On the Minimal Reset Words of Synchronizing Automata

David Stoner

under the direction of
Mr. Chiheon Kim
Massachusetts Institute of Technology

Research Science Institute
July 30, 2014

Abstract

Cerny's conjecture is a 50 year old conjecture which concerns the combinatoral field of synchronizing automata. In particular, it postulates that the maximal length of the minimal reset word among all n-state automata is $(n-1)^2$. We present a proof for Pin's Theorem, which applies Cerny's conjecture to p-state automata consisting of a cycle and a non-permutation, where $p \geq 3$ is an odd prime. We also introduce families of the form $F(p,k)$ of automata which consist of a cycle and a group of k simple merging arcs, and we define $C(p,k)$ to be the maximal length of minimal reset words within these families. We provide a lower bound of $C(p,k)$ for general k, and we find with proof the exact value of $C(p,2)$.

Summary

Suppose that you are given a group of identically shaped puzzle pieces, each of which is in one of finitely many possible orientations. Accompanying these pieces, you are given a set of machines, each of which can perform some operation which alters the orientation of each piece. Then this project examines the process of selecting the shortest possible series of machines to put in succession such that any puzzle piece entering the series leaves it with a fixed orientation.

1 Introduction

The automaton is a combinatorial object which has been of mathematical interest for centuries. During the 1960s, several mathematicians independently developed theories of a new property of automata, called their *synchronization*. Outside of mathematics, the study of this property has applications in the field of robotics [1]. In particular, suppose that some machine parts on a conveyor belt are identical, and they have a finite number of possible orientations. Then the graph of a synchronizing automata can be used to construct a machine which, given these parts as inputs, outputs a fixed orientation. This physical analogue of an automaton has been additionally utilized in nanoscale operations within biocomputing [1]. In a 1964 paper by Jan Cerny[2], he proposed a conjecture which has been investigated deeply, and which provides the basis for our research.

Given a set of states $Q = \{1, 2, \cdots, n\}$ and an alphabet of letters A, each of which defines an action from $Q \to Q$, we construct an **automaton** $\alpha = (Q, A)$. We define a **word** w to be some composition of functions described by letters of the alphabet A. For a set of states $S \subseteq Q$, the set Sw is defined as the set of all possible state outputs obtained when applying w to each element of X, applying each letter from left to right.

A **reset word** is a word r such that $|Qr| = 1$; in other words, applying the word r to every state in Q gives the same result. If an automaton α has some reset word, then α is said to be **synchronizing**. The reset word of shortest length for a given synchronizing automaton α is the **minimal reset word** of α. Its length is given by $r(\alpha)$.

Let $C(n)$ denote the largest value of $r(\alpha)$ with n states. That is, let:

$$C(n) = \max\{r(\alpha) \mid \alpha = (Q, A), |Q| = n\}$$

Cerny's Conjecture states that $C(n) = (n-1)^2$. Cerny showed that $C(n) \geq (n-1)^2$ by constructing a family of synchronizing automata with shortest reset words of length $(n-1)^2$.

His construction was the following:

For an automata with n states, let $l(\pi)$ denote the letter which sends state i to state $i-1$, where states are considered modulo n. For two disjoint subsets $B = \{b_1, b_2, \cdots, b_j\}$ and $C = \{c_1, c_2, \cdots, c_j\}$, let $l(B \to C)$ denote the letter which sends b_i to c_i for $1 \leq i \leq j$, and sends x to itself if $x \notin B$. Each pair (b_i, c_i) will be called an **arc** of the automaton. Then the infinite class of automata which Cerny found satisfied:

$$|Q| = n, A = \{l(\pi), l(\{1\} \to \{n\})\}.$$

The fact that this automaton synchronizes in exactly $(n-1)^2$ steps is a corollary of our Theorem 3.1.

The upper bound of $C(n)$ has been improved over time. Cerny [3] proved an upper bound $C(n) \leq 2^n - n - 1$. Using the greedy algorithm and results from Frankl [4], this bound was improved to $\frac{n^3-n}{6}$, where it remained for a long time. In 2011, A. N. Trahtman [5] reduced this to the currently best-known upper bound of $\frac{n(7n^2+6n-16)}{48}$.

Cerny's conjecture has been proven for some particular classes of automata. For example, if the automaton's digraph is Eulerian, or if the automata is orientable [1], then Cerny's conjecture has been proven. The general problem, however, remains open and difficult.

We focus on automata of the form $\alpha = (Q, A)$, where:

$$\begin{aligned} |Q| = p \quad & p \text{ is prime} \\ A = \{l(\pi), l(B \to C)\}&. \end{aligned}$$

According to a theorem by Pin [6], an automaton which has a prime number p of states, contains some cycle, and contains some letter which is a non-permutation on the states is synchronizing, and furthermore has a reset word of length at most $(p-1)^2$. We present

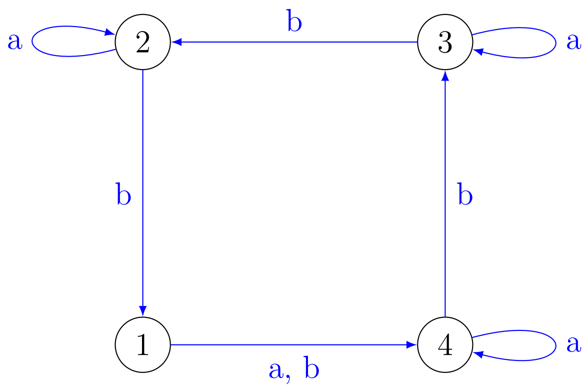

Figure 1: An Automaton

improvements of this bound within specific subclasses of automata.

To make progress in this direction, it is useful to represent each letter of a given alphabet as a $p \times p$ matrix. In particular, for some letter $a \in A$, we define M_a as:

$$(M_a)_{ij} = \begin{cases} 1 & : ia = j \\ 0 & : ia \neq j \end{cases}$$

We now provide a sample automaton which illustrates these definitions: The automata shown in Figure 1 represents $|Q| = 4, A = \{a, b\}$. Note that $b = l(\pi)$ and $a = l(\{1\} \to \{4\})$. It's minimal reset word is ab^3ab^3a, which has length $9 = (4-1)^2$. The matrices corresponding to a, b are:

$$M_a = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad M_b = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Given some subset $S \subseteq Q$, We define $[S]$ to be a p-element horizontal vector where:

$$[S]_i = \begin{cases} 1 & : i \in S \\ 0 & : i \notin S \end{cases}$$

In particular, $[Q] = [11 \cdots 1]$. Note that for a given letter a, the vector $[S]M_a$ is exactly the same as the vector $[Sa]$; this follows from the definition of M_a.

Given some word $w = a_1 a_2 \cdots$, where each a_i is some letter, we define M_w to be the product $M_{a_1} M_{a_2} \cdots M_{a_n}$. Repeated applications of $[S]M_a = [Sa]$ prove that $[Sw] = [S]M_w$ for any word w.

2 A lower bound on $C(p, k)$

Let $F(p, k)$ denote the family of automata which are characterized by $|Q| = p$ and $A = \{l(\pi), l(B \to C)\}$ for $|B| = |C| = k$. Let $C(p, k)$ denote the maximum possible length of the minimal reset word among automata in $F(p, k)$.

Theorem 1. *For any prime p, and any integer $1 \leq k \leq \frac{p-1}{2}$, a lower bound for $C(p, k)$ is given by*

$$C(p, k) \geq (p-1)(p-k). \tag{1}$$

Proof. Since we know that every member of $F(p, k)$ synchronizes, it suffices to find some automaton which has a reset word with length at least $(p-1)(p-k)$. Consider the automaton in $F(p, k)$ defined by $B = \{1, 2, \cdots, k\}$ and $C = \{p-k+1, p-k+2, \cdots, p\}$. For convenience, let the letter representing $l(\pi)$ be b and let the letter representing $l(B \to C)$ be a.

Now consider a coin representation of the automaton. On each state, a coin is initially placed, and when a letter is called, the coins move along the respective arrows. If two coins are both directed to the same position, then the coin which was initially at that position remains and the other coin is removed. Now given some synchronizing word, there exists some coin, call it the "gold coin", which is never removed and remains until it is the only coin left. So the initial layout can be described as one gold coin covering some state and $p-1$ regular coins covering the rest of the states. For a coin c, define $p(c)$ to be the value of the state it is currently occupying. Furthermore, let $d(c)$ denote the number of clockwise

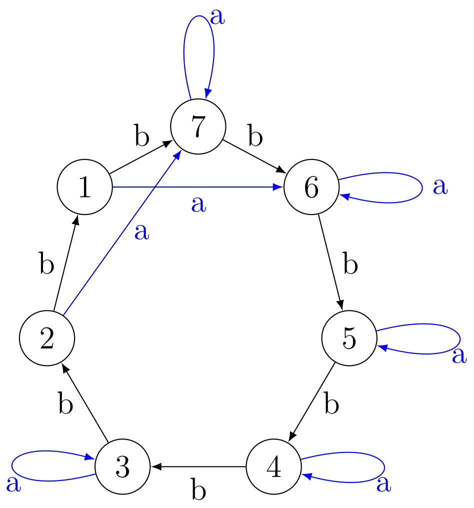

Figure 2: Extremal Automaton in F(7, 2)

jumps of distance k that are necessary to reach the gold coin from $p(c)$. Formally, if g is the gold coin, then:

$$d(c) \equiv \frac{p(c) - p(g)}{k} \pmod{p}, \quad d(c) \in \{0, 1, \cdots, p-1\}.$$

This is always well defined because $\gcd(k, p) = 1$.

Now consider the following quantity:

$$Z = \max\{(p - k + 1)d(c) + p(c) \mid \text{coin } c\}$$

Given a reset word of length r, let $Z_0, Z_1, \cdots, Z_r$ be the Z quantities corresponding to the automaton after $0, 1, \cdots, r$ steps respectively. Note that initially, there exists some coin for which $d(c) = p - 1$; hence, $Z_0 \geq (p-k+1)(p-1) + p(c) \geq (p-k+1)(p-1) + 1$.

After the last letter of the reset word has been applied, only the gold coin is left. Since $d(g) = 0$, it follows that $Z_r \leq p(g) \leq p$.

Lemma 1. *For $i \in \{0, 1, \cdots, r-1\}$:*

$$Z_i - Z_{i+1} \leq 1. \tag{2}$$

Proof. It suffices to prove that (2) is true when each of a and b is applied to some set of states. If b is applied, then $d(c)$ does not change for any of the coins, and $p(c)$ either decreases by one or increases by $p-1$. Hence, $(p-k+1)d(c)+p(c)$ decreases by at most one for each coin, and it follows that $Z_i - Z_{i+1} \leq 1$ in this case,as desired.

If instead a is applied, then denote by $c*$ the coin which holds the maximum value of $(p-k+1)d(c)+p(c)$ after the ith letter, and denote by g the gold coin. If neither $c*$ nor g moves when a is applied, then $d(c*), p(c)$ remain constant, so $Z_{i+1} \geq Z_i$ in this case. If they both move, then $p(c*)$ increases while $d(c*)$ remains constant, so $Z_{i+1} > Z_i$. If only the gold coin moves, then it moves k spaces clockwise; it follows that $d(c*)$ increases by 1, while $p(c*)$ remains the same. So, again, $Z_{i+1} > Z_i$.

We are left with checking the case where $c*$ moves, while the gold coin does not. Consider the coin c_1*, possibly equal to $c*$, which rests in the space where $c*$ was going when the operation a was performed. Then c_1* is k spaces clockwise from where $c*$ originated, so $d(c_1*)$ at state $i+1$ is one less than $d(c_1)$ at stage $i+1$. Furthermore, the position of coin c_1* at state $i+1$ is $p-k$ greater than the position of coin $c*$ at state i. It follows that:

$$Z_{i+1} \geq d(c_1*)(p-k+1) + p(c_1*) = Z_i - (p-k+1) + (p-k) = Z_i - 1$$

as desired. □

Now:

$$Z_0 - Z_r \geq [(p-k+1)(p-1)+1] - p = (p-1)(p-k)$$

and Lemma 1 demonstrates that Z decreases by at most 1 for each letter applied. Hence this automaton's reset word has length $|r| \geq (p-1)(p-k)$, as desired. □

We propose the following conjecture:

Conjecture 1. *For any prime p and integer k with $1 \leq k \leq \frac{p-1}{2}$, the value of $C(p,k)$ is given by*

$$C(p,k) = (p-1)(p-k).$$

3 Pin's Theorem

We now consider a reverse approach to the synchronizing problem. Instead of reducing a set of full states down to some singleton, we will select a singleton and "explode" it until the full set is obtained.

The **inverse** a^{-1} of a letter a has a matrix corresponding to the transpose of M_a. Given a word $w = a_1 a_2 \cdots a_n$, its inverse is defined as $w^{-1} = a_n^{-1} a_{n-1}^{-1} \cdots$. It follows that:

$$M_{w^{-1}} = M_{a_n^{-1}} M_{a_{n-1}^{-1}} \cdots M_{a_1^{-1}} = M_{a_n}^T M_{a_{n-1}}^T \cdots M_{a_1}^T = M_w^T$$

We now present a proof of the following theorem, which is due to Pin [7]. Many of the ideas involved with this proof are similar to those used by Steinberg [8].

Theorem 2. *Let α be an automaton with a a cycle $b = l(\pi)$ and a letter a which is a non-permutation. Then there exists a reset word of α with length at most $(p-1)^2$.*

Proof. Our proof of this theorem is derived from the following key lemma:

Lemma 2. *Assume a set $S \subseteq Q$ is given such that $|S| = i$, $2 \leq i \leq p-1$. Then there exists some integer k, $0 \leq k \leq p-1$, such that for the word $w = ab^k$, we have $|Sw^{-1}| > |S|$.*

Proof. First, note that the following identity holds, where $\langle x, y \rangle$ denote the dot product of x and y:

$$|S| = \sum_{i=1}^{S} [S]_i = \langle [S], [Q] \rangle.$$

Therefore, for a word w:

$$|Sw^{-1}| = \langle [S] M_{w^{-1}}, [Q] \rangle = \langle [S] M_w^T, [Q] \rangle = \langle [S], [Q] M_w \rangle.$$

Note that $[Q](M_b)^k = [Q]$ for any integer k, since b is just a permutation. It follows that:

$$|S| = \langle [S], [Q] \rangle = \langle [S], [Q](M_b)^k \rangle.$$

So, for $w = ab^k$:

$$|Sw^{-1}| - |S| = \langle [S], [Q] M_a (M_b)^k - [Q](M_b)^k \rangle = \langle [S], [Q](M_a - I)(M_b)^k \rangle.$$

Let $[A] = [Q](M_a - I)$. Then:

$$|Sw^{-1}| - |S| = \langle [S], [A](M_b)^k \rangle. \tag{3}$$

Note that by the assumption, a is a nonpermutation, so $[Q]M_a \neq [Q]$, and it follows that $[A] \neq [0, 0, \cdots, 0]$. Now since b is just a simple cycle which takes p to $p-1$, $p-1$ to $p-2$, $\cdots$, 1 to p, it follows that $[A](M_b)^k$ is just a shift of $[A]$ k units to the left. That is,

$$([A](M_b)^k)_i = [A]_{i+k}.$$

Where indices are taken modulo p.

Now let ω_p be a primitive pth root of unity. Then it is known that over $\mathbb{Z}$, the minimal polynomial of ω is $x^{p-1} + x^{p-2} + \cdots + 1$. We define $[S]', [A]'$ as follows:

$$[S]' = \sum_{i=1}^{p} \omega_p^{p-i} [S]_i.$$

$$[A]' = \sum_{i=1}^{p} \omega_p^{i} [A]_i.$$

We call $[A]'$ the signature of the automaton α. Since $2 \leq |S| \leq p-1$, it follows that $[S]' \neq 0$. Also, since the sum of the entries in $[A]$ is zero but $[A] \neq [0, 0, \cdots, 0]$, it follows that $[A]' \neq 0$. Now note that:

$$\begin{aligned} [S]'[A]' &= \left(\sum_{i=1}^{p} \omega_p^{p-i} [S]_i \right) \left(\sum_{i=1}^{p} \omega_p^{i} [A]_i \right) \\ &= \sum_{k=0}^{p-1} \left(\omega_p^k \sum_{i=1}^{p} \left([S]_i [A]_{i+k} \right) \right) \\ &= \sum_{k=0}^{p-1} \omega_p^k \langle [S], [A](M_b)^k \rangle. \end{aligned}$$

Since neither $[S]'$ nor $[A]'$ is equal to zero, it follows that their product must be nonzero as well. Therefore:

$$\text{There exists } k, \quad 0 \leq k \leq p-1 \quad \text{such that} \quad \langle [S], [A](M_b)^k \rangle \neq 0. \tag{4}$$

Now since the sum of the elements in $[A]$ is zero, it follows that:

$$(\sum_{k=0}^{p-1}[A](M_b)^k)_i = [A]_1 + [A]_2 + \cdots + [A]_p = 0$$

for $0 \leq i \leq p-1$. Therefore

$$\begin{aligned}\sum_{k=0}^{p-1}\langle [S],[A](M_b)^k\rangle &= \langle [S], \sum_{k=0}^{p-1}[A](M_b)^k\rangle \\ &= \langle [S],[0,0,\cdots,0]\rangle \\ &= 0\end{aligned}$$

Combining this with (4), it follows that:

$$\text{There exists} \quad k, 0 \leq k \leq p-1 \quad \text{such that} \quad \langle [S],[A](M_b)^k\rangle > 0. \tag{5}$$

Combine this with (3) to see that $|Sw^{-1}| > |S|$ for this k, so the lemma is proved. □

Now choose some "singleton" S with $|S| = 1$ such that $|Sa| > 1$. (Such a singleton must exist because a is not a permutation.)

By Lemma 2, we can now always find some word w which strictly increases the size of S while using at most p letters. After doing this at most $p-2$ times, we necessarily obtain $|S| = p$; that is, $S = Q$. Then the concatenation of all words obtained in this manner is necessarily a reset word of the automaton α. The total length of this reset word is at most:

$$1 + (p-2)p = (p-1)^2$$

as desired. □

Corollary 1. *For a prime p and an integer $1 \leq k \leq \frac{p-1}{2}$, it is true that:*

$$C(p,k) \leq (p-1)^2$$

4 The Cyclotomic Ring $\mathbb{Z}[\omega_p]$

We work now in the ring $\mathbb{Z}[\omega_p]$, where ω_p is a primitive pth root of unity. For $z \in \mathbb{Z}[\omega_p]$, define $\sigma_i(z)$ as the algebraic integer which results when ω_p is replaced everywhere with ω_p^i in z. We define the norm $N(z)$ as follows:

$$N(z) = \prod_{i=1}^{p-1} \sigma_i(z).$$

Lemma 3. *An algebraic integer u within this ring is a unit iff $|N(u)| = 1$.*

The following lemmata appear in Weston's Algebraic Number Theory [9]; our proofs of them are similar to the proofs given. Proofs of lemmata 3, 4, and 5 are given in Appendix B.

Lemma 4. *Let $z \in \mathbb{Z}[\omega_p]$ be some polynomial such that $|\sigma_i(z)| = 1$ for $i = 1, 2, \cdots, p-1$. Then $z = \pm\omega_p^i$ for some integer i.*

Lemma 5. *Let $u \in \mathbb{Z}[p]$ be a unit. Then $\frac{u}{\bar{u}} = \omega_p^i$ for some integer i.*

These lemmata lead to the following theorem:

Theorem 3. *Let α be a p-state automaton with a cycle $b = l(\pi)$ and a non-permutation a with signature $[A]'$. Then if $N([A]') \neq p$, it follows that for any set S with $2 \leq |S| \leq p-1$, there exists either a word w of length at most $p-1$ for which $|Sw^{-1}| \geq |S|+1$, or a word w_1 of length p for which $|Sw_1^{-1}| \geq |S|+2$.*

Proof. We prove the theorem's contrapositive. Assume that neither of the given words exist.

It follows that

$$\langle [S], [A](M_b)^k \rangle \leq 0 \quad \text{for} \quad k = 0, 1, \cdots, p-2$$

and that

$$\langle [S], [A](M_b)^{p-1} \rangle = 1.$$

Because $\sum_{k=0}^{p-1} \langle [S], [A](M_b)^k \rangle = 0$, it follows that exactly one of the coefficients of the product $[S]'[A]'$ is -1 and the other is 1. Hence $[S]'[A]'$ must be of the form $\omega_p^d - \omega_p^c$ for some d, c. But note that:

$$\begin{aligned} N(\omega_p^d - \omega_p^c) &= \prod_{i=1}^{p-i} (\omega_p^{di} - \omega_p^{ci}) \\ &= \prod_{i=1}^{p-i} \omega^{ci} (\omega_p^{di-ci} - 1) \\ &= \omega_p^{\frac{p(p+1)}{2}} \prod_{i=1}^{p-1} (\omega_p^i - 1) \\ &= p, \end{aligned}$$

where the last equality holds due to $\prod_{i=1}^{p-1}(x - \omega_p^i) = 1 + x + \cdots + x^{p-1}$. From $N(\omega_p^d - \omega_p^c) = p$, it follows that $N(1 - \omega_p) = p$. Because the sum of the elements in $[A]$ is zero, it follows that $(1 - \omega_p) \mid [A]'$, and so $p \mid N([A]')$. But we also have

$$N([A]') \mid N([A]')N([S]') = N([A]'[S]') = p.$$

So that $N([A]') = p$, as desired. □

5 Conjecture 1 for $k = 2$

Here we prove the following theorem about the maximal reset word of automata within $F(p, 2)$. Recall that $F(p, 2)$ is the set of automata which consist of $|Q| = p$, and $A = \{l(\pi), l(B \to C\}$, where $|B| = |C| = 2$.

Theorem 4. *Let $p \geq 5$ be an odd prime. Then:*

$$C(p, 2) = (p-1)(p-2). \tag{6}$$

Proof. By Theorem 1, it is true that $C(p, 2) \geq (p-1)(p-2)$. It suffices to prove that some reset word of length at most $(p-1)(p-2)$ exists for all automata in the family $F(p, 2)$.

Take some $\alpha \in F(p, 2)$, with a letter $b = l(\pi)$ and a letter a corresponding to the nonpermutation. The two merging arcs of α are given by $a_1 = (x_1, y_1)$ and $a_2 = (x_2, y_2)$, so that $x_1 a = y_1 a = x_1$, and $x_2 a = y_2 a = x_2$. Throughout this proof, we will define the distance from state i to state j to be the integer $k, 0 \leq k \leq p-1$ such that $i(b^k) = j$. The length of a given arc a_i is the distance between state x_i and state y_i. We will assume WLOG that the distance from x_1 to x_2 is less than the distance between x_2 to x_1; since the sum of these distances is p, it follows that the distance from x_1 to x_2 is at most $\frac{p-1}{2}$. From the definition of p, the distance from state i to state j is always equivalent to $i - j$ modulo p.

Note that the signature $[A]'$ of this automaton is of the form $\omega_p^f + \omega_p^g - \omega_p^c - \omega_p^d$ for some distinct f, g, c, d. Rotations of the letter a do not affect the automaton's nature as the letter b is invariant under any rotation. Therefore, we may WLOG suppose that $f = \min\{f, g, c, d\}$, and $d = \max\{f, g, c, d\}$.

Lemma 6. *Suppose that a_1, a_2 have different lengths. Let $z = x_2 - x_1$,so that $z \leq \frac{p-1}{2}$. Then for $w = ab^z a$, we can choose some S with $|S| = 1$ and $|Sw^{-1}| \geq 3$.*

Proof. We claim that $S = \{x_2\}$ works. Indeed, it suffices to find three distinct elements

$e_1, e_2, e_3 \in Q$ such that $e_1w = e_2w = e_3w = x_2$. Since the arcs involved have different lengths, it follows that $x_1 - y_1 \neq x_2 - y_2$, so $y_2 + z = y_2 + (x_1 - y_1) \neq y_1$. Also $y_1 + z \neq y_1$ since $t \neq 0$, so $y_2 + z$ is not the head end of any arc. It follows that $(y_2 + z)a = y_2 + z$. This means that

$$(y_2 + z)w = (y_2 + z)ab^z a = (y_2 + z)b^z a = y_2 a = x_2.$$

We also have

$$x_1 w = (x_1 a)b^z a = (x_1 b^z)a = x_2 a = x_2,$$

$$y_1 w = (y_1 a)b^z a = (x_1 b^z)a = x_2 a = x_2.$$

Since $y_2 + z = (y_2 - y_1) + x_1$, it follows that $y_2 + z, x_1, y_1$ are distinct. So $|Sw^{-1}| \geq 3$ as desired. □

Lemma 7. *Given distinct integers* $0 \leq \{f, g, c, d\} \leq p - 1$ *such that* $f = \min\{f, g, c, d\}$ *and* $d = \max\{f, g, c, d\}$,

$$N(\omega_p^f + \omega_p^g - \omega_p^c - \omega_p^d) = p \implies |f - g| = |c - d|. \tag{7}$$

Proof. There are two cases here: $f < g < c < d$ and $f < c < g < d$. In the first case,

$$\begin{aligned}
[A]' &= (\omega_p^f - \omega_p^c) + (\omega_p^g - \omega_p^d) \\
&= (1 - \omega_p)(\omega_p^f + \omega_p^{f+1} + \cdots + \omega_p^{c-1} + \omega_p^g + \omega_p^{g+1} + \cdots + \omega_p^{d-1} \\
&= (1 - \omega_p)(\omega_p^f + \omega_p^{f+1} + \cdots + \omega_p^{g-1} + 2(\omega_p^g + \omega_p^{g+1} + \cdots + \omega_p^{c-1}) + \omega_p^c + \omega_p^{c+1} + \cdots + \omega_p^d)
\end{aligned}$$

Let

$$u = (\omega_p^f + \omega_p^{f+1} + \cdots + \omega_p^{g-1} + 2(\omega_p^g + \omega_p^{g+1} + \cdots + \omega_p^{c-1}) + \omega_p^c + \omega_p^{c+1} + \cdots + \omega_p^d)$$

Because $N(1-\omega_p) = p$, $N([A]') = p$ only if u is a unit. Then according to Lemma 5, there exists some integer i such that $u = \bar{u}\omega_p^i$. In other words, a reversal of the coefficients in u results in an algebraic integer which is a shift of u by ω_p^i. This means that the first and third sequences must have equal length, so $g - f = d - c$, which means that $|f - g| = |c - d|$, as desired. The second case is analogous. □

Now if $|f - g| \neq |c - d|$, then according to the contrapositive of Lemma 7, it follows that $N([A]') \neq p$. Theorem 3 shows that for any $S \subseteq Q$ such that $|S| \geq 3$, we can find a word w such that either $|Sw^{-1}| \geq |S| + 1$ and w has length at most $p - 1$, or $|Sw^{-1}| \geq |S| + 2$ and w has length at most p. This means that from $|S| = 3$ to $|S| = p$, the average length of the word required to increase $|S|$ by 1 is at most $p - 1$. By Lemma 6, there exists a word of length at most $\frac{p-1}{2} + 2$ which takes some $|S| = 1$ to some $|S| \geq 3$. Therefore, there exists a reset word of length at most:

$$\left(\frac{p-1}{2} + 2\right) + (p-1)(p-3) = p - 1 - \frac{p-5}{2} + (p-1)(p-3) \leq (p-1)(p-2)$$

as desired.

It remains to check the cases where $|f - g| = |c - d|$. The analysis of these cases is provided in Appendix C. This exhausts all possible cases, and so the theorem is proved. □

6 Conclusion

We defined $C(p, k)$ to be the maximal possible length of the minimal reset word of automata within the family $F(p, k)$. We have proven that

$$(p-1)(p-k) \leq C(p,k) \leq (p-1)^2 \tag{8}$$

for $k \geq 3$, where the right hand side of this[6] is due to Pin's Theorem. We proved the left side by utilizing an extension of Volkov's [10] gold coin argument. Using the ring $\mathbb{Z}[\omega_p]$, we further proved that

$$C(p, 2) = (p - 1)(p - 2). \tag{9}$$

We conjecture that in general, equality holds on the left side of equation (8).

7 Acknowledgments

I would like to thank the Research Science Institute and the Center for Excellence in Education for making this project possible. I thank Ph.D. Ellen J. Maycock, Associate Executive Director from American Mathematical Society, Mr. John Yochelson, President from Building Engineering and Science Talent (BEST), Laura Stubbs, Ph.D., Director of Science and Technology Initiatives from the Department of Defense, Mr. Chad Gerson, Senator Lindsey Graham, Mr. Douglas E. Heimburger, Ms. Susan Lee Ko, and Mr. David T. Leighton, who helped sponsor my participation. I extend additional thanks to my mentor, Mr. Chiheon Kim for his time, expertise, and advice. I thank my tutor, Dr. John Rickert, for his assistance with editing and refining this paper. Finally, I thank the MIT math department and all of the staff at RSI who assisted me throughout the summer.

References

[1] M. V. Volkov. Synchronizing automata and the cerny conjecture. *Proc. LATA*, '08:11–27, 2008.

[2] J. Cerny. Poznmka k homognnym experimentom s konenmi automatami. *Matematicko-fyziklny asopis Slovenskej Akadmie Vied*, 14:208–216, 1964.

[3] A. Roman. Experiments on synchronizing automata. *Schedae Informaticae*, 19:35–51, 2010.

[4] P. Frankl. An extremal problem for two families of sets. *Eur. J. Comb.*, 3:120–135, 1982.

[5] A.-N. Trahtman. Modifying the upper bound on the length of a minimal synchronizing word. *LNCS*, 6914:173–180, 2011.

[6] F. Arnold and B. Steinberg. Synchronizing groups and automata. 6281:1–12, 2005.

[7] J.-E. Pin. On two combinatorial problems arising from automata theory. *Proc. Colloq. Marsaille-Luminy*, 17:535–548, 1981.

[8] F. Arnold. A linear algebra approach to synchronizing automata. *Master Thesis*, pages 1–46, 2004.

[9] T. Weston. *Algebraic Number Theory.* AMS, 2001.

[10] D. Ananichev and M. V. Volkov. Synchronizing automata with a letter of deficiency 2. *Theoretical Computer Science*, 376:30–41, 2007.

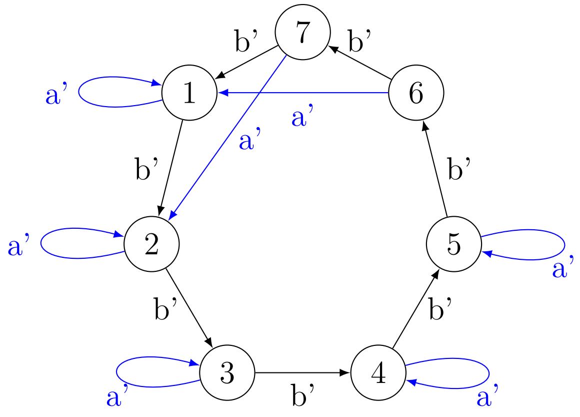

Figure 3: Inverse of Figure 1

A Algorithm

Figure 3 shows the inverse of Figure 1; we use l' to denote the path of l^{-1} for a letter l. We will use it to demonstrate the intuition behind our algorithm. First, the singleton $\{1\}$ is chosen, exploded into $\{1, 6\}$. It is then rotated to $\{2, 4\}$ and exploded to $\{7, 2, 4\}$. Notice that a path of length 3 along the graph G_m is created with its head located at 6. Notice also that if we try to apply $(b^{-1})^5 a^{-1}$, then it would not increase the size of S; indeed, the other arc "gets in the way," and seems to prevent this pattern from continuing. To adjust for this, the algorithm now expands once with the other arc; indeed, applying instead $(b^{-1})^6 a^{-1}$ gives a successful explosion along the other arc. Then the algorithm switches back to the original arc, here applying $(b^{-1})^6 a^{-1}$ before finishing with $(b^{-1})^5 a^{-1}$.

In summary, the algorithm explodes along a chosen arc until it is prevented from doing so, at which point it switches momentarily to the other arc, then back, where it remains.

B Lemmata

Lemma 3. *An algebraic integer u within this ring is a unit iff $|N(u)| = 1$.*

Proof. If u is a unit, then $uv = 1$ for some $v \in \mathbb{Z}[\omega_p]$. Hence $N[u]N[v] = 1$, so $|N(u)| = 1$. If $|N(u)| = 1$, then $u\left(\prod_{i=2}^{p-1} \sigma_i(z)\right) = \pm 1$, so u is a unit. □

The following lemmata appear in Weston's Algebraic Number Theory [9]; our proofs of them are similar to the proofs given.

Lemma 4. *Let $z \in \mathbb{Z}[\omega_p]$ be some polynomial such that $|\sigma_i(z)| = 1$ for $i = 1, 2, \cdots, p-1$. Then $z = \pm\omega_p^i$ for some integer i.*

Proof. Let S be the family of algebraic integers z which satisfy $|\sigma_i(z)| = 1$ for $i = 1, 2, \cdots, p-1$. Then S is closed under multiplication. Indeed, if $u, v \in S$, then $|\sigma_i(u)||\sigma_i(v)| = 1$ for $i = 1, 2, \cdots, p-1$, and it follows that $uv \in S$. Now we will prove that $|S|$ is finite. Consider the characteristic polynomial $f(x) \in \mathbb{Z}[x]$ defined as:

$$f(x) = \prod_{i=1}^{p-1}(x - f(w_p^i)).$$

For $0 \leq k \leq p-1$, the coefficient of x^k in $f(x)$ is the sum of $\binom{p-1}{k}$ elements, each with absolute value equal to 1. Hence, each coefficient is bounded in some finite range, which implies that only a finite possible number of such characteristic polynomials exist. Each polynomial has a degree at most $p-1$, and therefore has at most $p-1$ roots. It follows that $|S|$ is indeed finite. But S is closed under multiplication, so S must contain only algebraic integers which are roots of 1. It follows that $z = \pm\omega_p^i$ for some integer i, as desired. □

Lemma 5. *Let $u \in \mathbb{Z}[p]$ be a unit. Then $\frac{u}{\bar{u}} = \omega_p^i$ for some integer i.*

Proof. Let $u = U(\omega)$. Since $\bar{u}$ is also a unit, it follows from $N(\bar{u}) = N(u) = 1$ that $\frac{u}{\bar{u}}$ is an algebraic integer. But $\left|\frac{\sigma_i(u)}{\sigma_i(u)}\right| = 1$ for each i, so by Lemma 5, $\frac{u}{\bar{u}} = \pm\omega_p^i$. Now, it suffices to prove that for any integer i, $u \neq -\omega_p^i \bar{u}$.

Assume otherwise. Let $u = \sum_{i=0}^{p-1} a_i \omega_p^i$. Then $\bar{u} = \sum_{i=0}^{p-1} a_i \omega_p^{p-i}$. Since $1 - \omega_p^i | 1 - \omega_p$, it follows that:

$$u \equiv a_0 + a_1 + \cdots + a_{p-1} \equiv \bar{u} \mod (1-\omega_p^i).$$

But this means that:

$$\bar{u} \equiv u \equiv -\omega_p^i \bar{u} \equiv -\bar{u} \mod (1-\omega_p^i).$$

So $2\bar{u} \equiv 0 \mod (1-\omega_p^i)$, which is an impossibility since 2 is not an ideal in $\mathbb{Z}[\omega_p]$. Hence $\frac{u}{\bar{u}} = \omega_p^i$ for some integer i, as desired. □

C Remaining Cases of Theorem 4

Here, we discuss the case when $|f-g| = |c-d|$.

In this case, the two arcs are either have the same length and are in the same direction, or are parallel to each other when the states are represented along a regular $p-$gon. We consider these cases separately.

First we consider the case where the given arcs are parallel. Algebraically, this means that $x_1 - x_2 = -(y_1 - y_2)$. Now we provide a lemma concerning the explosion which occurs from $|S| = p-1$ to $S = q$ within this class of automata.

Lemma 8. *Assume that $|S| = p-1$. Then there exists some word w with length at most $p-z$ such that $|Sw^{-1}| = Q$.*

Proof. Because $z = x_1 - x_2 = y_2 - y_1$ is the shorter distance between the arc heads, it follows that there exists a rotation of the states in S of length at most $p-z-1$ which sends the only element not in S to either y_1 or y_2. This is true regardless of the direction of rotation, so choose the direction to be opposite to that of b. This implies that we can choose some k, with $0 \le k \le p-z-1$, such that $[S](M_b^T)^k$ results in the vector representation of a subset which is missing only y_1 or y_2. This means $[S](M_b^T)^k M_a^T = [Q]$, so that ab^k is a word which satisfies $|Sw^{-1}| = Q$ and has length at most $p - z$, as desired. □

By Lemma 6, there exists a word with length at most $z + 2$ which takes some $|S| = 1$ to some $|S| = 3$. Then, due to Lemma 2, it is possible to explode from $|S| \geq 3$ to $|S| \geq p - 1$ with at most $(p - 4)p$ letters. Finally, Lemma 8 shows that is it possible to explode from $|S| = p - 1$ to $|S| = p$ in at most $p - z$ steps. Therefore, there exists a reset word with a length at most equal to:

$$(z + 2) + p(p - 4) + (p - z) = (p - 1)(p - 2)$$

as desired.

Finally, it suffices to consider the case where the two given arcs have equal length. Once again, we approach this with several cases.

First, assume that the common arc length is at least 3. Then $y_1 - x_1 = y_2 - x_2 = m$ for some $m \geq 3$. To retain generality, we no longer assume anything about the distance from x_1 to x_2. We now algorithmically construct a reset word of length at most $(p-1)(p-2)$. Instead of constructing the word directly, we construct the inverse of the word which explodes some singleton S, $|S| = 1$ to the full set Q. Consider the graph G_m which appears when every pair of states with a distance k are connected. Then our algorithm constructs a path of on states along the edges of G_m which grows with each step. The algorithm is as follows:

1. Start with $S = \{x_1\}$, and apply a^{-1} to obtain $S = \{x_1, x_1 - m\}$.
2. While it still increases the size of $|S|$, continue applying $(b^{-1})^{p-m}a^{-1}$, taking $S = \{x_1, x_1 - m, \cdots, x_1 - im\}$ to $S = \{x_1, x_1 - m, \cdots, x_1 - (i + 1)m\}$ for some i.

3. The first time that $(b^{-1})^{p-m}a^{-1}$ would not increase $|S|$, apply instead $(b^{-1})^{|x_1-y_2|}a^{-1}(b^{-1})^{|x_2-y_1|}a^{-1}$, increasing the size of S by 2 and taking $S = \{x_1, x_1 - m, \cdots, x_1 - jm\}$ to $S\{x_1, x_1 - m, \cdots, x_1 - (j+2)m\}$ for some j.
4. Continue applying $(b^{-1})^{p-m}a^{-1}$ until the full set Q is obtained.

For an example of this algorithm in action, see Appendix A. This algorithm produces a reset word of length of length $1 + (1 + |x_1 - y_2|) + (1 + |x_2 - y_1|) + (p-4)(p-m+1)$. Note that (x_1, y_2) and (x_2, y_1) cannot both be adjacent pairs, and these quantities have the same parity so their sum is even. It follows that $|x_1 - y_2| + |x_2 - y_1| \leq 2p - 4$. Therefore, the length of the reset word is at most:

$$\begin{aligned}1 + (1 + |x_1 - y_2|) + (1 + |x_2 - y_1|) + (p-4)(p-m+1) &\leq 3 + (2p-4) + (p-2)(p-4)\\ &\leq p^2 - 4p + 7 = (p-1)(p-2) - (p-5)\\ &\leq (p-1)(p-2)\end{aligned}$$

as desired.

If $m = 2$, then there exists some $k, 0 \leq k \leq p-3$ and some singleton $S, |S| = 1$ such that $|Sa^{-1}(b^{-1})^k a^{-1}| \geq 3$. Then we proceed with the algorithm from step 2 onward to achieve a reset word with length at most

$$\begin{aligned}(p-1) + (1 + |x_1 - y_2|) + (1 + |x_2 - y_1|) + (p-5)(p-1) &\leq (p+1) + (2p-4) + (p-5)(p-1)\\ &\leq p^2 - 3p + 2\\ &= (p-1)(p-2).\end{aligned}$$

Note that equality holds when the arcs of length 2 cross; indeed, in this case $\{|x_1 - y_2|, |x_2 - y_1|\} = \{p-1, p-3\}$ so the above inequality is sharp.

Finally, we consider the case where the arc lengths are each equal to 1. First, assume that these arcs are directly next to each other, say $a_1 = (1, 2)$ and $b_1 = (3, 4)$. Consider the word $w = abab^{p-3}a$. One can check that $1w = 2w = 3w = 4w = 3$. Therefore, if $S = \{3\}$, then $|Sw^{-1}| \geq 4$. Furthermore, the length of w is $p+1$. But by Lemma 2, it is possible to explode from $|S| \geq 4$ to Q in at most $p(p-4)$ steps; therefore there exists a reset word of length at most $p(p-4)+p+1 = p^2-3p+1 \leq (p-1)(p-2)$ as desired.

The very last case concerns arc pairs of the form $(1, 2), (h, h+1)$, where $4 \leq h \leq \frac{p+1}{2}$; due to symmetry, the upper bound can be assumed WLOG. Note that we must necessarily have $p \geq 7$ for this case to exist, so $p-1 \geq \frac{p+5}{2} > h+1$ here. A similar idea works now; let $w = ab^{p-h}ab^{h-2}a$. One can check that $(p-1)w = pw = 1w = 2w = 1$. Therefore, if $S = \{1\}$, then $|Sw^{-1}| \geq 4$. Furthermore, the length of w is $p+1$. But by Lemma 2, it is possible to explode from $|S| \geq 4$ to Q in at most $p(p-4)$ steps; therefore there exists a reset word of length at most $p(p-4)+p+1 = p^2-3p+1 \leq (p-1)(p-2)$ as desired.