{4} \\
&= c^3 - \frac{3c}{63} + \frac{1}{256} \\
&= \left(c - \frac{1}{8}\right)^2\left(c + \frac{1}{4}\right)
\end{aligned}$$

$0 \leq \left(c - \frac{1}{8}\right)^2\left(c + \frac{1}{4}\right)$ holds for all $c \geq -\frac{1}{4}$. And since we have $c \in \left[\frac{1}{n}, \frac{1}{8}\right]$, this always holds.
Therefore, for n large enough and if all assumptions of Lemma 3.27 are satisfied, Lemma 3.27 gives a better result (upper bound) then $C\left(n, \frac{n}{2}\right)$ gives.

Lemma 3.28. *Let $\mathcal{A}$ be a synchronising, n-state automaton without a sink state. Then for every integer $1 \leq k \leq \frac{n}{8}$ there exists a reset word $w \in \Sigma^*$ with*

$$|w| \leq max\left\{k\frac{3n^2 - 64k^2 + 144k + 13}{12}, k\left(n-1\right) + C\left(n-k, \left\lfloor\frac{n}{2}\right\rfloor\right)\right\} + C\left(\left\lfloor\frac{n}{2}\right\rfloor, 1\right)$$

Proof. Let k be any integer with $1 \leq k \leq \frac{n}{8}$.
Let $\mathcal{A}$ be a synchronising, n-state automaton with no sink state. Then we know that for all $\emptyset \neq A \subset Q$ there exist a word $w \in \Sigma^*$ such that $A \not\subseteq Q \circ w$.
So we can use Lemma 3.18 with $S = Q$.

There are two cases, either for all $\emptyset \neq A \subset Q$ case 1 of Lemma 3.18 hold, or there exists a subset $\emptyset \neq A \subset Q$ for which case 2 of Lemma 3.18 holds.

Suppose for all $\emptyset \neq A \subset Q$ case 1 of Lemma 3.18 holds. So for all $\emptyset \neq A \subset Q$ there exist a word $w \in \Sigma^{\leq k(n-|A|)}$ such that $A \not\subseteq Q \circ w$.
Then we know by Lemma 3.27 that there exists a word $w \in \Sigma^*$ with $|w| \leq k\frac{3n^2-64k^2+144k+13}{12}$, such that $|Q \circ w| \leq \frac{n}{2}$ (which implies $|Q \circ w| \leq \left\lfloor \frac{n}{2} \right\rfloor$, since $|Q \circ w|$ is an integer).

Suppose there exist some subset $\emptyset \neq A \subset Q$ for which case 2 of Lemma 3.18 holds. Then we know that for this subset $\emptyset \neq A \subset Q$ $(1 \leq |A| \leq n-1)$ there exists a word $w \in \Sigma^{k(n-|A|)}$ such that $|Q \circ w| \leq |Q| - k = n - k$. We have $|w| \leq k\,(n - |A|) \leq k\,(n-1)$.
We know there exist a word $v \in \Sigma^*$ with $|v| \leq C\left(n-k, \left\lfloor \frac{n}{2} \right\rfloor\right)$ which compresses the subset $Q \circ w$ to some set of size less or equal to $\left\lfloor \frac{n}{2} \right\rfloor$.
Together this gives that there exist a word $w \in \Sigma^*$ with $|w| \leq k\,(n-1) + C\left(n-k, \left\lfloor \frac{n}{2} \right\rfloor\right)$ such that $|Q \circ w| \leq \left\lfloor \frac{n}{2} \right\rfloor$.

Combining these two cases gives that there exists a word $w \in \Sigma^*$ of length $|w| \leq \max\left\{k\frac{3n^2-64k^2+144k+13}{12}, k\,(n-1) + C\left(n-k, \left\lfloor \frac{n}{2} \right\rfloor\right)\right\}$ such that $|Q \circ w| \leq \left\lfloor \frac{n}{2} \right\rfloor$.

Finally we need to compress a subset of size less of equal to $\left\lfloor \frac{n}{2} \right\rfloor$, to a subset of size 1. We know that there exist such word $w \in \Sigma^*$ with $|w| \leq C\left(\left\lfloor \frac{n}{2} \right\rfloor, 1\right)$.
So we can conclude that there exist a reset word $w \in \Sigma^*$ of length $|w| \leq \max\left\{k\frac{3n^2-64k^2+144k+13}{12}, k\,(n-1) + C\left(n-k, \left\lfloor \frac{n}{2} \right\rfloor\right)\right\} + C\left(\left\lfloor \frac{n}{2} \right\rfloor, 1\right)$. □

Theorem 3.29.

$$C\,(n) \leq 0.166421334n^3 + 1.42781363n^2 - 0.210099161n$$

Proof. To prove our theorem we use Lemma 3.22 with a suitable k, which minimizes $\max\left\{k\frac{3n^2-64k^2+144k+13}{12}, k\,(n-1) + C\left(n-k, \left\lfloor \frac{n}{2} \right\rfloor\right)\right\}$, for n large enough.

Take a look at $C\left(n-k, \left\lfloor \frac{n}{2} \right\rfloor\right)$ for $n \geq 2$.
If n is even, then we get with the use of Corollary 3.26 the following.

$$\begin{aligned}
C\left(n-k, \left\lfloor \frac{n}{2} \right\rfloor\right) =& C\left(n-k, \frac{n}{2}\right) \\
=& \frac{1}{2}\left(n-k-\frac{n}{2}\right)n^2 + \left(\left(n-k-\frac{n}{2}\right) - \frac{1}{2}\left((n-k)^2 - \left(\frac{n}{2}\right)^2\right)\right)n \\
&+ \frac{1}{6}\left((n-k)^3 - \left(\frac{n}{2}\right)^3\right) - \frac{1}{2}\left((n-k)^2 - \left(\frac{n}{2}\right)^2\right) + \frac{1}{3}\left(n-k-\frac{n}{2}\right) \\
=& \frac{1}{2}\left(\frac{n}{2}-k\right)n^2 + \left(\left(\frac{n}{2}-k\right) - \frac{1}{2}\left(\frac{3n^2}{4} - 2kn + k^2\right)\right)n \\
&+ \frac{1}{6}\left(\frac{7n^3}{8} - 3kn^2 + 3k^2n - k^3\right) - \frac{1}{2}\left(\frac{3n^2}{4} - 2kn + k^2\right) + \frac{1}{3}\left(\frac{n}{2}-k\right)
\end{aligned}$$

$$
\begin{aligned}
=&\frac{n^3}{4} - \frac{kn^2}{2} - \frac{3n^3}{8} + \left(\frac{1}{2} + k\right) n^2 - \left(k + \frac{k^2}{2}\right) n + \frac{7n^3}{48} - \frac{kn^2}{2} + \frac{k^2 n}{2} \\
&- \frac{k^3}{6} - \frac{3n^2}{8} + kn - \frac{k^2}{2} + \frac{n}{6} - \frac{k}{3} \\
=&\frac{1}{48}n^3 + \frac{1}{8}n^2 + \frac{1}{6}n - \frac{1}{6}k^3 - \frac{1}{2}k^2 - \frac{1}{3}k \\
=&\frac{n^3 + 6n^2 + 8n - 8k^3 - 24k^2 - 16k}{48}
\end{aligned}
$$

Analogue we get, if n is odd the following.

$$
\begin{aligned}
C\left(n-k, \left\lfloor \frac{n}{2} \right\rfloor\right) &= C\left(n-k, \frac{n-1}{2}\right) \\
&= \frac{n^3 + 9n^2 + 23n - 8k^3 - 24k^2 - 16k + 15}{48}
\end{aligned}
$$

This is larger than $C\left(n-k, \left\lfloor \frac{n}{2} \right\rfloor\right)$ with n is even. So we have that

$$
C\left(n-k, \left\lfloor \frac{n}{2} \right\rfloor\right) \leq \frac{n^3 + 9n^2 + 23n - 8k^3 - 24k^2 - 16k + 15}{48}
$$

Take a look at $C\left(\left\lfloor \frac{n}{2} \right\rfloor, 1\right)$ for $n \geq 2$. We use again Corollary 3.26
If n is even then we get:

$$
\begin{aligned}
C\left(\left\lfloor \frac{n}{2} \right\rfloor, 1\right) &= C\left(\frac{n}{2}, 1\right) \\
&= \frac{7n^3 - 6n^2 - 16n}{48}
\end{aligned}
$$

If n is odd then we get:

$$
\begin{aligned}
C\left(\left\lfloor \frac{n}{2} \right\rfloor, 1\right) &= C\left(\frac{n-1}{2}, 1\right) \\
&= \frac{7n^3 - 9n^2 - 31n - 15}{48}
\end{aligned}
$$

This is smaller than $C\left(\left\lfloor \frac{n}{2} \right\rfloor, 1\right)$ with n is even. So, we have that

$$
C\left(\left\lfloor \frac{n}{2} \right\rfloor, 1\right) \leq \frac{7n^3 - 6n^2 - 16n}{48}
$$

We wanted to improve the coefficient of n^3 (compared to the upper bound $C(n) \leq \frac{n^3-n}{6}$, which has coefficient $\frac{1}{6}$ before n^3). So, we want a coefficient of n^3 smaller then $\frac{1}{6}$.

If $k \in o(n)$, then for n large enough is $\max\left\{k\frac{3n^2-64k^2+144k+13}{12}, k(n-1) + \frac{n^3+9n^2+23n-8k^3-24k^2-16k+15}{48}\right\}$ determined by the second argument. Since the second argument has a n^3 term and the first argument

doesn't.
In this case we get

$$C(n) \leq \frac{n^3 + 9n^2 + 23n - 8k^3 - 24k^2 - 16k + 15}{48} + \frac{7n^3 - 6n^2 - 16n}{48}$$

Here is the coefficient before n^3 equal to $\frac{1+7}{48} = \frac{1}{6}$. This doesn't give us an improved upper bound.

Therefore we let k be linear dependent on n. Let's assume $k := cn$ for some constant $c \in \mathbb{R}$.
Since both functions $k\frac{3n^2-64k^2+144k+13}{12}$ and $k\,(n-1) + \frac{n^3+9n^2+23n-8k^3-24k^2-16k+15}{48}$ are continuous and one is increasing with k and the other decreasing with k, it is enough to consider the values of k such that both functions are equal.
For n large enough we have $cn\frac{3n^2-64c^2n^2+144cn+13}{12} \sim \frac{3c-64c^3}{12}n^3$ and
$cn\,(n-1) + \frac{n^3+9n^2+23n-8c^3n^3-24c^2n^2-16cn+15}{48} \sim \frac{1-8c^3}{48}n^3$.
So we want the coefficients before n^3 in both function to be equal. This gives us the following.

$$\frac{3c - 64c^3}{12} = \frac{1 - 8c^3}{48}$$
$$3c - 64c^3 = \frac{1 - 8c^3}{4}$$

The approximate solution of this is $c \approx 0.11375462$. Thus, we choose $k = 0.11375462n$.
With this value of k, we get the following.

$$\begin{aligned} k\frac{3n^2 - 64k^2 + 144k + 13}{12} &= 0.11375462n\frac{3n^2 - 64 \cdot 0.11375462^2n^2 + 144 \cdot 0.11375462n + 13}{12} \\ &= \frac{0.2470565007n^3 + 1.863376354n^2 + 1.4788106n}{12} \\ &= 0.020588001n^3 + 1.55281363n^2 + 0.123234172n \end{aligned}$$

and

$$\begin{aligned} k\,(n-1) + &\frac{n^3 + 9n^2 + 23n - 8k^3 - 24k^2 - 16k + 15}{48} \\ =&0.11375462n\,(n-1) \\ &+ \frac{n^3 + 9n^2 + 23n - 8 \cdot 0.11375462^3n^3 - 24 \cdot 0.11375462^2n^2 - 16 \cdot 0.11375462n + 15}{48} \\ =&0.11375462n^2 - 0.11375462n \\ &+ \frac{n^3 + 9n^2 + 23n - 0.011775982n^3 - 0.310562726n^2 - 1.82007392n + 15}{48} \\ =&0.11375462n^2 - 0.11375462n \\ &+ \frac{0.988224018n^3 + 8.689437274n^2 + 21.17992608n + 15}{48} \end{aligned}$$

$$
\begin{aligned}
=&0.11375462n^2 - 0.11375462n + 0.020588n^3 + 0.181029943n^2 \\
&+ 0.44124846n + 0.3125 \\
=&0.020588n^3 + 0.294784563n^2 + 0.32749384n + 0.3125 \\
\leq&0.020588001n^3 + 1.55281363n^2 + 0.123234172n
\end{aligned}
$$

With this and Lemma 3.28 we can conclude the following.

$$
\begin{aligned}
C(n) &\leq 0.020588001n^3 + 1.55281363n^2 + 0.123234172n + \frac{7n^3 - 6n^2 - 16n}{48} \\
&= 0.166421334n^3 + 1.42781363n^2 - 0.210099161n
\end{aligned}
$$

□

Theorem 3.29 gives the coefficient of n^3 to be $0.166421334 < \frac{1}{6}$. So we have found an improved upper bound of $C(n)$.
Marek Szykuła finds the coefficient of n^3 to be $\frac{85059}{511104} = 0.166422098$. Our Theorem is slightly more accurate because we used $k = 0.11375462n$ instead of the rational approximation $k = \left\lfloor \frac{5}{44}n \right\rfloor$.

Marek Szykuła was able to improve the upper bound, found by J.-E Pin and P. Frankl, by the factor $\frac{85059}{85184} \approx 0.998532588$. We improved the upper bound, found by J.-E Pin and P. Frankl, by the factor $0.166421334 \cdot 6 = 0.998528004$. Since $0.998528004 < \frac{85059}{85184}$ holds we again see that our found upper bound is slightly more accurate. We have improved the upper bound found by Marek Szykuła by the factor $0.166421334 \cdot \frac{511104}{85059} = 0.999995409$.

Chapter 4

Random words

In this chapter we are still interested in finding the length of the shortest reset word, but now we have a probability distribution on the letters of our alphabet. This means that our words aren't fixed, but are somewhat random.
Let $\Sigma = \{a, b\}$, then a probability distribution is:

$$\mathbb{P}(a) = p \qquad\qquad \mathbb{P}(b) = 1 - p$$

with $p \in [0, 1]$.
This means that with probability p we get the letter a and with probability $1 - p$ the letter b. With this probability distribution we again have an automaton and power automaton, but then with probabilities next to the letters.

Since we now have no influence over the words and letters, we can only look at the expected length of a reset word. If we have a synchronizing automaton $\mathcal{A}$ with n states, then the probability that the expected length of a reset word is finite is equal to one.

Example 4.1. For the C_4 shown in Figure 2.3, we then get the following automaton:

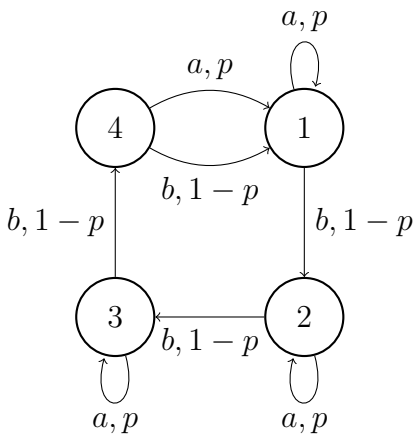

Figure 4.1: C_4 with probability distribution on the alphabet.

For C_3, we have the following automaton:

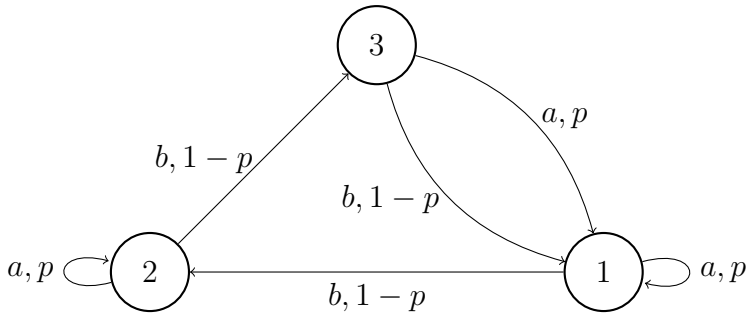

Figure 4.2: C_3 with probability distribution on the alphabet.

The corresponding power automaton of automaton in Figure 4.2 is shown in Figure 4.3.

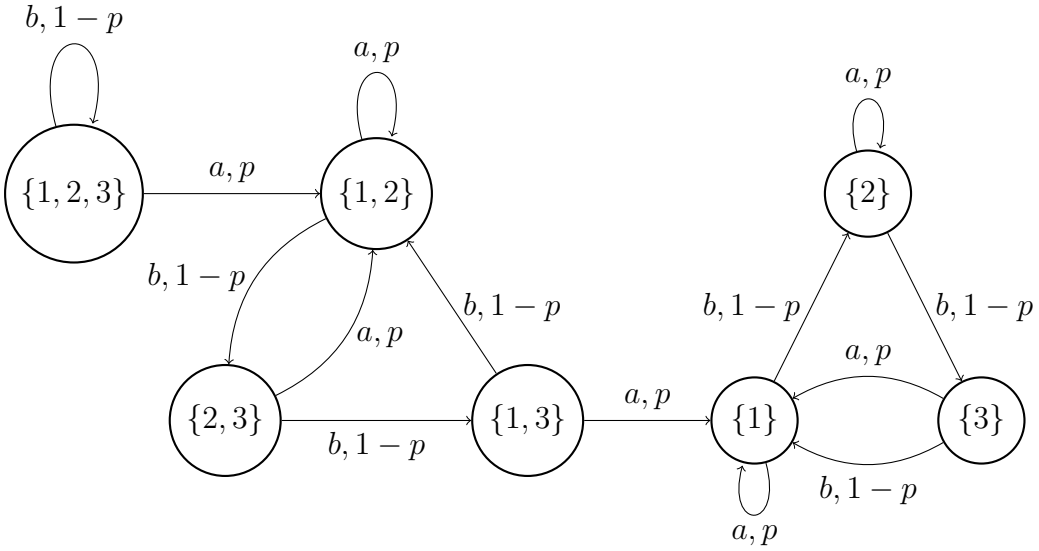

Figure 4.3: Power automaton of Figure 4.2.

4.1 Markov chains

We can see the automaton in Example 4.1 as a Markov chain. To understand what this means we first need some definitions [10].

Definition 4.2. An *E-valued process* is a function $\xi : I \to E$, where I is an index set.

Definition 4.3. An *E-valued stochastic process* is an E-valued process in which: $\forall i \in I$: $\xi(i) \in E$ is a random variable. In a discrete time stochastic process, the index set I is finite or countable.

We can write:

$$\begin{aligned}\mathbb{P}(\xi_{i_1} = x_1, \ldots, \xi_{i_t} = x_t) &= \mathbb{P}(\xi_{i_t} = x_t | \xi_{i_1} = x_1, \ldots, \xi_{i_{t-1}} = x_{t-1}) \cdot \mathbb{P}(\xi_{i_1} = x_1, \ldots, \xi_{i_{t-1}} = x_{t-1}) \\ &\vdots \\ &= \mathbb{P}(\xi_{i_1} = x_1) \prod_{j=2}^{t} \mathbb{P}(\xi_{i_j} = x_j | \xi_{i_1} = x_1, \ldots, \xi_{i_{j-1}} = x_{j-1})\end{aligned}$$

Definition 4.4. A *discrete time Markov chain (MC)* is a stochastic process with $\mathbb{P}(\xi_{i_t} = x_t | \xi_{i_1} = x_1, \ldots, \xi_{i_{t-1}} = x_{t-1}) = \mathbb{P}(\xi_{i_t} = x_t | \xi_{i_{t-1}} = x_{t-1})$

with the same process as before we get for discrete time Markov chains the following.

$$\mathbb{P}(\xi_{i_1} = x_1, \ldots, \xi_{i_t} = x_t) = \mathbb{P}(\xi_{i_1} = x_1) \prod_{j=2}^{t} \mathbb{P}(\xi_{i_j} = x_j | \xi_{i_{j-1}} = x_{j-1})$$

Definition 4.5. A *homogeneous Markov chain* is a Markov chain for which the following holds.

$$\forall m \in \mathbb{N} : \mathbb{P}(\xi_t = y | \xi_{t-1} = x) = \mathbb{P}(\xi_{t+m} = y | \xi_{t+m-1} = x)$$

In this case we define a *transition matrix*, or *Kernel*, or *transition probability* K as $K_{ij} := \mathbb{P}(\xi_t = j | \xi_{t-1} = i)$

Let $\mu_{t,i} = \mathbb{P}(\xi_t = i)$, then $\mu_{t+1,j} = \sum_i \mu_{t,i} K_{ij}$. In vector notation this is:
$\overrightarrow{\mu}_{t+1} = \overrightarrow{\mu}_t K$.

Example 4.6. Look at the automaton in Figure 4.1 in Example 4.1. Here interpret ξ_t as the (random) state at time $t \in \mathbb{N}$.Then we have

$$p_{xy} := \mathbb{P}(\xi_{t+m} = y | \xi_{t+m-1} = x) = \begin{cases} p & \text{if } \delta(x, a) = y \\ 1 - p & \text{if } \delta(x, b) = y \\ 0 & \text{otherwise} \end{cases}$$

Since $\mathbb{P}(\xi_{t+m} = y | \xi_{t+m-1} = x)$ is independent of m we get,
$\forall m \in \mathbb{N} : \mathbb{P}(\xi_t = y | \xi_{t-1} = x) = \mathbb{P}(\xi_{t+m} = y | \xi_{t+m-1} = x)$. So we have a homogeneous Markov chain.

The transition matrix for this automaton is: $K_{C_4} = \begin{pmatrix} p & 1-p & 0 & 0 \\ 0 & p & 1-p & 0 \\ 0 & 0 & p & 1-p \\ 1 & 0 & 0 & 0 \end{pmatrix}$

Here is $K_{ij} = \mathbb{P}(\xi_t = j | \xi_{t-1} = i)$ $\forall i, j = 1, 2, 3, 4$.
K_{ij} are calculated as follows:

- $K_{44} = \mathbb{P}(\xi_t = 4 | \xi_{t-1} = 4) = 0$, since there is no loop at state 4 to itself.
- $K_{41} = \mathbb{P}(\xi_t = 1 | \xi_{t-1} = 4) = p + 1 - p = 1$, since both letters a and b send state 4 to state 1.
- $K_{23} = \mathbb{P}(\xi_t = 2 | \xi_{t-1} = 3) = 1 - p$, since only letter b sends state 2 to state 3 and $\mathbb{P}(b) = 1 - p$.
- Etc.

4.2 Expected length of reset word

With our knowledge of a Markov chain, we can take a look at the expected length of a reset word for a synchronizing automaton $\mathcal{A}$. Let $p \in [0,1]$ and $n \geq 2$ an integer. Then we consider synchronizing automata $\mathcal{A} = (Q, \Sigma, \delta)$, with $Q = \{1, \ldots, n\}$ and $\Sigma = \{a, b\}$ with $\mathbb{P}(a) = p$ and $\mathbb{P}(b) = 1 - p$.
First, we are going to make this more precise with some definitions. Thereafter, we will discuss how to calculate the expected length of a reset word of a synchronizing automaton $\mathcal{A}$. Finally, we end this section with the exact value of the expected length of a reset word, for the Černý automaton $\mathcal{C}_n$.

Definition 4.7. Let $Q = \{1, \ldots, n\}$ the set with all n states. Then we define A to be the set of singletons from Q. So $A = \{S \subset Q \mid |S| = 1\} = \{\{q\} \mid q \in Q\}$

Definition 4.8. For $t \geq 1$ we define the stochastic process $(W_t)_{t\in\mathbb{N}}$ with $W_t \in \Sigma$ by the following probabilities.

$$\mathbb{P}(W_t = a) = p \qquad\qquad \mathbb{P}(W_t = b) = 1 - p$$

Remark. By definition of the stochastic process $(W_t)_{t\in\mathbb{N}}$, W_t is independent of the time $t \in \mathbb{N}$ and independent of any other letter W_r (with $r \in \mathbb{N}$ and $r \neq t$).
Since $\mathbb{P}(W_t = a)$ and $\mathbb{P}(W_t = b)$ don't depend on time $t \in \mathbb{N}$, we use the notations $\mathbb{P}(W_t = a) = \mathbb{P}(a)$ and $\mathbb{P}(W_t = b) = \mathbb{P}(b)$

Definition 4.9. We define the Markov chain $(V_t)_{t\in\mathbb{N}}$ associated with a particular automaton $\mathcal{A}$, with $V_t \in \mathcal{P}(Q)\backslash\emptyset$ as follows.
Start in some subset $S \subseteq Q$, say $V_0 := S$ and for $t \geq 1$ we have $V_t := V_{t-1} \circ W_t$.

Since $\mathbb{P}(W_t = a)$ and $\mathbb{P}(W_t = b)$ don't depend on time $t \in \mathbb{N}$, we have that $\mathbb{P}(V_t = Y \mid V_{t-1} = Z) = \mathbb{P}(V_{t+m} = Y \mid V_{t+m-1} = Z)$ holds for all $m \in \mathbb{N}$. So the chain $(V_t)_{t\in\mathbb{N}}$ is indeed a (homogeneous) Markov chain (see Definitions 4.4 and 4.5).

Remark. When $X = V_t$ then we have the following transition probabilities:
$\mathbb{P}(V_{t+1} = X \circ a) = p$
$\mathbb{P}(V_{t+1} = X \circ b) = 1 - p$

Definition 4.10. Let $S \subseteq Q$, then we define $T_{\mathcal{A}}(S) := \min\{t \mid |V_t| = 1\}$, where $(V_t)_{t\in\mathbb{N}}$ is the Markov chain of automaton $\mathcal{A}$ with $V_0 = S$.
We write $T_{\mathcal{A}} := T_{\mathcal{A}}(Q)$.

Remark. $(|V_t|)_{t\in\mathbb{N}}$ is a decreasing sequence and at time $T_{\mathcal{A}}(S)$ we have come across a reset word for S in the automaton $\mathcal{A}$ ($W_1 \cdots W_{T_{\mathcal{A}}(S)}$), since $|V_{T_{\mathcal{A}}(S)}| = 1$.
So $q_1 \circ W_1 \cdots W_{T_{\mathcal{A}}(S)} = q_2 \circ W_1 \cdots W_{T_{\mathcal{A}}(S)}$ for all $q_1, q_2 \in S$.
Consider a synchronizing automaton $\mathcal{A} = (Q, \Sigma, \delta)$, with $Q = \{1, \ldots, n\}$ ($n \geq 2$ an integer) and $\Sigma = \{a, b\}$, with $\mathbb{P}(a) = p$ and $\mathbb{P}(b) = 1 - p$. Then $\mathbb{E}[T_{\mathcal{A}}]$ is the expected length of a reset word for automaton $\mathcal{A}$.

Definition 4.11. Let $\mathcal{A} = (Q, \Sigma, \delta)$ be a synchronizing automaton with n states and $S \subseteq Q$. Then we define E_S^A as the expected number of letters (elements of Σ) we need to get to some element of A, starting in S.
By definition of $T_{\mathcal{A}}(S)$, we get

$$E_S^A = \mathbb{E}[T_{\mathcal{A}}(S)]$$

As a corollary of Proposition 2.22 we then know that $E_Q^A (= \mathbb{E}[T_{\mathcal{A}}])$ is the expected length of a reset word in automaton $\mathcal{A}$. There are multiple ways to calculate E_Q^A.

4.2.1 Calculating E_Q^A: System 1

Since we can see the power automaton in the case of random input as a Markov chain, we can compute E_S^A with the following linear system [9].

$$\begin{cases} E_S^A = 0 & \text{if } S \in A \\ E_S^A = 1 + \sum_{\alpha \in \Sigma} \mathbb{P}(\alpha) E_{S \circ \alpha}^A & \text{if } S \notin A \end{cases} \tag{4.1}$$

Recall that $S \circ \alpha = \delta(S, \alpha) \subseteq Q$, and $\mathbb{P}(\alpha)$ is the probability of letter $\alpha \in \Sigma$.

Example 4.12. Take the automaton in Figure 4.2. So we have the Černý automaton C_3 with $\Sigma = \{a, b\}$ and $\mathbb{P}(a) = p$ and $\mathbb{P}(b) = 1 - p$.
The system for this automaton is:

$$\begin{cases} E_{\{1,2,3\}}^A = 1 + pE_{\{1,2\}}^A + (1-p)\, E_{\{1,2,3\}}^A \\ E_{\{1,2\}}^A = 1 + pE_{\{1,2\}}^A + (1-p)\, E_{\{2,3\}}^A \\ E_{\{2,3\}}^A = 1 + pE_{\{1,2\}}^A + (1-p)\, E_{\{1,3\}}^A \\ E_{\{1,3\}}^A = 1 + pE_{\{1\}}^A + (1-p)\, E_{\{1,2\}}^A = 1 + (1-p)\, E_{\{1,2\}}^A \end{cases}$$

Substituting $E_{\{1,3\}}^A = 1 + (1-p)\, E_{\{1,2\}}^A$ in $E_{\{2,3\}}^A = 1 + pE_{\{1,2\}}^A + (1-p)\, E_{\{1,3\}}^A$ gives:

$$\begin{aligned} E_{\{2,3\}}^A &= 1 + pE_{\{1,2\}}^A + (1-p)\, E_{\{1,3\}}^A \\ &= 1 + pE_{\{1,2\}}^A + (1-p)\left(1 + (1-p)E_{\{1,2\}}^A\right) \\ &= 1 + 1 - p + \left(p + (1-p)^2\right) E_{\{1,2\}}^A \\ &= 2 - p + \left(p + (1-p)^2\right) E_{\{1,2\}}^A \end{aligned}$$

This we can again substitute in $E_{\{1,2\}}^A = 1 + pE_{\{1,2\}}^A + (1-p)\, E_{\{2,3\}}^A$.

$$\begin{aligned} E_{\{1,2\}}^A &= 1 + pE_{\{1,2\}}^A + (1-p)\, E_{\{2,3\}}^A \\ &= 1 + pE_{\{1,2\}}^A + (1-p)\left(2 - p + \left(p^2 - p + 1\right) E_{\{1,2\}}^A\right) \\ &= 1 + pE_{\{1,2\}}^A + (1-p)\,(2-p) + (1-p)\left(p + (1-p)^2\right) E_{\{1,2\}}^A \end{aligned}$$

This gives the following.

$$\begin{aligned} (1 - p - p(1-p) - (1-p)^3) E_{\{1,2\}}^A &= 1 + (1-p)(2-p) \\ (1 - p + p^3 - 2p^2 + 2p - 1) E_{\{1,2\}}^A &= p^2 - 3p + 3 \\ (p^3 - 2p^2 + p) E_{\{1,2\}}^A &= p^2 - 3p + 3 \\ E_{\{1,2\}}^A &= \frac{p^2 - 3p + 3}{p^3 - 2p^2 + p} \end{aligned}$$

Then at last we have $E^A_{\{1,2,3\}} = 1 + pE^A_{\{1,2\}} + (1-p)\,E^A_{\{1,2,3\}}$, this gives with the calculation below our result.

$$\begin{aligned}
E^A_{\{1,2,3\}} &= 1 + pE^A_{\{1,2\}} + (1-p)\,E^A_{\{1,2,3\}} \\
(1-1+p)\,E^A_{\{1,2,3\}} &= 1 + pE^A_{\{1,2\}} \\
pE^A_{\{1,2,3\}} &= 1 + pE^A_{\{1,2\}} \\
E^A_{\{1,2,3\}} &= \frac{1}{p} + E^A_{\{1,2\}} \\
&= \frac{1}{p} + \frac{p^2-3p+3}{p^3-2p^2+p} \\
&= \frac{2p^2-5p+4}{p^3-2p^2+p} = \frac{2p^2-5p+4}{p(1-p)^2}
\end{aligned}$$

Suppose $\mathbb{P}(a) = \mathbb{P}(b) = \frac{1}{2}$, then we get
$E^A_{\{1,2,3\}} = \frac{2\cdot\frac{1}{2}^2-5\cdot\frac{1}{2}+4}{\frac{1}{2}^3-2\cdot\frac{1}{2}^2+\frac{1}{2}} = \frac{\frac{2}{4}-\frac{5}{2}+4}{\frac{1}{8}-\frac{2}{4}+\frac{1}{2}} = \frac{2}{\frac{1}{8}} = 2\cdot 8 = 16.$
The expected length of a reset word of the automaton in Figure 4.2 with $p = \frac{1}{2}$ is 16.

4.2.2 Calculating E^A_Q: System 2

We will describe another way to compute E^A_Q. We still use the power automaton, but now we compute for each arrow in the power automaton the expected number of times we use that arrow and then we sum up all these expected numbers. To make this more precise we need to define variable m_{IJ} and p_{IJ}, where I, J are states in the power automaton ($I, J \in \mathcal{P}(Q)\backslash\emptyset$).

Definition 4.13. Let $(V_t)_{t\in\mathbb{N}}$ be the Markov chain with $V_0 = Q$ as defined in Definition 4.9. When $|V_t| = 1$ ($V_t \in A$) we stop our chain.
We define $m_{IJ} := \mathbb{E}\left[\#\{0 \le t \le T \mid V_t = I, V_{t+1} = J\}\right]$ as the expected number of times we go from state I to state J, and $p_{IJ} := \mathbb{P}\left(V_{t+1} = J \mid V_t = I\right)$ as the probability of going to state J, given that we are in state I.

Then we have that $E^A_Q = \sum_{I,J\subseteq Q} m_{IJ}$.

Remark. In the power automaton, a state I is a non-empty subset of Q.
We use one more notation, namely m_{IA}, which is the expected number of times we go from state $\emptyset \neq I \subseteq Q$ (with $|I| \ge 2$) to some state in A.

To calculate m_{IJ} for all states, I and J, in the power automaton we use the following rules [9].

1. We enter A precisely one time and $m_{IA} \in \{0,1\}$ for all $\emptyset \neq I \subset Q$. There is exactly one $I \subseteq Q$ for which $m_{IA} = 1$. For $J \neq I$, we have $m_{JA} = 0$. This translates to $\sum_{J\in\mathcal{P}(Q)\backslash\{\emptyset\}} m_{JA} = 1$.

2. The expected number of times we go from state I to state J must (relative to p) be the same expected number times we go from state I to state K, where $J \neq K$. This translates to $p_{IK}m_{IJ} = p_{IJ}m_{IK}$, for all $I, J, K \in \mathcal{P}(Q)\backslash\{\emptyset\}$.

3. The expected total number of times that we go out of state I, must be equal to the expected total number of times we go in to state I, unless $I = Q$ or $I \in A$. This translates to $\sum_{J \in \mathcal{P}(Q)\setminus\{\emptyset\}} m_{IJ} = \sum_{J \in \mathcal{P}(Q)\setminus\{\emptyset\}} m_{JI}$, if $I \neq Q$, $I \notin A$.

4. For state $I = Q$, it holds that we travel exactly one more time out of state Q then that we travel in to state Q. So $\sum_{J \in \mathcal{P}(Q)\setminus\{\emptyset\}} m_{IJ} = 1 + \sum_{J \in \mathcal{P}(Q)\setminus\{\emptyset\}} m_{JI}$, if $I = Q$.

5. The expected number of times that we go from one state in A to another state in A is zero. This translates to $m_{IJ} = 0$ for $I, J \in A$.

Rule 4 is necessary, because Q is our starting point and we are looking for a path from Q to some state in A. Thus we have to exit state Q one time more than we enter Q. We have rule 1 and 5 because A is our endpoint. Once we reach some state in A we stop. Rule 3 exists because we can't travel more times out (in) a state than that we travel in to (out of) that same state.
All these rules together are sufficient to get a unique result about E_Q^A.
In short we get:

$$\begin{cases} \sum_{J \notin A} m_{JA} = 1 & \\ p_{IK} m_{IJ} = p_{IJ} m_{IK} & I, J, K \in \mathcal{P}(Q)\setminus\{\emptyset\} \\ \sum_{J \in \mathcal{P}(Q)\setminus\{\emptyset\}} m_{IJ} = \sum_{J \in \mathcal{P}(Q)\setminus\{\emptyset\}} m_{JI} & \text{if } I \neq Q, I \notin A \\ \sum_{J \in \mathcal{P}(Q)\setminus\{\emptyset\}} m_{IJ} = 1 + \sum_{J \in \mathcal{P}(Q)\setminus\{\emptyset\}} m_{JI} & \text{if } I = Q \\ m_{IJ} = 0 & \text{if } I, J \in A \end{cases} \tag{4.2}$$

Example 4.14. Take again the automaton in Figure 4.2. So, we have the Černý automaton C_3 with $\Sigma = \{a, b\}$ and $\mathbb{P}(a) = p$ and $\mathbb{P}(b) = 1 - p$.
You start with the fact that you know that $m_{\{1,3\}\{1\}} = 1$. Then rule 2 gives that $m_{\{1,3\}\{1,2\}} = \frac{1-p}{p}$. Rule 3 gives then that $m_{\{2,3\}\{1,3\}} = \frac{1}{p}$. Etc.
This gives you the end result given in Figure 4.4, here are the m_{IJ} values indicated in red.

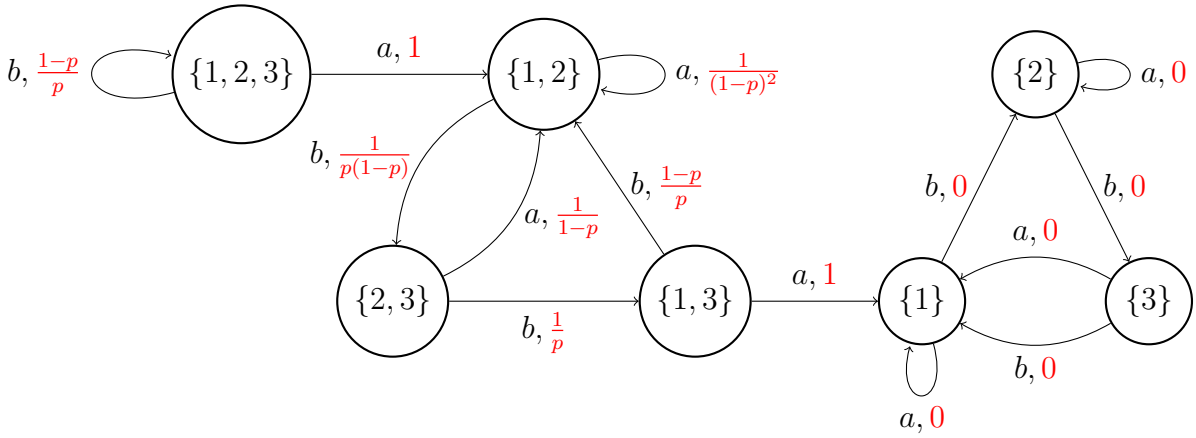

Figure 4.4: Power automaton of Figure 4.2, with m_{IJ} in red.

Then we get:

$$\begin{aligned} E_Q^A = E_{\{1,2,3\}}^A &= \frac{1-p}{p} + 1 + \frac{1}{(1-p)^2} + \frac{1}{p(1-p)} + \frac{1}{(1-p)} + \frac{1-p}{p} + \frac{1}{p} + 1 \\ &= \frac{-2p+4}{p(1-p)} + \frac{1}{(1-p)^2} \\ &= \frac{2p^2-6p+4}{p(1-p)^2} + \frac{p}{p(1-p)^2} = \frac{2p^2-5p+4}{p(1-p)^2} \end{aligned}$$

We can again take $p = \frac{1}{2}$. This would give:
$E_{\{1,2,3\}}^A = \frac{2\cdot\frac{1}{2}^2 - 5\cdot\frac{1}{2}+4}{\frac{1}{2}\cdot\frac{1}{2}^2} = \frac{\frac{2}{4}-\frac{5}{2}+4}{\frac{1}{8}} = \frac{2}{\frac{1}{8}} = 2 \cdot 8 = 16.$

We can see that the answer with this method is exactly the same as the answer we got in Example 4.12.

4.2.3 Calculating E_Q^A exact for the Černý automaton $\mathcal{C}_n$.

In this subsection we only look at the Černý automaton with n states, $\mathcal{C}_n = (Q, \Sigma, \delta)$. We have $Q = \{1, \ldots, n\}$, $\Sigma = \{a, b\}$ and

$$\delta : Q \times \Sigma \to Q : \begin{cases} \delta(i,a) = i & \text{for } i = 1, \ldots, n-1 \\ \delta(i,b) = i+1 & \text{for } i = 1, \ldots, n-1 \\ \delta(n,a) = \delta(n,b) = 1 & \end{cases}$$

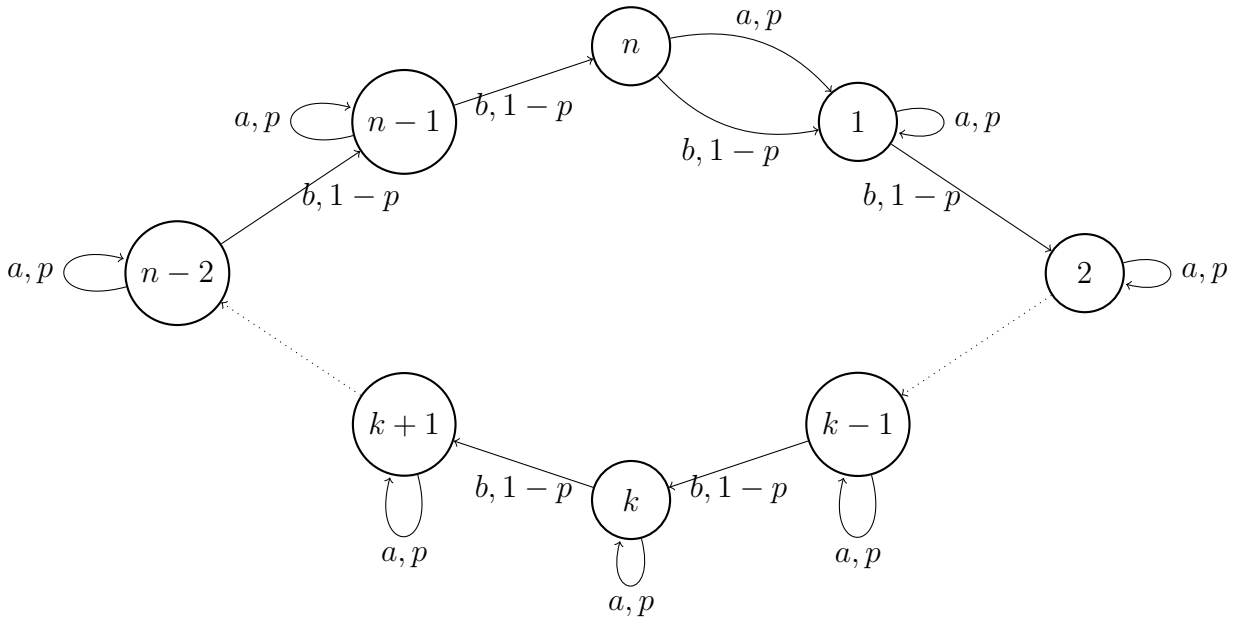

Figure 4.5: The Černý automaton with n states ($\mathcal{C}_n$) and $\mathbb{P}(a) = p$, $\mathbb{P}(b) = 1 - p$.

We want to calculate $\mathbb{E}[T_{\mathcal{C}_n}]$, recall that this is the expected length of a reset word (E_Q^A) for the Černý automaton $\mathcal{C}_n$ with $\mathbb{P}(a) = p$ and $\mathbb{P}(b) = 1 - p$.

Note that if $p = 0$ or $p = 1$ then $\mathbb{E}[T_{\mathcal{C}_n}]$ is infinite. Since any reset word for the Černý automaton $\mathcal{C}_n$ contains both letters a and b.

Theorem 4.15. *Let $\mathcal{A}$ be the Černý automaton with $n \geq 2$ states ($\mathcal{C}_n$) and $\mathbb{P}(a) = p$, $\mathbb{P}(b) = 1 - p$ for some $p \in (0, 1)$. Then the expected length of a reset word ($\mathbb{E}[T_{\mathcal{C}_n}]$) only depends on n and p, and can be calculated as follows.*

$$\mathbb{E}[T_{\mathcal{C}_n}] = \frac{(n-1)p^2 - \left(\sum_{i=2}^{n} i\right)p + \binom{n+1}{n-2}}{p(1-p)^2}$$

Begin proof Theorem 4.15. Suppose $n = 2$. Then by the use of system 2 (Subsection 4.2.2) we have $m_{\{1,2\}\{1,2\}} = \frac{1-p}{p}$, $m_{\{1,2\}\{1\}} = 1$, $m_{\{1\}\{1\}} = 0$,$m_{\{1\}\{2\}} = 0$ and $m_{\{2\}\{1\}} = 0$. So $\mathbb{E}[T_{\mathcal{C}_2}] = E_Q^A = 1 + \frac{1-p}{p} = \frac{1}{p}$.
If we fill in $n = 2$ in $\frac{(n-1)p^2 - \left(\sum_{i=2}^{n} i\right)p + \binom{n+1}{n-2}}{p(1-p)^2}$, we get the following:

$$\begin{aligned}
\frac{(n-1)p^2 - \left(\sum_{i=2}^{n} i\right)p + \binom{n+1}{n-2}}{p(1-p)^2} &= \frac{p^2 - 2p + \binom{3}{0}}{p(1-p)^2} \\
&= \frac{p^2 - 2p + 1}{p(1-p)^2} \\
&= \frac{(1-p)^2}{p(1-p)^2} \\
&= \frac{1}{p}
\end{aligned}$$

For $n = 2$ the theorem is correct.

The proof of this theorem for $n \geq 3$ is quite extensive. We need several lemmas and propositions. In the end we calculate $\mathbb{E}[T_{\mathcal{C}_n}]$ exactly for arbitrary $n \geq 3$ and $p \in (0, 1)$ by conditional probabilities and expected values.

Proof Theorem 4.15 ([11])

From now on assume $n \geq 3$.
First we can do the following calculations

$$\begin{aligned}
\frac{(n-1)p^2 - \left(\sum_{i=2}^{n} i\right)p + \binom{n+1}{n-2}}{p(1-p)^2} &= \frac{np^2 - p^2 - \frac{1}{2}n^2p - \frac{1}{2}np + p + \frac{1}{6}n^3 - \frac{1}{6}n}{p(1-p)^2} \\
&= \frac{\frac{1}{6}n^3 - \frac{1}{2}pn^2 + (p^2 - \frac{1}{2}p - \frac{1}{6})n + p(1-p)}{p(1-p)^2} \\
&= \frac{n^3 - 3pn^2 + (6p^2 - 3p - 1)n + 6p(1-p)}{6p(1-p)^2}
\end{aligned}$$

Here we use the following facts.

$$\begin{aligned}\sum_{i=2}^{n} i =& \frac{1}{2}n(n+1) - 1 \\ =& \frac{1}{2}n^2 + \frac{1}{2}n - 1\end{aligned}$$

$$\begin{aligned}\binom{n+1}{n-2} =& \frac{(n+1)!}{3!(n-2)!} = \frac{(n-1)n(n+1)}{6} \\ =& \frac{1}{6}n(n^2-1) = \frac{1}{6}n^3 - \frac{1}{6}n\end{aligned}$$

If we can prove that $\mathbb{E}[T_{\mathcal{C}_n}] = \frac{n^3-3pn^2+(6p^2-3p-1)n+6p(1-p)}{6p(1-p)^2}$ then Theorem 4.15 is proven.

We are going to calculate $\mathbb{E}[T_{\mathcal{C}_n}]$ by conditional probabilities and expected values. But before we can start with that we have to consider a particular situation, in which we can apply these conditional probabilities.

Consider an analogue situation of the one we saw in the proof of Theorem 3.3. Here we start with a pawn on each state, let say pawn k starts at state k, where $k = 1, \ldots, n$.

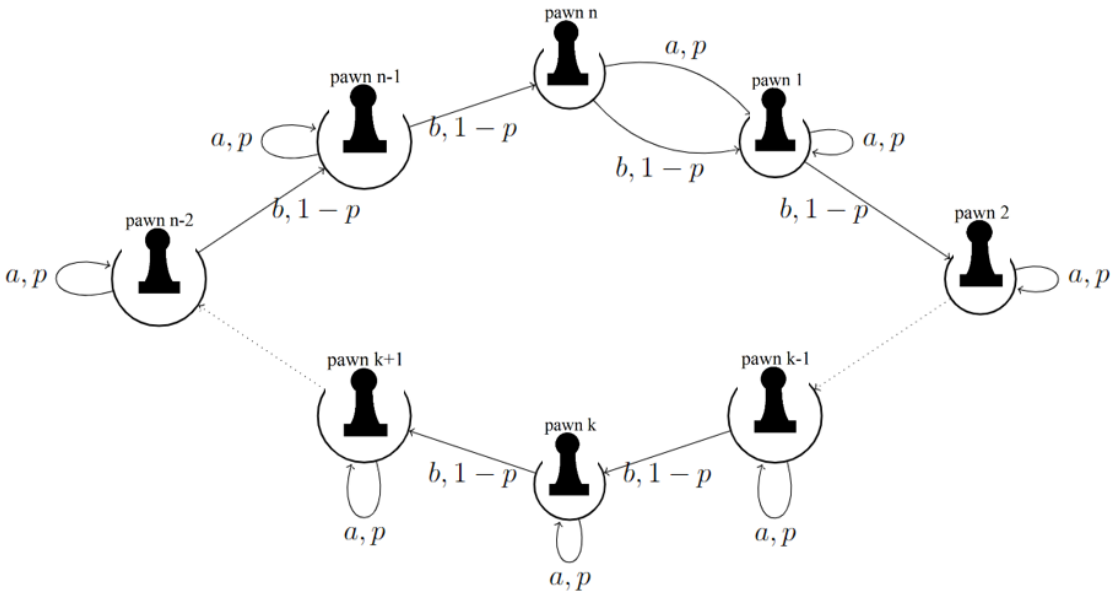

Figure 4.6: Starting situation: pawn k on state k.

If we read the letter b, starting in the starting position, then all pawns move one state forward. So pawn k will be on state $k+1$ for all $k = 1, \ldots, n-1$ and pawn n will be on state 1.

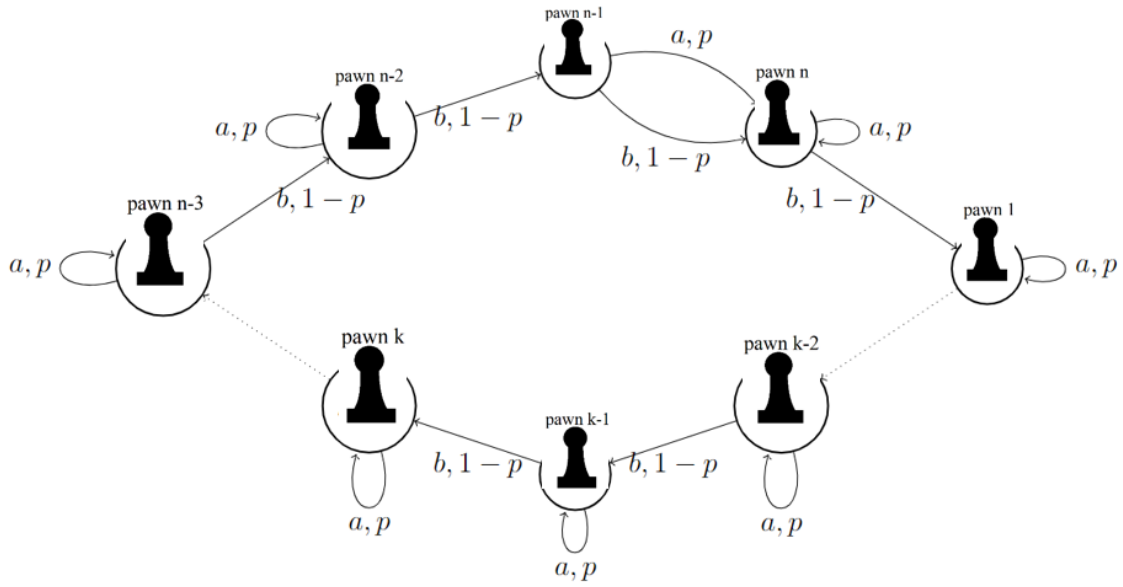

Figure 4.7: Situation after reading letter b.

If we read the letter a, starting in the starting position, then pawn k stays at state k for all $k = 1, \ldots, n-1$. Pawn n will go to state 1 after reading the letter a. In this situation, pawn n has caught up with pawn 1. Pawn n and 1 now follow the same path, thus will always be on the same state together.

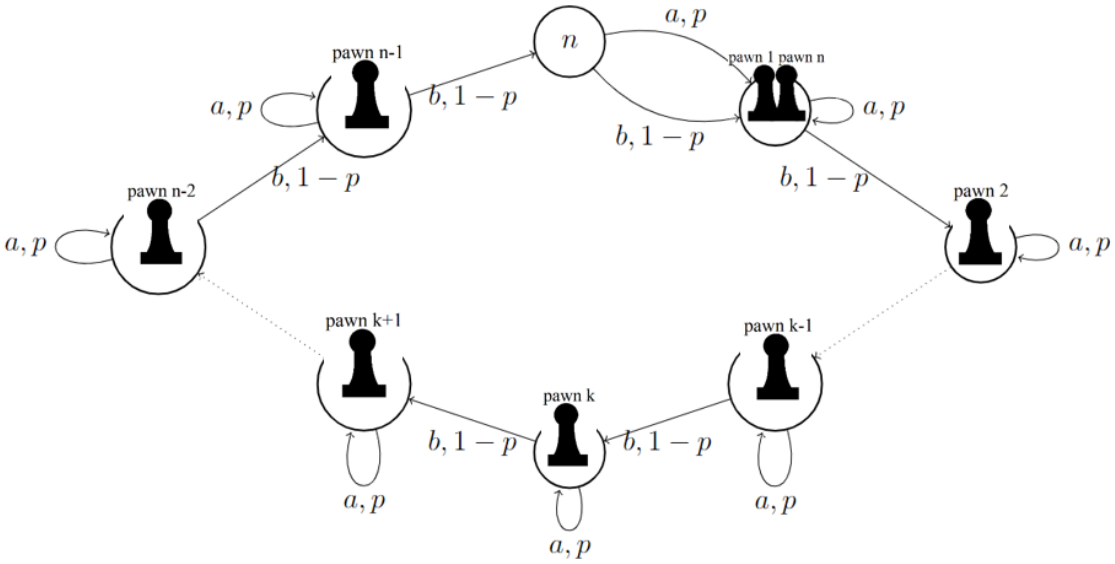

Figure 4.8: Situation after reading letter a.

Because of how the Černý automaton on n states is defined, all pawns can only walk circles in a clockwise direction. If $w \in \Sigma^*$ is a reset word, then after reading w all

pawns must end at the same state. This means that there must be a $k \in \{1, \ldots, n\}$ such that pawn k catches up with pawn $k-1$ (without pawn $k-1$ catching up to pawn k).
It also holds that once we have a $k \in \{1, \ldots, n\}$, such that pawn k catches up with pawn $k-1$ (without pawn $k-1$ catching up to pawn k), we have a reset word. Because once a pawn catches up to another pawn, they will follow the same path from that point on. And for pawn k to catch up to pawn $k-1$ he first has to catch up to all other pawns, since all pawns can only walk in clockwise circles.

Let's make this more precise with some extra definitions, in addition to the Definitions 4.8, 4.9, 4.10 and there corresponding remarks.

Definition 4.16. Let $k \in Q$ and $t \geq 0$. Define $W_1 \cdots W_t = \lambda$ for $t = 0$. Then we define the following stochastic process: $D(k, 0) = 0$ and

$$D(k, t+1) = \begin{cases} D(k,t) & \text{if } k \circ W_1 \cdots W_t = k \circ W_1 \cdots W_{t+1} \\ D(k,t) + 1 & \text{otherwise} \end{cases}$$

We say that pawn k has traveled distance $D(k,t)$ after reading word $W_1 \cdots W_t$.

Remark. The distance that pawn k travels is determined by the number of clockwise steps it takes. The letter b always causes pawn k to take a step clockwise. But only when pawn k is standing on state n, the letter a (and b) causes a clockwise step for pawn k. If pawn k is standing on any other state i ($i = 1, \ldots, n-1$), the letter a causes pawn k to stand still, and thus it does not travel any distance in that step. We have $D(k,t) \geq |W_1 \cdots W_t|_b$.

Example 4.17. Consider the Černý automaton $\mathcal{C}_n$. Let $k = n-2$ and suppose $W_1 = b$, $W_2 = a$, $W_3 = b$, $W_4 = a$. Then calculating $D(k, 4)$ goes as follows:

$(n-2) \circ bab = n \neq 1 = (n-2) \circ baba \quad \rightarrow D(n-2, 4) = 1 + D(n-2, 3)$
$(n-2) \circ ba = n-1 \neq n = (n-2) \circ bab \quad \rightarrow D(n-2, 3) = 1 + D(n-2, 2)$
$(n-2) \circ b = n-1 = (n-2) \circ ba \quad \rightarrow D(n-2, 2) = D(n-2, 1)$
$(n-2) \circ \lambda = n-2 \neq n-1 = (n-2) \circ b \quad \rightarrow D(n-2, 1) = 1 + D(n-2, 0) = 1$

This together gives:
$D(n-2, 4) = 1 + D(n-2, 3) = 1 + 1 + D(n-2, 2) = 1 + 1 + D(n-2, 1) = 1 + 1 + 1 = 3$

With this distance random variable we can define the event that pawn k catches up to pawn j.

Definition 4.18. Let $k, j \in Q$ where $k \neq j$. Then $E_{k,j} := \{D(k, T_{\mathcal{C}_n}) > D(j, T_{\mathcal{C}_n})\}$ is the event that pawn k catches up to pawn j.

In our calculation we use conditional probabilities. We look at the probability that we start with a certain letter (a or b), given the event $E_{k,k-1}$.
$\mathbb{P}(W_1 = a \mid E_{k,k-1})$ and $\mathbb{P}(W_1 = b \mid E_{k,k-1})$.

Let $w = W_1 \cdots W_T$, we want to know the value of $\mathbb{E}[T_{\mathcal{C}_n}]$.
We have defined $T_{\mathcal{C}_n} = T_{\mathcal{C}_n}(Q) = \min\{t \mid |V_t| = 1\}$, where $(V_t)_{t \in \mathbb{N}}$ is the Markov chain of automaton $\mathcal{C}_n$ with $V_0 = Q$. There must be precisely one $k \in \{1, \ldots, n\}$

such that pawn k catches up to pawn $k-1$, in other words $\exists! k \in Q$ such that event $E_{k,k-1}$ takes place. This means we can write $\mathbb{E}[T_{\mathcal{C}_n}]$ as follows.

$$\mathbb{E}[T_{\mathcal{C}_n}] = \sum_{k=1}^{n} \mathbb{P}(E_{k,k-1}) \cdot \mathbb{E}[T_{\mathcal{C}_n} \mid E_{k,k-1}] \tag{4.3}$$

Therefore, we have to calculate $\mathbb{P}(E_{k,k-1})$ and $\mathbb{E}[T_{\mathcal{C}_n} \mid E_{k,k-1}]$ for all $k = 1, \ldots, n$. For $\mathbb{P}(E_{k,k-1})$ we have the following result.

Lemma 4.19. *Let $w \in \Sigma^*$ be a reset word, then the following holds.*

1. $\mathbb{P}(E_{2,1}) = \cdots = \mathbb{P}(E_{n,n-1}) = \frac{1}{n-p}$.
2. $\mathbb{P}(E_{1,n}) = (1-p) \cdot \frac{1}{n-p} = \frac{1-p}{n-p}$

Proof. Since for pawn 1 to catch up to pawn n, we can never start with the letter a, We have:

$$\mathbb{P}(E_{1,n}) = (1-p)\,\mathbb{P}(E_{2,1}) \tag{4.4}$$

For $k = 2, \ldots, n-1$ we have the following calculation.

$$\begin{aligned} \mathbb{P}(E_{k,k-1}) &= p \cdot \mathbb{P}(E_{k,k-1}) + (1-p) \cdot \mathbb{P}(E_{k+1,k}) \\ (1-p)\,\mathbb{P}(E_{k,k-1}) &= (1-p)\,\mathbb{P}(E_{k+1,k}) \\ \mathbb{P}(E_{k,k-1}) &= \mathbb{P}(E_{k+1,k}) \end{aligned}$$

This results in the following.

$$\mathbb{P}(E_{2,1}) = \cdots = \mathbb{P}(E_{n,n-1}) \tag{4.5}$$

Besides Equations 4.5 and 4.4 we also know that $1 = \sum_{k=1}^{n} \mathbb{P}(E_{k,k-1})$. Together, this gives us the following.

$$\begin{aligned} 1 &= \mathbb{P}(E_{1,n}) + \sum_{k=2}^{n} \mathbb{P}(E_{k,k-1}) \\ &= (1-p)\,\mathbb{P}(E_{2,1}) + (n-1)\,\mathbb{P}(E_{2,1}) \\ &= (n-p)\,\mathbb{P}(E_{2,1}) \end{aligned}$$

With this we can conclude that $\mathbb{P}(E_{2,1}) = \frac{1}{n-p}$. This in turn, together with Equations 4.5 and 4.4, gives us our proposition. □

Now we are going to look at the values $\mathbb{E}[T_{\mathcal{C}_n} \mid E_{k,k-1}]$ (for all $k = 1, \ldots, n$).
We can calculate these values by conditioning on with which letter (a or b) we start.

$$\begin{aligned} \mathbb{E}[T_{\mathcal{C}_n} \mid E_{k,k-1}] =& \mathbb{P}(W_1 = a \mid E_{k,k-1})\,\mathbb{E}[T_{\mathcal{C}_n} \mid E_{k,k-1} \;\&\; W_1 = a] \\ &+ \mathbb{P}(W_1 = b \mid E_{k,k-1})\,\mathbb{E}[T_{\mathcal{C}_n} \mid E_{k,k-1} \;\&\; W_1 = b] \end{aligned}$$

To be able to use this we need to know $\mathbb{P}(V_1 = V_0 \circ l \mid E_{k,k-1})$ for $l = a, b$.

Lemma 4.20. *Let $w \in \Sigma^*$ be a reset word, then the following holds.*

- $\mathbb{P}(W_1 = b \mid E_{1,n}) = 1$
- $\mathbb{P}(W_1 = b \mid E_{k,k-1}) = 1 - p \qquad \forall k = 2, \ldots, n-1.$
- $\mathbb{P}(W_1 = b \mid E_{n,n-1}) = (1-p)^2$

Proof. If we start with an a, we have that pawn n always catches up with pawn 1, but never the other way around. Hence, if we know that pawn 1 catches up with pawn n, we always start with the letter b. So $\mathbb{P}(W_1 = b \mid E_{1,n}) = 1$.
For $k \in \{2, \ldots, n\}$ we use Bayes Theorem: $\mathbb{P}(A \mid B) = \frac{\mathbb{P}(A) \cdot \mathbb{P}(B|A)}{\mathbb{P}(B)}$.

For $k = 2, \ldots, n-1$ we have:

$$\begin{aligned}\mathbb{P}(W_1 = b \mid E_{k,k-1}) &= \frac{\mathbb{P}(W_1 = b) \cdot \mathbb{P}(E_{k,k-1} \mid W_1 = b)}{\mathbb{P}(E_{k,k-1})} \\ &= \frac{(1-p)\,\mathbb{P}(E_{k+1,k})}{\mathbb{P}(E_{k,k-1})} \\ &= \frac{(1-p)\,\mathbb{P}(E_{k,k-1})}{\mathbb{P}(E_{k,k-1})} = 1 - p\end{aligned}$$

For $k = n$ we get (by using Equations 4.4 and 4.5):

$$\begin{aligned}\mathbb{P}(W_1 = b \mid E_{n,n-1}) &= \frac{\mathbb{P}(W_1 = b) \cdot \mathbb{P}(E_{n,n-1} \mid W_1 = b)}{\mathbb{P}(E_{n,n-1})} \\ &= \frac{(1-p)\,\mathbb{P}(E_{1,n})}{\mathbb{P}(E_{n,n-1})} \\ &= \frac{(1-p)(1-p)\,\mathbb{P}(E_{n,n-1})}{\mathbb{P}(E_{n,n-1})} = (1-p)^2\end{aligned}$$

□

Lemma 4.21. *Let $w \in \Sigma^*$ be a reset word, then the following holds.*

- $\mathbb{P}(W_1 = a \mid E_{1,n}) = 0$
- $\mathbb{P}(W_1 = a \mid E_{k,k-1}) = p \qquad \forall k = 2, \ldots, n-1.$
- $\mathbb{P}(W_1 = a \mid E_{n,n-1}) = p(2-p)$

Proof. This lemma is proven by Lemma 4.20 and the fact that $\forall k = 1, \ldots, n$:

$$\mathbb{P}(W_1 = a \mid E_{k,k-1}) + \mathbb{P}(W_1 = b \mid E_{k,k-1}) = 1$$

□

Now we can for all $k \in \{1, \ldots, n\}$ express $\mathbb{E}[T_{\mathcal{C}_n} \mid E_{k,k-1}]$ in terms of $\mathbb{E}[T_{\mathcal{C}_n} \mid E_{1,n-1}]$.

Proposition 4.22. *Let $k = 2, \ldots, n-1$, then we have the following.*

- $\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n}\right] = 1 + \frac{n-2}{1-p} + \frac{p^2-np+n}{p(2-p)} + \mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-1}\right]$
- $\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{k,k-1}\right] = \frac{n-k}{1-p} + \frac{p^2-np+n}{p(2-p)} + \mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-1}\right]$
- $\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{n,n-1}\right] = \frac{p^2-np+n}{p(2-p)} + \mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-1}\right]$

Proof. We can calculate $\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{k,k-1}\right]$ by

$$\begin{aligned}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{k,k-1}\right] =& \mathbb{P}\left(W_1 = a \mid E_{k,k-1}\right)\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{k,k-1} \;\&\; W_1 = a\right] \\ &+ \mathbb{P}\left(W_1 = b \mid E_{k,k-1}\right)\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{k,k-1} \;\&\; W_1 = b\right]\end{aligned}$$

With Lemma 4.20 and 4.21 we get the following calculations.
For $k = 2, \ldots, n-1$ we get:

$$\begin{aligned}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{k,k-1}\right] &= p \cdot \mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{k,k-1} \;\&\; W_1 = a\right] + \\ &\quad (1-p) \cdot \mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{k,k-1} \;\&\; W_1 = b\right] \\ &= p \cdot \left(\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{k,k-1}\right] + 1\right) + (1-p) \cdot \left(\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{k+1,k}\right] + 1\right) \\ &= p + 1 - p + p \cdot \mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{k,k-1}\right] + (1-p) \cdot \mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{k+1,k}\right] \\ &= 1 + p \cdot \mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{k,k-1}\right] + (1-p) \cdot \mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{k+1,k}\right]\end{aligned}$$

This gives:

$$\begin{aligned}(1-p)\,\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{k,k-1}\right] &= 1 + (1-p)\,\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{k+1,k}\right] \\ \mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{k,k-1}\right] &= \frac{1}{1-p} + \mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{k+1,k}\right]\end{aligned}$$

By repetition of these calculations, this translates to:

$$\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{k,k-1}\right] = \frac{n-k}{1-p} + \mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{n,n-1}\right] \tag{4.6}$$

With Equation 4.6 (with $k = 2$) and the fact that $\mathbb{P}\left(W_1 = b \mid E_{1,n}\right) = 1$ and $\mathbb{P}\left(W_1 = a \mid E_{1,n}\right) = 0$ we get:

$$\begin{aligned}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n}\right] &= 0 + 1 \cdot \mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n} \;\&\; W_1 = b\right] \\ &= 1 + \mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{2,1}\right] \\ &= 1 + \frac{n-2}{1-p} + \mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{n,n-1}\right]\end{aligned} \tag{4.7}$$

With the use of Equation 4.7 and Lemma 4.20 and 4.21, we get for $k = n$ the following.

$$\begin{aligned}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{n,n-1}\right] &= p\,(2-p)\,\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{n,n-1} \;\&\; W_1 = a\right] + \\ &\quad (1-p)^2\,\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{n,n-1} \;\&\; W_1 = b\right] \\ &= p\,(2-p)\left(\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-1}\right] + 1\right) + (1-p)^2\left(\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n}\right] + 1\right) \\ &= p\,(2-p) + (1-p)^2 + p\,(2-p)\,\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-1}\right] + (1-p)^2\,\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n}\right] \\ &= 1 + p\,(2-p)\,\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-1}\right] + (1-p)^2\left(1 + \frac{n-2}{1-p} + \mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{n,n-1}\right]\right) \\ &= 1 + p\,(2-p)\,\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-1}\right] + (1-p)^2 + (n-2)\,(1-p) \\ &\quad + (1-p)^2\,\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{n,n-1}\right]\end{aligned}$$

This gives:

$$\begin{aligned}\left(1-(1-p)^2\right)\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{n,n-1}\right] &= 1+(1-p)^2+(n-2)(1-p)+p(2-p)\,\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-1}\right]\\ p(2-p)\,\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{n,n-1}\right] &= p^2-np+n+p(2-p)\,\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-1}\right]\\ \mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{n,n-1}\right] &= \frac{p^2-np+n}{p(2-p)}+\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-1}\right]\end{aligned}$$

Substitute this in earlier computations about $\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n}\right]$ and $\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{k,k-1}\right]$, then we get:

$$\begin{aligned}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n}\right] &= 1+\frac{n-2}{1-p}+\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{n,n-1}\right]\\ &= 1+\frac{n-2}{1-p}+\frac{p^2-np+n}{p(2-p)}+\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-1}\right]\end{aligned}$$

And for $k=2,\ldots,n-1$ we get:

$$\begin{aligned}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{k,k-1}\right] =& \frac{n-k}{1-p}+\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{n,n-1}\right]\\ =& \frac{n-k}{1-p}+\frac{p^2-np+n}{p(2-p)}+\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-1}\right]\end{aligned}$$

With this we have proven all items in our proposition. □

Proposition 4.22, Lemma 4.19 and the fact that $\sum_{k=1}^{n} k = \frac{1}{2}n(n+1)$ together gives us our first (semi) result about $\mathbb{E}\left[T_{\mathcal{C}_n}\right]$.

Proposition 4.23.

$$\mathbb{E}\left[T_{\mathcal{C}_n}\right] = \frac{n-p-1}{n-p}+\frac{p^2-np+n}{p(2-p)}+\frac{(n-2)(n-1)}{2(n-p)(1-p)}+\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-1}\right]$$

Proof. This proof consists of a calculation which combines Proposition 4.22, Lemma 4.19 and Equations 4.3.

$$\begin{aligned}\mathbb{E}\left[T_{\mathcal{C}_n}\right] &= \sum_{k=1}^{n}\mathbb{P}\left(E_{k,k-1}\right)\cdot\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{k,k-1}\right]\\ &= \frac{1-p}{n-p}\cdot\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n}\right]+\sum_{k=2}^{n}\left(\frac{1}{n-p}\cdot\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{k,k-1}\right]\right)\\ &= \frac{1-p}{n-p}\cdot\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n}\right]+\frac{1}{n-p}\sum_{k=2}^{n}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{k,k-1}\right]\\ &= \frac{1-p}{n-p}\left(1+\frac{n-2}{1-p}+\frac{p^2-np+n}{p(2-p)}+\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-1}\right]\right)\\ &\quad+\frac{1}{n-p}\sum_{k=2}^{n}\left(\frac{n-k}{1-p}+\frac{p^2-np+n}{p(2-p)}+\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-1}\right]\right)\end{aligned}$$

$$
\begin{aligned}
&= \frac{1-p}{n-p} + \frac{n-2}{n-p} + \frac{(p^2-np+n)(1-p)}{p(2-p)(n-p)} + \frac{1-p}{n-p}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-1}\right] \\
&\quad + \frac{n-1}{n-p}\left(\frac{p^2-np+n}{p(2-p)} + \mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-1}\right]\right) + \frac{1}{(n-p)(1-p)}\sum_{k=2}^{n}(n-k) \\
&= \frac{n-p-1}{n-p} + \frac{p^2-np+n}{p(2-p)} + \frac{1}{(n-p)(1-p)}\left(n(n-1) - \sum_{k=2}^{n} k\right) \\
&\quad + \left(\frac{1-p}{n-p} + \frac{n-1}{n-p}\right)\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-1}\right] \\
&= \frac{n-p-1}{n-p} + \frac{p^2-np+n}{p(2-p)} + \frac{1}{(n-p)(1-p)}\left(n(n-1) - \left(\frac{1}{2}n(n+1) - 1\right)\right) \\
&\quad + \mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-1}\right] \\
&= \frac{n-p-1}{n-p} + \frac{p^2-np+n}{p(2-p)} + \frac{(n-2)(n-1)}{2(n-p)(1-p)} + \mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-1}\right]
\end{aligned}
$$

□

As we can see in Proposition 4.23 we still can't know what $\mathbb{E}\left[T_{\mathcal{C}_n}\right]$ is without the value of $\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-1}\right]$. Calculating this takes a bit more work, first we need some lemmas and propositions.

Lemma 4.24. *Let $1 \leq m \leq n-1$. Then $\mathbb{P}\left(E_{n,n-m}\right) = \frac{m}{m+1}\mathbb{P}\left(E_{n,n-m-1}\right)$*

Proof. The proof of this lemma is given in Appendix A.1 □

Lemma 4.25. *Let $1 \leq r \leq n-1$, then we have that the following holds:*

$$
\mathbb{P}\left(E_{k,k-r}\right) = \begin{cases} \frac{r-p}{n-p} & k = 1, \ldots, r \\ \frac{r}{n-p} & k = r+1, \ldots, n \end{cases}
$$

(For all $k = 1, \ldots, r$ we use $k - r \equiv n + k - r$.)

Proof. This proof uses Lemma 4.19 and Lemma 4.24 and can be found in Appendix A.2. □

With Lemma 4.25 we can prove the following two lemmas about $\mathbb{P}\left(W_1 = l \mid E_{r,s}\right)$ where $r, s = 1, \ldots, n$, $r \neq s$ and $l = a, b$.

Lemma 4.26. *Let $s = r + 1 \pmod n$ then we have the following results about $\mathbb{P}\left(W_1 = l \mid E_{r,s}\right)$ where $r = 1, \ldots, n$ and $l = a, b$.*

$$
\mathbb{P}\left(W_1 = l \mid E_{k-1,k}\right) = \begin{cases} p & \text{if } l = a \text{ and } k = 2, \ldots, n-1 \\ 1-p & \text{if } l = b \text{ and } k = 2, \ldots, n-1 \end{cases}
$$

$$\mathbb{P}(W_1 = a \mid E_{n-1,n}) = \frac{p(n-2)}{n-1-p}$$
$$\mathbb{P}(W_1 = b \mid E_{n-1,n}) = \frac{(1-p)(n-1)}{n-1-p}$$
$$\mathbb{P}(W_1 = a \mid E_{n,1}) = \frac{p(n-p)}{n-1}$$
$$\mathbb{P}(W_1 = b \mid E_{n,1}) = \frac{(1-p)(n-1-p)}{n-1}$$

Proof. To prove this lemma we are going to calculate all values using Lemma 4.25 (and 4.19), Bayes Theorem and the fact that
$\mathbb{P}(W_1 = a \mid E_{1,2}) + \mathbb{P}(W_1 = b \mid E_{1,2}) = 1$.

$$\begin{aligned}\mathbb{P}(W_1 = a \mid E_{1,2}) &= \frac{\mathbb{P}(W_1 = a) \cdot \mathbb{P}(E_{1,2} \mid W_1 = a)}{\mathbb{P}(E_{1,2})} \\ &= \frac{p \cdot \mathbb{P}(E_{1,2})}{\mathbb{P}(E_{1,2})} = p\end{aligned}$$

$$\mathbb{P}(W_1 = b \mid E_{1,2}) = 1 - \mathbb{P}(W_1 = a \mid E_{1,2}) = 1 - p$$

The same we can do for $\mathbb{P}(W_1 = a \mid E_{k-1,k})$ and $\mathbb{P}(W_1 = b \mid E_{k-1,k})$, where $k = 2, \ldots, n-1$. This gives us:

$$\mathbb{P}(W_1 = a \mid E_{1,2}) = \cdots = \mathbb{P}(W_1 = a \mid E_{n-2,n-1}) = p$$
$$\mathbb{P}(W_1 = b \mid E_{1,2}) = \cdots = \mathbb{P}(W_1 = b \mid E_{n-2,n-1}) = 1 - p$$

$$\begin{aligned}\mathbb{P}(W_1 = a \mid E_{n-1,n}) &= \frac{\mathbb{P}(W_1 = a) \cdot \mathbb{P}(E_{n-1,n} \mid W_1 = a)}{\mathbb{P}(E_{n-1,n})} \\ &= \frac{p \cdot \mathbb{P}(E_{n-1,1})}{\mathbb{P}(E_{n-1,n})} \\ &= \frac{p \cdot \frac{n-2}{n-p}}{\frac{n-1-p}{n-p}} = \frac{p(n-2)}{n-1-p}\end{aligned}$$
$$\mathbb{P}(W_1 = b \mid E_{n-1,n}) = 1 - \mathbb{P}(W_1 = a \mid E_{n-1,n}) = \frac{(1-p)(n-1)}{n-1-p}$$

$$\begin{aligned}\mathbb{P}(W_1 = a \mid E_{n,1}) &= \frac{\mathbb{P}(W_1 = a) \cdot \mathbb{P}(E_{n,1} \mid W_1 = a)}{\mathbb{P}(E_{n,1})} \\ &= \frac{p \cdot 1}{\mathbb{P}(E_{n,1})} \\ &= \frac{p}{\frac{n-1}{n-p}} = \frac{p(n-p)}{n-1}\end{aligned}$$
$$\mathbb{P}(W_1 = b \mid E_{n,1}) = 1 - \mathbb{P}(W_1 = a \mid E_{n,1}) = \frac{p(n-1-p)}{n-1}$$

□

Lemma 4.27. *Let $1 \leq t \leq n-3$ and $s = r+n-t-1 \pmod n$ then we have the following results about $\mathbb{P}(W_1 = l \mid E_{r,s})$ where $r = 1, \ldots, n$ and $l = a, b$.*

$$\mathbb{P}(W_1 = l \mid E_{k,k+n-1-t}) = \begin{cases} p & \text{if } l = a \text{ and } k = 1, \ldots, t \\ 1-p & \text{if } l = b \text{ and } k = 1, \ldots, t \end{cases}$$

$$\mathbb{P}(W_1 = a \mid E_{t+1,n}) = \frac{pt}{t+1-p}$$
$$\mathbb{P}(W_1 = b \mid E_{t+1,n}) = \frac{(1-p)(t+1)}{t+1-p}$$

$$\mathbb{P}(W_1 = l \mid E_{k,k-1-t}) = \begin{cases} p & \text{if } l = a \text{ and } k = t+2, \ldots, n-1 \\ 1-p & \text{if } l = b \text{ and } k = t+2, \ldots, n-1 \end{cases}$$

$$\mathbb{P}(W_1 = a \mid E_{n,n-t-1}) = \frac{p(t+2-p)}{t+1}$$
$$\mathbb{P}(W_1 = b \mid E_{n,n-t-1}) = \frac{(1-p)(t+1-p)}{t+1}$$

Proof. This proof is analogue to the proof of Lemma 4.26 and can be found in Appendix A.3. □

With all these conditional probabilities we can start computing $\mathbb{E}[T_{\mathcal{C}_n} \mid E_{1,n-1}]$. This we do by first computing $\mathbb{E}[T_{\mathcal{C}_n} \mid E_{1,n-m}]$, where $1 \leq m \leq n-3$.

Proposition 4.28. *Let $1 \leq m \leq n-3$, then the following holds.*

$$\begin{aligned}\mathbb{E}[T_{\mathcal{C}_n} \mid E_{1,n-m}] = &\frac{n-2p}{2p(1-p)^2} + \frac{m}{2(1-p)^2(m+1-p)} \\ &+ \frac{m-p}{2(m+1-p)}\mathbb{E}[T_{\mathcal{C}_n} \mid E_{1,n-m+1}] + \frac{m+2-p}{2(m+1-p)}\mathbb{E}[T_{\mathcal{C}_n} \mid E_{1,n-m-1}]\end{aligned}$$

Proof. To prove this we again use:

$$\begin{aligned}\mathbb{E}[T_{\mathcal{C}_n} \mid E_{k,k-1}] = &\mathbb{P}(W_1 = a \mid E_{k,k-1})\,\mathbb{E}[T_{\mathcal{C}_n} \mid E_{k,k-1} \,\&\, W_1 = a] \\ &+ \mathbb{P}(W_1 = b \mid E_{k,k-1})\,\mathbb{E}[T_{\mathcal{C}_n} \mid E_{k,k-1} \,\&\, W_1 = b]\end{aligned}$$

With our knowledge about $\mathbb{P}(V_1 = V_0 \circ l \mid E_{k,k-1})$, where $l = a, b$ and $k = 1, \ldots, n$, obtained in lemmas 4.26 and 4.27.

First we can see that $\mathbb{E}[T_{\mathcal{C}_n} \mid E_{1,n-m}]$ only depends on m, p and $\mathbb{E}[T_{\mathcal{C}_n} \mid E_{m+1,n}]$.

$$\begin{aligned}\mathbb{E}[T_{\mathcal{C}_n} \mid E_{1,n-m}] &= \mathbb{P}(W_1 = a \mid E_{1,n-m})\,(\mathbb{E}[T_{\mathcal{C}_n} \mid E_{1,n-m}] + 1) \\ &\quad + \mathbb{P}(W_1 = b \mid E_{1,n-m})\,(\mathbb{E}[T_{\mathcal{C}_n} \mid E_{2,n-m+1}] + 1) \\ &= 1 + p \cdot \mathbb{E}[T_{\mathcal{C}_n} \mid E_{1,n-m}] + (1-p) \cdot \mathbb{E}[T_{\mathcal{C}_n} \mid E_{2,n-m+1}] \\ (1-p)\,\mathbb{E}[T_{\mathcal{C}_n} \mid E_{1,n-m}] &= 1 + (1-p)\,\mathbb{E}[T_{\mathcal{C}_n} \mid E_{2,n-m+1}] \\ \mathbb{E}[T_{\mathcal{C}_n} \mid E_{1,n-m}] &= \frac{1}{1-p} + \mathbb{E}[T_{\mathcal{C}_n} \mid E_{2,n-m+1}] \\ &\vdots \\ \mathbb{E}[T_{\mathcal{C}_n} \mid E_{1,n-m}] &= \frac{m}{1-p} + \mathbb{E}[T_{\mathcal{C}_n} \mid E_{m+1,n}]\end{aligned}$$

So we like to know what $\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{m+1,n}\right]$ is.

$$\begin{aligned}
\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{m+1,n}\right] &= \mathbb{P}\left(W_1 = a \mid E_{m+1,n}\right)\left(\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{m+1,1}\right] + 1\right) \\
&\quad + \mathbb{P}\left(W_1 = b \mid E_{m+1,n}\right)\left(\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{m+2,1}\right] + 1\right) \\
&= \frac{pm}{m+1-p}\left(\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{m+1,1}\right] + 1\right) + \frac{(1-p)(m+1)}{m+1-p}\left(\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{m+2,1}\right] + 1\right) \\
&= 1 + \frac{pm}{m+1-p}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{m+1,1}\right] + \frac{(1-p)(m+1)}{m+1-p}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{m+2,1}\right]
\end{aligned}$$

This means we have to take a look at $\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{m+1,1}\right]$ and $\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{m+2,1}\right]$.
For $\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{m+1,1}\right]$ we find the following.

$$\begin{aligned}
\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{m+1,1}\right] &= \mathbb{P}\left(W_1 = a \mid E_{m+1,1}\right)\left(\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{m+1,1}\right] + 1\right) \\
&\quad + \mathbb{P}\left(W_1 = b \mid E_{m+1,1}\right)\left(\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{m+2,2}\right] + 1\right) \\
&= 1 + p \cdot \mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{m+1,1}\right] + (1-p) \cdot \mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{m+2,2}\right] \\
(1-p)\,\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{m+1,1}\right] &= 1 + (1-p)\,\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{m+2,2}\right] \\
\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{m+1,1}\right] &= \frac{1}{1-p} + \mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{m+2,2}\right] \\
&\vdots \\
\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{m+1,1}\right] &= \frac{n-m-1}{1-p} + \mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{n,n-m}\right]
\end{aligned}$$

$$\begin{aligned}
\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{n,n-m}\right] &= \mathbb{P}\left(W_1 = a \mid n \cdots n-m\right)\left(\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-m}\right] + 1\right) \\
&\quad + \mathbb{P}\left(W_1 = b \mid n \cdots n-m\right)\left(\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-m+1}\right] + 1\right) \\
&= 1 + \frac{p(m+1-p)}{m}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-m}\right] + \frac{(1-p)(m-p)}{m}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-m+1}\right]
\end{aligned}$$

$$\begin{aligned}
\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{m+1,1}\right] = \frac{n-m-1}{1-p} + 1 + \frac{p(m+1-p)}{m}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-m}\right] \\
+ \frac{(1-p)(m-p)}{m}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-m+1}\right]
\end{aligned} \tag{4.8}$$

For $\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{m+2,1}\right]$ we find the following.

$$\begin{aligned}
\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{m+2,1}\right] &= \mathbb{P}\left(W_1 = a \mid E_{m+2,1}\right)\left(\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{m+2,1}\right] + 1\right) \\
&\quad + \mathbb{P}\left(W_1 = b \mid E_{m+2,1}\right)\left(\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{m+3,2}\right] + 1\right) \\
&= 1 + p \cdot \mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{m+2,1}\right] + (1-p) \cdot \mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{m+3,2}\right] \\
(1-p)\,\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{m+2,1}\right] &= 1 + (1-p)\,\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{m+3,2}\right] \\
\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{m+2,1}\right] &= \frac{1}{1-p} + \mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{m+3,2}\right] \\
&\vdots \\
\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{m+2,1}\right] &= \frac{n-m-2}{1-p} + \mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{n,n-m-1}\right]
\end{aligned}$$

$$\begin{aligned}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{n,n-m-1}\right] &= \mathbb{P}\left(W_1 = a \mid E_{n,n-m-1}\right)\left(\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-m-1}\right] + 1\right) \\ &\quad + \mathbb{P}\left(W_1 = b \mid E_{n,n-m-1}\right)\left(\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-m}\right] + 1\right) \\ &= 1 + \frac{p\left(m+2-p\right)}{m+1}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-m-1}\right] \\ &\quad + \frac{\left(1-p\right)\left(m+1-p\right)}{m+1}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-m}\right]\end{aligned}$$

$$\begin{aligned}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{m+2,1}\right] &= \frac{n-m-2}{1-p} + 1 + \frac{p\left(m+2-p\right)}{m+1}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-m-1}\right] \\ &\quad + \frac{\left(1-p\right)\left(m+1-p\right)}{m+1}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-m}\right]\end{aligned} \tag{4.9}$$

Equations 4.8 and 4.9 together with our first computations about $\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-m}\right]$ gives us the following recursive formula for $\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-m}\right]$.

$$\begin{aligned}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-m}\right] &= \frac{m}{1-p} + \mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{m+1,n}\right] \\ &= \frac{m}{1-p} + 1 + \frac{pm}{m+1-p}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{m+1,1}\right] + \frac{\left(1-p\right)\left(m+1\right)}{m+1-p}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{m+2,1}\right] \\ &= \frac{m}{1-p} + 1 + \frac{pm}{m+1-p}\left(\frac{n-m-1}{1-p} + 1 + \frac{p\left(m+1-p\right)}{m}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-m}\right]\right. \\ &\qquad \left. + \frac{\left(1-p\right)\left(m-p\right)}{m}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-m+1}\right]\right) \\ &\quad + \frac{\left(1-p\right)\left(m+1\right)}{m+1-p}\left(\frac{n-m-2}{1-p} + 1 + \frac{p\left(m+2-p\right)}{m+1}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-m-1}\right]\right. \\ &\qquad \left. + \frac{\left(1-p\right)\left(m+1-p\right)}{m+1}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-m}\right]\right) \\ &= 1 + \frac{m}{1-p} + \frac{pm\left(n-m-1\right)}{\left(m+1-p\right)\left(1-p\right)} + \frac{pm}{m+1-p} + p^2\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-m}\right] \\ &\quad + \frac{p\left(1-p\right)\left(m-p\right)}{m+1-p}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-m+1}\right] + \frac{\left(m+1\right)\left(n-m-2\right)}{m+1-p} \\ &\quad + \frac{\left(1-p\right)\left(m+1\right)}{m+1-p} + \frac{p\left(1-p\right)\left(m+2-p\right)}{m+1-p}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-m-1}\right] \\ &\quad + \left(1-p\right)^2\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-m}\right]\end{aligned}$$

$$\begin{aligned}\left(1-p^2-\left(1-p\right)^2\right)\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-m}\right] &= 1 + \frac{m}{1-p} + \frac{pm\left(n-m-1\right)}{\left(m+1-p\right)\left(1-p\right)} + \frac{pm}{m+1-p} \\ &\quad + \frac{p\left(1-p\right)\left(m-p\right)}{m+1-p}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-m+1}\right] \\ &\quad + \frac{\left(m+1\right)\left(n-m-2\right)}{m+1-p} + \frac{\left(1-p\right)\left(m+1\right)}{m+1-p} \\ &\quad + \frac{p\left(1-p\right)\left(m+2-p\right)}{m+1-p}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-m-1}\right]\end{aligned}$$

$$
\begin{aligned}
2p\,(1-p)\,\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-m}\right] = 1 &+ \frac{m}{1-p} + \frac{pm\,(n-m-1)}{(m+1-p)\,(1-p)} \\
&+ \frac{pm}{m+1-p} + \frac{p\,(1-p)\,(m-p)}{m+1-p}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-m+1}\right] \\
&+ \frac{(m+1)\,(n-m-2)}{m+1-p} + \frac{(1-p)\,(m+1)}{m+1-p} \\
&+ \frac{p\,(1-p)\,(m+2-p)}{m+1-p}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-m-1}\right]
\end{aligned}
$$

$$
\begin{aligned}
\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-m}\right] &= \frac{1}{2p\,(1-p)} + \frac{m}{2p\,(1-p)^2} + \frac{m\,(n-m-1)}{2\,(m+1-p)\,(1-p)^2} + \frac{m}{2\,(m+1-p)\,(1-p)} \\
&\quad + \frac{m-p}{2\,(m+1-p)}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-m+1}\right] + \frac{(m+1)\,(n-m-2)}{2p\,(1-p)\,(m+1-p)} \\
&\quad + \frac{m+1}{2p\,(m+1-p)} + \frac{m+2-p}{2\,(m+1-p)}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-m-1}\right] \\
&= \frac{1-p+m}{2p\,(1-p)^2} + \frac{(m+1-p)\,(n-m-1-p)+mp}{2p\,(1-p)^2\,(m+1-p)} \\
&\quad + \frac{m-p}{2\,(m+1-p)}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-m+1}\right] + \frac{m+2-p}{2\,(m+1-p)}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-m-1}\right] \\
&= \frac{1-p+m+n-1-m-p}{2p\,(1-p)^2} + \frac{mp}{2p\,(1-p)^2\,(m+1-p)} \\
&\quad + \frac{m-p}{2\,(m+1-p)}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-m+1}\right] + \frac{m+2-p}{2\,(m+1-p)}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-m-1}\right] \\
&= \frac{n-2p}{2p\,(1-p)^2} + \frac{m}{2\,(1-p)^2\,(m+1-p)} + \frac{m-p}{2\,(m+1-p)}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-m+1}\right] \\
&\quad + \frac{m+2-p}{2\,(m+1-p)}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-m-1}\right]
\end{aligned}
$$

With this we have proved the proposition. □

With the use of Proposition 4.28 we can prove that $\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-m}\right]$ can be expressed in terms of m and $\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-m-1}\right]$.

Proposition 4.29. *For $1 \leq m \leq n-3$, the following holds:*

$$
\begin{aligned}
\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-m}\right] = &\frac{(n-2p)\,(m+1-p)}{p\,(1-p)^2\,(m+2-p)} + \frac{m}{(1-p)^2\,(m+2-p)} + \frac{(1-p)\,(2-p)}{(m+1-p)\,(m+2-p)} \\
&+ \frac{(n-2)\,(2-p)}{(m+1-p)\,(m+2-p)} + \frac{(1-p)\,(p^2-np+n)}{p\,(m+1-p)\,(m+2-p)} \\
&+ \sum_{i=2}^{m} \frac{(i-1)\,(i-p)}{(1-p)^2\,(m+1-p)\,(m+2-p)} \\
&+ \sum_{i=2}^{m} \frac{(n-2p)\,(i-p)^2}{p\,(1-p)^2\,(m+1-p)\,(m+2-p)} + \mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-m-1}\right]
\end{aligned}
$$

Proof. The proof goes by induction on m and uses Proposition 4.28. The full proof is stated in Appendix A.4. □

We can further rewrite our result from Proposition 4.29.

Corollary 4.30. *For $1 \leq m \leq n-3$, the following holds.*

$$\begin{aligned}
&\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-m}\right] \\
&\quad = \frac{-2\left(m+1\right)p^3 + \frac{1}{2}\left(m+1\right)\left(3m+2n+8\right)p^2 - \frac{1}{3}\left(m+1\right)\left(m+2\right)\left(m+3n+3\right)p}{p\left(1-p\right)^2\left(m+1-p\right)\left(m+2-p\right)} \\
&\qquad + \frac{\frac{1}{6}\left(2m+3\right)\left(m+1\right)\left(m+2\right)n}{p\left(1-p\right)^2\left(m+1-p\right)\left(m+2-p\right)} + \mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-m-1}\right]
\end{aligned}$$

Proof. To prove this we take Proposition 4.29 and calculate the finite sums. For the complete calculations see Appendix A.5. □

With this corollary we can calculate $\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,2}\right]$ explicitly.

Proposition 4.31. $\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,2}\right]$ *can be calculated as follows.*

$$\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,2}\right] = \frac{\left(n-1\right)\left(2n^3 - 8n^2p - n^2 + 15np^2 - 2np - 12p^3 + 6p^2\right)}{6p\left(1-p\right)^2\left(n-1-p\right)\left(n-p\right)}$$

Proof. For $m = n-3$ Corollary 4.30 gives us the following.

$$\begin{aligned}
&\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,3}\right] = \\
&\quad = \frac{-2\left(n-2\right)p^3 + \frac{1}{2}\left(n-2\right)\left(5n-1\right)p^2 - \frac{4}{3}\left(n-2\right)\left(n-1\right)np + \frac{1}{6}\left(2n-3\right)\left(n-2\right)\left(n-1\right)n}{p\left(1-p\right)^2\left(n-2-p\right)\left(n-1-p\right)} \\
&\qquad + \mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,2}\right]
\end{aligned} \tag{4.10}$$

We can also express $\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,2}\right]$ in terms of $\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,3}\right]$ by the following calculations (using Proposition 4.26).

$$\begin{aligned}
\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,2}\right] =& \mathbb{P}\left(W_1 = a \mid E_{1,2}\right)\left(\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,2}\right] + 1\right) \\
&+ \mathbb{P}\left(W_1 = b \mid E_{1,2}\right)\left(\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{2,3}\right] + 1\right) \\
=& 1 + p \cdot \mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,2}\right] + \left(1-p\right) \cdot \mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{2,3}\right] \\
\left(1-p\right)\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,2}\right] =& 1 + \left(1-p\right)\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{2,3}\right] \\
\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,2}\right] =& \frac{1}{1-p} + \mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{2,3}\right] \\
&\vdots \\
=& \frac{n-2}{1-p} + \mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{n-1,n}\right]
\end{aligned}$$

$$\begin{aligned}
\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{n-1,n}\right] =& \mathbb{P}\left(W_1 = a \mid E_{n-1,n}\right)\left(\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{n-1,1}\right] + 1\right) \\
&+ \mathbb{P}\left(W_1 = b \mid E_{n-1,n}\right)\left(\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{n,1}\right] + 1\right) \\
=& 1 + \frac{p\left(n-2\right)}{n-1-p}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{n-1,1}\right] + \frac{\left(1-p\right)\left(n-1\right)}{n-1-p}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{n,1}\right]
\end{aligned}$$

We can express $\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{n-1,1}\right]$ as follows.

$$\begin{aligned}
\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{n-1,1}\right] =& \mathbb{P}\left(W_1 = a \mid E_{n-1,1}\right)\left(\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{n-1,1}\right] + 1\right) \\
&+ \mathbb{P}\left(W_1 = b \mid E_{n-1,1}\right)\left(\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{n,2}\right] + 1\right) \\
=& 1 + p \cdot \mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{n-1,1}\right] + (1-p) \cdot \mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{n,2}\right] \\
(1-p)\,\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{n-1,1}\right] =& 1 + (1-p)\,\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{n,2}\right] \\
\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{n-1,1}\right] =& \frac{1}{1-p} + \mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{n,2}\right] \\
=& \frac{1}{1-p} + \mathbb{P}\left(W_1 = a \mid E_{n,2}\right)\left(\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,2}\right] + 1\right) \\
&+ \mathbb{P}\left(W_1 = b \mid E_{n,2}\right)\left(\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,3}\right] + 1\right) \\
=& \frac{1}{1-p} + 1 + \frac{p\,(n-1-p)}{n-2}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,2}\right] + \frac{(1-p)\,(n-2-p)}{n-2}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,3}\right]
\end{aligned}$$

We can express $\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{n,1}\right]$ as follows.

$$\begin{aligned}
\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{n,1}\right] =& \mathbb{P}\left(W_1 = a \mid E_{n,1}\right) \cdot 1 + \mathbb{P}\left(W_1 = b \mid E_{n,1}\right)\left(\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,2}\right] + 1\right) \\
=& \frac{p\,(n-p)}{n-1} + \frac{(1-p)\,(n-1-p)}{n-1}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,2}\right] + \frac{(1-p)\,(n-1-p)}{n-1} \\
=& 1 + \frac{(1-p)\,(n-1-p)}{n-1}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,2}\right]
\end{aligned}$$

All this together gives the following expression of $\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,2}\right]$.

$$\begin{aligned}
\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,2}\right] =& \frac{n-2}{1-p} + 1 + \frac{p\,(n-2)}{n-1-p}\left(\frac{1}{1-p} + 1 + \frac{p\,(n-1-p)}{n-2}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,2}\right]\right. \\
&\left. + \frac{(1-p)\,(n-2-p)}{n-2}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,3}\right]\right) \\
&+ \frac{(1-p)\,(n-1)}{n-1-p}\left(1 + \frac{(1-p)\,(n-1-p)}{n-1}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,2}\right]\right) \\
=& \frac{n-2}{1-p} + 1 + \frac{p\,(n-2)}{(n-1-p)\,(1-p)} + \frac{p\,(n-2)}{n-1-p} + p^2\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,2}\right] \\
&+ \frac{p\,(1-p)\,(n-2-p)}{n-1-p}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,3}\right] + \frac{(1-p)\,(n-1)}{n-1-p} \\
&+ (1-p)^2\,\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,2}\right]
\end{aligned}$$

$$\begin{aligned}
\left(1 - p^2 - (1-p)^2\right)\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,2}\right] =& 1 + \frac{n-2}{1-p} + \frac{p\,(n-2)}{(n-1-p)\,(1-p)}\frac{p\,(n-2) + (1-p)\,(n-1)}{n-1-p} \\
&+ \frac{p\,(1-p)\,(n-2-p)}{n-1-p}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,3}\right] \\
2p\,(1-p)\,\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,2}\right] =& 1 + \frac{n-2}{1-p} + \frac{p\,(n-2)}{(n-1-p)\,(1-p)}\frac{n-1-p}{n-1-p} \\
&+ \frac{p\,(1-p)\,(n-2-p)}{n-1-p}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,3}\right]
\end{aligned}$$

$$\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,2}\right] = \frac{2}{2p\left(1-p\right)} + \frac{n-2}{2p\left(1-p\right)^2} + \frac{n-2}{2\left(n-1-p\right)\left(1-p\right)^2} + \frac{n-2-p}{2\left(n-1-p\right)}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,3}\right]$$

Now substitute Equation 4.10 into the expression of $\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,2}\right]$ stated above. With this we can calculate $\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,2}\right]$.
To improve readability, let's define B as follows.

$$B := \frac{-2\left(n-2\right)p^3 + \frac{1}{2}\left(n-2\right)\left(5n-1\right)p^2 - \frac{4}{3}\left(n-2\right)\left(n-1\right)np + \frac{1}{6}\left(2n-3\right)\left(n-2\right)\left(n-1\right)n}{p\left(1-p\right)^2\left(n-2-p\right)\left(n-1-p\right)}$$

With the calculation below we get exactly what we wanted to prove.

$$\begin{aligned}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,2}\right] =& \frac{n-2}{2p\left(1-p\right)^2} + \frac{2}{2p\left(1-p\right)} + \frac{n-2}{2\left(1-p\right)^2\left(n-1-p\right)} \\ &+ \frac{n-2-p}{2\left(n-1-p\right)}\left(B + \mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,2}\right]\right) \\ =& \frac{n^2-2np-n+2p^2}{2p\left(1-p\right)^2\left(n-1-p\right)} + \frac{n-2-p}{2\left(n-1-p\right)}B + \frac{n-2-p}{2\left(n-1-p\right)}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,2}\right]\end{aligned}$$

$$\begin{aligned}\frac{n-p}{2\left(n-1-p\right)}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,2}\right] &= \frac{n^2-2np-n+2p^2}{2p\left(1-p\right)^2\left(n-1-p\right)} + \frac{n-2-p}{2\left(n-1-p\right)}B \\ \mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,2}\right] &= \frac{n^2-2np-n+2p^2}{p\left(1-p\right)^2\left(n-p\right)} + \frac{n-2-p}{n-p}B \\ &= \frac{\left(n-1\right)\left(2n^3-8n^2p-n^2+15np^2-2np-12p^3+6p^2\right)}{6p\left(1-p\right)^2\left(n-1-p\right)\left(n-p\right)}\end{aligned}$$

□

With all our propositions, lemmas and corollaries we now can prove Theorem 4.15.

Continuation of proof of Theorem 4.15. Substitute the result from Proposition 4.31 in the result of Corollary 4.30, to calculate $\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-1}\right]$. We use the computer to calculate the finite sum.

$$\begin{aligned}&\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-1}\right] = \\ &= \sum_{m=1}^{n-3}\left(\frac{-2\left(m+1\right)p^3 + \frac{1}{2}\left(m+1\right)\left(3m+2n+8\right)p^2 - \frac{1}{3}\left(m+1\right)\left(m+2\right)\left(m+3n+3\right)p}{p\left(1-p\right)^2\left(m+1-p\right)\left(m+2-p\right)}\right. \\ &\qquad \left. + \frac{\frac{1}{6}\left(2m+3\right)\left(m+1\right)\left(m+2\right)n}{p\left(1-p\right)^2\left(m+1-p\right)\left(m+2-p\right)}\right) + \mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,2}\right] \\ &= \frac{\left(n-3\right)\left(n^3\left(2-p\right) - 4n^2\left(2-p\right)p - n\left(6p^3-15p^2+2p+2\right) - 2p\left(5p-4\right)\right)}{6p\left(1-p\right)^2\left(2-p\right)\left(n-1-p\right)} \\ &\quad + \frac{\left(n-1\right)\left(2n^3-8n^2p-n^2+15np^2-2np-12p^3+6p^2\right)}{6p\left(1-p\right)^2\left(n-1-p\right)\left(n-p\right)}\end{aligned}$$

At last, we substitute this expression of $\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-1}\right]$ in our result from Proposition 4.23.

$$\begin{aligned}
\mathbb{E}\left[T_{\mathcal{C}_n}\right] =& \frac{n-p-1}{n-p} + \frac{p^2-np+n}{p\left(2-p\right)} + \frac{\left(n-2\right)\left(n-1\right)}{2\left(n-p\right)\left(1-p\right)} + \mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-1}\right] \\
=& \frac{n-p-1}{n-p} + \frac{p^2-np+n}{p\left(2-p\right)} + \frac{\left(n-2\right)\left(n-1\right)}{2\left(n-p\right)\left(1-p\right)} \\
&+ \frac{\left(n-3\right)\left(n^3\left(2-p\right) - 4n^2\left(2-p\right)p - n\left(6p^3-15p^2+2p+2\right) - 2p\left(5p-4\right)\right)}{6p\left(1-p\right)^2\left(2-p\right)\left(n-1-p\right)} \\
&+ \frac{\left(n-1\right)\left(2n^3-8n^2p-n^2+15np^2-2np-12p^3+6p^2\right)}{6p\left(1-p\right)^2\left(n-1-p\right)\left(n-p\right)} \\
=& \frac{n^3-3n^2p+6np^2-3np-n-6p^2+6p}{6p\left(1-p\right)^2}
\end{aligned}$$

With this Theorem 4.15 is proven. □

Remarks on $\mathbb{E}[T_{\mathcal{C}_n}]$

The dominating part of $\mathbb{E}[T_{\mathcal{C}_n}]$ is $\frac{1}{6p(1-p)^2}n^3$. Therefore, by solving $\frac{\partial\left(\frac{1}{6p(1-p)^2}n^3\right)}{\partial p} = 0$, we can determine, for n large enough, for which $p \in (0,1)$ $\mathbb{E}[T_{\mathcal{C}_n}]$ has a local minimum or local maximum.

$$\begin{aligned}
\frac{\partial\left(\frac{1}{6p(1-p)^2}n^3\right)}{\partial p} &= \frac{0\cdot 6p\left(1-p\right)^2 - n^3\left(6\left(1-p\right)^2 - 12p\left(1-p\right)\right)}{36p^2\left(1-p\right)^4} \\
&= \frac{-6n^3\left(\left(1-p\right)^2 - 2p\left(1-p\right)\right)}{36p^2\left(1-p\right)^4} \\
&= \frac{-n^3\left(\left(1-p\right) - 2p\right)}{6p^2\left(1-p\right)^3} \\
&= \frac{n^3\left(3p-1\right)}{6p^2\left(1-p\right)^3}
\end{aligned}$$

$\frac{n^3(3p-1)}{6p^2(1-p)^3} = 0$ for $p = \frac{1}{3}$. By looking at the second derivative at $p = \frac{1}{3}$ we can check whether $p = \frac{1}{3}$ gives a local minimum or local maximum of $\mathbb{E}[T_{\mathcal{C}_n}]$.

$$\begin{aligned}
\frac{\partial^2\left(\frac{1}{6p(1-p)^2}n^3\right)}{\partial p^2} &= \frac{18n^3p^2\left(1-p\right)^3 - \left(3p-1\right)n^3\left(12p\left(1-p\right)^3 - 18p^2\left(1-p\right)^2\right)}{36p^4\left(1-p\right)^6} \\
\frac{\partial^2\left(\frac{1}{6p(1-p)^2}n^3\right)}{\partial p^2}\left(\frac{1}{3}\right) &= \frac{18n^3\frac{1}{3}^2\left(1-\frac{1}{3}\right)^3}{36\frac{1}{3}^4\left(1-\frac{1}{3}\right)^6} \\
&\approx 15.1875n^3 \geq 0
\end{aligned}$$

Thus, for n large enough, $\mathbb{E}[T_{\mathcal{C}_n}]$ has a local minimum at $p = \frac{1}{3}$.

In 2019, Anouk Jansen proved that for all $n \in \mathbb{N}$ the following holds
$n^3 - \frac{3}{2}n^2 + \frac{1}{2} \leq \mathbb{E}[T_{\mathcal{C}_n}] \leq 4n^3\log(n) + O(n^3)$. [9]
In 2014, Vladimir V. Gusev proved that for n, a positive odd integer, the expected number of letters to synchronize $\{1, \frac{n+1}{2}\}$ in the Černý automaton $\mathcal{C}_n$ is equal to $\frac{(n-1)\left((n-1)^2+(1-p)(3n-5)+4(1-p)^2\right)}{8p(1-p)^2} = O\left(\frac{1}{8p(1-p)^2}n^3\right)$. [6]
With Vladimir V. Gusev result we can only bound $\mathbb{E}[T_{\mathcal{C}_n}]$
($\mathbb{E}[T_{\mathcal{C}_n}] \geq \frac{(n-1)\left((n-1)^2+(1-p)(3n-5)+4(1-p)^2\right)}{8p(1-p)^2}$).
In this thesis we have improved both statements, since Theorem 4.15 gives the exact value of $\mathbb{E}[T_{\mathcal{C}_n}]$.
With Theorem 4.15 we observe that $\mathbb{E}[T_{\mathcal{C}_n}] = O\left(\frac{1}{6p(1-p)^2}n^3\right)$. This indicates that the expected number of letters to synchronize Q isn't much larger than the expected number of letters to synchronize $\{1, \frac{n+1}{2}\}$ (in the Černý automaton).

4.3 Automata with large expected length of a reset word

In the previous section we started looking at the expected length of a reset word, in which we took a closer look at the Černý automaton $\mathcal{C}_n$. But there are a lot more different synchronizing automata with n states. What can we say about their expected length of a reset word?
We know that the shortest reset word for the Černý automaton $\mathcal{C}_n$ has length $(n-1)^2$. To the present days, we haven't found a synchronizing automaton with n states which has a shortest reset word $w \in \Sigma^*$ with $|w| > (n-1)^2$. But does this mean that the Černý automaton $\mathcal{C}_n$ also has the largest expected length of a reset word?

In this section we are going to look at all synchronizing automata $\mathcal{A} = (Q, \Sigma, \delta)$ with n states and look at which of these automata has the largest expected length of a reset word.
Here we choose $\Sigma = \{a, b\}$. In theory we could take every alphabet with $|\Sigma| \geq 2$. Note that if $|\Sigma| = 1$, then the expected length of a reset word of a synchronizing automaton is always equal to one. But if we would choose Σ to be infinitely large, then the largest expected length of a reset word also becomes infinitely large. To let our values be relatively small but still interesting to research we choose $|\Sigma| = 2$.

First let's recall some definitions and remarks from Section 4.2.

Definition 4.8. For $t \geq 1$ we define the stochastic process $(W_t)_{t\in\mathbb{N}}$ with $W_t \in \Sigma$ by the following probabilities.

$$\mathbb{P}(W_t = a) = p \qquad\qquad \mathbb{P}(W_t = b) = 1 - p$$

Remark. By definition of the stochastic process $(W_t)_{t\in\mathbb{N}}$, W_t is independent of the time $t \in \mathbb{N}$ and independent of any other letter W_r ($r \in \mathbb{N}$) for $r \neq t$.

Since $\mathbb{P}(W_t = a)$ and $\mathbb{P}(W_t = b)$ don't depend on time $t \in \mathbb{N}$, we use the notation $\mathbb{P}(W_t = a) = \mathbb{P}(a)$ and $\mathbb{P}(W_t = b) = \mathbb{P}(b)$

Definition 4.9. We define the Markov chain $(V_t)_{t\in\mathbb{N}}$ associated with a particular automaton $\mathcal{A}$, with $V_t \in \mathcal{P}(Q)\backslash\emptyset$ as follows.
Start in some subset $S \subseteq Q$, say $V_0 := S$ and for $t \geq 1$ we have $V_t := V_{t-1} \circ W_t$.

Since $\mathbb{P}(W_t = a)$ and $\mathbb{P}(W_t = b)$ don't depend on time $t \in \mathbb{N}$, we have that $\mathbb{P}(V_t = Y \mid V_{t-1} = Z) = \mathbb{P}(V_{m+t} = Y \mid V_{m+t-1} = Z)$ holds for all $m \in \mathbb{N}$. So the chain $(V_t)_{t\in\mathbb{N}}$ is indeed a Markov chain (see Definitions 4.4 and 4.5).

Remark. When $X = V_t$ then we have the following transition probabilities:
$\mathbb{P}(V_{t+1} = X \circ a) = p$
$\mathbb{P}(V_{t+1} = X \circ b) = 1 - p$

Definition 4.10. Let $S \subseteq Q$, then we define $T_{\mathcal{A}}(S) := \min\{t \mid |V_t| = 1\}$, where $(V_t)_{t\in\mathbb{N}}$ is the Markov chain of automaton $\mathcal{A}$ with $V_0 = S$.
We write $T_{\mathcal{A}} := T_{\mathcal{A}}(Q)$.

Remark. $(|V_t|)_{t\in\mathbb{N}}$ is a decreasing sequence and at time $T_{\mathcal{A}}(S)$ we have come across a reset word for S in the automaton $\mathcal{A}$ ($W_1 \cdots W_{T_{\mathcal{A}}(S)}$), since $|V_{T_{\mathcal{A}}(S)}| = 1$.
So $q_1 \circ W_1 \cdots W_{T_{\mathcal{A}}(S)} = q_2 \circ W_1 \cdots W_{T_{\mathcal{A}}(S)}$ for all $q_1, q_2 \in S$.

Definition 4.32. Let $S \subseteq Q$. Then we define the following values.

$$d(S) = \begin{cases} 0 & \text{if } |S| = 1 \\ \min\left\{k \mid \exists v \in \Sigma^k \text{ with } |S \circ v| = 1\right\} & \text{if } |S| \geq 2 \end{cases}$$

We say that the distance from S to some singleton is $d(S)$.

Recall that we defined A to be the set of singletons from Q (see Definition 4.7). So $d(S)$ is the distance from S to A.

Consider an automaton $\mathcal{A} = (Q, \Sigma, \delta)$, with $Q = \{1, \ldots, n\}$ ($n \geq 2$ an integer) and $\Sigma = \{a, b\}$, with $\mathbb{P}(a) = p$ and $\mathbb{P}(b) = 1 - p$. Then is $\mathbb{E}[T_{\mathcal{A}}]$ the expected length of a reset word for automaton $\mathcal{A}$.

We have seen that $\mathbb{E}[T_{\mathcal{C}_n}] = \frac{(n-1)p^2 - \left(\sum_{i=2}^{n} i\right)p + \binom{n+1}{n-2}}{p(1-p)^2}$ for the Černý automaton $\mathcal{C}_n$ with $\mathbb{P}(a) = p$, $\mathbb{P}(b) = 1 - p$, where $p \in (0, 1)$ (see Theorem 4.15).

$\mathbb{E}[T_{\mathcal{A}}]$ strongly depends on $p \in (0, 1)$. Suppose we have an automaton with a reset word (or multiple) in which the letter a occurs very often, then this automaton gives a really large value of $\mathbb{E}[T_{\mathcal{A}}]$ if p goes to zero (since $\mathbb{P}(a) = p$).
Analogue we have that an automaton gives a really large value of $\mathbb{E}[T_{\mathcal{A}}]$ if p goes to one (since $\mathbb{P}(b) = 1 - p$) if it has a reset word (or multiple) in which the letter b occurs very often.
To be able to compare the value $\mathbb{E}[T_{\mathcal{A}}]$ of different automata, we choose
$\mathbb{P}(a) = \mathbb{P}(b) = \frac{1}{2}$. So from now on we have $p = \frac{1}{2}$, unless otherwise specified. This

way the number of a's (or b's) in the reset words of an automaton won't play a role in the value $\mathbb{E}[T_{\mathcal{A}}]$.

Definition 4.33. Let $\mathbb{P}(a) = \mathbb{P}(b) = \frac{1}{2}$. Then we define the value $R(n)$ as follows.

$$R(n) := \max\{\mathbb{E}[T_{\mathcal{A}}] \mid \mathcal{A} \text{ a synchronizing automaton with } n \text{ states}\}$$

The Černý automaton $\mathcal{C}_n$ has (as far as we know) the largest shortest reset word, but does this also mean that $R(n) = \mathbb{E}[T_{\mathcal{C}_n}]$?
In this section we are going to investigate the value of $R(n)$. So we are going to look for the automaton $\mathcal{A}$ with with the largest value $\mathbb{E}[T_{\mathcal{A}}]$.

Since the states of an automaton can always be numbered differently, we use Greek letters to indicate the states of an automaton.

Let $n = 2$ and $Q = \{\alpha, \beta\}$. Since we have $\mathbb{P}(a) = \mathbb{P}(b) = \frac{1}{2}$, we can omit the automata in which only the letters a and b are switched. Then we have the following possible synchronizing automata.

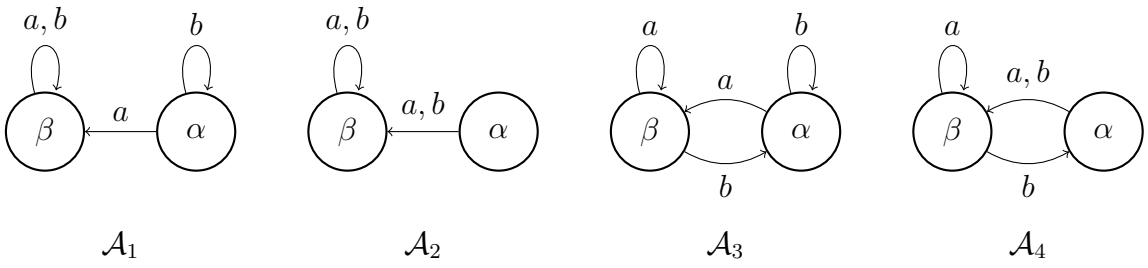

Figure 4.9: All synchronizing automata with $n = 2$.

Note that $T_{\mathcal{A}_1}, T_{\mathcal{A}_4} \sim Geo(p)$ ($T_{\mathcal{A}_1}$ and $T_{\mathcal{A}_4}$ are geometrically distributed). Both automata $\mathcal{A}_1$ and $\mathcal{A}_4$ have as reset word $w = a$. So in both cases we are waiting until the one moment we get a "success" (the letter a). Since $\mathbb{P}(a) = \frac{1}{2}$, we get that the probability of "success" is $\frac{1}{2}$.
This gives us immediately $\mathbb{E}[T_{\mathcal{A}_1}] = \mathbb{E}[T_{\mathcal{A}_4}] = 2$. If you want, you could also calculate these values with the discussed systems in Subsection 4.2.1 and Subsection 4.2.2.

For automata $\mathcal{A}_2$ and $\mathcal{A}_3$ we have $\mathbb{E}[T_{\mathcal{A}_2}] = \mathbb{E}[T_{\mathcal{A}_3}] = 1$. Since for these two automaton we have that $w = a$ and $v = b$ are both reset words.

This gives us that automata $\mathcal{A}_1$ and $\mathcal{A}_4$ give the largest value for $\mathbb{E}[T_{\mathcal{A}}]$, for $n = 2$ and $p = \frac{1}{2}$.

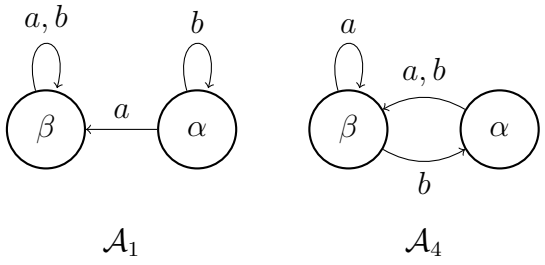

Figure 4.10: The automata with the largest value of $\mathbb{E}[T_{\mathcal{A}}]$ with $n = 2$ and $p = \frac{1}{2}$.

Observe that $\mathcal{A}_4 = C_2$ the Černý automaton with $n = 2$. With $p = \frac{1}{2}$ we have $\mathbb{E}[T_{\mathcal{C}_2}] = \mathbb{E}[T_{\mathcal{A}_4}] = \mathbb{E}[T_{\mathcal{A}_1}] = 2$. This gives us the following value for $R(2)$.

$$R(2) = 2$$

For $n = 2$ we could determine $R(n)$ by checking all synchronizing automata. Now we are interested in the case that we have n states, where $n \in \mathbb{N}$. For $n \geq 2$ an integer, $R(n)$ isn't that easy to determine. So for the general case (n states), we are going to look at lower and upper bounds of $R(n)$.
We are going to start with the upper bound of $R(n)$.

4.3.1 Upper bound of $R(n)$

Let $\mathcal{A} = (Q, \Sigma, \delta)$ be a synchronizing automaton, with $Q = \{1, \ldots, n\}$ ($n \geq 2$ an integer) and $\Sigma = \{a, b\}$ with

$$\mathbb{P}(a) = \mathbb{P}(b) = \frac{1}{2}$$

Definition 4.34. Let $\mathcal{A} = (Q, \Sigma, \delta)$ be a synchronizing automaton, with
$Q = \{1, \ldots, n\}$ ($n \geq 2$ an integer) and $\Sigma = \{a, b\}$.
For $t \geq 1$ we define the stochastic process $(X_i)_{i \in \mathbb{N}}$ with $X_i \in \Sigma$ by the following probabilities:

$$\mathbb{P}(X_i = a) = \mathbb{P}(X_i = b) = \frac{1}{2}$$

Let $w \in \Sigma^*$, then we define the following

$$t_w := \min\left\{k \mid w = X_{k-|w|+1} \ldots X_k\right\}$$

In other words, t_w is the amount of letters we need to get the word $w \in \Sigma^*$.

Remark. Note that t_w is a random variable, since it depends on the stochastic process $(X_t)_{t \in \mathbb{N}}$. But also observe that $t_w \geq |w|$.

If $w \in \Sigma^*$ is a reset word for automaton $\mathcal{A}$, then we are interested in the value of $\mathbb{E}[t_w]$, since $\mathbb{E}[T_{\mathcal{A}}]$ and $\mathbb{E}[t_w]$ are related (for $w \in \Sigma^*$ a reset word).
Observe that $\mathbb{E}[t_w] \geq \mathbb{E}[T_{\mathcal{A}}]$ if $w \in \Sigma^*$ is a reset word for automaton $\mathcal{A}$. $\mathbb{E}[t_w]$ isn't necessarily equal to $\mathbb{E}[T_{\mathcal{A}}]$, because there might be more different reset words of automaton $\mathcal{A}$, besides $w \in \Sigma^*$.
Note that $\mathbb{E}[t_\lambda] = 0$.

If we have a word $w \in \Sigma^*$ with $|w| = 1$ (in other words $w \in \Sigma$), then we get $\mathbb{P}(t_w = k) = \left(\frac{1}{2}\right)^k$. To have $t_w = k$, we must have that $X_1, \ldots, X_{k-1} \neq w$ and $X_k = w$. Since we have $\mathbb{P}(X_i = a) = \mathbb{P}(X_i = b) = \frac{1}{2}$, this gives
$\mathbb{P}(t_w = k) = \left(\frac{1}{2}\right)^{k-1} \cdot \frac{1}{2} = \left(\frac{1}{2}\right)^k$.

Example 4.35. Let take a look at two different words $w = ab$ and $v = aa$ and calculate $\mathbb{E}[t_w]$ and $\mathbb{E}[t_v]$.
Let $i \geq 1$ be an integer, then we have

$$\mathbb{P}(X_i X_{i+1} = v) = \mathbb{P}(X_i = a) \cdot \mathbb{P}(X_{i+1} = a) = \frac{1}{2}^2 = \frac{1}{4}$$

and

$$\mathbb{P}(X_i X_{i+1} = w) = \mathbb{P}(X_i = a) \cdot \mathbb{P}(X_{i+1} = b) = \frac{1}{2}^2 = \frac{1}{4}$$

This gives that $\mathbb{E}[t_w] = \frac{1}{\mathbb{P}(X_i X_{i+1} = w)} = 4$. Since $t_w \sim Geo(\mathbb{P}(X_i X_{i+1} = w))$ for $w = ab$.
Let $i \in \mathbb{N}$, then consider the following situation, we have $X_i = a$, but $X_{i+1} \neq b$. So we have $X_{i+1} = a$, this gives immediately a new start for word w. Thus $\mathbb{E}[t_w]$ is equal to 1 divided by the probability that word w occurs.
Meanwhile if we consider the following situation, let $X_i = a$, but $X_{i+1} \neq a$. So we have $X_{i+1} = b$, this doesn't gives us a new start for word v. We have to wait until word v starts again. So by the calculation of $\mathbb{E}[t_v]$ we have to add the expected time before we again start with word v. This gives $\mathbb{E}[t_v] = \frac{1}{\mathbb{P}(X_i X_{i+1} = v)} + \frac{1}{\mathbb{P}(X_i = a)} = 4 + 2 = 6$

In Example 4.35 we have seen that $\mathbb{E}[t_w]$ depends on the word $w \in \Sigma^*$. So to make a more precise statement about $\mathbb{E}[t_w]$ we need a extra definition.

Definition 4.36. Let $m \in \mathbb{N}$ and $w = X_1 \ldots X_m$, with $X_i \in \Sigma$,
$\mathbb{P}(X_i = a) = \mathbb{P}(X_i = b) = \frac{1}{2}$.
Then we define the following

$$k^* := \max\{k < m \mid X_1 \ldots X_k = X_{m-k+1} \ldots X_m\}$$

Thus $X_1 \ldots X_{k^*}$ is the longest subword that is both a prefix and suffix of word w.

Remark. Since we have $k < m$ in the definition of k^*, we get that $X_1 \ldots X_{k^*}$ a subword is of w (so $X_1 \ldots X_{k^*} \neq w$).

We could say that $X_1 \ldots X_{k^*}$ is the largest overlapping part of word w
($w = X_1 \ldots X_{k^*} v X_1 \ldots X_{k^*}$ for some $v \in \Sigma^*$ with $|v| = m - 2k^*$).

Example 4.37. Let's look at some example words and their value of k^*.
Let $w = aaaa$ then $k^* = 3$, since $u := aaa$ is both a prefix and suffix of word w and $k^* < |w| = 4$ must hold.
Let $w = abba$ then $k^* = 1$. Because $u := a$ is both a prefix and suffix of word w, but ab is only a prefix and not a suffix of word w.

Let $w = aa$ then $k^* = 1$, since $u := a$ is both a prefix and suffix of word w and $k^* < |w| = 2$ must hold.
Let $w = ab$ then $k* = 0$, since there is no word that is both a prefix and suffix of word w.

With the definition of k^* we can formulate a general statement about $\mathbb{E}[t_w]$.

Lemma 4.38. *Let $w \in \Sigma^*$ be a word, then we have the following.*

$$\mathbb{E}[t_w] = 2^{|w|} + \mathbb{E}[t_{w_{[k^*]}}]$$

Proof. ([11]) Suppose we have an infinite sequence $X_1X_2\cdots$, where $X_i \in \Sigma$ with $\mathbb{P}(X_i = a) = \mathbb{P}(X_i = b) = \frac{1}{2}$.
Since the row in infinite long, w must occur almost surely in this row.
Let $I := \{i \mid X_{i-|w|+1}\cdots X_i = w\}$ the set of indices where a occurrence of w ends.
Let T_j be the index of the last letter of w, in the jth occurrence of w. Thus, X_{T_j} is the last letter of w in the jth occurrence of w. Observe that by definition of T_j, we have $T_1 = t_w$.

If $i \in I$, then it must hold that $i \geq |w|$. For all $i \geq |w|$ we have $\mathbb{P}(i \in I) = \frac{1}{2^{|w|}}$, since $\mathbb{P}(X_i = a) = \mathbb{P}(X_i = b) = \frac{1}{2}$.

Let m be an integer, then we have the following.

$$\begin{aligned}
\mathbb{E}\left[|I \cap \{1,\ldots,m\}|\right] &= \mathbb{E}\left[\sum_{i=|w|}^{m} 1_{\{i\in I\}}\right] \\
&= \sum_{i=|w|}^{m} \mathbb{E}\left[1_{\{i\in I\}}\right] \\
&= \sum_{i=|w|}^{m} \mathbb{P}\left(i \in I\right) \\
&= \frac{m - |w| + 1}{2^{|w|}}
\end{aligned}$$

Define $k := |I \cap \{1,\ldots,m\}|$. By definition of T_j we know that $T_k \leq m \leq T_{k+1}$. We can write $T_k = T_1 + \sum_{j=2}^{k} T_j - T_{j-1}$. This gives us the following.

$$\begin{aligned}
T_1 + \sum_{j=2}^{k} T_j - T_{j-1} \leq m \leq T_1 + \sum_{j=2}^{k+1} T_j - T_{j-1} \\
\frac{T_1}{m} + \frac{1}{m}\sum_{j=2}^{k} T_j - T_{j-1} \leq 1 \leq \frac{T_1}{m} + \frac{1}{m}\sum_{j=2}^{k+1} T_j - T_{j-1} \\
\frac{T_1}{m} + \frac{1}{m}\sum_{j=2}^{k} T_j - T_{j-1} \leq 1 \leq \frac{T_1 + T_{k+1} - T_k}{m} + \frac{1}{m}\sum_{j=2}^{k} T_j - T_{j-1}
\end{aligned}$$

$$\mathbb{E}\left[\frac{T_1}{m}+\frac{1}{m}\sum_{j=2}^{k}T_j-T_{j-1}\right]\leq 1\leq \mathbb{E}\left[\frac{T_1+T_{k+1}-T_k}{m}+\frac{1}{m}\sum_{j=2}^{k}T_j-T_{j-1}\right]$$

$$\mathbb{E}\left[\frac{T_1}{m}\right]+\mathbb{E}\left[\frac{1}{m}\sum_{j=2}^{k}T_j-T_{j-1}\right]\leq 1\leq \mathbb{E}\left[\frac{T_1+T_{k+1}-T_k}{m}\right]+\mathbb{E}\left[\frac{1}{m}\sum_{j=2}^{k}T_j-T_{j-1}\right]$$

$$\frac{\mathbb{E}\left[T_1\right]}{m}+\mathbb{E}\left[\frac{k}{m}\frac{1}{k}\sum_{j=2}^{k}T_j-T_{j-1}\right]\leq 1\leq \frac{\mathbb{E}\left[T_1+T_{k+1}-T_k\right]}{m}+\mathbb{E}\left[\frac{k}{m}\frac{1}{k}\sum_{j=2}^{k}T_j-T_{j-1}\right]$$

For m fixed we have the following.

$$\begin{aligned}\mathbb{E}\left[\frac{k}{m}\right]&=\frac{1}{m}\mathbb{E}\left[k\right]\\&=\frac{1}{m}\cdot\frac{m-|w|+1}{2^{|w|}}\\&=\frac{m-|w|+1}{m2^{|w|}}\end{aligned}$$

Take limits with $m\to\infty$.
Since w occurs almost surely in our infinite sequence, we have that the variable T_1 is finite almost surely. This gives that $\lim_{m\to\infty}\frac{\mathbb{E}[T_1]}{m}=0$. Analogue we have $\lim_{m\to\infty}\frac{\mathbb{E}[T_1+T_{k+1}-T_k]}{m}=0$.
If $m\to\infty$ then $\frac{1}{k}\sum_{j=2}^{k}T_j-T_{j-1}=\mathbb{E}[T_j-T_{j-1}]$. Hence we have the following.

$$\begin{aligned}\lim_{m\to\infty}\mathbb{E}\left[\frac{k}{m}\frac{1}{k}\sum_{j=2}^{k}T_j-T_{j-1}\right]&=\mathbb{E}[T_j-T_{j-1}]\lim_{m\to\infty}\mathbb{E}\left[\frac{k}{m}\right]\\&=\mathbb{E}[T_j-T_{j-1}]\lim_{m\to\infty}\frac{m-|w|+1}{m2^{|w|}}\\&=\mathbb{E}[T_j-T_{j-1}]\frac{1}{2^{|w|}}\end{aligned}$$

Together this results in the following equations.

$$\lim_{m\to\infty}\left(\frac{\mathbb{E}\left[T_1\right]}{m}+\mathbb{E}\left[\frac{k}{m}\frac{1}{k}\sum_{j=2}^{k}T_j-T_{j-1}\right]\right)\leq 1\leq \lim_{m\to\infty}\left(\frac{\mathbb{E}\left[T_1+T_{k+1}-T_k\right]}{m}+\mathbb{E}\left[\frac{k}{m}\frac{1}{k}\sum_{j=2}^{k}T_j-T_{j-1}\right]\right)$$

$$\mathbb{E}[T_j-T_{j-1}]\frac{1}{2^{|w|}}\leq 1\leq \mathbb{E}[T_j-T_{j-1}]\frac{1}{2^{|w|}}$$

Thus, there must hold $\mathbb{E}[T_j-T_{j-1}]\frac{1}{2^{|w|}}=1$, which gives us $\mathbb{E}[T_j-T_{j-1}]=2^{|w|}$. With this we can give an equation for $\mathbb{E}[t_w]$, which concludes our proof.

$$\begin{aligned}\mathbb{E}[t_w]=\mathbb{E}[T_1]&=\mathbb{E}[t_{w_{[k^*]}}]+\mathbb{E}[T_2-T_1]\\&=\mathbb{E}[t_{w_{[k^*]}}]+2^{|w|}\end{aligned}$$

□

By applying Lemma 4.38 iteratively, you can calculate $\mathbb{E}[t_w]$ for each word $w \in \Sigma^*$. Let's look at an example.

Example 4.39. Let $v = abbb$, then we have $|v| = 4$ and $k^* = 0$. By applying Lemma 4.38 we get:

$$\begin{aligned}\mathbb{E}[t_v] &= 2^4 + \mathbb{E}[t_\lambda] \\ &= 2^4 + 0 = 16\end{aligned}$$

Let $w = aaaa$ ($|w| = 4$). We have seen in Example 4.37 that $k^* = 3$. By applying Lemma 4.38 we get the following.

$$\begin{aligned}\mathbb{E}[t_w] &= 2^4 + \mathbb{E}[t_{w_{[3]}}] \\ &= 16 + \mathbb{E}[t_{aaa}]\end{aligned}$$

We can again apply Lemma 4.38 on word $u = aaa$. For word u we have $k^* = 2$ and $m = |u| = 3$, so we get the following.

$$\begin{aligned}\mathbb{E}[t_w] &= 16 + \mathbb{E}[t_{aaa}] \\ &= 16 + 2^3 + \mathbb{E}[t_{w_{[2]}}] \\ &= 16 + 8 + \mathbb{E}[t_{aa}]\end{aligned}$$

This we can do again and again until we have at some point $k^* = 0$ ($u = \lambda$). This results in the following calculation.

$$\begin{aligned}\mathbb{E}[t_w] &= 16 + \mathbb{E}[t_{aaa}] \\ &= 16 + 8 + \mathbb{E}[t_{aa}] \\ &= 16 + 8 + 4 + \mathbb{E}[t_a] \\ &= 16 + 8 + 4 + 2 + \mathbb{E}[t_\lambda] \\ &= 16 + 8 + 4 + 2 + 0 = 30\end{aligned}$$

Corollary 4.40. *Let $w \in \Sigma^*$ be a word with $|w| = m \in \mathbb{N}$, then we have the following.*

$$\mathbb{E}[t_w] \leq \sum_{i=1}^{m} 2^i$$

Proof. If we want an upper bound for $\mathbb{E}[t_w]$, we have to look at the worst case scenario.
Since we have $\mathbb{E}[t_w] = 2^{|w|} + \mathbb{E}[t_{w_{[k^*]}}]$, the worst case presents if in every iteration (in the calculation of $\mathbb{E}[t_{w_{[k^*]}}]$) k^* is a large as possible. This occurs with two words $u = a^m$ and $v = b^m$. In the first iteration we have $k^* = m-1$, then $k^* = m-2$, then $k^* = m-3$, etc., until $k^* = 0$. Here is k^* maximal in each iteration, since $k^* < |w|$ must hold in each iteration.
Since $\mathbb{P}(X_i = a) = \mathbb{P}(X_i = b) = \frac{1}{2}$ we have that $\mathbb{E}[t_u] = \mathbb{E}[t_v]$.
Applying Lemma 4.38 gives

$$\mathbb{E}[t_v] = \sum_{i=1}^{m} 2^i$$

Thus $\mathbb{E}[t_w] \leq \sum_{i=1}^{m} 2^i$ holds for all words $w \in \Sigma^*$ with $|w| = m$. □

Corollary 4.41. *Let $w \in \Sigma^*$ be a word with $|w| = m \in \mathbb{N}$, then the following holds.*

$$\mathbb{E}[t_w] \leq 2^{m+1} - 2$$

Proof. We use Corollary 4.40 and then calculate the sum $\sum_{i=1}^{m} 2^i$. Here we use the fact that $\sum_{i=1}^{n} a^i = \frac{a^{n+1}-a}{a-1}$ for $a \neq 1$.

$$\begin{aligned}\sum_{i=1}^{m} 2^i &= \frac{2^{m+1}-2}{2-1} \\ &= 2^{m+1} - 2\end{aligned}$$

□

Proposition 4.42. *Let $\mathcal{A} = (Q, \Sigma, \delta)$ be a synchronizing automaton with n states. Let $\theta_1 := -0.210099161$, $\theta_2 := 1.42781363$ and $\theta_3 := 0.166421334$. Then the following holds.*

$$\mathbb{E}[T_{\mathcal{A}}] \leq 2^{\theta_3 n^3 + \theta_2 n^2 + \theta_1 n + 1} - 2 = 2^{\theta_3 n^3 + o(n^2)}$$

Proof. By Theorem 3.29 we know that there exists a reset word w, with $|w| \leq 0.166421334n^3 + 1.42781363n^2 - 0.210099161n$. By Corollary 4.41 and our definitions of θ_1, θ_2 and θ_3 we then know the following.

$$\begin{aligned}\mathbb{E}[T_{\mathcal{A}}] &\leq \mathbb{E}[t_w] \\ &\leq 2^{\theta_3 n^3 + \theta_2 n^2 + \theta_1 n + 1} - 2 \\ &= 2^{\theta_3 n^3 + o(n^2)}\end{aligned}$$

□

We can improve this upper bound of $\mathbb{E}[T_{\mathcal{A}}]$, to an upper bound of order $2^{\frac{1}{2}n^2 + o(n)}$ in the following way.

Proposition 4.43. *Let $\mathcal{A} = (Q, \Sigma, \delta)$ be a synchronizing automaton with n states, then we have the following.*

$$\mathbb{E}[T_{\mathcal{A}}] \leq (n-1)\left(2^{\binom{n}{2}+1} - 2\right) = 2^{\frac{1}{2}n^2 + o(n)}$$

Proof. In the proof of Lemma 3.5 we have seen the following:
Let $S \subset Q$, with $|S| \geq 2$ arbitrary. Take a $p, q \in Q$ with $p, q \in S$ and $p \neq q$. Then there exists a word $w \in \Sigma^*$ for which $\delta(p, w) = \delta(q, w)$ with $|w| \leq \binom{n}{2}$.
By Corollary 4.41 we then have for this word w, $\mathbb{E}[t_w] \leq 2^{\binom{n}{2}+1} - 2$.

Now we do the same iteration as in the proof of Lemma 3.5. We start with $S = Q$.
If $|S| = 1$, then we are done.
If $|S| \geq 2$, then we can pick a $p, q \in S$ with $p \neq q$. We know that there exists a reset word $w \in \Sigma^*$ for p and q with $|w| \leq \binom{n}{2}$.
According to Corollary 4.41, we expect that we need $\mathbb{E}[t_w] \leq 2^{|w|+1} - 2 \leq 2^{\binom{n}{2}+1} - 2$

letters before word w occurs in our random word. After all iterations, we concatenate all found random words (in each random word, per iteration, occurs the corresponding word w). This is a reset word for $\mathcal{A}$ of length $\mathbb{E}[T_{\mathcal{A}}]$.

In the worst case we have $|\delta(S,w)| = |S|-1$, in each iteration. So, in the worst case, we need $n-1$ iteration. This gives $\mathbb{E}[T_{\mathcal{A}}] = \sum_{i=1}^{n-1}\left(2^{\binom{n}{2}+1}-2\right) = (n-1)\left(2^{\binom{n}{2}+1}-2\right)$

Since $\binom{n}{2} = \frac{1}{2}n^2 - \frac{1}{2}n$, we get $(n-1)\left(2^{\binom{n}{2}+1}-2\right) = 2^{\frac{1}{2}n^2+o(n)}$ □

Proposition 4.43 gives us the following theorem.

Theorem 4.44. *Let $n \geq 2$ be an integer. Then the following holds*

$$R(n) \leq (n-1)\,2^{\binom{n}{2}+1} - 2 = 2^{\frac{1}{2}n^2+o(n)}$$

Proof. The proof follows from Definition 4.33 and Proposition 4.43. □

4.3.2 $R(n)$ for small n

Before we are going to look at the lower bound of $R(n)$, we would like to get some feeling of the value $R(n)$. So we are first going to look at the value $R(n)$, for small n. We have already seen that $R(2) = 2$. We calculated this by going through all synchronizing automata $\mathcal{A}$ and calculating their value $\mathbb{E}[T_{\mathcal{A}}]$.

In this section we are going to look at the value of $R(n)$ for $n = 3, 4, 5$.

Automaton with 3 states

We only consider synchronizing automata of the form $\mathcal{A} = (\{\alpha,\beta,\gamma\},\{a,b\},\delta)$, with $\mathbb{P}(a) = \mathbb{P}(b) = \frac{1}{2}$.

We know from Proposition 2.22 that $w \in \Sigma^*$ is a reset word if and only if w indicates a path from Q to a singleton in the power automaton $\mathcal{P}_{\mathcal{A}}$. We also have seen in Subsection 4.2.2 that we can calculate $\mathbb{E}[T_{\mathcal{A}}]$ by looking at the power automaton. So to find the "worst" automaton with 3 states, let's first look at the "worst" power automaton with $n = 3$. Thus, we search for the power automaton with $n = 3$ which gives the largest possible value for $\mathbb{E}[T_{\mathcal{A}}]$ with $p = \frac{1}{2}$.

Proposition 4.45. *Let $\mathcal{A} = (Q,\Sigma,\delta)$, with $Q = \{\alpha,\beta,\gamma\}$ and $\Sigma = \{a,b\}$. Let $A := \{\{q\} \mid q \in Q\}$ be the set of singletons and $\mathbb{P}(a) = \mathbb{P}(b) = \frac{1}{2}$. Then the following power automaton gives the biggest value of $\mathbb{E}[T_{\mathcal{A}}]$ (with $p = \frac{1}{2}$), and thus determines $R(3)$.*

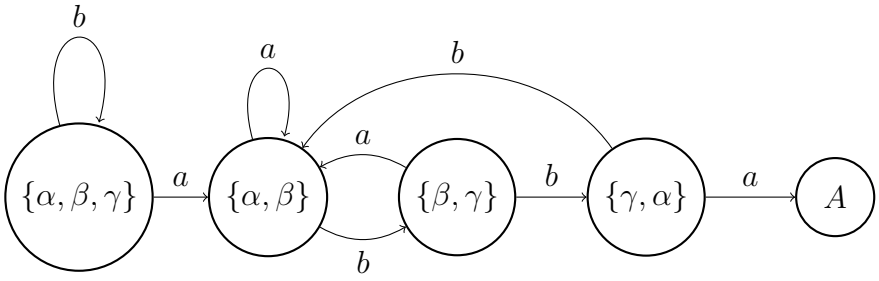

Figure 4.11: The power automaton with the largestvalue of $\mathbb{E}[T_{\mathcal{A}}]$ with $n = 3$ and $p = \frac{1}{2}$.

Proof. We are going to proof this by construction. We start with the "empty" power automaton.

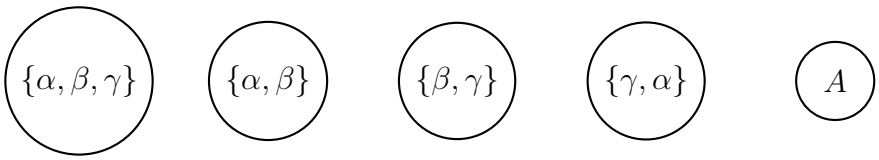

Figure 4.12: The "empty" power automaton.

First, we are going to show which arrows in a power automaton causes $\mathbb{E}[T_{\mathcal{A}}]$ to as large as possible. Later we are going to look if these arrows are possible with the letters in Σ.

Since we look at a synchronizing automaton there must be a path from $\{\alpha, \beta, \gamma\}$ to A.
Suppose we have a reset word $v \in \Sigma$ with $|v| = 3$. Then by Lemma 4.38 we get $\mathbb{E}[t_w] = 2^3 + 2^2 + 2 = 8 + 4 + 2 = 14$. Since we know that $\mathbb{E}[T_{\mathcal{A}}] \leq \mathbb{E}[t_w]$, we then get $\mathbb{E}[T_{\mathcal{A}}] \leq 14$. This is in contradiction with the fact that $\mathbb{E}[T_{\mathcal{C}_n}] = 16$ (Theorem 4.15). Thus, if we want $\mathbb{E}[T_{\mathcal{A}}]$ to be as large as possible, we can't have a path of length 3 from Q to A.
Then, the only possible way for a automaton with $n = 3$ to be synchronizing is, when we have a path from Q through all states $\{\alpha, \beta\}, \{\beta, \gamma\}$ and $\{\alpha, \gamma\}$ and then end up in A.
This gives us the following situation.

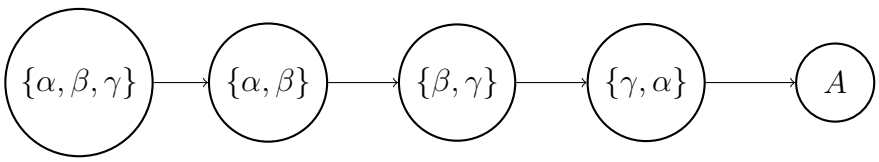

Figure 4.13: The power automaton with path from Q to A.

Since we have an alphabet of two letters, each state (exclusive A) in the power automaton has two outgoing arrows. At the moment each state in the power au-

tomaton (exclusive A) has one outgoing arrow. We have yet to determine the second outgoing arrow for each state in the power automaton.

For all $S \subseteq Q$ and $w \in \Sigma^*$, we have $|S \circ w| \leq |S|$. In other words, the number of states is decreasing. We can't have arrows, from some $S \subseteq Q$ with $|S| \leq 2$, to Q.

We also have seen that we can't have a reset word of length 3. This gives that the second arrow out of Q must be a self loop. This together with the fact that the number of states must decrease, gives that the second arrow out of $\{\alpha, \beta\}$ must also be a self loop.
This gives the following situation.

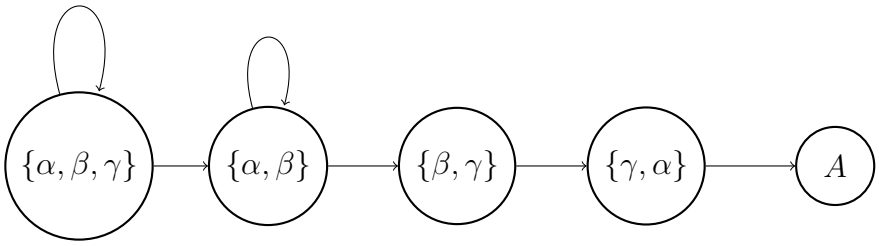

Figure 4.14: The power automaton with second arrows out of state Q and $\{\alpha, \beta\}$.

For the second arrows out of state $\{\beta, \gamma\}$ and $\{\gamma, \alpha\}$ there are still multiple options. We go through all possible options for the power automaton and calculate $\mathbb{E}[T_{\mathcal{A}}]$ with the use of System 2 (described in Subsection 4.2.2). All different options with there value of $\mathbb{E}[T_{\mathcal{A}}]$ are listed in Appendix B.1.

We see that the following power automaton gives the largest value of $\mathbb{E}[T_{\mathcal{A}}]$.

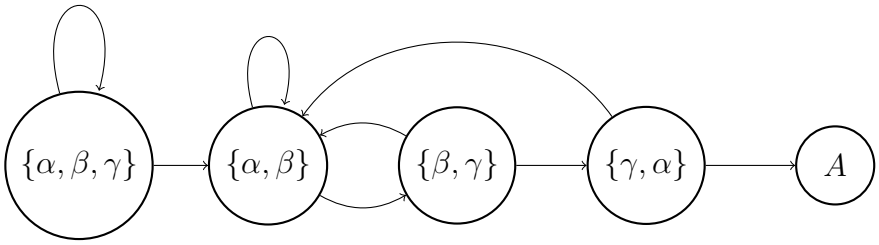

Figure 4.15: Possible the "worst" power automaton with $n = 3$ and $p = \frac{1}{2}$.

If this power automaton is possible, then we know by construction that it will give the largest value of $\mathbb{E}[T_{\mathcal{A}}]$. It remains to check whether this power automaton is possible. To check this, let's assume such power automaton is possible and try to assigning our letters to the arrows.
Since we can always exchange the letters a and b, we can without loss of generality start with assigning the letters a and b to the outgoing arrows of state Q, anyway we like. Let's say we label the self loop of Q with the letter b and the outgoing arrow into state $\{\alpha, \beta\}$ with the letter a.

Now that the letter a is the letter which decreases the number of states, we also know that the arrow from $\{\gamma, \alpha\}$ to A must be labeled with the letter a. This means that the other outgoing arrow from state $\{\gamma, \alpha\}$ must be labeled with the letter b. This gives us the following situation.

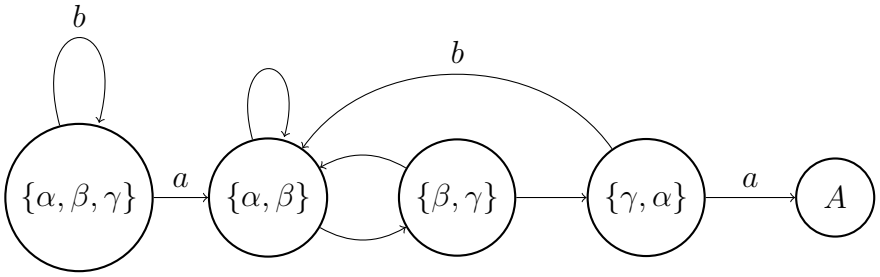

Figure 4.16: Possible the "worst" power automaton with $n = 3$ and $p = \frac{1}{2}$.

$\{\alpha, \beta, \gamma\} \xrightarrow{b} \{\alpha, \beta, \gamma\}$ and $\{\gamma, \alpha\} \xrightarrow{b} \{\alpha, \beta\}$ gives $\beta \xrightarrow{b} \gamma$. Which would mean that in our possible power automaton we get $\{\beta, \gamma\} \xrightarrow{b} \{\gamma, \alpha\}$.
Note that this gives $\beta \xrightarrow{b} \gamma \xrightarrow{b} \alpha$ and $\alpha \xrightarrow{b} \beta$.

Now that we know all the b arrows we can also fill in the a's in our power automaton. So if our power automaton is possible we should get the following power automaton.

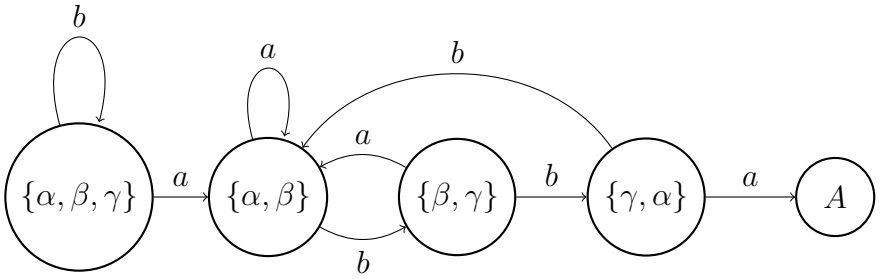

Figure 4.17: Possible the "worst" power automaton with $n = 3$ and $p = \frac{1}{2}$.

We have to check if the a's are possible in an automaton. We have the following a arrow's:

1. $\{\alpha, \beta, \gamma\} \xrightarrow{a} \{\alpha, \beta\}$
2. $\{\alpha, \beta\} \xrightarrow{a} \{\alpha, \beta\}$
3. $\{\beta, \gamma\} \xrightarrow{a} \{\alpha, \beta\}$
4. $\{\alpha, \gamma\} \xrightarrow{a} A$

We have $\{\alpha, \beta, \gamma\} \xrightarrow{a} \{\alpha, \beta\}$, so this means either $\gamma \xrightarrow{a} \alpha$ or $\gamma \xrightarrow{a} \beta$.

Suppose $\gamma \xrightarrow{a} \alpha$, then $\{\beta, \gamma\} \xrightarrow{a} \{\alpha, \beta\}$ gives that $\beta \xrightarrow{a} \beta$. This in turn must mean that $\alpha \xrightarrow{a} \alpha$.
This would give us the following:

- $\gamma \xrightarrow{a} \alpha$
- $\beta \xrightarrow{a} \beta$
- $\alpha \xrightarrow{a} \alpha$

Suppose $\gamma \xrightarrow{a} \beta$, then $\{\beta, \gamma\} \xrightarrow{a} \{\alpha, \beta\}$ gives that $\beta \xrightarrow{a} \alpha$. Then $\{\alpha, \gamma\} \xrightarrow{a} A$ also gives that $\alpha \xrightarrow{a} \beta$.
This would give us the following:

- $\gamma \xrightarrow{a} \beta$
- $\beta \xrightarrow{a} \alpha$
- $\alpha \xrightarrow{a} \beta$

Thus, there exists an automata with corresponding automaton shown in Figure 4.11. This proves our proposition. □

Remark. In the proof of Proposition 4.45 we see the following. The second arrow out of state $\{\beta, \gamma\}$ and state $\{\gamma, \alpha\}$ that makes $\mathbb{E}[T_{\mathcal{A}}]$ the largest, are the arrows to the state $\{\alpha, \beta\}$. We observe that this is the state with the highest value of $d(S)$ ($d(\{\alpha, \beta\}) = 3$, $d(\{\beta, \gamma\}) = 2$, $d(\{\gamma, \alpha\}) = 1$), besides state Q.
If we look at all second arrows out of each state in the power automaton we see that all second arrows go to state S with $d(S)$ maximal, taking into account the fact that the number of states must be decreasing.

Corollary 4.46. *We have*

$$R(3) = 16$$

Proof. Proposition 4.45 gives the power automaton corresponding to the largest possible value of $\mathbb{E}[T_{\mathcal{A}}]$ with $n = 3$.
In Appendix B.1 we have seen that $\mathbb{E}[T_{\mathcal{A}}] = 16$ for the power automaton in Proposition 4.45 with $p = \frac{1}{2}$. Thus, we have $R(3) = 16$. □

Remark. The power automaton in Proposition 4.45 is similar to the power automaton of the Černý automaton C_3. The arrows within A could be different but according to Subsections 4.2.1 and 4.2.2 this doesn't matter in the calculation of $\mathbb{E}[T_{\mathcal{A}}]$.
So the Černý automaton C_3 determines $R(3)$.

Corollary 4.47. *Let $Q = \{\alpha, \beta, \gamma\}$ and $\mathbb{P}(a) = \mathbb{P}(b) = \frac{1}{2}$. Then the following two automata give the largest value of $\mathbb{E}[T_{\mathcal{A}}]$.*

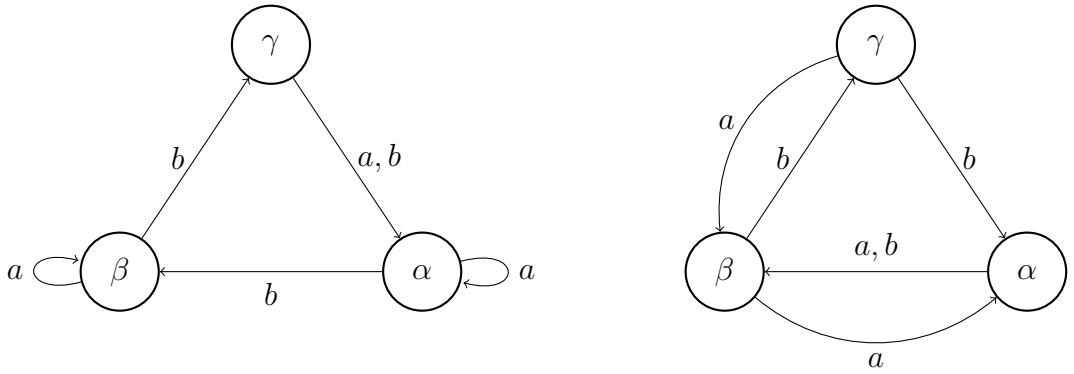

Figure 4.18: Automata with the largest value of $\mathbb{E}[T_{\mathcal{A}}]$, with $n = 3$ and $p = \frac{1}{2}$.

Proof. With Proposition 4.45 we have seen what the worst power automaton is for synchronizing automata with $n = 3$. In the proof of this Proposition we have shown that this power automaton exists by giving the possible transition functions.

For the letter b we got: $\beta \xrightarrow{b} \gamma \xrightarrow{b} \alpha$ and $\alpha \xrightarrow{b} \beta$.

For the letter a we got two possibilities. First, $\gamma \xrightarrow{a} \alpha$, $\beta \xrightarrow{a} \beta$ and $\alpha \xrightarrow{a} \alpha$.
Second, $\gamma \xrightarrow{a} \beta \xrightarrow{a} \alpha$ and $\alpha \xrightarrow{a} \beta$.

This gives us the two automata that give the largest possible value of $\mathbb{E}[T_{\mathcal{A}}]$ (shown in Figure 4.18). □

There are 3! possible permutations for α, β and γ. With this and Corollary 4.46 we know all synchronizing automata with $n = 3$ which give the (same) largest expected length of a reset word.

Automaton with 4 states

Here, we only consider synchronizing automata of the form $\mathcal{A} = (\{\alpha, \beta, \gamma, \mu\}, \{a, b\}, \delta)$, with $\mathbb{P}(a) = \mathbb{P}(b) = \frac{1}{2}$.
Since we have four states, we have a lot more states in the corresponding power automaton. For $n = 4$ we have $2^4 - 4 - 1 = 11$ not singleton states in the corresponding power automaton.
To find the synchronizing automata with the largest value for $\mathbb{E}[T_{\mathcal{A}}]$, we do a brute force search with the use of Matlab. The code, inclusive further explanation on how the code works can be found in Appendix C. The main function we use for the brute force search is discussed in Appendix C.7, here we use $p = \frac{1}{2}$ as chosen in the beginning of this section.

We know that for the Černý automaton with 4 states holds $\mathbb{E}[T_{C_4}] = \frac{3p^2-9p+10}{p(1-p)^2}$, which is equal to 50 for $p = \frac{1}{2}$. Since we look for the automata with maximal $\mathbb{E}[T_{\mathcal{A}}]$, we only have to save the automata with $\mathbb{E}[T_{\mathcal{A}}] \geq 50$ for $p = \frac{1}{2}$.

The Matlab program gives 24 automata with $\mathbb{E}[T_{\mathcal{A}}] = 67$ for $p = \frac{1}{2}$ and there are no synchronizing automata $\mathcal{A}$ with $\mathbb{E}[T_{\mathcal{A}}] > 67$ for $p = \frac{1}{2}$.
Below you see the automaton, let's call this automata $\mathcal{A}$, which together with the 4! possible permutation of the states, gives all these 24 automata.

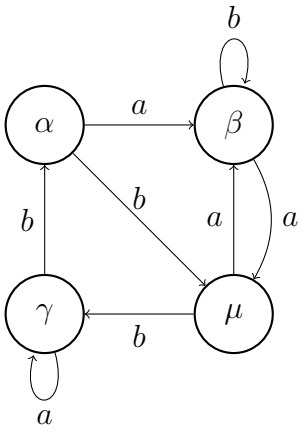

Figure 4.19: Automaton $\mathcal{A}$ with the largest value of $\mathbb{E}[T_{\mathcal{A}}]$, with $n = 4$ and $p = \frac{1}{2}$.

With a Matlab program of system 1 (see Appendix C.5) described in Subsection 4.2.1 we have calculated the exact expected length of a reset word for the automaton in Figure 4.19. This gives us the following.

$$\mathbb{E}[T_{\mathcal{A}}] = \frac{-p^3 + 8p^2 - 19p + 16}{p(1-p)^2}$$

Filling in $p = \frac{1}{2}$ (or looking at the result of our brute force Matlab program), we get the following value for $R(4)$.

$$R(4) = 67$$

Remark. Automaton $\mathcal{A}$ in Figure 4.19 isn't the Černý automaton C_4.
We have $-p^3+8p^2-19p+16 > 3p^2-9p+10$ for all $p < 1$, so $\frac{-p^3+8p^2-19p+16}{p(1-p)^2} > \frac{3p^2-9p+10}{p(1-p)^2}$ for all $p < 1$. This gives us that for all $p \in (0, 1)$ $\mathbb{E}[T_{\mathcal{A}}] > \mathbb{E}[T_{C_4}]$. Which tells us that $R(n)$ is not always determined by the Černý automaton $\mathcal{C}_n$.

Let's take a look at the power automaton, corresponding to automaton $\mathcal{A}$ (Figure 4.19).

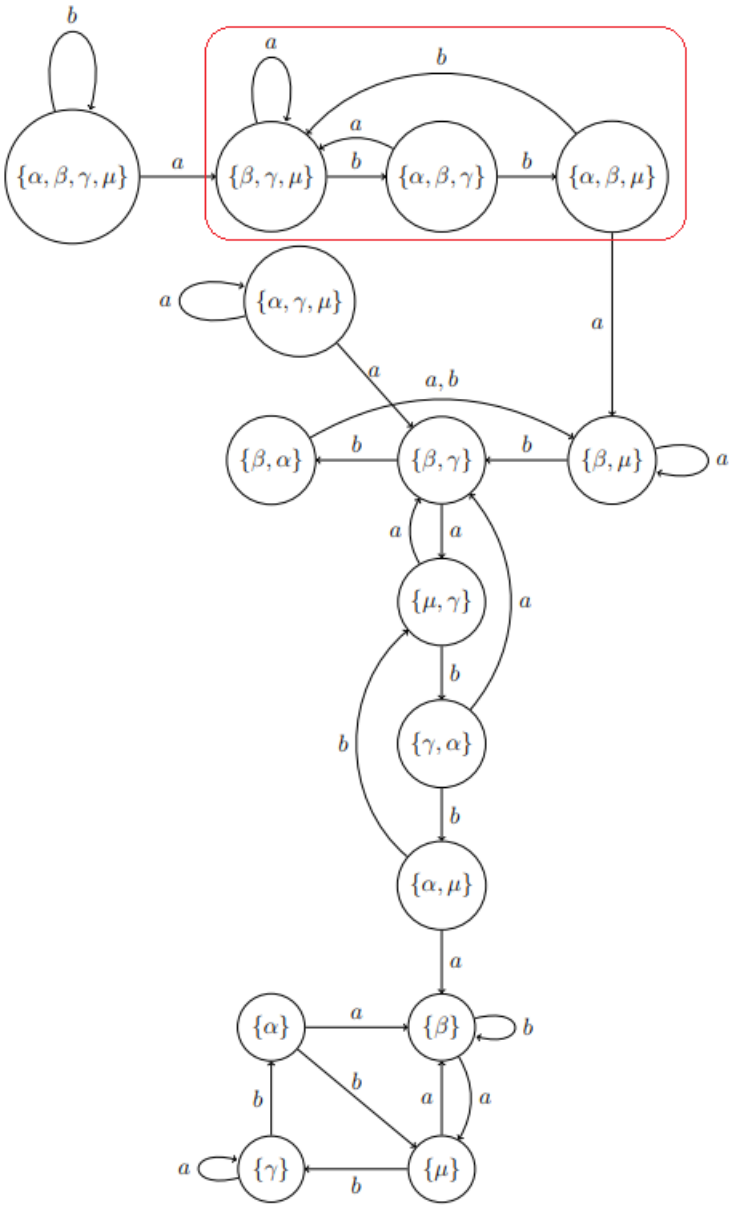

Figure 4.20: Power automaton of automaton $\mathcal{A}$ (the automaton in Figure 4.19).

Remark. In the with red marked part of the power automaton, we see a similar structure as in our proof of Proposition 4.45. With the second arrows in this part we each time we increase the distance $d(S)$ to A.

Remark. The shortest reset word of this automaton is $w = abbababbb$. So the length of the shortest reset word is $|w| = 9 = 3^2 = (n-1)^2$, which is the same length of the shortest reset word of C_4.

For $n = 4$ we have that automaton $\mathcal{A}$ has the largest value for $\mathbb{E}[T_{\mathcal{A}}]$. This automaton is not equal to the Černý automaton C_4, but is still an automaton with the length of the shortest reset word equal to $(n-1)^2$ (for $n = 4$), just like the Černý automaton C_4.

Automaton with 5 states

Consider synchronizing automata of the form $\mathcal{A} = (\{\alpha, \beta, \gamma, \mu, \varphi\}, \{a, b\}, \delta)$, with $\mathbb{P}(a) = \mathbb{P}(b) = \frac{1}{2}$.
We again do a brute force search (with Matlab), to search for the automaton with the largest value of $\mathbb{E}[T_{\mathcal{A}}]$.

Definition 4.48. Let $\mathcal{A}_1 = (Q, \Sigma, \delta_1)$ and $\mathcal{A}_2 = (Q, \Sigma, \delta_2)$ be synchronizing automata with n states. Then we say that automata $\mathcal{A}_1$ and $\mathcal{A}_2$ are *isomorphic* if there exist a bijection $f : Q \to Q$ which preserves the transition function. In other words, for every $l \in \Sigma$ it must hold that $\delta_2(f(q), l) = f(\delta_1(q, l))$

Remark. If automaton $\mathcal{A}_1$ and $\mathcal{A}_2$ are isomorphic, then we have that $\mathbb{E}[T_{\mathcal{A}_1}] = \mathbb{E}[T_{\mathcal{A}_2}]$.
Knowing the above remark, we can make our program more efficient by excluding the isomorphic automata. There are $5! = 120$ different permutations $\alpha, \beta, \gamma, \varphi, \delta$.

We know that the Černý automaton with 5 states has $\mathbb{E}[T_{C_5}] = \frac{4p^2-14p+20}{p(1-p)^2}$, which is equal to 112 for $p = \frac{1}{2}$. Since we look for the automata with maximal $\mathbb{E}[T_{\mathcal{A}}]$, we only have to save the automata with $\mathbb{E}[T_{\mathcal{A}}] \geq 112$ for $p = \frac{1}{2}$.

The Matlab program (see Appendix C.7) gives that the automaton below (Figure 4.21), has the largest value for $\mathbb{E}[T_{\mathcal{A}}]$ for $p = \frac{1}{2}$ (in this case we have $\mathbb{E}[T_{\mathcal{A}}] = \frac{36{,}5625}{0{,}21875} = \frac{1170}{7} \approx 167,143$ for $p = \frac{1}{2}$). Let's call this automaton $\mathcal{A}$.

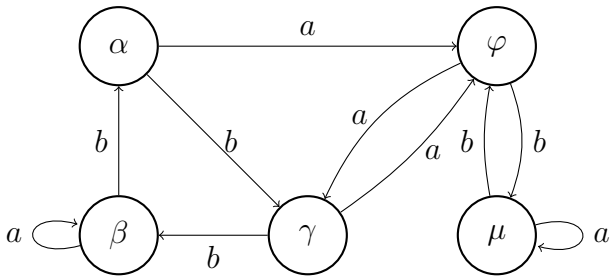

Figure 4.21: Automaton $\mathcal{A}$ with the largest value of $\mathbb{E}[T_{\mathcal{A}}]$, with $n = 5$ and $p = \frac{1}{2}$.

With a Matlab program of system 1 (see Appendix C.5) described in Subsection 4.2.1 we have calculated the exact expected length of a reset word for the automaton in Figure 4.21. This gives us the following.

$$\mathbb{E}[T_{\mathcal{A}}] = \frac{-4p^5 + 27p^4 - 80p^3 + 136p^2 - 140p + 81}{p(1-p)^2(p^2 - p + 2)}$$

Filling in $p = \frac{1}{2}$ (or looking at the result of our brute force Matlab program), we get the following value for $R(5)$.

$$R(5) = \frac{1170}{7}$$

Remark. Automaton $\mathcal{A}$ in Figure 4.21 isn't the Černý automaton $\mathcal{C}_5$.
We have $\frac{-4p^5+27p^4-80p^3+136p^2-140p+81}{p(1-p)^2(p^2-p+2)} > \frac{(4p^2-14p+20)}{p(1-p)^2}$ for all $p \in (0, 1)$. This gives that,

for all $p \in (0,1)$ $\mathbb{E}[T_{\mathcal{A}}] > \mathbb{E}[T_{\mathcal{C}_5}]$ holds.
Thus also for $n = 5$, $R(n)$ isn't determined by the Černý automaton $\mathcal{C}_n$.

Let's take a look at the power automaton corresponding to the automaton in Figure 4.21 ($\mathcal{P}_{\mathcal{A}}$). And compare this to the power automaton of the Černý automaton C_5 (C_5 is show in Figure 4.22). The power automaton of $\mathcal{C}_n$ ($\mathcal{P}_{\mathcal{C}_n}$) is shown in Appendix B.2.

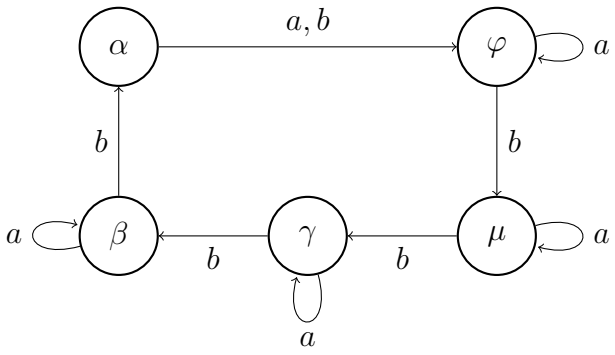

Figure 4.22: The Černý automaton C_5.

In $\mathcal{P}_{\mathcal{A}}$ (Figure 4.23) we have indicated the shortest path from Q to $\{\varphi\}$ with the color green.
Note that in any path from Q to $\{\varphi\}$ in this power automaton, you will never go through the states $\{\alpha, \beta, \gamma, \varphi\}$, $\{\alpha, \beta, \gamma, \mu\}$ and $\{\alpha, \gamma, \beta\}$. So these states (and arrows out of these states) don't contribute to the value of $\mathbb{E}[T_{\mathcal{A}}]$. That is why these states and arrows are colored light grey.

Remark. The shortest reset word of automaton $\mathcal{A}$ (Figure 4.21) is
$u = abbababbaababba$. The path indicated by u is green in Figure 4.23. The length of the shortest reset word is $|u| = 15 < 16 = 4^2 = (n-1)^2$. This implies that the shortest reset word of the automaton in Figure 4.21 is smaller then the shortest reset word of $\mathcal{C}_5$.
Thus, the automaton $\mathcal{A}$ with the largest value of $\mathbb{E}[T_{\mathcal{A}}]$, isn't necessarily the automaton with the largest shortest reset word.

Remark. In the with red marked parts of the power automaton in Figure 4.23 we see again the similar structure as in our proof of Proposition 4.45 and Figure 4.20. We do not see this structure in the power automaton of the Černý automaton C_5 (Figure B.7).

Remark. In the power automaton of automaton $\mathcal{A}$ we have light grey states and arrows, while we don't have those in the power automaton of the Černý automaton C_5 (Figure B.7). We also have $\mathbb{E}[T_{\mathcal{A}}] > \mathbb{E}[T_{\mathcal{C}_n}]$. This indicates that for a high value of $\mathbb{E}[T_{\mathcal{A}}]$, not necessarily every state in the power automaton should play a role in the path from Q to a singleton.

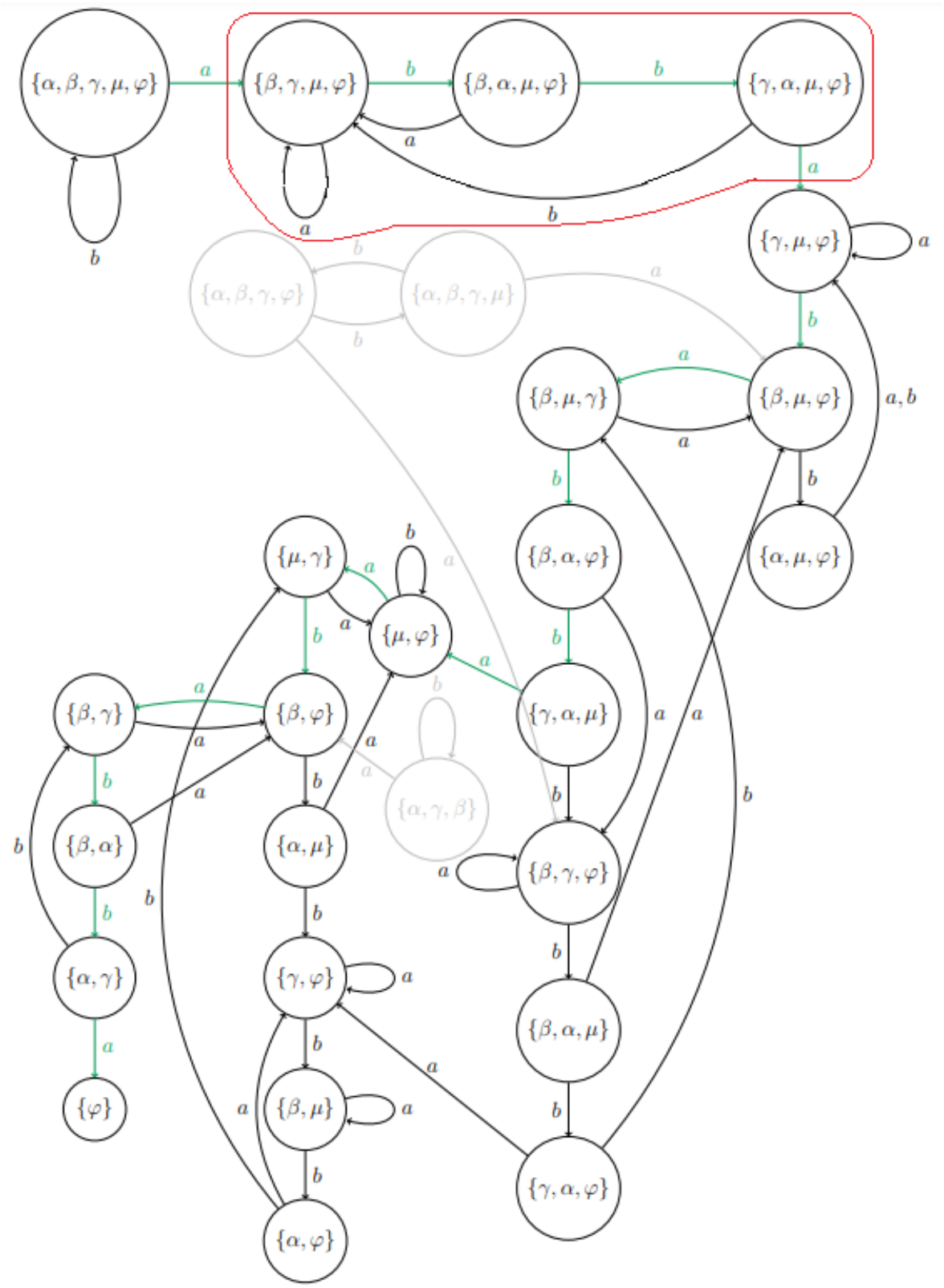

Figure 4.23: Power automaton of automaton $\mathcal{A}$ (the automaton in Figure 4.21).

If we further compare the power automaton of automaton $\mathcal{A}$ (Figure 4.23) to the power automaton of the Černý automaton C_5 (Figure B.7), we have that the following stands out. Take any $\emptyset \neq S \subset Q$ that lies on the green path. Then for $\mathcal{P}_\mathcal{A}$ (Figure 4.23) holds that, if we divert from the green path then $d(S \circ l) > d(S)$ ($l \in \Sigma$) unless $S \circ l = S$. While in $\mathcal{P}_{\mathcal{C}_5}$ (Figure B.7) we see
$d(\{\beta, \alpha, \varphi\}) = 7 = d(\{\beta, \varphi\}) = d(\{\beta, \alpha, \varphi\} \circ a)$.
In $\mathcal{P}_{\mathcal{C}_5}$ (Figure B.7) we can see that there are two paths (they have some overlap) from Q to $\{\varphi\}$ indicated by $w = abbbbabbbbabbbba$ (color green in Figure B.7) and $v = abbabbabbbbabbbba$ (color green/purple in Figure B.7). We see that w indicates the shortest path $|w| = 4^2 = 16$, but that $|v| = 17 = |w| + 1$.
If we are in state $\{\beta, \alpha, \varphi\}$ and then have letter a, we move of the green path, onto a state on the purple path. For all states S on the purple path holds that $d(S) \leq d(\{\gamma, \alpha, \beta, \varphi\}) = 13$, so in this case if we divert from the green path to somewhere on the purple path we still have a relative small distance to state $\{\varphi\}$. This might be an reason why we have $\mathbb{E}[T_\mathcal{A}] > \mathbb{E}[T_{\mathcal{C}_5}]$

Since the light grey parts of the power automaton in Figure 4.23 don't contribute to the value of $\mathbb{E}[T_\mathcal{A}]$, we don't draw the light grey parts of a power automaton anymore.

4.3.3 Lower bound of $R(n)$

The lower bound for $R(n)$ is done by construction. We look for a synchronizing automaton $\mathcal{A}$ with n states where $\mathbb{E}[T_\mathcal{A}]$, with $p = \frac{1}{2}$, is as large as possible. This gives us a lower bound on $R(n)$ by definition of $R(n)$ (Definition 4.33).

For the cases $n = 3, 4, 5$ we have seen which automaton has the largest value for $\mathbb{E}[T_\mathcal{A}]$. These automata all have similar structures. Let's look at two possible automata that continue this trend (Definition 4.49 and 4.50).

Definition 4.49. For $n \geq 4$ we define automaton $\mathcal{A}_1 = (\Sigma, Q, \delta)$ as follows.
$\Sigma = \{a, b\}$, $Q = \{1, \ldots, n\}$ and

$$\delta(q, a) = \begin{cases} n & \text{if } q = 1, 2 \\ q & \text{if } q = 3, \ldots, n-1 \\ 2 & \text{if } q = n \end{cases}$$

$$\delta(q, b) = \begin{cases} q+1 & \text{if } q = 1, 2, 4, \ldots, n-1 \\ 1 & \text{if } q = 3 \\ 4 & \text{if } q = n \end{cases}$$

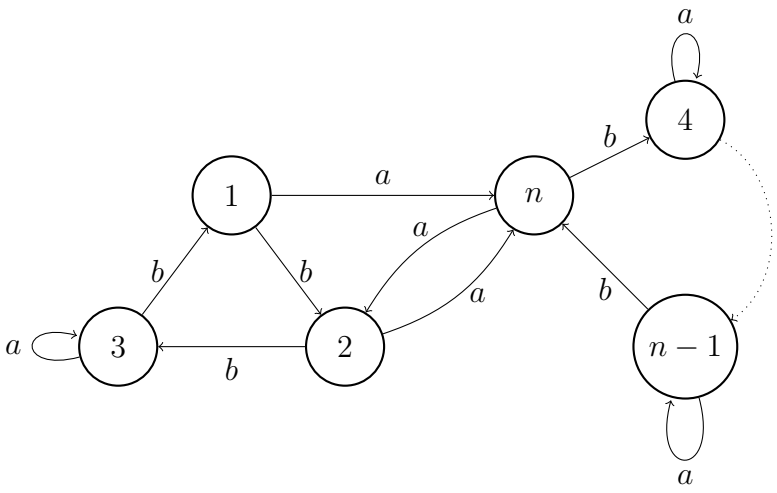

Figure 4.24: Automaton $\mathcal{A}_1$ (Definition 4.49 with $n \geq 4$ states and $\mathbb{P}(a) = p$, $\mathbb{P}(b) = 1 - p$.

Definition 4.50. For $n \geq 6$ we define automaton $\mathcal{A}_2 = (\Sigma, Q, \delta)$ as follows.
$\Sigma = \{a, b\}$, $Q = \{1, \ldots, n\}$ and

$$\delta(q, a) = \begin{cases} n & \text{if } q = 1, 2 \\ q & \text{if } q = 3, \ldots, n-1 \\ 2 & \text{if } q = n \end{cases}$$

$$\delta(q, b) = \begin{cases} q + 1 & \text{if } q = 1, 2, \ldots, \lfloor \frac{n}{2} \rfloor - 1, \lfloor \frac{n}{2} \rfloor + 1, \ldots, n-1 \\ 1 & \text{if } q = \lfloor \frac{n}{2} \rfloor \\ \lfloor \frac{n}{2} \rfloor + 1 & \text{if } q = n \end{cases}$$

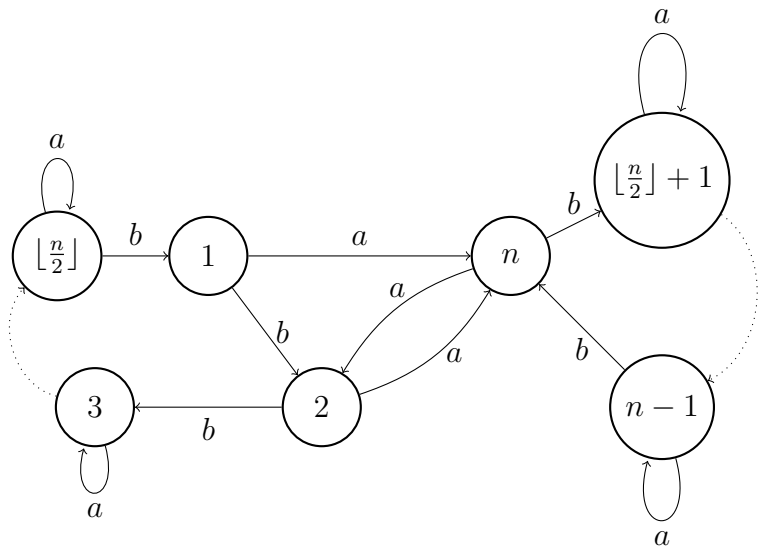

Figure 4.25: Automaton $\mathcal{A}_2$ (Definition 4.50) with $n \geq 6$ states and $\mathbb{P}(a) = p$, $\mathbb{P}(b) = 1 - p$.

With a Matlab program described in Appendix C.9 we can compare these two automata with $p = \frac{1}{2}$. Since we wondered whether $R(n)$ is determined by the Černý automaton $\mathcal{C}_n$, we immediately compare these automata to the Černý automaton $\mathcal{C}_n$.
The values of $\mathbb{E}[T_{\mathcal{A}_1}]$, $\mathbb{E}[T_{\mathcal{A}_2}]$ and $\mathbb{E}[T_{\mathcal{C}_n}]$ are calculated with system 1 (Subsection 4.2.1, Matlab program in Appendix C.5), rounded to one decimal. The results are given in Table 4.1.

n	$\mathbb{E}[T_{\mathcal{C}_n}]$	$\mathbb{E}[T_{\mathcal{A}_1}]$	$\mathbb{E}[T_{\mathcal{A}_2}]$
6	210	328.6	328.6
7	352	513.0	513.0
8	546	768.6	648.3
9	800	1068.0	898.3
10	1122	1401.2	1112.3

Table 4.1: Rounded values of $\mathbb{E}[T_{\mathcal{A}}]$ for automata $\mathcal{C}_n$, $\mathcal{A}_1$ and $\mathcal{A}_2$ with $p = \frac{1}{2}$.

From now on if we talk about the value $\mathbb{E}[T_{\mathcal{A}}]$, we talk about the value $\mathbb{E}[T_{\mathcal{A}}]$ for $p = \frac{1}{2}$ unless otherwise specified.

Note that for $n = 6$ and $n = 7$ the automata $\mathcal{A}_1$ and $\mathcal{A}_2$ are the same, so they have the same value for $\mathbb{E}[T_{\mathcal{A}}]$. We see that $\mathbb{E}[T_{\mathcal{A}_1}] > \mathbb{E}[T_{\mathcal{C}_n}]$ and $\mathbb{E}[T_{\mathcal{A}_2}] > \mathbb{E}[T_{\mathcal{C}_n}]$, for all $n = 6, \ldots, 9$. However, for $n = 10$ we have $\mathbb{E}[T_{\mathcal{A}_2}] < \mathbb{E}[T_{\mathcal{C}_n}]$ while we still have $\mathbb{E}[T_{\mathcal{A}_1}] > \mathbb{E}[T_{\mathcal{C}_n}]$.
Further, we see that $\mathbb{E}[T_{\mathcal{A}_1}] > \mathbb{E}[T_{\mathcal{A}_2}]$, for $n = 6, \ldots, 10$. Finally note that the growth rate of $\mathbb{E}[T_{\mathcal{A}_2}]$ is lower then the growth rate of $\mathbb{E}[T_{\mathcal{A}_1}]$. For instance from $n = 8$ to $n = 9$, the value $\mathbb{E}[T_{\mathcal{A}_1}]$ grows with factor 1.390, while the value $\mathbb{E}[T_{\mathcal{A}_2}]$ grows with factor 1.386.
This convinces us to say that for n large we have $\mathbb{E}[T_{\mathcal{A}_1}] > \mathbb{E}[T_{\mathcal{A}_2}]$. Since we are looking for the best possible lower bound, we can disregard automaton $\mathcal{A}_2$. We can't however disregard the Černý automaton $\mathcal{C}_n$ yet, since the growth rate of $\mathbb{E}[T_{\mathcal{C}_n}]$ is larger than that of $\mathbb{E}[T_{\mathcal{A}_1}]$. This means that for n large enough, it could be that $\mathbb{E}[T_{\mathcal{A}_1}] < \mathbb{E}[T_{\mathcal{C}_n}]$.

We want to find the best lower bound for $R(n)$. To find the synchronizing automaton $\mathcal{A}$, with largest value for $\mathbb{E}[T_{\mathcal{A}}]$, we have to look at more different automata.
When we were looking at the upper bound for $R(n)$, we used that in the worst case we had an automaton with as shortest reset word a repetition of only one letter (for example $w = bbbbbb$). Since we can always exchange the letter a and b, lets look at an automata with shortest reset words consisting of only the letter b.

Let's consider the following automaton.

Definition 4.51. Let $n \geq 2$. We define the following automaton $\mathcal{A}_3 = (\Sigma, Q, \delta)$. $\Sigma = \{a, b\}$, $Q = \{1, \ldots, n\}$ and the transition function is defined as follows.[9]

$$\delta(q, a) = \begin{cases} 1 & \text{if } q \text{ is odd} \\ 2 & \text{if } q \text{ is even} \end{cases} \text{ and } \delta(q, b) = \begin{cases} q+1 & \text{if } q = 1, \ldots, n-1 \\ n & \text{if } q = n \end{cases}$$

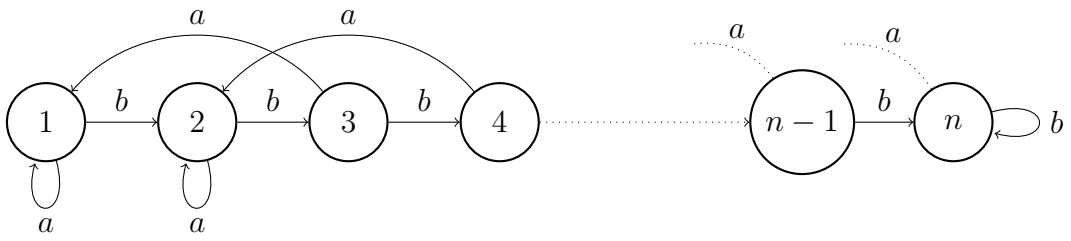

Figure 4.26: Automaton $\mathcal{A}_3$ (Definition 4.51) with n states and $\mathbb{P}(a) = p$, $\mathbb{P}(b) = 1 - p$.

The corresponding Powerautomaton $\mathcal{P}_{\mathcal{A}_3}$ is given in Figure 4.27.

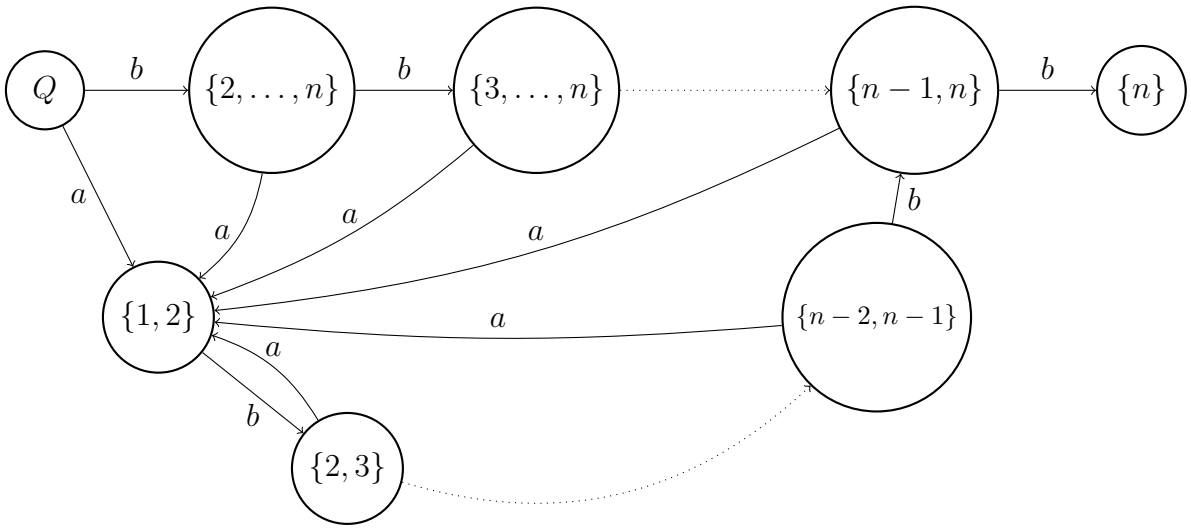

Figure 4.27: Powerautomaton of automaton $\mathcal{A}_3$ (Figure 4.26).

Remark. The shortest reset word of automaton $\mathcal{A}_3$ is $w = b^{n-1}$, because this is the shortest path from Q to a singleton (in this case $\{n\}$). The shortest reset word has length $n-1$, which is much smaller then the length of the shortest reset word of the Černý automaton $\mathcal{C}_n$ (which is $(n-1)^2$).

Proposition 4.52. *Let $p \in (0, 1)$, $\mathbb{P}(a) = p$ and $\mathbb{P}(b) = 1 - p$, then the following holds.*

$$\mathbb{E}[T_{\mathcal{A}_3}] = \frac{1}{p\,(1-p)^{n-1}} - \frac{1}{p}$$

Proof. We are going to calculate $\mathbb{E}[T_{\mathcal{A}_3}]$ with system 1 (Subsection 4.2.1), so we are going to calculate E^A_Q. First we have the following equations.

$$\begin{aligned}
E^A_Q &= 1 + pE^A_{\{1,2\}} + (1-p)\, E^A_{\{2,\dots,n\}} \\
E^A_{\{2,\dots,n\}} &= 1 + pE^A_{\{1,2\}} + (1-p)\, E^A_{\{3,\dots,n\}} \\
E^A_{\{3,\dots,n\}} &= 1 + pE^A_{\{1,2\}} + (1-p)\, E^A_{\{4,\dots,n\}} \\
&\vdots \\
E^A_{\{n-2,\dots,n\}} &= 1 + pE^A_{\{1,2\}} + (1-p)\, E^A_{\{n-1,n\}} \\
E^A_{\{n-1,n\}} &= 1 + pE^A_{\{1,2\}} + (1-p)\, E^A_{\{n\}} = 1 + pE^A_{\{1,2\}}
\end{aligned}$$

With these equation we can express E^A_Q in terms of p and $E^A_{\{1,2\}}$. Here we use the fact that $\sum_{j=1}^{n} a^j = \frac{a^{n+1}-a}{a-1}$ (for $a \neq 1$).

$$\begin{aligned}
E^A_Q =& 1 + pE^A_{\{1,2\}} + (1-p)\, E^A_{\{2,\dots,n\}} \\
=& 1 + pE^A_{\{1,2\}} + (1-p)\left(1 + pE^A_{\{1,2\}} + (1-p)\, E^A_{\{3,\dots,n\}}\right) \\
=& 1 + (1-p) + p\left(1 + (1-p)\right) E^A_{\{1,2\}} + (1-p)^2\, E^A_{\{3,\dots,n\}} \\
=& 1 + (1-p) + p\left(1 + (1-p)\right) E^A_{\{1,2\}} + (1-p)^2 \left(1 + pE^A_{\{1,2\}} + (1-p)\, E^A_{\{4,\dots,n\}}\right) \\
=& 1 + (1-p) + (1-p)^2 + p\left(1 + (1-p) + (1-p)^2\right) E^A_{\{1,2\}} + (1-p)^3\, E^A_{\{4,\dots,n\}} \\
&\vdots \\
=& 1 + (1-p) + \cdots + (1-p)^{n-3} + p\left(1 + (1-p) + \cdots + (1-p)^{n-3}\right) E^A_{\{1,2\}} \\
&+ (1-p)^{n-2}\, E^A_{\{n-1,n\}} \\
=& 1 + (1-p) + \cdots + (1-p)^{n-3} + p\left(1 + (1-p) + \cdots + (1-p)^{n-3}\right) E^A_{\{1,2\}} \\
&+ (1-p)^{n-2}\left(1 + pE^A_{\{1,2\}}\right) \\
=& 1 + (1-p) + \cdots + (1-p)^{n-2} + p\left(1 + (1-p) + \cdots + (1-p)^{n-2}\right) E^A_{\{1,2\}} \\
=& \sum_{j=0}^{n-2} (1-p)^j + p\left(\sum_{j=0}^{n-2} (1-p)^j\right) E^A_{\{1,2\}} \\
=& \frac{1-(1-p)^{n-1}}{p} + p\left(\frac{1-(1-p)^{n-1}}{p}\right) E^A_{\{1,2\}} \\
=& \frac{1-(1-p)^{n-1}}{p} + \left(1-(1-p)^{n-1}\right) E^A_{\{1,2\}}
\end{aligned}$$

Now we need to calculate $E^A_{\{1,2\}}$. This we do with the rest of the equation according to system 1.

$$
\begin{aligned}
E^A_{\{1,2\}} &= 1 + pE^A_{\{1,2\}} + (1-p)\, E^A_{\{2,3\}} \\
E^A_{\{2,3\}} &= 1 + pE^A_{\{1,2\}} + (1-p)\, E^A_{\{3,4\}} \\
E^A_{\{3,4\}} &= 1 + pE^A_{\{1,2\}} + (1-p)\, E^A_{\{4,5\}} \\
&\vdots \\
E^A_{\{n-2,n-1\}} &= 1 + pE^A_{\{1,2\}} + (1-p)\, E^A_{\{n-1,n\}} \\
E^A_{\{n-1,n\}} &= 1 + pE^A_{\{1,2\}} + (1-p)\, E^A_{\{n\}} = 1 + pE^A_{\{1,2\}}
\end{aligned}
$$

Analogue to the calculations for E^A_Q we get the following.

$$
\begin{aligned}
E^A_{\{1,2\}} =& 1 + pE^A_{\{1,2\}} + (1-p)\, E^A_{\{2,3\}} \\
=& 1 + pE^A_{\{1,2\}} + (1-p)\left(1 + pE^A_{\{1,2\}} + (1-p)\, E^A_{\{3,4\}}\right) \\
=& 1 + (1-p) + p\,(1 + (1-p))\, E^A_{\{1,2\}} + (1-p)^2\, E^A_{\{3,4\}} \\
&\vdots \\
=& 1 + (1-p) + \cdots + (1-p)^{n-2} + p\left(1 + (1-p) + \cdots + (1-p)^{n-2}\right) E^A_{\{1,2\}} \\
=& \sum_{j=0}^{n-2} (1-p)^j + p\left(\sum_{j=0}^{n-2} (1-p)^j\right) E^A_{\{1,2\}} \\
=& \frac{1-(1-p)^{n-1}}{p} + p\left(\frac{1-(1-p)^{n-1}}{p}\right) E^A_{\{1,2\}} \\
=& \frac{1-(1-p)^{n-1}}{p} + \left(1-(1-p)^{n-1}\right) E^A_{\{1,2\}}
\end{aligned}
$$

With this we can calculate $E^A_{\{1,2\}}$, which we can then substitute in the equation for E^A_Q.

$$
\begin{aligned}
\left(1 - \left(1-(1-p)^{n-1}\right)\right) E^A_{\{1,2\}} =& \frac{1-(1-p)^{n-1}}{p} \\
(1-p)^{n-1}\, E^A_{\{1,2\}} =& \frac{1-(1-p)^{n-1}}{p} \\
E^A_{\{1,2\}} =& \frac{1-(1-p)^{n-1}}{p\,(1-p)^{n-1}} = \frac{1}{p\,(1-p)^{n-1}} - \frac{1}{p}
\end{aligned}
$$

$$
\begin{aligned}
E_Q^A =& \frac{1-(1-p)^{n-1}}{p} + \left(1-(1-p)^{n-1}\right) E_{\{1,2\}}^A \\
=& \frac{1-(1-p)^{n-1}}{p} + \left(1-(1-p)^{n-1}\right) \left(\frac{1-(1-p)^{n-1}}{p\,(1-p)^{n-1}}\right) \\
=& \frac{(1-p)^{n-1}\left(1-(1-p)^{n-1}\right)}{p\,(1-p)^{n-1}} + \frac{\left(1-(1-p)^{n-1}\right)^2}{p\,(1-p)^{n-1}} \\
=& \frac{1-(1-p)^{n-1}}{p\,(1-p)^{n-1}} = \frac{1}{p\,(1-p)^{n-1}} - \frac{1}{p}
\end{aligned}
$$

□

Remark. For $p = \frac{1}{2}$, proving that $\mathbb{E}[T_{\mathcal{A}_3}] = 2^n - 2$ is much easier. We know that $w \in \Sigma^*$ is a reset word for automaton $\mathcal{A}_3$ if and only if b^{n-1} is a subword of w. This implies that $\mathbb{E}[T_{\mathcal{A}_3}] = \mathbb{E}[t_{b^{n-1}}]$. Lemma 4.38 then gives our wanted result.

$$
\begin{aligned}
\mathbb{E}[T_{\mathcal{A}_3}] &= \mathbb{E}[t_{b^{n-1}}] \\
&= \sum_{i=1}^{n-1} 2^i \\
&= \frac{2^n - 2}{2-1} = 2^n - 2
\end{aligned}
$$

Comparing automata $\mathcal{A}_1$, $\mathcal{A}_3$ and $\mathcal{C}_n$ with the Matlab program described in Appendix C.9 gives us the results in Table 4.2.

n	$\mathbb{E}[T_{\mathcal{C}_n}]$	$\mathbb{E}[T_{\mathcal{A}_1}]$	$\mathbb{E}[T_{\mathcal{A}_3}]$
6	210	328.6	62
7	352	513.0	126
8	546	768.6	254
9	800	1068.0	510
10	1122	1401.2	1022

Table 4.2: Rounded values of $\mathbb{E}[T_{\mathcal{A}}]$ for automata $\mathcal{C}_n$, $\mathcal{A}_1$ and $\mathcal{A}_3$ with $p = \frac{1}{2}$.

Table 4.2 indicates that automaton $\mathcal{A}_3$ probably gives a better lower bound than $\mathcal{C}_n$. But there are more automata with shortest reset words, which consist mostly out of one letter. Let's take a look at the following automaton.

Definition 4.53. Let $n \geq 2$. We define the following automaton $\mathcal{A}_4 = (\Sigma, Q, \delta)$. $\Sigma = \{a, b\}$, $Q = \{1, \ldots, n\}$ and the transition function is defined as follows.[11]

$$
\delta(q,a) = \begin{cases} 1 & \text{if } q \text{ is odd} \\ 2 & \text{if } q \text{ is even} \end{cases} \text{ and } \delta(q,b) = \begin{cases} q+1 & \text{if } q = 1, \ldots, n-1 \\ 1 & \text{if } q = n \end{cases}
$$

Remark. Automaton $\mathcal{A}_4$ is only synchronizing if n is odd. If n would be even, then there is no path from Q to A. This can be seen in the Power automaton $\mathcal{P}_{\mathcal{A}_4}$ with n even (Figure 4.28).

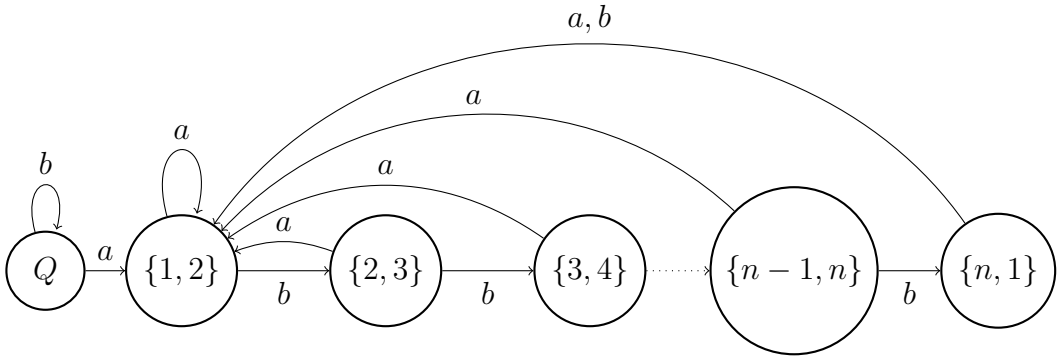

Figure 4.28: Powerautomaton of automaton $\mathcal{A}_4$ with n even

Let's assume that n is odd. Then automaton $\mathcal{A}_4$ is given in Figure 4.29, and the corresponding power automaton $\mathcal{P}_{\mathcal{A}_4}$ is given in Figure 4.30.

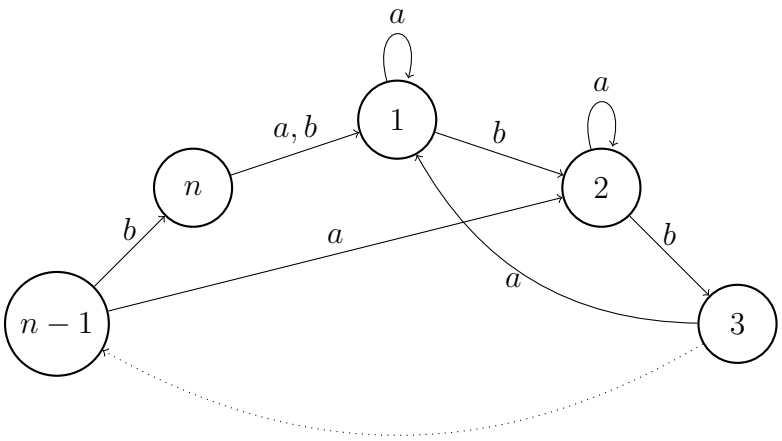

Figure 4.29: Automaton $\mathcal{A}_4$ (Definition 4.53) with n (odd) states and $\mathbb{P}(a) = p$, $\mathbb{P}(b) = 1 - p$.

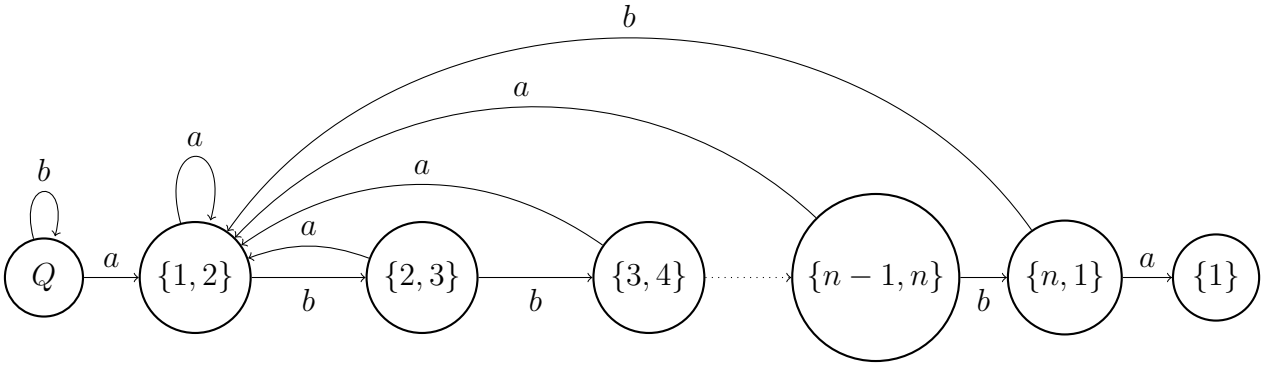

Figure 4.30: Powerautomaton of automaton $\mathcal{A}_4$ with n odd (Figure 4.29)

Remark. The shortest reset word of automaton $\mathcal{A}_4$ is $v = ab^{n-1}a$, because this is the shortest path from Q to a singleton (in this case $\{1\}$).
The length of this word is $|v| = n+1 > n-1 = |b^{n-1}|$, which is again much smaller then $(n-1)^2$ (the length of the shortest reset word of the Černý automaton $\mathcal{C}_n$).
The length of this word is larger than the length of the shortest reset word of automaton $\mathcal{A}_3$.

Proposition 4.54. *Let $n \geq 3$ be an odd integer, $p \in (0,1)$, $\mathbb{P}(a) = p$ and $\mathbb{P}(b) = 1-p$, then the following holds.*

$$\mathbb{E}[T_{\mathcal{A}_4}] = \frac{1}{p} + \frac{1}{p(1-p)^{n-1}} + \frac{1-(1-p)^{n-1}}{p^2(1-p)^{n-2}} = \frac{(1-p)^{n-1}(2p-1)+1}{p^2(1-p)^{n-1}}$$

Proof. We are going to calculate $\mathbb{E}[T_{\mathcal{A}_4}]$ with system 1 (Subsection 4.2.1), so we are going to calculate E_Q^A. We have the following equations.

$$\begin{aligned}
E_Q^A &= 1 + pE_{\{1,2\}}^A + (1-p)\,E_Q^A \\
E_{\{1,2\}}^A &= 1 + pE_{\{1,2\}}^A + (1-p)\,E_{\{2,3\}}^A \\
E_{\{2,3\}}^A &= 1 + pE_{\{1,2\}}^A + (1-p)\,E_{\{3,4\}}^A \\
&\vdots \\
E_{\{n-1,n\}}^A &= 1 + pE_{\{1,2\}}^A + (1-p)\,E_{\{n,1\}}^A \\
E_{\{n,1\}}^A &= 1 + pE_{\{1\}}^A + (1-p)\,E_{\{1,2\}}^A = 1 + (1-p)\,E_{\{1,2\}}^A
\end{aligned}$$

We calculate E_Q^A in the same way as in the proof of Proposition 4.52. First we calculate $E_{\{1,2\}}^A$.

$$\begin{aligned}
E_{\{1,2\}}^A =& 1 + pE_{\{1,2\}}^A + (1-p)\,E_{\{2,3\}}^A \\
=& 1 + pE_{\{1,2\}}^A + (1-p)\left(1 + pE_{\{1,2\}}^A + (1-p)\,E_{\{3,4\}}^A\right) \\
=& 1 + (1-p) + p\,(1+(1-p))\,E_{\{1,2\}}^A + (1-p)^2\,E_{\{3,4\}}^A \\
&\vdots \\
=& 1 + (1-p) + \cdots + (1-p)^{n-2} + p\left(1 + (1-p) + \cdots + (1-p)^{n-2}\right)E_{\{1,2\}}^A \\
&+ (1-p)^{n-1}\,E_{\{n,1\}}^A \\
=& 1 + (1-p) + \cdots + (1-p)^{n-2} + p\left(1 + (1-p) + \cdots + (1-p)^{n-2}\right)E_{\{1,2\}}^A \\
&+ (1-p)^{n-1}\left(1 + (1-p)\,E_{\{1,2\}}^A\right) \\
=& 1 + (1-p) + \cdots + (1-p)^{n-1} + p\left(1 + (1-p) + \cdots + (1-p)^{n-2}\right)E_{\{1,2\}}^A \\
&+ (1-p)^n\,E_{\{1,2\}}^A \\
=& \sum_{j=0}^{n-1}(1-p)^j + p\left(\sum_{j=0}^{n-2}(1-p)^j\right)E_{\{1,2\}}^A + (1-p)^n\,E_{\{1,2\}}^A
\end{aligned}$$

$$
\begin{aligned}
&= \frac{(1-p)^n - (1-p)}{1-p-1} + 1 + p\left(\frac{(1-p)^{n-1} - (1-p)}{1-p-1} + 1\right) E^A_{\{1,2\}} + (1-p)^n E^A_{\{1,2\}} \\
&= \frac{(1-p) - (1-p)^n}{p} + 1 + \left((1-p) - (1-p)^{n-1} + p\right) E^A_{\{1,2\}} + (1-p)^n E^A_{\{1,2\}}
\end{aligned}
$$

$$
\begin{aligned}
\left(1 - \left((1-p) - (1-p)^{n-1} + p\right) - (1-p)^n\right) E^A_{\{1,2\}} &= \frac{(1-p) - (1-p)^n}{p} + 1 \\
\left(1 - (1-p) + (1-p)^{n-1} - p - (1-p)^n\right) &= \frac{(1-p) - (1-p)^n}{p} + 1 \\
\left((1-p)^{n-1} - (1-p)^n\right) E^A_{\{1,2\}} &= \frac{(1-p) - (1-p)^n}{p} + 1 \\
(1-p)^{n-1} p E^A_{\{1,2\}} &= \frac{(1-p) - (1-p)^n}{p} + 1 \\
E^A_{\{1,2\}} &= \frac{(1-p) - (1-p)^n}{p^2 (1-p)^{n-1}} + \frac{1}{p (1-p)^{n-1}} \\
&= \frac{1 - (1-p)^{n-1}}{p^2 (1-p)^{n-2}} + \frac{1}{p (1-p)^{n-1}}
\end{aligned}
$$

With this we can calculate E^A_Q as follows.

$$
\begin{aligned}
E^A_Q &= 1 + p E^A_{\{1,2\}} + (1-p) E^A_Q \\
(1 - (1-p)) E^A_Q &= 1 + p E^A_{\{1,2\}} \\
p E^A_Q &= 1 + p E^A_{\{1,2\}} \\
E^A_Q &= \frac{1}{p} + E^A_{\{1,2\}} \\
&= \frac{1}{p} + \frac{1 - (1-p)^{n-1}}{p^2 (1-p)^{n-2}} + \frac{1}{p (1-p)^{n-1}} \\
&= \frac{p (1-p)^{n-1} + p + (1-p)\left(1 - (1-p)^{n-1}\right)}{p^2 (1-p)^{n-1}} \\
&= \frac{(1-p)^{n-1} (p - (1-p)) + 1}{p^2 (1-p)^{n-1}} \\
&= \frac{(1-p)^{n-1} (2p-1) + 1}{p^2 (1-p)^{n-1}}
\end{aligned}
$$

□

As shown automaton $\mathcal{A}_4$ isn't synchronizing for n even. So If we want to use this automaton construction for a lower bound, we have to find some other bound for when n is even.
By definition of $R(n)$, we know that $R(n)$ increases as n increases. If n is odd, then we have $R(n) \geq 2^{n+1}$ ($\mathbb{E}[T_{\mathcal{A}_4}] = 2^{n+1}$ for $p = \frac{1}{2}$ and n states). If n is even, then $R(n) \geq R(n-1) \geq 2^n$ ($\mathbb{E}[T_{\mathcal{A}_4}] = 2^n$ for $p = \frac{1}{2}$ and $n-1$ states). This is the motivation for the following definition.

Definition 4.55. Let $n \geq 3$ the number of states and $p \in (0,1)$. We define the following function.

$$l(n,p) = \begin{cases} \frac{(1-p)^{n-1}(2p-1)+1}{p^2(1-p)^{n-1}} & \text{if } n \text{ odd} \\ \frac{(1-p)^{n-2}(2p-1)+1}{p^2(1-p)^{n-2}} & \text{if } n \text{ even} \end{cases}$$

We define $L(n) := l(n, \frac{1}{2}) = \begin{cases} 2^{n+1} & \text{if } n \text{ odd} \\ 2^n & \text{if } n \text{ even} \end{cases}$.
With $\mathcal{A}(n)$ we refer to automaton $\mathcal{A}$ with n states.

Lemma 4.56. *let $n \geq 3$ be an integer and $p = \frac{1}{2}$. Then the following holds.*

$$\mathbb{E}[T_{\mathcal{A}_3(n)}] < L(n)$$

Proof. We know that for $p = \frac{1}{2}$ we have $\mathbb{E}[T_{\mathcal{A}_3(n)}] = 2^n - 2$.
Since $2^{n+1} > 2^n > 2^n - 2$ holds for all $n \geq 3$, we have that $L(n) > \mathbb{E}[T_{\mathcal{A}_3(n)}]$ for all $n \geq 3$, by definition 4.55. □

Lemma 4.56 shows us that $L(n)$ gives a better lower bound then $\mathbb{E}[T_{\mathcal{A}_3}]$.
This leads to the question whether $\mathbb{E}[T_{\mathcal{C}_n}]$, $\mathbb{E}[T_{\mathcal{A}_1(n)}]$ or $L(n)$ gives a better lower found for $R(n)$.

Calculating $\mathbb{E}[T_{\mathcal{A}_1}]$ exactly for $p = \frac{1}{2}$ is more complicated then calculating $L(n)$ or $\mathbb{E}[T_{\mathcal{C}_n}]$. This is because for $L(n)$ and $\mathbb{E}[T_{\mathcal{C}_n}]$ we have exact values by Definition 4.55 and Theorem 4.15, but we don't have this for $\mathbb{E}[T_{\mathcal{A}_1}]$. Besides, the power automaton of automaton $\mathcal{A}_1$ isn't structured like we had with automata $\mathcal{A}_3$ and $\mathcal{A}_4$.

We take $p = \frac{1}{2}$. For $n = 3, \ldots, 10$ our Matlab program of system 1 (Subsection 4.2.1, Matlab program in Appendix C.5) can still calculate $\mathbb{E}[T_{\mathcal{A}_1(n)}]$ exactly. However, for $n \geq 11$ the numbers become inconveniently large. To still be able to give a value for $\mathbb{E}[T_{\mathcal{A}_1(n)}]$ with $n \geq 11$ we approximate $\mathbb{E}[T_{\mathcal{A}_1(n)}]$ with the use of some simulations.

For $n = 11, 12, 13$, we simulate random words ($\mathbb{P}(a) = \mathbb{P}(b) = \frac{1}{2}$). We start with a one letter word and check whether it is a reset word or not. If not, then we add a letter to the word and check again whether it is a reset word or not. And so on, we stop when our random simulated word is a reset word. We store the length of this word and start over. This we do 100 times (we have 100 samples). In the end we take the mean of the stored lengths, that is our approximated value of $\mathbb{E}[T_{\mathcal{A}_1}]$.
With this we get the results in Table 4.3.

n	$\mathbb{E}[T_{\mathcal{C}_n}]$	$\mathbb{E}[T_{\mathcal{A}_1}]$ ($n = 11, 12, 13$ approximations)	$L(n)$
6	210	328.6	64
7	352	513.0	256
8	546	768.6	256
9	800	1068.0	1024
10	1122	1401.2	1024
11	1520	1774	4096
12	2002	2216	4096
13	2576	2753	16384

Table 4.3: Values (rounded) of $\mathbb{E}[T_{\mathcal{C}_n}]$, $\mathbb{E}[T_{\mathcal{A}_1}]$ and $L(n)$ with $p = \frac{1}{2}$.

This gives us a good indication that for n large ($n \geq 11$), $L(n)$ gives a better lower bound. We also see that for $4 \leq n \leq 10$, $\mathbb{E}[T_{\mathcal{A}_1}]$ gives a better lower bound then $L(n)$.
In Subsection 4.3.2, we have even seen that automaton $\mathcal{A}_1$ gives the largest value of $\mathbb{E}[T_{\mathcal{A}}]$ for $n = 4$ and $n = 5$.
However, for $n = 2$ and $n = 3$, we have seen that $\mathbb{E}[T_{\mathcal{C}_n}]$ gives the largest value of $\mathbb{E}[T_{\mathcal{A}}]$.

Theorem 4.57. *Let $n \geq 11$ be an integer and $p = \frac{1}{2}$. Then we have the following.*

$$L(n) \leq R(n)$$

Proof. The proof follows directly from the definitions of $R(n)$ (Definition 4.33), automaton $\mathcal{A}_4$ (Definition 4.53) and $L(n)$ (Definition 4.55). □

This all together gives that for $n \geq 11$ Theorem 4.57 gives the best lower bound we have found so far. This is shown by all the comparisons between different automata and lower bounds we have performed. There could be an automaton, which we haven't looked at yet, that gives an even better lower bound. A way to determine the absolute best lower bound for $R(n)$ is by checking all possible synchronizing automata. We have experienced that, even for $n = 5$, this takes a long time, since there are so many different synchronizing automata, even if you remove all isomorphic automata. Thus, for synchronizing automata with $n \geq 11$ states, this is a really expensive option.

Chapter 5

Conclusion

This thesis is all about synchronizing automata $\mathcal{A} = (Q, \Sigma, \delta)$ and the (expected) length of their reset words. We mostly used $Q = \{1, \ldots, n\}$ and $\Sigma = \{a, b\}$. For all these synchronizing automata $\mathcal{A}$, we explored what we could say about the length of the largest shortest reset word ($C(n)$) and the largest value of the expected length of a reset word ($R(n)$).

We defined $C(n)$ to be the length of the largest shortest reset word, considering all synchronizing automata $\mathcal{A}$ with n states.
Černý's conjecture, stating $C(n) = (n-1)^2$, is still a conjecture. The shortest reset word for the Černý automata $\mathcal{C}_n$ is of length $(n-1)^2$. With this we proved that $C(n) \geq (n-1)^2$ holds. However proving $C(n) \leq (n-1)^2$ has not been accomplished. We did improve the upper bound found by J.-E Pin and P. Frankl (1982), stating $C(n) \leq \frac{n^3-n}{6}$. This we did by looking at the work of Marek Szykuła. Marek Szykuła was able to improve the upper bound of J.-E Pin and P. Frankl by the factor $\frac{85059}{85184}$. We succeeded in proving that the upper bound, found by J.-E Pin and P. Frankl, could be improved by the factor 0.998528004. This is a slightly better result than Marek Szykuła had found (See Theorem 3.29). Thus we can conclude the following.

$$(n-1)^2 \leq C(n) \leq 0.166421334n^3 + 1.42781363n^2 - 0.210099161n$$

For a synchronizing automaton we considered the situation that, instead of fixed letters, we have a probability distribution on the letters in our alphabet ($\mathbb{P}(a) = p$, $\mathbb{P}(b) = 1-p$, with $p \in [0, 1]$). We could identify automata with a probability distribution on the letters with a Markov chain and used this to calculate the expected length of a reset word of a certain automaton. We denoted the expected length of a reset word for a synchronizing automaton $\mathcal{A}$, with $\mathbb{E}[T_{\mathcal{A}}]$.
For the Černý automata $\mathcal{C}_n$, which proved that $C(n) \geq (n-1)^2$, we calculated the expected length of a reset word $\mathbb{E}[T_{\mathcal{C}_n}]$. For $\mathbb{P}(a) = p$, $\mathbb{P}(b) = 1-p$, with $p \in (0, 1)$, Theorem 4.15 showed us the following.

$$\mathbb{E}[T_{\mathcal{C}_n}] = \frac{(n-1)p^2 - \left(\sum_{i=2}^{n} i\right)p + \binom{n+1}{n-2}}{p(1-p)^2}$$

In section 4.3 we looked beyond the Černý automata $\mathcal{C}_n$. We researched the value of $R(n)$, by considering all synchronizing automata $\mathcal{A}$ with n states and searching for the maximal value of $\mathbb{E}[T_{\mathcal{A}}]$ with $p = \frac{1}{2}$. We have determined that $R(2) = 2$, $R(3) = 16$, $R(4) = 67$ and $R(5) = \frac{1170}{7}$. In the case $n = 4$, we discovered that $R(n)$ wasn't determined by the Černý automaton $\mathcal{C}_n$ (the value $\mathbb{E}[T_{\mathcal{C}_n}]$). In the case $n = 5$, we saw for the first time that the automaton with the largest value for $\mathbb{E}[T_{\mathcal{A}}]$ wasn't the automaton with the largest shortest reset word.
For $n \geq 6$ we looked at a lower and upper bound for $R(n)$. As upper bound we found that $R(n) \leq (n-1)\,2^{\binom{n}{2}+1} - 2 = 2^{\frac{1}{2}n^2+o(n)}$. For the lower bound we looked at different automata. With the use of automata $\mathcal{A}_4$ (Definition 4.53) we defined

$$L(n) = \begin{cases} 2^{n+1} & \text{if } n \text{ odd} \\ 2^n & \text{if } n \text{ even} \end{cases}.$$

For $n \geq 11$ the best lower bound found at the present time is $R(n) \geq L(n)$. However for $6 \leq n \leq 10$, we saw that the value $\mathbb{E}[T_{\mathcal{A}_1}]$ (automaton $\mathcal{A}_1$, defined in Definition 4.49) gave a better lower bound for $R(n)$.
Thus we can conclude that $R(n)$ isn't determined by the Černý automata $\mathcal{C}_n$ ($R(n) \neq \mathbb{E}[T_{\mathcal{C}_n}]$ for all $n \geq 4$). We know that the synchronizing automaton $\mathcal{A}$ which determines $R(n)$ ($R(n) = \mathbb{E}[T_{\mathcal{A}}]$), could have a largest shortest reset word $w \in \Sigma^*$ with $|w| < (n-1)^2$. In addition, we have the following results about the upper and lower bound of $R(n)$.
For $6 \leq n \leq 10$ we have

$$\mathbb{E}[T_{\mathcal{A}_1}] \leq R(n) \leq (n-1)\,2^{\binom{n}{2}+1} - 2 = 2^{\frac{1}{2}n^2+o(n)}$$

For $n \geq 11$ we have

$$L(n) \leq R(n) \leq (n-1)\,2^{\binom{n}{2}+1} - 2 = 2^{\frac{1}{2}n^2+o(n)}$$

Chapter 6

Further research

We have done a lot of research in this thesis about synchronizing automata and the (expected) length of their reset words, but there are many more interesting facets to explore in this subject. Below we mention some of the options for further research.

As stated in the conclusion, Černý's conjecture, stating $C(n) = (n-1)^2$, is still a conjecture. Therefore, the next steps in further research would be to prove or contradict Černý's conjecture. This can be achieved by further improving the upper bound of $C(n)$ until you get $C(n) \leq (n-1)^2$ or by finding a synchronizing automaton which has a shortest reset word $w \in \Sigma^*$ with $|w| > (n-1)^2$.

In the case that we have the probability distribution, $\mathbb{P}(a) = \mathbb{P}(b) = \frac{1}{2}$, on the letters of our alphabet, we saw that we could bound $R(n)$. These bounds (upper and lower bound) can perhaps be improved. For the lower bound we could for instance view even more different synchronizing automata. Perhaps this way, we can find an automaton $\mathcal{A}$ for which the value $\mathbb{E}[T_{\mathcal{A}}]$ gives a better lower bound for $R(n)$, than the one we currently have. In this thesis we used some Matlab programs to research the value of $R(n)$. These programs can be made more efficient by for example a more selective search (for instance, only check the synchronizing automata which probably have a high value of $\mathbb{E}[T_{\mathcal{A}}]$), or using simulations instead of using system 1 to calculate $\mathbb{E}[T_{\mathcal{A}}]$. In further research it is also possible to look at the value of $R(n)$ but then for a different value for $p \in [0,1]$ or for p as a variable.

In this thesis we researched the two extreme cases, either all letters were fixed or all letter were random (with probability distribution). In further research we could look at the expected length of a reset word in which $m \in \mathbb{N}$ letters are random and the rest of the letters fixed. What could we say about the expected length of a reset word if we don't know the placements of those m random letters? What could we say if we do know the placements of those m random letters?

In this thesis we mostly used $\Sigma = \{a, b\}$. In further research we could examine how much influence the size of our alphabet has on the expected length of a reset word, for a synchronizing automaton $\mathcal{A}$.

Bibliography

[1] Peter Frankl. "An extremal problem for two families of sets". In: *European Journal of Combinatorics* 3.2 (1982), pp. 125–127.

[2] David Eppstein. "Reset sequences for monotonic automata". In: *SIAM Journal on Computing* 19.3 (1990), pp. 500–510.

[3] Igor Rystsov. "Reset words for commutative and solvable automata". In: *Theoretical Computer Science* 172.1-2 (1997), pp. 273–279.

[4] Mikhail V Volkov. "Synchronizing automata and the Černý conjecture". In: *International conference on language and automata theory and applications*. Springer. 2008, pp. 11–27.

[5] Alexandra Silva. "Languages and Automata, Lecture notes". 2013.

[6] Vladimir V Gusev. "Synchronizing automata with random inputs". In: *International Conference on Developments in Language Theory*. Springer. 2014, pp. 68–75.

[7] Dmitry Ananichev. "A new lower bound for reset threshold of synchronizing automata with sink state". In: *arXiv preprint arXiv:1701.07954* (2017).

[8] Marek Szykuła. "Improving the upper bound on the length of the shortest reset words". In: *arXiv preprint arXiv:1702.05455* (2017).

[9] Anouk Jansen. "Bachelorscriptie wiskunde: Synchroniserende automaten". 2019.

[10] Laura Scarabosio. "Monte Carlo Methods, Lecture notes". 2021.

[11] Henk Don. "personal communication". 2021-2022.

Appendix A

Proofs of propositions and lemmas, needed for proving Theorem 4.15

A.1 Proof of Lemma 4.24

Proof. The proof goes by induction to m.
The base case: $m = 1$.
Because of Equation 4.4 we have the following.

$$\begin{aligned}\mathbb{P}(E_{n,n-1}) &= p \cdot \mathbb{P}(E_{1,n-1}) + (1-p) \cdot \mathbb{P}(E_{1,n}) \\ &= p \cdot \mathbb{P}(E_{1,n-1}) + (1-p)^2 \cdot \mathbb{P}(E_{2,1})\end{aligned}$$

We can calculate $\mathbb{P}(E_{1,n-1})$ as follows.

$$\begin{aligned}\mathbb{P}(E_{1,n-1}) &= p \cdot \mathbb{P}(E_{1,n-1}) + (1-p)\,\mathbb{P}(E_{2,n}) \\ (1-p)\,\mathbb{P}(E_{1,n-1}) &= (1-p)\,\mathbb{P}(E_{2,n}) \\ \mathbb{P}(E_{1,n-1}) &= \mathbb{P}(E_{2,n}) \\ &= p \cdot \mathbb{P}(E_{2,1}) + (1-p) \cdot \mathbb{P}(E_{3,1})\end{aligned}$$

We can see the following about $\mathbb{P}(E_{3,1})$.

$$\begin{aligned}\mathbb{P}(E_{3,1}) &= p \cdot \mathbb{P}(E_{3,1}) + (1-p) \cdot \mathbb{P}(E_{4,2}) \\ (1-p)\,\mathbb{P}(E_{3,1}) &= (1-p)\,\mathbb{P}(E_{4,2}) \\ \mathbb{P}(E_{3,1}) &= \mathbb{P}(E_{4,2}) \\ &= \cdots = \mathbb{P}(E_{n,n-2})\end{aligned}$$

An analogue calculation can be done for $\mathbb{P}(E_{2,1})$, which gives us the following result.

$$\mathbb{P}(E_{2,1}) = \mathbb{P}(E_{n,n-1})$$

Combining all found equations gives us:

$$\begin{aligned}
\mathbb{P}(E_{n,n-1}) &= p \cdot \mathbb{P}(E_{1,n-1}) + (1-p)^2 \cdot \mathbb{P}(E_{2,1}) \\
&= p \cdot (p \cdot \mathbb{P}(E_{2,1}) + (1-p) \cdot \mathbb{P}(E_{3,1})) + (1-p)^2 \cdot \mathbb{P}(E_{2,1}) \\
&= p \cdot (p \cdot \mathbb{P}(E_{n,n-1}) + (1-p) \cdot \mathbb{P}(E_{n,n-2})) + (1-p)^2 \cdot \mathbb{P}(E_{n,n-1}) \\
&= p^2 \cdot \mathbb{P}(E_{n,n-1}) + p(1-p) \cdot \mathbb{P}(E_{n,n-2}) + (1-p)^2 \cdot \mathbb{P}(E_{n,n-1}) \\
\left(1 - p^2 - (1-p)^2\right) \mathbb{P}(E_{n,n-1}) &= p(1-p)\,\mathbb{P}(E_{n,n-2}) \\
2p(1-p)\,\mathbb{P}(E_{n,n-1}) &= p(1-p)\,\mathbb{P}(E_{n,n-2}) \\
\mathbb{P}(E_{n,n-1}) &= \frac{1}{2}\mathbb{P}(E_{n,n-2})
\end{aligned}$$

Therefore, for $m = 1$ the lemma is correct.

For the induction step, we have the following induction hypothesis.
$\mathbb{P}(E_{n,n-m}) = \frac{m}{m+1}\mathbb{P}\left(E_{n,n-(m+1)}\right)$ holds for some $m \in \{1, \ldots, n-2\}$.
Now we want to prove that this also holds for $m+1$.

$$\mathbb{P}\left(E_{n,n-(m+1)}\right) = p \cdot \mathbb{P}\left(E_{1,n-(m+1)}\right) + (1-p) \cdot \mathbb{P}(E_{1,n-m})$$

We can calculate $\mathbb{P}\left(E_{1,n-(m+1)}\right)$ as follows.

$$\begin{aligned}
\mathbb{P}\left(E_{1,n-(m+1)}\right) &= p \cdot \mathbb{P}\left(E_{1,n-(m+1)}\right) + (1-p) \cdot \mathbb{P}(E_{2,n-m}) \\
(1-p)\,\mathbb{P}\left(E_{1,n-(m+1)}\right) &= (1-p)\,\mathbb{P}(E_{2,n-m}) \\
\mathbb{P}\left(E_{1,n-(m+1)}\right) &= \mathbb{P}(E_{2,n-m}) \\
&= \cdots = \mathbb{P}(E_{m+2,n}) \\
&= p \cdot \mathbb{P}(E_{m+2,1}) + (1-p) \cdot \mathbb{P}(E_{m+3,1})
\end{aligned}$$

$$\begin{aligned}
\mathbb{P}(E_{m+3,1}) &= p \cdot \mathbb{P}(E_{m+3,1}) + (1-p) \cdot \mathbb{P}(E_{m+4,2}) \\
\mathbb{P}(E_{m+3,1}) &= \mathbb{P}(E_{m+4,2}) \\
&= \cdots = \mathbb{P}\left(E_{n,n-(m+2)}\right)
\end{aligned}$$

Analogue we get the following.

$$\mathbb{P}(E_{m+2,1}) = \mathbb{P}\left(E_{n,n-(m+1)}\right)$$

Combining these three equations gives us the following equation for $\mathbb{P}\left(E_{n,n-(m+1)}\right)$.

$$\mathbb{P}\left(E_{n,n-(m+1)}\right) = p \cdot \mathbb{P}\left(E_{n,n-(m+1)}\right) + (1-p) \cdot \mathbb{P}\left(E_{n,n-(m+2)}\right)$$

The same kind of calculation we can do for $\mathbb{P}(E_{1,n-m})$, in short this gives the following.

$$\begin{aligned}
\mathbb{P}(E_{1,n-m}) &= \mathbb{P}(E_{m+1,n}) \\
&= p \cdot \mathbb{P}(E_{m+1,1}) + (1-p) \cdot \mathbb{P}(E_{m+2,1}) \\
&= p \cdot \mathbb{P}(E_{n,n-m}) + (1-p) \cdot \mathbb{P}\left(E_{n,n-(m+1)}\right)
\end{aligned}$$

If we now combine our calculation about $\mathbb{P}\left(E_{n,n-(m+1)}\right)$ and $\mathbb{P}\left(E_{1,n-m}\right)$ and use our induction hypothesis we get the following calculations. This immediately shows that the induction hypothesis is also correct for $m+1$.

$$\begin{aligned}
\mathbb{P}\left(E_{n,n-(m+1)}\right) &= p \cdot \mathbb{P}\left(E_{1,n-(m+1)}\right) + (1-p) \cdot \mathbb{P}\left(E_{1,n-m}\right) \\
&= p \cdot \left(p \cdot \mathbb{P}\left(E_{n,n-(m+1)}\right) + (1-p) \cdot \mathbb{P}\left(E_{n,n-(m+2)}\right)\right) \\
&\quad + (1-p) \cdot \left(p \cdot \mathbb{P}\left(E_{n,n-m}\right) + (1-p) \cdot \mathbb{P}\left(E_{n,n-(m+1)}\right)\right) \\
&= p^2 \cdot \mathbb{P}\left(E_{n,n-(m+1)}\right) + p\,(1-p) \cdot \mathbb{P}\left(E_{n,n-(m+2)}\right) \\
&\quad + p\,(1-p) \cdot \mathbb{P}\left(E_{n,n-m}\right) + (1-p)^2 \cdot \mathbb{P}\left(E_{n,n-(m+1)}\right) \\
&= p^2 \cdot \mathbb{P}\left(E_{n,n-(m+1)}\right) + p\,(1-p) \cdot \mathbb{P}\left(E_{n,n-(m+2)}\right) \\
&\quad + p\,(1-p)\,\frac{m}{m+1} \cdot \mathbb{P}\left(E_{n,n-(m+1)}\right) + (1-p)^2 \cdot \mathbb{P}\left(E_{n,n-(m+1)}\right)
\end{aligned}$$

$$\begin{aligned}
\left(1 - p^2 - (1-p)^2 - \frac{mp\,(1-p)}{m+1}\right) \mathbb{P}\left(E_{n,n-(m+1)}\right) &= p\,(1-p)\,\mathbb{P}\left(E_{n,n-(m+2)}\right) \\
\frac{(m+2)\,p\,(1-p)}{m+1} \mathbb{P}\left(E_{n,n-(m+1)}\right) &= p\,(1-p)\,\mathbb{P}\left(E_{n,n-(m+2)}\right) \\
\mathbb{P}\left(E_{n,n-(m+1)}\right) &= \frac{m+1}{m+2} \mathbb{P}\left(E_{n,n-(m+2)}\right)
\end{aligned}$$

With this we have proved our lemma. □

A.2 Proof of Lemma 4.25

Proof. We have already seen that this lemma is correct for $r = 1$ (see Lemma 4.19).

Take $2 \leq r \leq n-1$ arbitrary.

$$\begin{aligned}
\mathbb{P}\left(E_{r+1,1}\right) &= p \cdot \mathbb{P}\left(E_{r+1,1}\right) + (1-p) \cdot \mathbb{P}\left(E_{r+2,2}\right) \\
(1-p)\,\mathbb{P}\left(E_{r+1,1}\right) &= (1-p)\,\mathbb{P}\left(E_{r+2,2}\right) \\
\mathbb{P}\left(E_{r+1,1}\right) &= \mathbb{P}\left(E_{r+2,2}\right) \\
&= \cdots = \mathbb{P}\left(E_{n,n-r}\right)
\end{aligned}$$

$$\begin{aligned}
\mathbb{P}\left(E_{1,n-r+1}\right) &= p \cdot \mathbb{P}\left(E_{1,n-r+1}\right) + (1-p) \cdot \mathbb{P}\left(E_{2,n-r+2}\right) \\
(1-p)\,\mathbb{P}\left(E_{1,n-r+1}\right) &= (1-p)\,\mathbb{P}\left(E_{2,n-r+2}\right) \\
\mathbb{P}\left(E_{1,n-r+1}\right) &= \mathbb{P}\left(E_{2,n-r+2}\right) \\
&= \cdots = \mathbb{P}\left(E_{r,n}\right)
\end{aligned}$$

Now we compute $\mathbb{P}(E_{n,n-r})$ and $\mathbb{P}(E_{r,n})$. We know that for random input the Černý automaton must synchronize at some point. This means that at some point all pawns are together on the same state (and from then on, stay together). Which means that either pawn k catches up to pawn $k-1$, or the other way around, where $k = 1, \ldots, n$. This gives the following.

$$\mathbb{P}\left(E_{k,k-1}\right) = 1 - \mathbb{P}\left(E_{k-1,k}\right) \tag{A.1}$$

First we calculate $\mathbb{P}(E_{n,n-r})$ and $\mathbb{P}(E_{r,n})$ for $r = n-1$, with the use of Equation A.1.

$$\begin{aligned}
\mathbb{P}(E_{1,n}) &= 1 - \mathbb{P}(E_{n,1}) \\
\frac{1-p}{n-p} &= 1 - \mathbb{P}(E_{n,1}) \\
\mathbb{P}(E_{n,1}) &= 1 - \frac{1-p}{n-p} = \frac{n-p-(1-p)}{n-p} \\
&= \frac{n-1}{n-p}
\end{aligned}$$

$$\begin{aligned}
\mathbb{P}(E_{2,1}) &= 1 - \mathbb{P}(E_{1,2}) \\
\frac{1}{n-p} &= 1 - \mathbb{P}(E_{1,2}) \\
\mathbb{P}(E_{n-1,n}) = \mathbb{P}(E_{1,2}) &= 1 - \frac{1}{n-p} = \frac{n-p-1}{n-p} \\
&= \frac{n-1-p}{n-p}
\end{aligned}$$

Thus, our Proposition is correct for $r = n-1$.
The rest of this proof goes by induction to r, but then downwards. So our base case is $r = n-1$, which as we saw, checks out. Now for the induction step, assume that our lemma is correct for $r+1$. Then we want to check if it is also correct for r.
We can see this by the following computations, using Lemma 4.24 and our induction hypothesis.

$$\begin{aligned}
\mathbb{P}(E_{n,n-r}) &= \frac{r}{r+1}\mathbb{P}(E_{n,n-r-1}) = \frac{r}{r+1}\mathbb{P}\left(E_{n,n-(r+1)}\right) \\
&= \frac{r}{r+1}\frac{r+1}{n-p} = \frac{r}{n-p}
\end{aligned}$$

$$\begin{aligned}
\mathbb{P}(E_{n,n-r}) &= p \cdot \mathbb{P}(E_{1,n-r}) + (1-p) \cdot \mathbb{P}(E_{1,n-r+1}) \\
&= p \cdot \mathbb{P}(E_{r+1,n}) + (1-p) \cdot \mathbb{P}(E_{r,n}) \\
\frac{r}{n-p} &= p \cdot \frac{r+1-p}{n-p} + (1-p) \cdot \mathbb{P}(E_{r,n}) \\
(1-p)\,\mathbb{P}(E_{r,n}) &= \frac{r - p(r+1-p)}{n-p} \\
\mathbb{P}(E_{r,n}) &= \frac{r - p(r+1-p)}{(n-p)(1-p)} \\
&= \frac{r - pr - p + p^2}{(n-p)(1-p)} = \frac{(r-p)(1-p)}{(n-p)(1-p)} = \frac{r-p}{n-p}
\end{aligned}$$

This concludes our proof. □

A.3 Proof of Lemma 4.27

Proof. The proof of this lemma is analogue to the proof of Lemma 4.26.

$$\begin{aligned}\mathbb{P}(W_1 = a \mid E_{1,n-t}) = \cdots = \mathbb{P}(W_1 = a \mid E_{t,n-1}) = p\\ \mathbb{P}(W_1 = b \mid E_{1,n-t}) = \cdots = \mathbb{P}(W_1 = b \mid E_{t,n-1}) = 1-p\end{aligned}$$

$$\begin{aligned}\mathbb{P}(W_1 = a \mid E_{t+1,n}) &= \frac{p \cdot \mathbb{P}(E_{t+1,1})}{\mathbb{P}(E_{t+1,n})}\\ &= \frac{p \cdot \frac{t}{n-p}}{\frac{t+1-p}{n-p}} = \frac{pt}{t+1-p}\\ \mathbb{P}(W_1 = b \mid E_{t+1,n}) &= 1 - \mathbb{P}(W_1 = a \mid E_{t+1,n})\\ &= \frac{(1-p)(t+1)}{t+1-p}\end{aligned}$$

$$\begin{aligned}\mathbb{P}(W_1 = a \mid E_{t+2,1}) = \cdots = \mathbb{P}(W_1 = a \mid E_{n-1,n-t-2}) = p\\ \mathbb{P}(W_1 = b \mid E_{t+2,1}) = \cdots = \mathbb{P}(W_1 = b \mid E_{n-1,n-t-2}) = 1-p\end{aligned}$$

$$\begin{aligned}\mathbb{P}(W_1 = a \mid E_{n,n-t-1}) &= \frac{p \cdot \mathbb{P}(E_{1,n-t-1})}{\mathbb{P}(E_{n,n-t-1})}\\ &= \frac{p \cdot \frac{t+2-p}{n-p}}{\frac{t+1}{n-p}} = \frac{p(t+2-p)}{t+1}\\ \mathbb{P}(W_1 = b \mid E_{n,n-t-1}) &= 1 - \mathbb{P}(W_1 = a \mid E_{n,n-t-1})\\ &= \frac{(1-p)(t+1-p)}{t+1}\end{aligned}$$

□

A.4 Proof of Proposition 4.29

Proof. The proof of this proposition goes by induction to m.
The base case is $m = 1$.
Proposition 4.28 gives us the following.

$$\begin{aligned}\mathbb{E}[T_{\mathcal{C}_n} \mid E_{1,n-1}] = \frac{n-2p}{2p(1-p)^2} + \frac{1}{2(1-p)^2(2-p)}\\ + \frac{1-p}{2(2-p)}\mathbb{E}[T_{\mathcal{C}_n} \mid E_{1,n}] + \frac{3-p}{2(2-p)}\mathbb{E}[T_{\mathcal{C}_n} \mid E_{1,n-2}]\end{aligned}$$

Proposition 4.22 gives us the following.

$$\mathbb{E}[T_{\mathcal{C}_n} \mid E_{1,n}] = 1 + \frac{n-2}{1-p} + \frac{p^2 - np + n}{p(2-p)} + \mathbb{E}[T_{\mathcal{C}_n} \mid E_{1,n-1}]$$

Together this results in the following.

$$\begin{aligned}
\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-1}\right] =& \frac{n-2p}{2p\left(1-p\right)^2} + \frac{1}{2\left(1-p\right)^2\left(2-p\right)} \\
&+ \frac{1-p}{2\left(2-p\right)}\left(1 + \frac{n-2}{1-p} + \frac{p^2-np+n}{p\left(2-p\right)} + \mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-1}\right]\right) \\
&+ \frac{3-p}{2\left(2-p\right)}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-2}\right] \\
=& \frac{n-2p}{2p\left(1-p\right)^2} + \frac{1}{2\left(1-p\right)^2\left(2-p\right)} + \frac{1-p}{2\left(2-p\right)} + \frac{n-2}{2\left(2-p\right)} \\
&+ \frac{\left(1-p\right)\left(p^2-np+n\right)}{2p\left(2-p\right)^2} + \frac{1-p}{2\left(2-p\right)}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-1}\right] \\
&+ \frac{3-p}{2\left(2-p\right)}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-2}\right] \\
\left(1 - \frac{1-p}{2\left(2-p\right)}\right)\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-1}\right] =& \frac{n-2p}{2p\left(1-p\right)^2} + \frac{1}{2\left(1-p\right)^2\left(2-p\right)} + \frac{1-p}{2\left(2-p\right)} + \frac{n-2}{2\left(2-p\right)} \\
&+ \frac{\left(1-p\right)\left(p^2-np+n\right)}{2p\left(2-p\right)^2} + \frac{3-p}{2\left(2-p\right)}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-2}\right] \\
\frac{3-p}{2\left(2-p\right)}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-1}\right] =& \frac{n-2p}{2p\left(1-p\right)^2} + \frac{1}{2\left(1-p\right)^2\left(2-p\right)} + \frac{1-p}{2\left(2-p\right)} + \frac{n-2}{2\left(2-p\right)} \\
&+ \frac{\left(1-p\right)\left(p^2-np+n\right)}{2p\left(2-p\right)^2} + \frac{3-p}{2\left(2-p\right)}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-2}\right] \\
\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-1}\right] =& \frac{\left(n-2p\right)\left(2-p\right)}{p\left(1-p\right)^2\left(3-p\right)} + \frac{1}{\left(1-p\right)^2\left(3-p\right)} + \frac{1-p}{3-p} + \frac{n-2}{3-p} \\
&+ \frac{\left(1-p\right)\left(p^2-np+n\right)}{p\left(2-p\right)\left(3-p\right)} + \mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-2}\right]
\end{aligned}$$

Fill $m = 1$ in, in the formula of our proposition, this gives the following.

$$\begin{aligned}
\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-1}\right] =& \frac{\left(n-2p\right)\left(2-p\right)}{p\left(1-p\right)^2\left(3-p\right)} + \frac{1}{\left(1-p\right)^2\left(3-p\right)} + \frac{\left(1-p\right)\left(2-p\right)}{\left(2-p\right)\left(3-p\right)} \\
&+ \frac{\left(n-2\right)\left(2-p\right)}{\left(2-p\right)\left(3-p\right)} + \frac{\left(1-p\right)\left(p^2-np+n\right)}{p\left(2-p\right)\left(3-p\right)} \\
&+ \sum_{i=2}^{1} \frac{\left(i-1\right)\left(i-p\right)}{\left(1-p\right)^2\left(2-p\right)\left(3-p\right)} \\
&+ \sum_{i=2}^{1} \frac{\left(n-2p\right)\left(i-p\right)^2}{p\left(1-p\right)^2\left(2-p\right)\left(3-p\right)} + \mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-2}\right] \\
=& \frac{\left(n-2p\right)\left(2-p\right)}{p\left(1-p\right)^2\left(3-p\right)} + \frac{1}{\left(1-p\right)^2\left(3-p\right)} + \frac{1-p}{3-p} + \frac{n-2}{3-p} \\
&+ \frac{\left(1-p\right)\left(p^2-np+n\right)}{p\left(2-p\right)\left(3-p\right)} + 0 + 0 + \mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-2}\right]
\end{aligned}$$

This is exactly what we have calculated for $\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-1}\right]$. So, for $m = 1$ our proposition is correct.

For the induction step, we have the following induction hypothesis. For $m \in \{1, \ldots, n-4\}$ holds:

$$\begin{aligned}
\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-m}\right] =& \frac{(n-2p)(m+1-p)}{p(1-p)^2(m+2-p)} + \frac{m}{(1-p)^2(m+2-p)} + \frac{(1-p)(2-p)}{(m+1-p)(m+2-p)} \\
&+ \frac{(n-2)(2-p)}{(m+1-p)(m+2-p)} + \frac{(1-p)(p^2-np+n)}{p(m+1-p)(m+2-p)} \\
&+ \sum_{1=2}^{m} \frac{(i-1)(i-p)}{(1-p)^2(m+1-p)(m+2-p)} \\
&+ \sum_{i=2}^{m} \frac{(n-2p)(i-p)^2}{p(1-p)^2(m+1-p)(m+2-p)} + \mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-m-1}\right]
\end{aligned}$$

Now we want to proof that it also holds for $m+1$.
Substituting our induction hypothesis in Proposition 4.28 gives us the following.

$$\begin{aligned}
\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-(m+1)}\right] =& \mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-m-1}\right] \\
=& \frac{n-2p}{2p(1-p)^2} + \frac{m+1}{2(1-p)^2(m+2-p)} \\
&+ \frac{m+1-p}{2(m+2-p)}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-m}\right] + \frac{m+3-p}{2(m+2-p)}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-m-2}\right] \\
=& \frac{n-2p}{2p(1-p)^2} + \frac{m+1}{2(1-p)^2(m+2-p)} + \frac{m+1-p}{2(m+2-p)} \left(\frac{(n-2p)(m+1-p)}{p(1-p)^2(m+2-p)} \right. \\
&+ \frac{m}{(1-p)^2(m+2-p)} + \frac{(1-p)(2-p)}{(m+1-p)(m+2-p)} \\
&+ \frac{(n-2)(2-p)}{(m+1-p)(m+2-p)} + \frac{(1-p)(p^2-np+n)}{p(m+1-p)(m+2-p)} \\
&+ \sum_{i=2}^{m} \frac{(i-1)(i-p)}{(1-p)^2(m+1-p)(m+2-p)} \\
&\left. + \sum_{i=2}^{m} \frac{(n-2p)(i-p)^2}{p(1-p)^2(m+1-p)(m+2-p)} + \mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-m-1}\right] \right) + \\
&\frac{m+3-p}{2(m+2-p)}\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-m-2}\right]
\end{aligned}$$

$$
\begin{aligned}
=&\frac{n-2p}{2p\left(1-p\right)^2}+\frac{m+1}{2\left(1-p\right)^2\left(m+2-p\right)}+\frac{\left(n-2p\right)\left(m+1-p\right)^2}{2p\left(1-p\right)^2\left(m+2-p\right)^2}\\
&+\frac{m\left(m+1-p\right)}{2\left(1-p\right)^2\left(m+2-p\right)^2}+\frac{\left(1-p\right)\left(2-p\right)}{2\left(m+2-p\right)^2}+\frac{\left(n-2\right)\left(2-p\right)}{2\left(m+2-p\right)^2}\\
&+\frac{\left(1-p\right)\left(p^2-np+n\right)}{2p\left(m+2-p\right)^2}+\sum_{i=2}^{m}\frac{\left(i-1\right)\left(i-p\right)}{2\left(1-p\right)^2\left(m+2-p\right)^2}\\
&+\sum_{i=2}^{m}\frac{\left(n-2p\right)\left(i-p\right)^2}{2p\left(1-p\right)^2\left(m+2-p\right)^2}+\frac{m+1-p}{2\left(m+2-p\right)}\mathbb{E}\left[T_{\mathcal{C}_n}\mid E_{1,n-m-1}\right]\\
&+\frac{m+3-p}{2\left(m+2-p\right)}\mathbb{E}\left[T_{\mathcal{C}_n}\mid E_{1,n-m-2}\right]
\end{aligned}
$$

$$
\begin{aligned}
\left(1-\frac{m+1-p}{2\left(m+2-p\right)}\right)\mathbb{E}\left[T_{\mathcal{C}_n}\mid E_{1,n-m-1}\right]=&\frac{n-2p}{2p\left(1-p\right)^2}+\frac{m+1}{2\left(1-p\right)^2\left(m+2-p\right)}\\
&+\frac{\left(n-2p\right)\left(m+1-p\right)^2}{2p\left(1-p\right)^2\left(m+2-p\right)^2}+\frac{m\left(m+1-p\right)}{2\left(1-p\right)^2\left(m+2-p\right)^2}\\
&+\frac{\left(1-p\right)\left(2-p\right)}{2\left(m+2-p\right)^2}+\frac{\left(n-2\right)\left(2-p\right)}{2\left(m+2-p\right)^2}\\
&+\frac{\left(1-p\right)\left(p^2-np+n\right)}{2p\left(m+2-p\right)^2}+\sum_{i=2}^{m}\frac{\left(i-1\right)\left(i-p\right)}{2\left(1-p\right)^2\left(m+2-p\right)^2}\\
&+\sum_{i=2}^{m}\frac{\left(n-2p\right)\left(i-p\right)^2}{2p\left(1-p\right)^2\left(m+2-p\right)^2}\\
&+\frac{m+3-p}{2\left(m+2-p\right)}\mathbb{E}\left[T_{\mathcal{C}_n}\mid E_{1,n-m-2}\right]\\
\frac{m+3-p}{2\left(m+2-p\right)}\mathbb{E}\left[T_{\mathcal{C}_n}\mid E_{1,n-m-1}\right]=&\frac{n-2p}{2p\left(1-p\right)^2}+\frac{m+1}{2\left(1-p\right)^2\left(m+2-p\right)}\\
&+\frac{\left(n-2p\right)\left(m+1-p\right)^2}{2p\left(1-p\right)^2\left(m+2-p\right)^2}+\frac{m\left(m+1-p\right)}{2\left(1-p\right)^2\left(m+2-p\right)^2}\\
&+\frac{\left(1-p\right)\left(2-p\right)}{2\left(m+2-p\right)^2}+\frac{\left(n-2\right)\left(2-p\right)}{2\left(m+2-p\right)^2}\\
&+\frac{\left(1-p\right)\left(p^2-np+n\right)}{2p\left(m+2-p\right)^2}+\sum_{i=2}^{m}\frac{\left(i-1\right)\left(i-p\right)}{2\left(1-p\right)^2\left(m+2-p\right)^2}\\
&+\sum_{i=2}^{m}\frac{\left(n-2p\right)\left(i-p\right)^2}{2p\left(1-p\right)^2\left(m+2-p\right)^2}\\
&+\frac{m+3-p}{2\left(m+2-p\right)}\mathbb{E}\left[T_{\mathcal{C}_n}\mid E_{1,n-m-2}\right]
\end{aligned}
$$

$$
\begin{aligned}
\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-m-1}\right] =& \frac{(n-2p)(m+2-p)}{p(1-p)^2(m+3-p)} + \frac{m+1}{(1-p)^2(m+3-p)} \\
&+ \frac{(n-2p)(m+1-p)^2}{p(1-p)^2(m+2-p)(m+3-p)} \\
&+ \frac{m(m+1-p)}{(1-p)^2(m+2-p)(m+3-p)} + \frac{(1-p)(2-p)}{(m+2-p)(m+3-p)} \\
&+ \frac{(n-2)(2-p)}{2(m+2-p)(m+3-p)} + \frac{(1-p)(p^2-np+n)}{p(m+2-p)(m+3-p)} \\
&+ \sum_{i=2}^{m} \frac{(i-1)(i-p)}{(1-p)^2(m+2-p)(m+3-p)} \\
&+ \sum_{i=2}^{m} \frac{(n-2p)(i-p)^2}{p(1-p)^2(m+2-p)(m+3-p)} + \mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-m-2}\right] \\
=& \frac{(n-2p)(m+2-p)}{p(1-p)^2(m+3-p)} + \frac{m+1}{(1-p)^2(m+3-p)} + \frac{(1-p)(2-p)}{(m+2-p)(m+3-p)} \\
&+ \frac{(n-2)(2-p)}{2(m+2-p)(m+3-p)} + \frac{(1-p)(p^2-np+n)}{p(m+2-p)(m+3-p)} \\
&+ \sum_{i=2}^{m+1} \frac{(i-1)(i-p)}{(1-p)^2(m+2-p)(m+3-p)} \\
&+ \sum_{i=2}^{m+1} \frac{(n-2p)(i-p)^2}{p(1-p)^2(m+2-p)(m+3-p)} + \mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-m-2}\right]
\end{aligned}
$$

This is exactly what our propositions claims about $\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-m-1}\right]$. □

A.5 Proof of Corollary 4.30

Proof. To prove this Corollary, we first have to calculate the finite sums (from $i = 2$ to $m + 1$). Here we can use the facts that $\sum_{i=1}^{n} i = \frac{1}{2}n(n+1)$ and $\sum_{i=1}^{n} i^2 = \frac{1}{6}n(n+1)(2n+1)$.

Intermezzo

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

$$= \frac{1}{(1-p)^2 (m+1-p)(m+2-p)} \sum_{i=1}^{m} \left(i^2 - (1+p)\, i + p\right)$$

$$= \frac{1}{(1-p)^2 (m+1-p)(m+2-p)} \left(\frac{1}{6} m(m+1)(2m+1) - (1+p)\frac{1}{2} m(m+1) + pm\right)$$

$$= \frac{m(m-1)(2m-3p+2)}{6(1-p)^2 (m+1-p)(m+2-p)}$$

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

$$= \frac{n-2p}{p(1-p)^2 (m+1-p)(m+2-p)} \left(\sum_{i=1}^{m} \left(i^2 - 2pi + p^2\right) - (1-p)^2\right)$$

$$= \frac{n-2p}{p(1-p)^2 (m+1-p)(m+2-p)} \left(\frac{1}{6} m(m+1)(2m+1) - 2p\frac{1}{2} m(m+1) + p^2 m - (1-p)^2\right)$$

$$= \frac{(n-2p)\, m(m+1)(2m+1)}{6p(1-p)^2 (m+1-p)(m+2-p)} - \frac{(n-2p)\, m}{(1-p)^2 (m+2-p)} - \frac{n-2p}{p(m+1-p)(m+2-p)}$$

This intermezzo, together with Proposition 4.29 gives the following.

$$
\begin{aligned}
\mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-m}\right] =& \frac{(n-2p)(m+1-p)}{p(1-p)^2(m+2-p)} + \frac{m}{(1-p)^2(m+2-p)} + \frac{(1-p)(2-p)}{(m+1-p)(m+2-p)} \\
&+ \frac{(n-2)(2-p)}{(m+1-p)(m+2-p)} + \frac{(1-p)(p^2-np+n)}{p(m+1-p)(m+2-p)} \\
&+ \frac{m(m-1)(2m-3p+2)}{6(1-p)^2(m+1-p)(m+2-p)} \\
&+ \frac{(n-2p)m(m+1)(2m+1)}{6p(1-p)^2(m+1-p)(m+2-p)} - \frac{(n-2p)m}{(1-p)^2(m+2-p)} \\
&- \frac{n-2p}{p(m+1-p)(m+2-p)} + \mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-m-1}\right] \\
=& \frac{(n-2p)(m+1-p)+pm-pm(n-2p)}{p(1-p)^2(m+2-p)} \\
&+ \frac{p(2-p)(n-1-p)+(1-p)(p^2-np+n)-(n-2p)}{p(m+1-p)(m+2-p)} \\
&+ \frac{pm(m-1)(2m-3p+2)+(n-2p)m(m+1)(2m+1)}{6p(1-p)^2(m+1-p)(m+2-p)} \\
&+ \mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-m-1}\right] \\
=& \frac{(n-2p)(m+1-p)+pm-pm(n-2p)}{p(1-p)^2(m+2-p)} \\
&+ \frac{pm(m-1)(2m-3p+2)+(n-2p)m(m+1)(2m+1)}{6p(1-p)^2(m+1-p)(m+2-p)} \\
&+ \mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-m-1}\right] \\
=& \frac{-2(m+1)p^3+\frac{1}{2}(m+1)(3m+2n+8)p^2-\frac{1}{3}(m+1)(m+2)(m+3n+3)p}{p(1-p)^2(m+1-p)(m+2-p)} \\
&+ \frac{\frac{1}{6}(2m+3)(m+1)(m+2)n}{p(1-p)^2(m+1-p)(m+2-p)} + \mathbb{E}\left[T_{\mathcal{C}_n} \mid E_{1,n-m-1}\right]
\end{aligned}
$$

□

Appendix B

Additions Section 4.3

B.1 All possible power automata in the proof of Proposition 4.45.

In this section we give all possible power automata, which we discussed in the proof of Proposition 4.45. With each possible power automata we give the value of $\mathbb{E}[T_{\mathcal{A}}]$ with $p = \frac{1}{2}$, calculated with System 2 described in Subsection 4.2.2. In each figure with a possible power automaton we indicated the value of m_{IJ} in red.

Option 1:

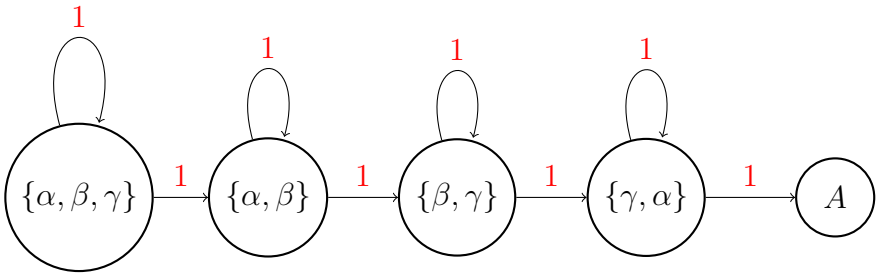

Figure B.1: Option 1 of the power automaton with second arrows, $n = 3$ and m_{IJ} in red.

With option 1 we have $\mathbb{E}[T_{\mathcal{A}}] = 8 \cdot 1 = 8$.

Option 2:

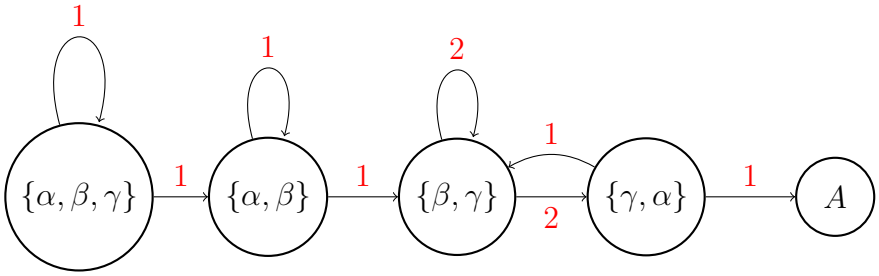

Figure B.2: Option 2 of the power automaton with second arrows, $n = 3$ and m_{IJ} in red.

With option 2 we have $\mathbb{E}[T_{\mathcal{A}}] = 6 \cdot 1 + 2 \cdot 2 = 10$.

Option 3:

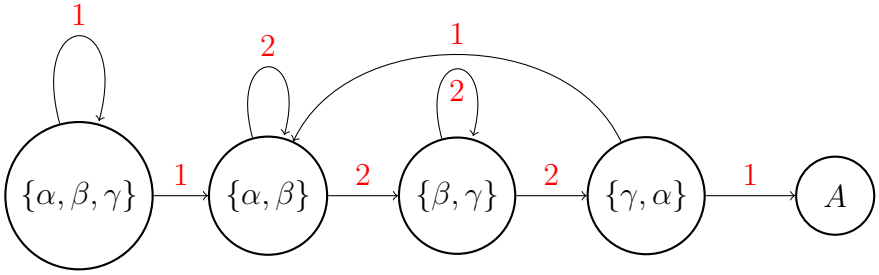

Figure B.3: Option 3 of the power automaton with second arrows, $n = 3$ and m_{IJ} in red.

With option 3 we have $\mathbb{E}[T_{\mathcal{A}}] = 4 \cdot 1 + 4 \cdot 2 = 12$.

Option 4:

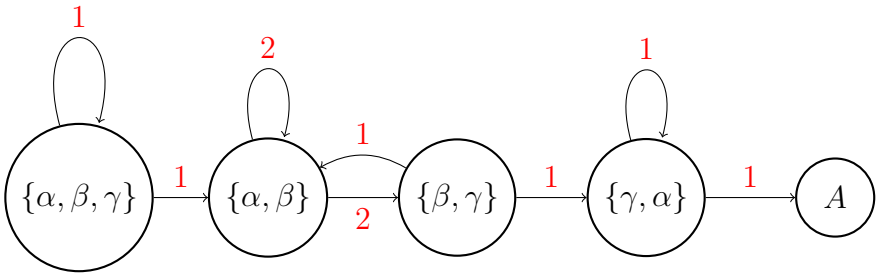

Figure B.4: Option 4 of the power automaton with second arrows, $n = 3$ and m_{IJ} in red.

With option 4 we have $\mathbb{E}[T_{\mathcal{A}}] = 6 \cdot 1 + 2 \cdot 2 = 10$.

Option 5:

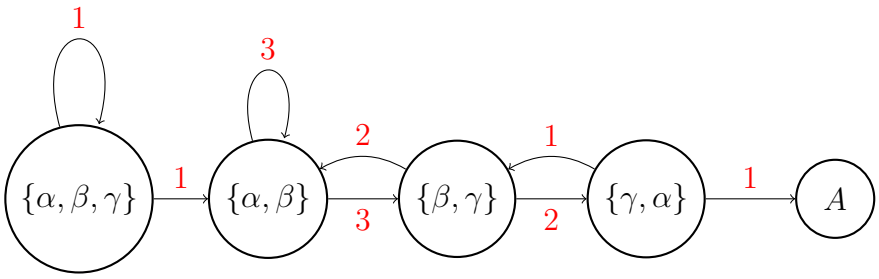

Figure B.5: Option 5 of the power automaton with second arrows, $n = 3$ and m_{IJ} in red.

With option 5 we have $\mathbb{E}[T_{\mathcal{A}}] = 4 \cdot 1 + 2 \cdot 2 + 2 \cdot 3 = 14$.

Option 6:

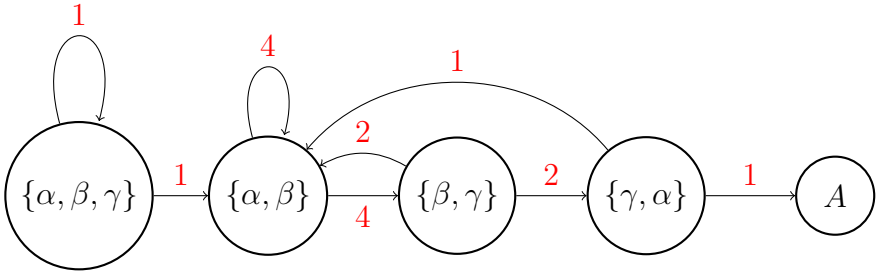

Figure B.6: Option 6 of the power automaton with second arrows, $n = 3$ and m_{IJ} in red.

With option 6 we have $\mathbb{E}[T_{\mathcal{A}}] = 4 \cdot 1 + 2 \cdot 2 + 2 \cdot 4 = 16$.

Comparing all six options gives us that the power automaton (if it exists) in option 6 has the largest value for $\mathbb{E}[T_{\mathcal{A}}]$.

B.2 Power automaton of the Černý automaton $\mathcal{C}_5$.

The power automaton of the Černý automaton $\mathcal{C}_5$ is shown on the next page in Figure B.7.

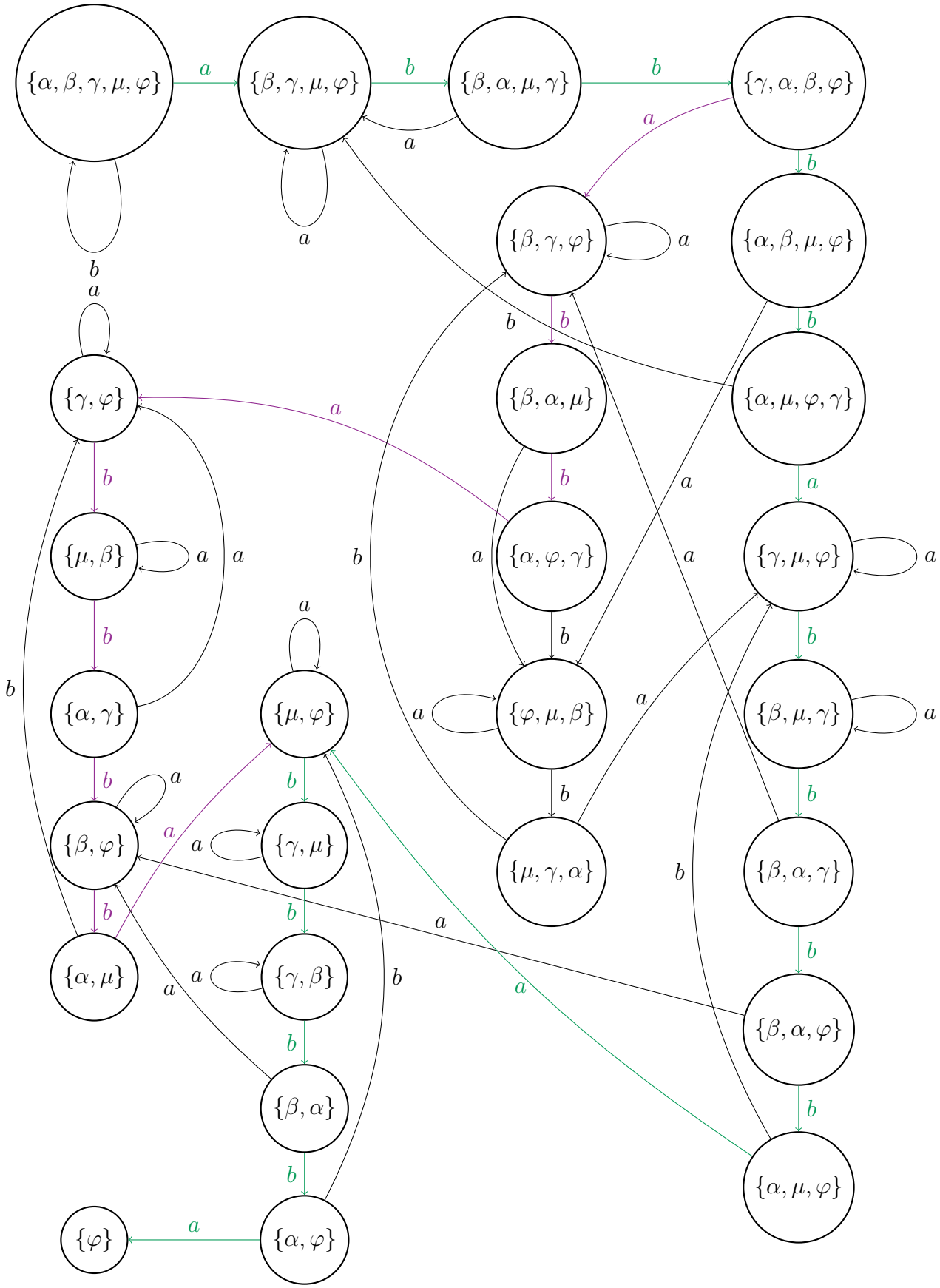

Figure B.7: Power automaton of the Černý automaton $\mathcal{C}_5$.

Appendix C

Matlab programs

For Chapter Random words we used some Matlab programs. These Matlab programs can be found through the following link.
`https://gitlab.science.ru.nl/vhoorn/synchronizing-automata-and-their-reset-words/-/tree/main/MatlabCode`

In this Chapter we give some more context and explanations on how these programs work. We only cover the most important (the ones that are most used) programs. In each subsection you can find a corresponding link that will take you directly to the used Matlab code.

C.1 Automaton

First we show how we program an automaton $\mathcal{A} = (Q, \Sigma, \delta)$ with n states.

We translate this automaton in Matlab in the following way. For each letter in the alphabet (Σ) we create a transition matrix. So, we will get a $n \times n$-matrix A for the letter a and a $n \times n$-matrix B for the letter b. We define matrix A en B as follows.

$$A_{ij} = \begin{cases} 1 & \text{if } \delta(i,a) = j \\ 0 & \text{otherwise} \end{cases} \qquad B_{ij} = \begin{cases} 1 & \text{if } \delta(i,b) = j \\ 0 & \text{otherwise} \end{cases}$$

The function **Automaton**(n, q, A, B, w) shown below, is the Matlab program for an automaton. The inputs of this function are, n the number of states, $q \in Q$ the start state, matrices A and B indicating automaton $\mathcal{A}$ and a word $w \in \Sigma^*$. A word $w \in \Sigma^*$ in Matlab is a array of zeros and ones. The zeros correspond with the letter a and the ones correspond with the letter b.
This function returns the value $\delta(q, w)$ for the automaton indicated by matrix A and B.

`https://gitlab.science.ru.nl/vhoorn/synchronizing-automata-and-their-reset-words/-/blob/main/MatlabCode/Automaton.m`

Let's go through this program with an example.

Example C.1. Consider the Černý automaton with $n = 4$ states shown in Figure 2.3, $\mathcal{C}_4 = (\{1,2,3,4\}, \{a,b\}, \delta)$. Here we have as transition function

$$\delta(q,a) = \begin{cases} q & \text{if } q = 1,2,3 \\ 1 & \text{if } q = 4 \end{cases} \qquad \delta(q,b) = \begin{cases} q+1 & \text{if } q = 1,2,3 \\ 1 & \text{if } q = 4 \end{cases}$$

This gives that the following matrices indicated the Černý automaton $\mathcal{C}_4$.

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \qquad B = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

Suppose we have the start state $q = 3$ and word $w = aba$. Our program we calculates $\delta(q,w)$. To do this we first convert our word into a array of zero's and one's. The letter a becomes a zero and the letter b becomes an one. So word $w = aba$ becomes $[0,1,0]$.

We run **Automaton**$(4,3,A,B,[0,1,0])$, this gives as outcome the value of $\delta(q,w)$ where matrix A and B indicate the automaton. This program's does the following. We start with state= 3 and we have length$(w) = 3$ so our for loop does three iterations.
In the first iteration in the for loop we have $w(1) = 0$. So we take a look at matrix A. With find$(A(startstate,:))$ Matlab searches for the 1 (there is only one 1 by definition of matrix A) in row 3 (start state = 3). In this example this 1 in row 3, is found in column 3. With [,state] = find$(A(3,:))$ we define the new state to be state= 3.
In the second iteration in the for loop we have $w(2) = 1$. So we take a look at matrix B. With find$(B(state,:))$ Matlab searches for the 1 (there is only one 1 by definition of matrix B) in row 3 (state= 3). In this example this 1 in row 3, is found in column 4. With [,state] = find$(A(3,:))$ we define the new state to be state= 4.
In the third and last iteration we have $w(3) = 0$. So we take a look at matrix A. With find$(A(state,:))$ Matlab searches for the 1 (there is only one 1 by definition of matrix A) in row 4 (state= 4). In this example this 1 in row 3, is found in column 1. With [,state] = find$(A(4,:))$ we define the new state to be state= 1.
So we get that **Automaton**$(4,3,A,B,[0,1,0])$ gives endstate=state= 1

C.2 Power automaton

With our program of the automaton, we can write a program of the corresponding power automaton. The function **Powerautomaton**(n,S,A,B,w) is the matlab program for the power automaton (of the automaton indicated by matrix A and B). This function returns the value of $\delta(S,w)$.

The input of this function is almost the same as with the function **Automaton**(n, q, A, B, w). The only difference is that we have some subset $S \subseteq Q$ instead of a state $q \in Q$.

`https://gitlab.science.ru.nl/vhoorn/synchronizing-automata-and-their-reset-words/-/blob/main/MatlabCode/Powerautomaton.m`

We again go through this program with an example. Let's continue with Example C.1.

Example C.2 (Continue of Example C.1)**.** We have automaton $\mathcal{C}_4$.
$n = 4$, $w = [0, 1, 0]$ and matrices A and B are shown in Example C.1. Suppose $S = \{3, 4\}$, to put this into matlab we have to write $S = [3, 4]$.

We start with Endsubset= [ ], an empty list. In each iteration we take the following state in S and calculate there endstate. We add this endstate to our list Endsubset.
In our example we first have $S(1) = 3$, with **Automaton**$(4, 3, A, B, [0, 1, 0])$ we calculated endstate= 1 (see Example C.1). So after the first iteration we have Endsubset= [1].
In our second (and last) iteration we have $S(2) = 4$, with **Automaton**$(4, 4, A, B, [0, 1, 0])$ we calculated endstate= 2. After this iteration we have Endsubset= $[1, 2]$.
Since $|S| = 2$ our for loop is done. Our function **Powerautomaton**$(4, [3, 4], A, B, [0, 1, 0])$ returns Endsubset= $[1, 2]$.

Remark. Suppose we have the same inputs, $n = 4$, $S = [3, 4]$ and automaton $\mathcal{C}_4$, but that our word would be $w = [1, 0]$. Then **Automaton**$(4, 3, A, B, [1, 0])$ and **Automaton**$(4, 4, A, B, [1, 0])$ would both return endstate= 1. But in our Endsubset we don't want duplicate numbers. We want that in this case the function **Powerautomaton**$(4, [3, 4], A, B, [1, 0])$ returns Endsubset= [1]. Therefore, we have included an if statement in our for loop. If the calculated endstate isn't in our current Endsubset, then we add this number to the Endsubset. But if it is an element in our current Endsubset, then we do nothing and just go to the next iteration in the for loop.
So in the first iteration we get Endsubset= [1], and after the second iteration this stays Endsubset= [1]. So our final result is Endsubset= [1].

C.3 Testing whether w is a reset word

With our function of the power automaton we can easily check whether some word $w \in \Sigma^*$ is a reset word for the automaton indicated by matrix A and B, or not. The input of this function is the number of states n, the word w and the matrices A and B which indicate the automaton. These are the same sort inputs as in the function of the automaton and the power automaton.

From Proposition 2.22 we know that w is a reset word if w indicates a path from Q to a singleton. Therefore, in the function **resetwordforAutomatonyesorno**(n, w, A, B),

we check whether w indicates such a path.
So this is what we are checking in the function
resetwordforAutomatonyesorno(n, w, A, B). Here we use the function **Powerautomaton**(n, Q, A, B, w), where $Q = \{1, \ldots, n\}$. If this function returns an Endsubset of lenght one, then $\delta(Q, w)$ is a singleton, and thus w is a reset word. If not (length(Endsubet)> 1), then w isn't a reset word.

`https://gitlab.science.ru.nl/vhoorn/synchronizing-automata-and-their-reset-words/-/blob/main/MatlabCode/resetwordforAutomatonyesorno.m`

Example C.3. Let's again consider the Černý automaton $\mathcal{C}_4$, so $n = 4$ and matrices A and B are shown in Example C.1.
Let $w = aba$ (in matlab $w = [0, 1, 0]$) and check whether this is a reset word for the Černý automaton $\mathcal{C}_4$ or not.
The function **Powerautomaton**$(4, [1, 2, 3, 4], A, B, [0, 1, 0])$ returns Endsubset$= [2, 3, 1]$. Length(Endsubset)$= 3$. Hence, $w = aba$ isn't a reset word. Our function returns TrueorFalse$= 0$.
Let $w = abbbabbba$ (in matlab $w = [0, 1, 1, 1, 0, 1, 1, 1, 0]$), then
Powerautomaton$(4, [1, 2, 3, 4], A, B, w)$ returns Endsubset$= [1]$.
Length(Endsubset)$= 1$, thus $w = abbbabbba$ is a reset word. Our function returns TrueorFalse$= 1$.

C.4 Find all subsets of $Q = \{1, \ldots, n\}$

In this section we deal with a help function. This function finds all non-empty subsets of Q ($\emptyset \neq S \subseteq Q = \{1, \ldots, n\}$). The only input of this function is n, the number of states.
The function **findallsubsets**(n) returns a cell (a list of matrices) ALLSUB. For $k = 1, \ldots, n$, ALLSUB$\{k\}$ is a $(\binom{n}{k} \times k)$-matrix with all subsets of Q of size k (the rows are the subsets).

`https://gitlab.science.ru.nl/vhoorn/synchronizing-automata-and-their-reset-words/-/blob/main/MatlabCode/findallsubsets.m`

Let's look at an example.

Example C.4. Suppose $n = 4$. Then ALLSUB=**findallsubsets**(n) gives the following matrices.

$$\text{ALLSUB}\{1\} = \begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \end{pmatrix} \qquad \text{ALLSUB}\{2\} = \begin{pmatrix} 3 & 4 \\ 2 & 4 \\ 2 & 3 \\ 1 & 4 \\ 1 & 3 \\ 1 & 2 \end{pmatrix}$$

$$\text{ALLSUB}\{3\} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 4 \\ 1 & 3 & 4 \\ 2 & 3 & 4 \end{pmatrix} \qquad \text{ALLSUB}\{4\} = \begin{pmatrix} 1 & 2 & 3 & 4 \end{pmatrix}$$

The rows of ALLSUB{1} gives all subsets of size 1: $\{\{1\},\{2\},\{3\},\{4\}\}$.
The rows of ALLSUB{2} gives all subsets of size 2: $\{\{3,4\},\{2,4\},\{2,3\},\{1,4\},\{1,3\},\{1,2\}\}$.
The rows of ALLSUB{3} gives all subsets of size 3: $\{\{1,2,3\},\{1,2,4\},\{1,3,4\},\{2,3,4\}\}$.
The rows of ALLSUB{4} gives all subsets of size 4: $\{\{1,2,3,4\}\}$.
In total this gives all non empty subset of $\{1,2,3,4\}$.

C.5 Calculating the Exact Expected length of the reset word

In this section we see the function
ExactExpectedlengthresetwordAutomaton$(n, pchance, A, B)$ (matlab program).
This function calculates $\mathbb{E}[T_{\mathcal{A}}]$ with the use of system 1 (described in Subsection 4.2.1).
The inputs of this function are the number of states n, matrices A and B which indicate the automaton $\mathcal{A}$ and $pchance \in [0,1)$. If $pchance = 0$, then we calculate $\mathbb{E}[T_{\mathcal{A}}]$ with p as a variable (the result is an expression depended on p). Otherwise we calculate $\mathbb{E}[T_{\mathcal{A}}]$ for a certain $p \in (0,1)$ (the result is a number). We have $\mathbb{P}(a) = p$ and $\mathbb{P}(b) = 1 - p$.

Within this Matlab function all equations of system 1 get saved in eqns. Thereafter we let Matlab solve the system of equations. At last we look at E_Q^A, this is the expected length of the reset word.

`https://gitlab.science.ru.nl/vhoorn/synchronizing-automata-and-their-reset-words/-/blob/main/MatlabCode/ExactExpectedlengthresetwordAutomaton.m`

C.6 Finding all permutation matrices

In Subsection 4.3.2 we do a brute force search across all synchronising automatons. Before we can do a brute force search we need to know which different automata exists. We have to find all possible matrices for matrix A and matrix B. Fortunately all possible matrices for matrix A are the same as all possible matrices for matrix B. So we only have to look for all possible matrices for matrix A.

The entries of matrices A are zeros and ones. For matrix A must hold that we have precisely one 1 in each row. Thus all possible matrices for matrix A are all $n \times n$ (column representation) permutation matrices.

Example C.5. Below we see all permutation matrices for $n = 2$.

$$\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$$

For $n = 4$ we have to find all possible 4×4 permutation matrices (function **findallpermutationmatrices4states**()) and for $n = 5$ we have to find all possible 5×5 permutation matrices (function **findallpermutationmatrices5states**()).

`https://gitlab.science.ru.nl/vhoorn/synchronizing-automata-and-their-reset-words/-/blob/main/MatlabCode/findallpermutationmatrices4states.m`

`https://gitlab.science.ru.nl/vhoorn/synchronizing-automata-and-their-reset-words/-/blob/main/MatlabCode/findallpermutationmatrices5states.m`

C.7 Brute force search of all synchronising automatons

With previous programs/function we can now do a brute force search for the synchronising automaton with the largest value of $\mathbb{E}[T_{\mathcal{A}}]$.

As input we have $p \in (0, 1)$, where $p = \mathbb{P}(a)$ and $\mathbb{P}(b) = 1 - p$.

With the functions **findallpermutationmatrices4states**() and **findallpermutationmatrices5states**() we find all possible matrices A and B for $n = 4$ and $n = 5$ respectively.

We go through all automatons, but we can only calculate $\mathbb{E}[T_{\mathcal{A}}]$ for synchronising automatons $\mathcal{A}$. So, first we have to check whether some automaton indicated by matrix A and B is synchronising or not. This is done by checking whether the automaton has a reset word or not.

According to Lemma 3.17 we have for $n = 4$: $C(4) \leq 2^4 - 4 - 1 = 11$. So if an automaton with $n = 4$ has a reset word, it must have a reset word $w \in \Sigma^*$ with $|w| \leq 11$.
According to the upper bound found by J.-E Pin and P. Frankl we have for $n = 5$: $C(5) \leq \frac{5^3-5}{6} = 20$. So if an automaton with $n = 5$ has a reset word, it must have a reset word $w \in \Sigma^*$ with $|w| \leq 20$.

In both cases $n = 4$ and $n = 5$ we check whether an automaton has a reset word or not. This is done by going through all words of length 11 and 20 respectively, and checking whether or not this is a reset word for this particular automaton (use function **resetwordforAutomatonyesorno**(n, w, A, B)).

If it turns out that this particular automaton has a reset word, we calculate the value $\mathbb{E}[T_{\mathcal{A}}]$ for the given p. Here we use the function **ExactExpectedlengthresetwordAutomaton**$(n, pchance, A, B)$ with $pchance = p$.

Since we are looking for the automaton with the largest value of $\mathbb{E}[T_{\mathcal{A}}]$ we only save the automatons $\mathcal{A}$ (and the value of $\mathbb{E}[T_{\mathcal{A}}]$) with $\mathbb{E}[T_{\mathcal{A}}] \geq \mathbb{E}[T_{\mathcal{C}_n}]$.

For $n = 4$ this gives the following Matlab program.

`https://gitlab.science.ru.nl/vhoorn/synchronizing-automata-and-their-reset-words/-/blob/main/MatlabCode/lookformaximalexpectedresetlenght4states.m`

For $n = 5$ there are even more possible matrices for A and B. This means that there are a lot more automatons we need to check. To make our program a bit more efficient, we do the following two things.
We can disregard all automatons with reset word $w \in \Sigma^*$ with $|w| = 1$, since for these automatons $\mathbb{E}[T_{\mathcal{A}}]$ will be small.
We can disregard all isomorphic automatons, since they give the same value of $\mathbb{E}[T_{\mathcal{A}}]$.
For $n = 5$ this gives the following Matlab program.

`https://gitlab.science.ru.nl/vhoorn/synchronizing-automata-and-their-reset-words/-/blob/main/MatlabCode/lookformaximalexpectedresetlenght5states.m`

C.8 Calculate length of randomly generated reset word

In this section we are dealing with a function, which we use by approximating $\mathbb{E}[T_{\mathcal{A}_1}]$ and $\mathbb{E}[T_{\mathcal{A}_2}]$ for large n. The function **randomAutomatonresetword**(n, p, A, B) calculates the length of a randomly generated reset word, with $\mathbb{P}(a) = p$ and $\mathbb{P}(b) = 1 - p$, of an automaton (with n states) indicated by matrix A and B.

We start with the empty word, which isn't a reset word. Each iteration we add a letter, randomly chosen with $\mathbb{P}(a) = p$ and $\mathbb{P}(b) = 1 - p$. Then check whether the new word is a reset word for the automaton indicated by matrix A and B. We stop this process when we have found a reset word. Then we return the length of this word.

`https://gitlab.science.ru.nl/vhoorn/synchronizing-automata-and-their-reset-words/-/blob/main/MatlabCode/randomAutomatonresetword.m`

C.9 Compare $\mathbb{E}[T_{\mathcal{A}}]$ of different automatons

To compare different automatons in Subsection 4.3.3 we have the following Matlab program.
compareautomatonsexpectedlenghtresetword$(minnumberofstates, maxnumberofstates, p)$
In this program we use our knowledge about the exact value of $\mathbb{E}[T_{\mathcal{C}_n}]$, $\mathbb{E}[T_{\mathcal{A}_3}]$ and $L(n)$ found in Theorem 4.15, Proposition 4.52 and Definition 4.55 respectively. For automatons $\mathcal{A}_1$ and $\mathcal{A}_2$ we use the function
ExactExpectedlengthresetwordAutomaton(n, p, A, B), or we approximate the expected length of the reset word with (100 times)
randomAutomatonresetword(n, p, A, B).

With our function we compare the different values for
$n = minnumberofstates, minnumberofstates + 1, \ldots, maxnumberofstates$, with $\mathbb{P}(a) = p$.

For $n \geq 11$ it's gets to hard to calculate $\mathbb{E}[T_{\mathcal{A}_1}]$ and $\mathbb{E}[T_{\mathcal{A}_2}]$ exact. That is why for $n \geq 11$ we approximate $\mathbb{E}[T_{\mathcal{A}_1}]$ and $\mathbb{E}[T_{\mathcal{A}_2}]$ by taking 100 samples of randomly generated reset words and calculate the mean of the length of all those words.

Our function gives a table with n and all corresponding calculated values $\mathbb{E}[T_{\mathcal{C}_n}]$, $\mathbb{E}[T_{\mathcal{A}_1}]$, $\mathbb{E}[T_{\mathcal{A}_2}]$, $\mathbb{E}[T_{\mathcal{A}_3}]$ and $L(n)$.

`https://gitlab.science.ru.nl/vhoorn/synchronizing-automata-and-their-reset-words/-/blob/main/MatlabCode/compareautomatonsexpectedlenghtresetword.m`