SYNCHRONIZING GROUPS AND AUTOMATA

FREDRICK ARNOLD AND BENJAMIN STEINBERG

Abstract. Pin showed that every p-state automaton (p a prime) containing a cyclic permutation and a non-permutation has a synchronizing word of length at most $(p-1)^2$. In this paper we consider permutation automata with the property that adding any non-permutation will lead to a synchronizing word and establish bounds on the lengths of such synchronizing words. In particular, we show that permutation groups whose permutation character over the rationals splits into a sum of only two irreducible characters have the desired property.

1. Introduction

An automaton is called *synchronizing* if there is a word, called a *synchronizing word*, that sends each state to the same element. 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 the following theorem of Pin.

Theorem 1.1 (Pin). *An automaton with a prime number of states p whose alphabet contains a cyclic permutation and at least one non-permutation is automatically synchronizing and has a synchronizing word of length at most* $(p-1)^2$.

Černý's conjecture has since been proved for all automata with a cyclic permutation by Dubuc [5], but in the general situation one does not obtain automatic synchronization.

This motivates us to consider permutation automata with the property that as soon as a non-permutation is added to the automaton, the automaton can be synchronized.

More precisely, we denote by T_n the full transformation monoid on the set $[n] = \{1, \ldots, n\}$; the group of units of T_n is the symmetric group S_n. A *permutation group* of *degree* n is a subgroup $G \leq S_n$. We say that G has the *synchronization property* if whenever $f \in T_n \setminus S_n$, the submonoid $\langle G \cup \{f\}\rangle$ generated by G and f contains a constant map. In this terminology, the first part of Pin's theorem says that a permutation group of prime degree containing a cyclic permutation has the synchronizing property. On the other hand, it is well known that any doubly transitive permutation group has the sychronization property (Zalcstein [10] attributes this to Rhodes).

Date: August 31, 2005.

This work was supported by NSERC.

Using representation theory, we give a common generalization of these two cases, which includes several new cases. Also we obtain bounds on the size of synchronizing words in the case G is given by generators, letting us obtain the full strength of Pin's theorem as well as some new examples where Černý's conjecture holds.

2. Synchronizing automata

For us, an *automaton* of *degree* n (that is with n states in the usual terminology) will be a subset A of T_n. If A^* denotes the free monoid on A, then each word $w \in A^*$ has a natural interpretation as an element of T_n and we do not distinguish between the word and its interpretation. If $i \in [n]$ and $w \in A^*$, we use iw for the image of i under w. By $M(A)$ we denote the *transition monoid* of A; it is precisely the submonoid of T generated by A. A word $w \in A^*$ is called a *synchronizing word* if the element of T_n it represents is a constant map. An automaton $A \subseteq T_n$ is said to be *sychronizing* if it admits a synchronizing word; that is $M(A)$ contains a constant map. If $f \in T_n$, by the *rank* of f we mean the size of the image of f. So a constant map is the same thing as a rank one map.

For $w \in A^*$ and $S \subseteq [n]$, we set

$$Sw^{-1} = \{i \mid iw \in S\}.$$

Our strategy for finding synchronizing words will then be to show that, given $\emptyset \neq S \subsetneq [n]$, 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 $k = n$, 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* $(n-1)^2$.

The intuition is that on average we should be able to expand a set going backwards via a word of size n.

3. Groups with the synchronization property

As per the introduction, we say that $G \leq S_n$ has the *synchronization property* if, for all $f \in T_n \setminus S_n$, the automaton $G \cup \{f\}$ has the synchronization property. It is immediate from the definition that any permutation group of degree one or two has the synchronization property. Another immediate observation is that if $G \leq H \leq S_n$ and G has the synchronization property, then so does H. It is clear that any permutation group of degree at most 2 has the synchronization property. So in what follows we shall always tacitly assume that the degree is greater than 2.

Before continuing, we need some basic notations from the theory of permutation groups; a good reference is the book of Dixon and Mortimer [4]. A permutation group $G \leq S_n$ is said to be *transitive* if, for all $i, j \in [n]$, there exists $g \in G$ with $ig = j$. In this case, the action is isomorphic to the action of G on G/H where H is the stabilizer of 1. The group G is said to be *doubly transitive* if given $i \neq j$ and $k \neq l$ in $[n]$, there is an element $g \in G$ such that $ig = k$ and $jg = l$; for instance S_n is doubly transitive all $n \geq 2$ and A_n is doubly transitive for $n \geq 4$. The group G is said to be *2-homogeneous* if for all $i \neq j$ and $k \neq l$ in $[n]$ there exists $g \in G$ with $\{ig, jg\} = \{kg, lg\}$. It is clear that double transitivity implies 2-homogeneity but the converse is false.

Finally, we turn to primitivity. A permutation group $G \leq S_n$ is called *primitive* if there is no equivalence relation R on $[n]$ such that the blocks of the partition associated to R are permuted by G, that is such that

$$i \, R \, j \implies ig \, R \, jg,$$

except the identity relation and the universal relation. If $n > 2$, primitivity implies transitivity since the orbits of G give such an equivalence relation. Many authors include transitivity in the definition of primitivity to avoid the trivial case $n = 2$ where primitivity in our sense is automatic but not transitivity.

If $G \leq S_n$ is a transitive permutation group, then, as mentioned above, we can identify $[n]$ with G/H where H is the stabilizer of 1. In this case, one can easily show that G is primitive if and only if H is a maximal proper subgroup of G [4]. The following lemma is well known, we include a proof for completeness.

Lemma 3.1. *Let $G \leq S_p$ be a permutation group with $p > 2$ prime. Then the following are equivalent:*

1. *G contains a cyclic permutation of $[p]$;*
2. *G is transitive;*
3. *G is primitive.*

If $p = 2$, then (1) and (3) are equivalent.

Proof. Clearly if G contains a cyclic permutation of $[p]$, then G is transitive. Suppose that G is transitive. Then we know that $p = [G : H]$ where H is the stabilizer of 1. Hence $p \mid |G|$ and so G has an element g of order p. Since g is not trivial, it must have a non-trivial orbit. But since the size of any orbit of g must divide the order of g, which is p, we see that g has an orbit of size p and hence is a cyclic permutation of $[p]$.

If G is transitive, then the stabilizer H of 1 has index p and so is a maximal subgroup. Thus G is primitive. If G is primitive, then G must be transitive in the case $p > 2$. □

We now show that primitivity is necessary in order to have the synchronization property.

Proposition 3.2. *Suppose $G \leq S_n$ has the synchronization property. Then G is primitive.*

Proof. Suppose that G is not primitive. Let R be a non-trivial equivalence relation on $[n]$ whose blocks $\{B_1, \ldots, B_r\}$ are permuted by G. For each block B_i choose a representative b_i. Define an idempotent map $f \in T_n$ by $xf = b_i$ where $x \in B_i$. We claim that $G \cup \{f\}$ is not synchronizing. Indeed, if $M = \langle G \cup \{f\} \rangle$, then M has a natural action of $[n]/R$ since G preserves the relation R and so does f (by construction). If M contains a constant map, then so would the action of M on $[n]/R$. But since f acts as the identity on $[n]/R$, we see that the action of M on $[n]/R$ is by permutations and so cannot contain a constant map as $|[n]/R| > 1$. This contradiction shows that G must be primitive. □

From Pin's Theorem and Proposition 3.2 we immediately obtain:

Corollary 3.3. *A permutation group of prime degree p has the synchronization property if and only if it is primitive. This is equivalent to transitivity for $p > 2$.*

Another case, as mentioned in the introduction, where the synchronization property holds is the 2-homogeneous case. This is a folklore result, the earliest attribution I know of is to Rhodes [10].

Proposition 3.4. *A 2-homogeneous permutation group $G \leq S_n$ has the synchronization property. In particular doubly transitive permutation groups have the synchronization property.*

Proof. Let $f \in T_n \setminus S_n$ and let $M = \langle G \cup \{f\} \rangle$. We show that given $h \in M$ that is not a constant map, there exists $h' \in M$ of strictly smaller rank. It will then follow that any minimal rank element of M is a constant map. So suppose $i \neq j \in [n]h$. Since $f \in T_n \setminus S_n$, there exist $k, l \in [n]$ such that $kf = lf$. By 2-homogeneity there exists $g \in G$ with $\{ig, jg\} = \{k, l\}$. Clearly, then $\operatorname{rank}(hgf) < \operatorname{rank}(h)$. This completes the proof. □

A well-known theorem of Schur [9] says that a primitive permutation group of degree n, with n a composite number, is necessarily doubly transitive. Putting this together with the previous result for the prime case we obtain.

Proposition 3.5. *A permutation group containing a cyclic permutation has the synchronization property if and only if it is primitive.*

We do not know of an example of a primitive permutation group that does not have the synchronization property but we are sure they exist. The problem lies in the ability to do hand computations since primitive groups of small degree tend to fall into the cases we have covered above.

Our main goal in this paper is to give a simultaneous generalization of the prime degree and the doubly transitive cases. To describe our results we need to use some representation theoretic language.

4. Linearization of the problem

Let M be a monoid and K a field of characteristic 0. Then a representation of M of degree n over K is a (monoid) homomorphism $\varphi : M \to M_n(K)$, where $M_n(K)$ denotes the monoid of $n \times n$ matrices with entries in K. The vector space $V = K^n$ 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.

For a representation $\varphi : G \to M_n(K)$, the *trivial component* is the subspace V^G of the representation space V consisting of those vectors fixed by $G\varphi$. A projection of V onto V^G is given by $\frac{1}{|G|}\sum_{g\in G} g\varphi$ [8]. We include the proof for completeness.

Proposition 4.1. *Let φ be a representation of G over a field of characteristic 0. Then $\frac{1}{|G|}\sum_{g\in G} g\varphi$ is a projection to V^G.*

Proof. Let $p = \frac{1}{|G|}\sum_{g\in G} g\varphi$. It suffices to show that p fixes each element of V^G and that the image of p is contained in V^G. So suppose $v \in V^G$. Then

$$vp = \frac{1}{|G|}\sum_{g\in G} vg\varphi = \frac{1}{|G|}\sum_{g\in G} v = v.$$

Now if $v \in V$ is arbitrary and $h \in G$, then

$$vph\varphi = \frac{1}{|G|}\sum_{g\in G} vg\varphi h\varphi = \frac{1}{|G|}\sum_{g\in G} v(gh)\varphi = vp$$

where the last equality holds by making the change of variables $g \mapsto gh^{-1}$. □

We fix for the rest of the section a transformation monoid $M \leq T_n$ of degree n and a field K of characteristic 0. Then we define the *standard representation* of M as follows. We consider the vector space $V = K^n$ with canonical basis $\{e_1, \dots, e_n\}$. We define a representation $\varphi : M(A) \to M_n(K)$ by $f \mapsto f\varphi$ where

$$e_i f\varphi = e_{if}$$

for $f \in M(A)$. Notice that φ gives a faithful representation of M.

If $f \in M$, then $f\varphi^t$ denotes the transpose of $f\varphi$. The following observation is key to what follows.

$$(f\varphi^t)_{ij} = \begin{cases} 1 & \text{if } jf = i; \\ 0 & \text{else.} \end{cases} \tag{4.1}$$

So it is reasonable to define $f^{-1}\varphi = f\varphi^t$.

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 $e_1, \dots, e_p$ and the generator acts by the cyclic permutation matrix.

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

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

To avoid cumbersome notation, we shall write $[n]$ for the characteristic vector of $[n]$. So, $[n] = (1, \ldots, 1)$.

With this notation we have the following proposition.

Proposition 4.2. *If $S \subseteq [n]$ and $f \in M$, then*

$$[Sf^{-1}] = [S]f^{-1}\varphi = [S]f\varphi^t.$$

Proof. First observe

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

where the last equality follows from (4.1). Hence,

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

Thus, $[S]f^{-1}\varphi = [Sf^{-1}]$. □

Recall that our strategy for obtaining a synchronizing word for an automaton is to find, for each non-empty, proper subset $S \subsetneq [n]$, 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 canonical basis an orthonormal basis. We then have

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

Thus, for $f \in M$, we have

$$|Sf^{-1}| = \langle [S]f^{-1}\varphi, [n] \rangle = \langle [S]f\varphi^t, [n] \rangle = \langle [S], [n]f\varphi \rangle.$$

Definition 4.3. *Define, for $f \in M$ and a subset $S \subseteq [n]$,*

$$f\alpha_S = |Sf^{-1}| - |S|.$$

We aim to compute $f\alpha_S$. First a lemma.

Lemma 4.4. $[n](f\varphi - I) \perp [n]$.

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

$$\langle [n], [n](f\varphi - I)\rangle = \langle [n]f\varphi^t, [n]\rangle - \langle [n], [n]\rangle. \tag{4.2}$$

But, $[n]f\varphi^t = [[n]f^{-1}] = [n]$. Therefore, the right hand side of (4.2) is equal to zero. □

Set $V_1 = \mathrm{Span}\{[n]\}$; this is then the space of constant vectors. The subscript 1 is used because in some sense V_1 is a trivial subspace for us. In representation theory [8], the orthogonal complement of V_1 plays a key role. So set

$$V_0 = V_1^{\perp} = \{v = (c_1, \ldots, c_n) \in K^n \mid c_1 + \cdots + c_n = 0\}.$$

Notice that $\dim(V_0) = n-1$. The fact that this dimension is $n-1$ was used by Kari [6] to obtain good bounds for synchronizing words.

The following proposition appears in some form in [5, 6].

Proposition 4.5. *Let $f \in M \leq T_n$ and $S \subseteq [n]$. Also, let $[S] = S' + U$, where $S' \in V_0$ and $U \in V_1$, be the orthogonal decomposition. Then*

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

Proof. We begin by calculating

$$\begin{aligned} f\alpha_S &= |Sf^{-1}| - |S| \\ &= \langle [S]f\varphi^t, [n]\rangle - \langle [S], [n]\rangle \\ &= \langle [S](f\varphi^t - I), [n]\rangle \\ &= \langle [S], [n](f\varphi - I)\rangle \\ &= \langle S' + U, [n](f\varphi - I)\rangle \\ &= \langle S', [n](f\varphi - I)\rangle + \langle U, [n](f\varphi - I)\rangle \\ &= \langle S', [n](f\varphi - I)\rangle \end{aligned}$$

by Lemma 4.4 since $U \in V_1$ and $[n](f\varphi - I) \in V_0 = V_1^{\perp}$.

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

$$\begin{aligned} f\alpha_S &= \langle S', [n](f\varphi - I)\rangle \\ &= \langle S', [n]f\varphi\rangle - \langle S', [n]\rangle \\ &= \langle S', [n]f\varphi\rangle. \end{aligned}$$

This completes the proof. □

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

Proposition 4.6. *V_0 is an $M(\mathcal{A})$-invariant subspace. That is, if $v \in V_0$, then $vf\varphi \in V_0$ for all $w \in A^*$.*

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

$$\begin{aligned}\langle v_0 f\varphi, [n]\rangle &= \langle v_0, [n]f\varphi^t\rangle \\ &= \langle v_0, [[n]f^{-1}]\rangle \\ &= \langle v_0, [n]\rangle = 0\end{aligned}$$

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

5. The synchronization property and irreducible representations

We are almost ready to formulate our main result. Let $G \leq S_n$ be a permutation group of degree n. We shall, following Dixon [3], call G a *QI-group* if, for the standard representation $\varphi : G \to M_n(\mathbb{Q})$, the subrepresentation carried by $V_0 = \{(c_1, \ldots, c_n) \mid c_1 + \cdots + c_n = 0\}$ is irreducible. It is clear from the definition that if $G \leq H \leq S_n$ and G is a QI-group, then so is H. Every permutation group of degree two is a QI-group since in this case $\dim(V_0) = 1$. Permutation groups of degree one are vacuously QI-groups. Our main result is that QI-groups have the synchronization property.

Before proving this we remark that every doubly transitive group is a QI-group. Indeed it is a well-known result of Burnside that $G \leq S_n$ is doubly transitive if and only if, for the standard representation $\varphi : G \to M_n(\mathbb{C})$, the subrepresentation carried by V_0 (defined as above) is irreducible [8]. This immediately implies that the subrepresentation carried by V_0 over $\mathbb{Q}$ is irreducible.

Permutation groups of prime degree containing a cyclic permutation are QI-groups. This follows from standard representation theory, but we give an argument for completeness. Let q be a prime. It suffices to show that if $p = (1 \ldots q)$ then $G = \langle p\rangle \leq S_q$ is a QI-group. Let V be the representation space for the standard representation of G, V_1 be the space of constant vectors and $V_0 = V_1^{\perp}$. The space V_0 has basis $f_0, \ldots, f_{q-2}$ where $f_i = e_i - e_{i+1}$. The action of $p\varphi$ is given by

$$f_i p\varphi = \begin{cases} f_{i+1} & i \neq q-2 \\ \sum_{i=0}^{q-2} -f_i & i = q-2. \end{cases} \tag{5.1}$$

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

$$\omega^{q-1} = \sum_{i=0}^{q-2} -\omega^i. \tag{5.2}$$

Viewing G and $\langle\omega\rangle$ as isomorphic copies of the cyclic group $\mathbb{Z}_q$, we see by comparing (5.1) and (5.2) 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.

The paper of Dixon [3] gives a partial classification of QI-groups. In particular, he proves they are primitive (this will also follow from our main result and Proposition 3.2) and that they must be almost simple or of affine type. In the case of affine type, if $G \leq S_n$ is a QI-group, then there is a doubly transitive group $H \leq S_n$ such that $[H, H] \leq G \leq H$ where $[H, H]$ is the commutator subgroup of H. There are further restrictions, we refer the reader to [3, Theorem 4]. Dixon also gives a "procedure" to construct such groups [3].

For the almost simple case, Dixon shows that a QI-group with socle isomorphic to A_n with $n \geq 5$ must be doubly transitive. On the other hand he shows that there are QI-groups that are not doubly transitive of degree $2^{k-1}(2^k - 1)$ with socle the simple group $\mathrm{PSL}(2, 2^k)$ when $2^k - 1$ is prime; moreover, these are the only conditions for which $\mathrm{PSL}(2, q)$ can be the socle of a QI-group [3, Theorem 11].

To apply our results to the Černý problem, we need the following definition. Let $A \leq T_n$ be an automaton and $M \leq M(A)$. Then $\mathrm{diam}_A(M)$ (read the diameter of M) denotes the least integer n such that every element of M can be represented by a word of A^* of at length at most n.

Theorem 5.1. *Let $G \leq S_n$ be a QI-group ($n \geq 2$). Then G has the synchronization property. Suppose, moreover, that $A \leq T_n$ is an automaton with $G \leq M(A)$ and $M(A) \nleq S_n$. Then a synchronizing word for A can be found of length at most $1 + (n - 2)(\mathrm{diam}_A(G) + 1)$.*

Proof. Let $G \leq S_n$ be a QI-group. We carry over the notation from the previous section. We may assume that $n > 2$ since otherwise the conclusion of the theorem is trivial.

To prove the theorem it suffices to show that if $A \leq T_n$ is any automaton with $G \leq M(A)$ containing an element $a \notin T_n$, then A is synchronizing and has a synchronizing word of length at most $m = 1 + (n-1)(\mathrm{diam}_A(G) + 1)$. Let $\varphi : M(A) \to M_n(\mathbb{Q})$ be the standard representation. We shall use the strategy of Section 2. So let $\emptyset \neq S \subsetneq [n]$. We want to find a word $w \in A^*$ of length at most m such that $|Sw^{-1}| > |S|$.

Recall from Definition 4.3 that, for $f \in M(A)$, $f\alpha_S = |Sf^{-1}| - |S|$. As before, let $[S] = S' + U$ be the orthogonal decomposition with $S' \in V_0$, and $U \in V_1$, as in Proposition 4.5. Since $\emptyset \neq S \subsetneq [n]$, $[S] \notin V_1$ and so we have $S' \neq 0$.

Claim 1. *Let $\emptyset \neq S \subsetneq [n]$. Suppose $a \in A$ is any non-permutation. Then there exists $g \in G$ such that $ag\alpha_S \neq 0$.*

Proof. First, note that $[n](a\varphi - I) \neq 0$. Indeed, if $[n](a\varphi - I) = 0$, then $[n]a\varphi = [n]$ and hence, a is a permutation, contradicting our choice of a.

Now, set

$$W = \mathrm{Span}\{[n](a\varphi - I)g\varphi \mid g \in G\}.$$

Note that $W \neq \{0\}$ since $[n](a\varphi - I) \in W$. 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 $[n](a\varphi - I)g\varphi$, $g \in G$, there exists $g \in G$ such that

$$\begin{align} 0 &\neq \langle S', [n](a\varphi - I)g\varphi\rangle \tag{5.3}\\ &= \langle S', [n]a\varphi g\varphi\rangle - \langle S', [n]g\varphi\rangle \tag{5.4}\\ &= ag\alpha_S - \langle S', [n]\rangle \tag{5.5}\\ &= ag\alpha_S \tag{5.6}\end{align}$$

where the passage from (5.4) to (5.5) follows from Proposition 4.5 and the fact that $g\varphi$ is a permutation matrix, while the last equality follows since $S' \perp [n]$. □

Recall that V^G denotes the space of vectors in V fixed by G. We claim that $V^G \cap V_0 = \{0\}$. Indeed, if $0 \neq v \in V^G \cap V_0$, then we have that $\mathrm{Span}(v) \subseteq V_0$ is fixed by G and hence G-invariant. By G-irreducibility of V_0 we obtain that $V_0 = \mathrm{Span}(v)$, showing $\dim(V_0) = 1$ and thus $n = 2$, contrary to our assumption.

Let $p = \frac{1}{|G|}\sum_{h\in H} h\varphi$. Then $V_0 p \subseteq V_0$ since V_0 is G-invariant. Proposition 4.1 shows that p is a projection to V^G. Hence $V_0 p \subseteq V^G \cap V_0 = \{0\}$ establishing:

Claim 2. *Suppose $v \in V_0$. Then $v(\sum_{h\in G} h\varphi) = 0$.* □

In Claim 1, we found some $g \in G$ such that $(ag)\alpha_S \neq 0$. We calculate $\sum_{h\in G}(ah)\alpha_S$ as follows,

$$\begin{align}\sum_{h\in G}(ah)\alpha_S &= \sum_{h\in G}\langle S', [n]a\varphi h\varphi\rangle \text{ (by Propostion 4.5)}\\ &= \langle S', [n]a\varphi(\sum_{h\in G} h\varphi)\rangle \tag{5.7}\\ &= \langle S', [n](a\varphi - I)(\sum_{h\in G} h\varphi)\rangle\end{align}$$

The last equality holds because

$$\langle S', [n](a\varphi - I)(\sum_{h\in G} h\varphi)\rangle = \langle S', [n]a\varphi(\sum_{h\in G} h\varphi)\rangle - \langle S', [n](\sum_{h\in G} h\varphi)\rangle.$$

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

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

since $S' \perp [n]$.

Since $[n](a\varphi - I) \in V_0$ by Lemma 4.4, we have by Claim 2 that

$$[n](a\varphi - I)(\sum_{h\in G} h\varphi) = 0$$

Thus, by (5.7),

$$\sum_{h\in G}(ah)\alpha_S = 0. \tag{5.8}$$

But, we already found some $g \in G$ such that $(ag)\alpha_S \neq 0$. Therefore, in order for (5.8) to hold, not all the $(ah)\alpha_S$ can be negative and so there exists $g' \in G$ such that $(ag')\alpha_S > 0$. 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 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. Since u represents ag', we can clearly choose u of length at most $\mathrm{diam}_A(G) + 1$. The strategy in Section 2 then shows that A has a synchronizing word of length at most $1 + (n-2)(\mathrm{diam}_A(G) + 1)$. This completes the proof. □

We can now deduce Pin's theorem, Theorem 1.1, as a corollary to Theorem 5.1 (though it should be mentioned that in this special case, our proof boils down to a "fancy" version of his proof in the language of representation theory). Indeed, let $A \leq T_p$ with p prime be an automaton containing a cyclic permutation g and some non-permutation. We saw earlier that $G = \langle g\rangle$ is a QI-group. Since

$$G = \{1, g, \ldots, g^{p-1}\},$$

we see that $\mathrm{diam}_A(G) \leq p - 1$ and so we obtain from Theorem 5.1 a synchronizing word of length at most $1 + (p-2)p = (p-1)^2$.

One can obtain new cases of the Černý conjecture from QI-groups $G \leq S_n$ as long as one chooses generators for G so that the diameter is at most $n - 1$. For instance, if $G = S_n$ and one chooses the transpositions $(ii+1)$, $i = 1, \ldots, n$ as generators, then the diameter of S_n is $\binom{n}{2}$, so one would only obtain from the above theorem a cubic bound after adding a non-permutation. On the other hand, if we take as the generating set all the transpositions, then the diameter of S_n is $n-1$ and so the bound of $(n-1)^2$ can be obtained from the above theorem when adding a non-permutation. If we take all of S_n as a generating set, then we would get a diameter of 1 and so a synchronzing word of length at most $2n - 3$ can be obtained as soon as a non-permutation is adjoined (this last case is of course artificial but emphasizes the dependence on the generating set). Similar considerations apply to any QI-group.

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), 208–216 [in Slovak].
3. J. D. Dixon, *Permutations representations and rational irreducibility*, B. Austral. Math. Soc.**71** (2005), 493–503.
4. J. D. Dixon and B. Mortimer, "Permutation groups." Springer-Verlag, New York 1996.
5. L. Dubuc, *Sur les automates circulaires et la conjecture de Černý.* [Circular automata and Cerny's conjecture], RAIRO Inform. Thor. Appl. **32** (1998), 21–34.
6. J. Kari, *Synchronizing finite automata on Eulerian digraphs*, Mathematical foundations of computer science (Mariánské Lázně, (2001). Theoret. Comput. Sci. **295** (2003), 223–232.
7. J.-E. Pin, *Sur un cas particulier de la conjecture de Černý.* Automata, languages and programming (Fifth Internat. Colloq., Udine, 1978), 345–352, Lecture Notes in Comput. Sci., **62**, Springer, Berlin-New York, 1978.
8. J.-P. Serre, "Linear representations of finite groups." Graduate Texts in Mathematics, Vol. **42**. Springer-Verlag, New York-Heidelberg, 1977.
9. H. Weilandt, "Finite permutation groups". Academic Press, New York, 1964.
10. Y. Zalcstein, *Studies in the representation theory of finite semigroups*, Trans. Amer. Math. Soc. **161** (1971), 71–87.

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

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