A REPRESENTATION THEORETIC APPROACH TO SYNCHRONIZING AUTOMATA

FREDRICK ARNOLD AND BENJAMIN STEINBERG

Abstract. This paper is a first attempt to apply the techniques of representation theory to synchronizing automata and the Černý conjecture. In particular, we obtain a new proof of Pin's theorem and generalizations.

1. Introduction

Černý conjectured that every sychronizing automaton with n states has a synchronizing word of length at most $(n-1)^2$ [2]. This problem has been open now for over forty years. One of the first breakthroughs was Pin's proof of the Černý conjecture for circular automata with a prime number of states; an automaton is said to be circular if there is an input that cyclically permutes the states. Pin's proof makes use of linear algebra and the irreducibility of the cyclotomic polynomial to prove the result. Since then, linear algebra has played an ever increasing role in the literature. For instance, Dubuc's solution of the Černý conjecture for circular automata [4] in general and Kari's solution for the case of Eulerian automata [5] both make heavy use of linear algebraic techniques. The right context for such an approach, it seems to us, is via representation theory [7]. In this paper, derived from the first author's Master's Thesis [1], we show how representation theory can be used to obtain a simple (and we believe elegant) proof of a more general version of Pin's result. Furthermore, it sheds light on why Pin's proof works: namely, it is shown that the irreducibility of the cyclotomic polynomial corresponds to the irreducibility of a certain representation and it is this that is needed to obtain the synchronizing word of the appropriate size.

We believe that by using representation theoretic means, it should eventually be possible to prove the Černý conjecture for synchronizing automata such that the group of units of the transition monoid contains a regular permutation group. Dubuc handled the case of a cyclic group (with one element generating set) essentially by using the representation theory of cyclic groups, but in the language of minimal polynomials. It seems likely that explicit use of representation theory will at least lead to a solution for regular Abelian permutation groups.

Date: July 20, 2005.

This work was supported by NSERC..

2. Synchronizing Automata

For us, an *automaton* $\mathcal{A} = (Q, A)$ over an alphabet A consists of a finite set of states Q and an action of A^* on Q by total functions (which we leave out of the notation). If $q \in Q$ and $w \in A^*$, then qw denotes the state reached when w acts on q. The *transition monoid* $M(\mathcal{A})$ is the quotient of A^* that identifies two words if they act the same on all states of Q. It is a finite monoid of functions acting on Q. So we are considering deterministic automata without initial or final states. An element $a \in A$ will be called a permutation if the map $q \mapsto qa$ is a permutation; otherwise, it will be called a non-permutation. An automaton (Q, A) is said to be *synchronizing* if there is a word w such that $qw = q'w$ for all $q, q' \in Q$, i.e. $q \mapsto qw$ is a constant map. Such a word w is called a *synchronizing* (or *reset*) word for (Q, A).

For $w \in A^*$ and $S \subseteq Q$, we set

$$Sw^{-1} = \{q' \mid q'w \in S\}.$$

Our strategy for finding synchronizing words will then be to show that, given $\emptyset \neq S \subset Q$, we can find a word $u \in A^*$ such that $|Su^{-1}| > |S|$. Then we will be able to find a synchronizing word by starting with a one element set and expanding repeatedly. If u can always be chosen to have size at most k, then we can construct a synchronizing word of size at most $1 + (n-2)k$. Indeed, we can expand a one element set with a single letter and then we have to expand $n-2$ more times using our bound k. In particular, if $k = n = |Q|$, then we get $1 + (n-2)n = (n-1)^2$. We now state Černý's conjecture.

Conjecture 1 (Černý's conjecture [2])**.** *Every synchronizing automaton with n states has a synchronizing word with length at most $(n-1)^2$.*

3. Linearization of the problem

Let M be a monoid. Then a representation of M (over the rationals) of degree n is a (monoid) homomorphism $\varphi : M \to M_n(\mathbb{Q})$, where $M_n(\mathbb{Q})$ denotes the monoid of $n \times n$ matrices with entries in the field $\mathbb{Q}$ of rational numbers. All vector spaces considered in this paper are over the field $\mathbb{Q}$. The vector space $V = \mathbb{Q}^n$ is called the *representation space* of φ. Sometimes we say that V *carries* the representation φ. A subspace $W \subseteq V$ is said to be *M-invariant*, if $WM\varphi \subseteq W$. The representation φ is said to be *irreducible* if the only M-invariant subspaces of V are $\{0\}$ and V itself.

If G is a finite group, then Maschke's theorem [7] shows that any representation of G splits into a direct sum of G-invariant subspaces such that the representation carried by each summand is irreducible. Moreover, this decomposition is essentially unique [7]. The *trivial representation* of G is the homomorphism $\varphi : G \to \mathbb{Q}$ given by $g\varphi = 1$ for all $g \in G$. This is an irreducible representation of degree 1. For a representation $\varphi : G \to M_n(\mathbb{Q})$, the *trivial component* is the subspace V^G of the representation space V consisting of those vectors fixed by $G\varphi$. It is the direct sum of the copies of the trivial representation in the aforementioned decomposition of φ into irreducible constituents. The projection of V onto V^G associated to this decomposition is given by $\frac{1}{|G|}\sum_{g\in G} g\varphi$ [7].

We fix for the rest of the section an automaton $\mathcal{A} = (Q, A)$. Set $n = |Q|$. Then we define the *standard representation* of $M(\mathcal{A})$ as follows. We consider the vector space V with basis

$$B = \{e_q \mid q \in Q\}. \tag{3.1}$$

We define a homomorphism $M : A^* \to M_n(\mathbb{Q})$ by $w \mapsto M_w$ where

$$e_q M_w = e_{qw}$$

for $w \in A^*$, $q \in Q$. It is clear that $M_u = M_w$ if and only if $qu = qw$ for all $q \in Q$, if and only if $u = w$ in $M(\mathcal{A})$. Hence M induces a faithful representation of $M(\mathcal{A})$. We abuse notation and do not distinguish this representation of $M(\mathcal{A})$ from that of A^*. When convenient we assume $Q = \{1, \dots, n\}$ and identify B with the standard basis for $\mathbb{Q}^n$.

More concretely, for any $a \in A$, we define M_a to be the incidence matrix of the graph consisting of only the edges of $\mathcal{A}$ labelled by a. That is,

$$(M_a)_{ij} = \begin{cases} 1, & \text{if } i \xrightarrow{a} j; \\ 0, & \text{else.} \end{cases}$$

The map M is extended to A^* in the natural way. The following observation is key to what follows.

$$(M_w^t)_{xy} = \begin{cases} 1, & \text{if } y \xrightarrow{w} x; \\ 0, & \text{else.} \end{cases}$$

So it is reasonable to define $M_{w^{-1}} = M_w^t$.

If M is a finite monoid, its *regular representation* is the standard representation associated to the action of M on the right of itself (viewed as an automaton with generators M). For example if $M = \mathbb{Z}_p$, this representation has basis $e_0, \dots, e_{p-1}$ and the generator acts by the cyclic permutation matrix.

We also associate to each $S \subseteq Q$ its characteristic vector $[S]$ given by:

$$[S]_i = \begin{cases} 1, & \text{if } i \in S; \\ 0, & \text{else.} \end{cases}$$

In particular, $[Q] = [1, \dots, 1]$.

With this notation we have the following proposition.

Proposition 3.1. *If $S \subseteq Q$ and $w \in A^*$, then*

$$[Sw^{-1}] = [S]M_{w^{-1}} = [S]M_w^t.$$

Proof. First observe

$$\begin{aligned}([S]M_{w^{-1}})_i &= ([S]M_w^t)_i \\ &= \sum_{k=1}^{n}[S]_k(M_w^t)_{ki} \\ &= \sum_{k=1}^{n}[S]_k(M_w)_{ik} \\ &= [S]_{i\cdot w}\end{aligned}$$

since

$$(M_w)_{ik} = \begin{cases} 1, & \text{if } i \xrightarrow{w} k; \\ 0, & \text{else.}\end{cases}$$

Hence,

$$\begin{aligned}([S]M_{w^{-1}})_i &= \begin{cases} 1, & \text{if } i \cdot w \in S; \\ 0, & \text{else.}\end{cases} \\ &= \begin{cases} 1, & \text{if } i \in Sw^{-1}; \\ 0, & \text{else.}\end{cases}\end{aligned}$$

Thus, $[S]M_{w^{-1}} = [Sw^{-1}]$. □

Recall that our strategy for obtaining a synchronizing word is to find, for any non-empty, proper subset $S \subset Q$, a word $u \in A^*$ such that $|Su^{-1}| > |S|$. We wish to reformulate this in terms of the standard representation. Let V be the representation space of the standard representation. We equip it with the usual inner product $\langle \cdot, \cdot \rangle$ that makes the basis B (3.1) an orthonormal basis. We then have

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

Thus,

$$|Su^{-1}| = \langle [S]M_{u^{-1}}, [Q] \rangle = \langle [S]M_u^t, [Q] \rangle = \langle [S], [Q]M_u \rangle.$$

Definition 3.2. *Define, for a word $w \in A^*$ and a subset $S \subseteq Q$,*

$$\alpha_S(w) = |Sw^{-1}| - |S|.$$

We aim to compute $\alpha_S(w)$. First a lemma.

Lemma 3.3. $[Q](M_w - I) \perp [Q]$.

Proof. To prove this lemma, we must show that $\langle [Q], [Q](M_w - I) \rangle = 0$. Indeed,

$$\langle [Q], [Q](M_w - I) \rangle = \langle [Q]M_w^t, [Q] \rangle - \langle [Q], [Q] \rangle. \tag{3.2}$$

But, $[Q]M_w^t = [Qw^{-1}] = [Q]$. Therefore, the right hand side of (3.2) is equal to zero. □

Set $V_1 = \mathrm{Span}\{[Q]\}$; this is the the space of constant vectors. The subscript 1 is used because in some sense V_1 is a trivial subspace for us; this will be made more precise below. In representation theory [7], the orthogonal complement of V_1 plays a key role. So set

$$V_0 = V_1^{\perp} = \{v = [c_1, \ldots, c_n] \in \mathbb{Q} \mid c_1 + \ldots + c_n = 0\}.$$

Notice that $\dim(V_0) = n - 1$. Indeed, if we take $Q = \{1, \ldots, n\}$, then $\{e_1 - e_2, \ldots, e_{n-1} - e_n\}$ is a basis for V_0. The fact that this dimension is $n - 1$ was used by Kari [5] to obtain good bounds for synchronizing words.

The following proposition appears in some form in [4, 5].

Proposition 3.4. *Let $w \in A^*$ and $S \subseteq Q$. Also, let $[S] = S' + U$, where $S' \in V_0$ and $U \in V_1$, be the orthogonal decomposition. Then*

$$\begin{aligned}\alpha_S(w) &= \langle S'M_w^t, [Q]\rangle \\ &= \langle S', [Q]M_w\rangle \\ &= \langle S', [Q](M_w - I)\rangle \\ &= \langle S'(M_w^t - I), [Q]\rangle.\end{aligned}$$

Proof. We begin by calculating

$$\begin{aligned}\alpha_S(w) &= |Sw^{-1}| - |S| \\ &= \langle [S]M_w^t, [Q]\rangle - \langle [S], [Q]\rangle \\ &= \langle [S](M_w^t - I), [Q]\rangle \\ &= \langle [S], [Q](M_w - I)\rangle \\ &= \langle S' + U, [Q](M_w - I)\rangle \\ &= \langle S', [Q](M_w - I)\rangle + \langle U, [Q](M_w - I)\rangle \\ &= \langle S', [Q](M_w - I)\rangle\end{aligned}$$

by Lemma 3.3 since $U \in V_1$ and $[Q](M_w - I) \in V_0 = V_1^{\perp}$.

Thus we have shown that $\alpha_S(w) = \langle S', [Q](M_w - I)\rangle$. Since $S' \in [Q]^{\perp}$, we may finish the proof as follows:

$$\begin{aligned}\alpha_S(w) &= \langle S', [Q](M_w - I)\rangle \\ &= \langle S', [Q]M_w\rangle - \langle S', [Q]\rangle \\ &= \langle S', [Q]M_w\rangle.\end{aligned}$$

This completes the proof. □

We now wish to show that V_0 is an $M(\mathcal{A})$-invariant subspace.

Proposition 3.5. *V_0 is an $M(\mathcal{A})$-invariant subspace. That is, if $v \in V_0$, then $vM_w \in V_0$ for all $w \in A^*$.*

Proof. Let $v_0 \in V_0$. Then,

$$\begin{aligned}\langle v_0 M_w, [Q]\rangle &= \langle v_0, [Q]M_w^t\rangle \\ &= \langle v_0, [Qw^{-1}]\rangle \\ &= \langle v_0, [Q]\rangle = 0\end{aligned}$$

So, $v_0 M_w \in V_0 = V_1^{\perp}$. □

4. Synchronizing words and irreducible representations

We want to use representation theoretic techniques to prove Pin's theorem [6] that the Černý conjecture holds for circular automata with a prime number of states. We prove a more general result. Namely, we prove the following theorem.

Theorem 4.1. *Let $\mathcal{A} = (Q, A)$ be an automaton and V be the representation space of the standard representation of $M(\mathcal{A})$. Suppose that there is a subgroup G of the group of units of $M(\mathcal{A})$ such that the orthogonal complement V_0 of the space of constant vectors in V carries a G-irreducible representation. Then if $M(\mathcal{A})$ is not a group, the automaton (Q, A) is synchronizing. Moreover, if each element of G can be represented by a word of length at most m, then a synchronizing word for $\mathcal{A}$ can be found of length at most* $1 + (n-2)(m+1)$.

Before proving this theorem, we show that it applies to the situation of circular automata with a prime number of states. So, suppose that $\mathcal{A} = (Q, A)$ where $Q = \{0, \ldots, q-1\}$ with q prime and A contains the cyclic permutation p of Q. Take $G = \langle p\rangle \subseteq M(\mathcal{A})$. Let V be the representation space for the standard representation of $M(\mathcal{A})$, V_1 be the space of constant vectors and $V_0 = V_1^{\perp}$. The G-irreducibility of V_1 (over $\mathbb{Q}$) is standard representation theory; we include a proof for completeness. The space V_0 has basis $f_0, \ldots, f_{q-2}$ where $f_i = e_i - e_{i+1}$. The action of M_p is given by

$$f_i M_p = \begin{cases} f_{i+1} & i \neq q-2 \\ \sum_{i=0}^{q-2} -f_i & i = q-2. \end{cases} \tag{4.1}$$

On the other hand, let ω be a primitive q^{th} root of unity and consider the action of ω on the cyclotomic field $\mathbb{Q}[\omega]$ by right multiplication. Since q is prime, ω has minimal polynomial $1 + x + x^2 + \cdots + x^{q-1}$ over $\mathbb{Q}$ and $\mathbb{Q}[\omega]$ has $\mathbb{Q}$-basis $\{1, \omega, \omega^2, \ldots, \omega^{q-2}\}$. Thus

$$\omega^{q-1} = \sum_{i=0}^{q-2} -\omega^i. \tag{4.2}$$

Viewing G and $\langle\omega\rangle$ as isomorphic copies of the cyclic group $\mathbb{Z}_q$, we see by comparing (4.1) and (4.2) that the map $V \to \mathbb{Q}[\omega]$ given by $f_i \mapsto \omega^i$ is an isomorphism of representations of the group $\mathbb{Z}_q$. Now a $\mathbb{Z}_q$-invariant subspace of $\mathbb{Q}[\omega]$ is the same thing as an additive subgroup of $\mathbb{Q}[\omega]$ closed under right multiplication by elements of $\mathbb{Q}$ and by ω; in other words, it is the same thing as an ideal in $\mathbb{Q}[\omega]$. But $\mathbb{Q}[\omega]$ is a field, so its only ideals are $\{0\}$ and $\mathbb{Q}[\omega]$. Thus the representation of G on V_0 is irreducible.

Hence we have the following corollary to Theorem 4.1.

Corollary 4.2 (Pin [6])**.** *Let (Q, A) be a circular automaton on q states with q prime. Suppose A contains a non-permutation. Then (Q, A) is synchronizing and has a synchronizing word of length at most $(q-1)^2$.*

Proof. Take $p \in A$ to be the cyclic permutation and $G = \langle p \rangle$. We just saw that V_0 carries an irreducible representation of G. Since

$$G = \{1, p, \dots, p^{q-1}\},$$

we may take $m = q - 1$ in Theorem 4.1, thereby obtaining a synchronizing word of length at most $1 + (q-2)q = (q-1)^2$. □

If $\mathcal{A} = (Q, A)$ is an automaton and G is a subgroup of the group of units of $M(\mathcal{A})$, then a sufficient condition for V_0 to carry an irreducible representation of G is that the action of G on Q is 2-transitive. In fact, this latter condition is equivalent to V_0 being irreducible over the complex field [7]; however, the conclusion of Theorem 4.1 can be obtained in this case by combinatorial means. But there are examples of permutation groups (Q, G) for which V_0 is G-irreducible, but which are neither 2-transitive nor regular representations of cyclic groups of prime order. These are partially classified by Dixon [3], where they are called QI-groups.

The remainder of this section is dedicated to proving Theorem 4.1. We fix an automaton $\mathcal{A} = (Q, A)$ satisfying the hypotheses of Theorem 4.1. We carry over the notation from the theorem statement and the notation from the previous section. Since $M(\mathcal{A})$ is assumed not to be a group, A contains at least one non-permutation.

Suppose first that G is trivial. Then, since V_0 is G-irreducible, it must be one-dimensional, in which case $|Q| = 2$. Assuming that $M(\mathcal{A})$ is not a group, we see that any non-permutation letter synchronizes $\mathcal{A}$. Thus the theorem is proved in this case. So from now on we assume that G is non-trivial.

We're going to show that (Q, A) is synchronizing and estimate the length of a synchronizing word using the strategy of Section 2. So let $\emptyset \neq S \subset Q$. We want to find a word $w \in A^*$ of length at most m such that $|Sw^{-1}| > |S|$. Recall from Definition 3.2 that $\alpha_S(w) = |Sw^{-1}| - |S|$. We can naturally view α_S as defined on $M(\mathcal{A})$ and we abuse notation accordingly. As before, let $[S] = S' + U$ be the orthogonal decomposition with $S' \in V_0$, and $U \in V_1$, as in Proposition 3.4. Since $\emptyset \neq S \subset Q$, $[S] \notin V_1$ and so we have $S' \neq 0$.

Lemma 4.3. *Let $\emptyset \neq S \subset Q$. Suppose $a \in A$ is any non-permutation. Then there exists $g \in G$ such that $\alpha_S(ag) \neq 0$.*

Proof. First, we remark that $[Q](M_a - I) \neq 0$. Indeed, if $[Q](M_a - I) = 0$, then $[Q]M_a = [Q]$ and hence, a is a permutation. But, this contradicts our choice of a.

Now, set

$$W = \mathrm{Span}\{[Q](M_a - I)M_g \mid g \in G\}.$$

Note that $W \neq \{0\}$ since $[Q](M_a - I) \in W$. By definition, W is G-invariant. Hence, since V_0 is G-irreducible, $W = V_0$. Thus $S' \in V_0 = W$ and so, since $0 \neq S'$, we have $S' \notin W^{\perp}$. Since W is spanned by $[Q](M_a - I)M_g$, $g \in G$, there exists $g \in G$ such that

$$\begin{aligned} 0 &\neq \langle S', [Q](M_a - I)M_g\rangle && (4.3)\\ &= \langle S', [Q]M_aM_g\rangle - \langle S', [Q]M_g\rangle && (4.4)\\ &= \alpha_S(ag) - \langle S', [Q]\rangle && (4.5)\\ &= \alpha_S(ag) && (4.6)\end{aligned}$$

where the passage from (4.4) to (4.5) follows from Proposition 3.4 and the fact that M_g is a permutation matrix, while the last equality follows since $S' \perp [Q]$. □

Notice that V_1 carries the trivial representation of G since $[Q]M_h = [Q]$ for any permutation matrix M_h. Since

$$V = V_0 \oplus V_1 \tag{4.7}$$

and V_0 is G-irreducible, (4.7) is the decomposition of V into irreducible representations. Hence we have $V^G = V_1$, where V^G is the fixed subspace of V under the action of G. As we mentioned in the previous section, $\sum_{h\in H} M_h$ is the projection to V^G and hence must annihilate V_0. This leads to the following lemma.

Lemma 4.4. *Suppose $v \in V_0$. Then $v(\sum_{h\in G} M_h) = 0$.* □

Proof of Theorem 4.1. In Lemma 4.3, we found some $g \in G$ such that $\alpha_S(ag) \neq 0$. We calculate $\sum_{h\in G} \alpha_S(ah)$ as follows,

$$\begin{aligned} \sum_{h\in G} \alpha_S(ah) &= \sum_{h\in G} \langle S', [Q]M_aM_h\rangle \\ &= \langle S', [Q]M_a(\sum_{h\in G} M_h)\rangle \\ &= \langle S', [Q](M_a - I)(\sum_{h\in G} M_h)\rangle \end{aligned} \tag{4.8}$$

The last equality holds because

$$\langle S', [Q](M_a - I)(\sum_{h\in G} M_h)\rangle = \langle S', [Q]M_a(\sum_{h\in G} M_h)\rangle - \langle S', [Q](\sum_{h\in G} M_h)\rangle.$$

But, $[Q]M_h = [Q]$ for all $h \in G$, since M_h is a permutation matrix. Thus,

$$\langle S', [Q]\sum_{h\in G} M_h\rangle = \langle S', |G|[Q]\rangle = 0$$

since $S' \perp [Q]$.

Since $[Q](M_a - I) \in V_0$ by Lemma 3.3, we have by Lemma 4.4 that

$$[Q](M_a - I)(\sum_{h \in G} M_h) = 0$$

Thus, by (4.8),

$$\sum_{h \in G} \alpha_S(ah) = 0. \qquad (4.9)$$

But, we already found some $g \in G$ such that $\alpha_S(ag) \neq 0$. Therefore, in order for (4.9) to hold, not all the $\alpha_S(ah)$ can be negative and so there exists $g' \in G$ such that $\alpha_S(ag') > 0$. This implies that

$$|S(ag')^{-1}| - |S| > 0.$$

Thus, if $u \in A^*$ represents ag', then $|Su^{-1}| > |S|$. We conclude, since S was arbitrary, that there must be a synchronizing word for (Q, A), as per the strategy of Section 2.

To bound the size of a synchronizing word, according to the aforementioned strategy, we must bound the length of u. For each $g \in G$, choose $U_g \in A^*$ to be a minimal length word representing g. Let $m = \max\{|U_g| \mid g \in G\}$. Then ag' can be represented by $aU_{g'}$, which has length at most $m + 1$. The strategy in Section 2 then shows that (Q, A) has a synchronizing word of length at most $1 + (n - 2)(m + 1)$. This completes the proof. □

References

1. F. Arnold, "A linear algebra approach to synchronizing automata", Master's Thesis, Carleton University, 2005.
2. J. Černý, *Poznámka k homogénnym eksperimentom s konecnými avtomatami*, Mat.-Fyz. Cas. Solvensk. Akad. Vied. **14** (1964), pp. 208–216 [in Slovak].
3. J. Dixon, *Permutations representations and rational irreducibility*, B. Austral. Math. Soc., to appear.
4. L. Dubuc, *Sur les automates circulaires et la conjecture de Černý.* [Circular automata and Cerny's conjecture], RAIRO Inform. Thor. Appl. **32** (1998), pp. 21–34.
5. J. Kari, *Synchronizing finite automata on Eulerian digraphs*, Mathematical foundations of computer science (Mariánské Lázně, (2001). Theoret. Comput. Sci. **295** (2003), pp. 223—232.
6. J.-E. Pin, *Sur un cas particulier de la conjecture de Černý.* Automata, languages and programming (Fifth Internat. Colloq., Udine, 1978), pp. 345–352, Lecture Notes in Comput. Sci., **62**, Springer, Berlin-New York, 1978.
7. J.-P. Serre, "Linear representations of finite groups." Translated by Leonard L. Scott. Graduate Texts in Mathematics, Vol. **42**. Springer-Verlag, New York-Heidelberg, 1977.

School of Mathematics and Statistics, Carleton University, 1125 Colonel By Drive, Ottawa ON, K1S 5B6, Canada

E-mail address: bsteinbg@math.carleton.ca