JORDAN FORMS AND NTH ORDER LINEAR RECURRENCES

THOMAS MCKENZIE, SHANNON OVERBAY, AND ROBERT RAY

Abstract. Let p be a prime number with $p \neq 2$. We consider sequences generated by nth order linear recurrence relations over the finite field Z_p. In the first part of this paper we generalize some of the ideas in [6] to nth order linear recurrences. We then consider the case where the characteristic polynomial of the recurrence has one root in Z_p of multiplicity n. In this case, we show that the corresponding recurrence can be generated by a relatively simple matrix.

1. Introduction

Let $p > 2$ be a prime number, $n > 1$ be an integer, and let

$$S_i = a_0 S_{i-n} + a_1 S_{i-(n-1)} + \cdots + a_{n-1} S_{i-1}$$

be an nth order linear recurrence with $a_0, \ldots, a_{n-1} \in Z_p$ and $a_0 \neq 0$. A very nice discussion of such recurrences can be found in [5]. Since $(Z_p)^n$ has a finite number of elements, it is clear that any such nth order linear recurrence with initial conditions $S_0, S_1, \ldots, S_{n-1} \in Z_p$ will eventually repeat itself. The sequence is called uniformly distributed if each element of Z_p appears the same number of times within these repeated periods.

Example 1.1. *Consider the recurrence defined by $S_0 = 0, S_1 = 1, S_2 = 3$, and $S_n = 3S_{n-3} + 3S_{n-2} + S_{n-1}$, taken over Z_5. This generates the following uniformly distributed sequence:*

$$0, 1, 3, 1, 3, 0, 2, 1, 2, 1, 0, 4, 2, 4, 2, 0, 3, 4, 3, 4.$$

Consider the $n \times n$ matrix

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 & 0 \\ . & . & . & . & \cdots & . & . \\ . & . & . & . & \cdots & . & . \\ 0 & 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 \\ a_0 & a_1 & a_2 & a_3 & \cdots & a_{n-2} & a_{n-1} \end{bmatrix}.$$

The sequences defined by the recurrence relation

$$S_i = a_0 S_{i-n} + a_1 S_{i-(n-1)} + \cdots + a_{n-1} S_{i-1}$$

can be generated by the matrix relation

$$\begin{bmatrix} S_i \\ . \\ . \\ . \\ S_{(n-1)+i} \end{bmatrix} = A^i \begin{bmatrix} S_0 \\ . \\ . \\ . \\ S_{n-1} \end{bmatrix}.$$

We note that A is the companion matrix of the polynomial

$$C(x) = \det(xI - A) = x^n - a_{n-1}x^{n-1} - \cdots - a_1 x - a_0$$

(see [3, p. 358]).

Since $a_0 \neq 0$, A is a unit in the ring of $n \times n$ matrices over Z_p (i.e., $A \in GL_n(Z_p)$). Further, since this group of invertible $n \times n$ matrices is finite, A generates a finite cyclic group of order m, for some natural number m. We will denote this group by

$$G = \left\{ A^i \mid 0 \leq i \ \leq m-1 \right\}.$$

Left multiplication of matrices on vectors defines a map from $G \times (Z_p)^n$ to $(Z_p)^n$. Since $A^j \left(A^i \mathbf{v} \right) = (A^j A^i)\mathbf{v}$, $(Z_p)^n$ is a G-set (see [1, p. 176]). If a subset U of $(Z_p)^n$ is closed under this action of G and has the property that for all $\mathbf{u}', \mathbf{u} \in U$ there exists a $g \in G$ such that $g\mathbf{u} = \mathbf{u}'$, then we call U a transitive G-set. In other words, the transitive G-sets are just the orbits of the elements of $(Z_p)^n$ under repeated left multiplication by A.

2. Transitive G-sets

If we select an arbitrary element $\mathbf{v}$ from $(Z_p)^n$, the orbit of $\mathbf{v}$ under the action of G is the transitive G-set containing $\mathbf{v}$. These transitive G-sets partition $(Z_p)^n$.

Example 2.1. *Consider the sequence defined by* $S_n = 3S_{n-3} + 3S_{n-2} + S_{n-1}$*, taken over* Z_5*. The action of the group generated by* $A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 3 & 3 & 1 \end{bmatrix}$ *partitions the* G*-set* $(Z_5)^3$ *into the following 8 transitive* G*-sets (orbits):*

$$H_1 = \left\{ \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \right\},$$

$$H_2 = \left\{ \begin{bmatrix}0\\0\\1\end{bmatrix}, \begin{bmatrix}0\\1\\1\end{bmatrix}, \begin{bmatrix}1\\1\\4\end{bmatrix}, \begin{bmatrix}1\\4\\0\end{bmatrix}, \begin{bmatrix}4\\0\\0\end{bmatrix}, \begin{bmatrix}0\\0\\2\end{bmatrix}, \begin{bmatrix}0\\2\\2\end{bmatrix}, \begin{bmatrix}2\\2\\3\end{bmatrix}, \begin{bmatrix}2\\3\\0\end{bmatrix}, \begin{bmatrix}3\\0\\0\end{bmatrix}, \begin{bmatrix}0\\0\\4\end{bmatrix}, \begin{bmatrix}0\\4\\4\end{bmatrix}, \begin{bmatrix}4\\4\\1\end{bmatrix}, \begin{bmatrix}4\\1\\0\end{bmatrix}, \begin{bmatrix}1\\0\\0\end{bmatrix}, \begin{bmatrix}0\\0\\3\end{bmatrix}, \begin{bmatrix}0\\3\\2\end{bmatrix}, \begin{bmatrix}3\\3\\2\end{bmatrix}, \begin{bmatrix}3\\2\\0\end{bmatrix}, \begin{bmatrix}2\\0\\0\end{bmatrix} \right\},$$

$$H_3 = \left\{ \begin{bmatrix}0\\1\\0\end{bmatrix}, \begin{bmatrix}1\\0\\3\end{bmatrix}, \begin{bmatrix}0\\3\\1\end{bmatrix}, \begin{bmatrix}3\\1\\0\end{bmatrix}, \begin{bmatrix}1\\0\\2\end{bmatrix}, \begin{bmatrix}0\\2\\0\end{bmatrix}, \begin{bmatrix}2\\0\\1\end{bmatrix}, \begin{bmatrix}0\\1\\2\end{bmatrix}, \begin{bmatrix}1\\2\\0\end{bmatrix}, \begin{bmatrix}2\\0\\4\end{bmatrix}, \begin{bmatrix}0\\4\\0\end{bmatrix}, \begin{bmatrix}4\\0\\2\end{bmatrix}, \begin{bmatrix}0\\2\\4\end{bmatrix}, \begin{bmatrix}2\\4\\0\end{bmatrix}, \begin{bmatrix}4\\0\\3\end{bmatrix}, \begin{bmatrix}0\\3\\0\end{bmatrix}, \begin{bmatrix}3\\0\\4\end{bmatrix}, \begin{bmatrix}0\\4\\3\end{bmatrix}, \begin{bmatrix}4\\3\\0\end{bmatrix}, \begin{bmatrix}3\\0\\1\end{bmatrix} \right\},$$

$$H_4 = \left\{ \begin{bmatrix}0\\1\\3\end{bmatrix}, \begin{bmatrix}1\\3\\1\end{bmatrix}, \begin{bmatrix}3\\1\\3\end{bmatrix}, \begin{bmatrix}1\\3\\0\end{bmatrix}, \begin{bmatrix}3\\0\\2\end{bmatrix}, \begin{bmatrix}0\\2\\1\end{bmatrix}, \begin{bmatrix}2\\1\\2\end{bmatrix}, \begin{bmatrix}1\\2\\1\end{bmatrix}, \begin{bmatrix}2\\1\\0\end{bmatrix}, \begin{bmatrix}1\\0\\4\end{bmatrix}, \begin{bmatrix}0\\4\\2\end{bmatrix}, \begin{bmatrix}4\\2\\4\end{bmatrix}, \begin{bmatrix}2\\4\\2\end{bmatrix}, \begin{bmatrix}4\\2\\0\end{bmatrix}, \begin{bmatrix}2\\0\\3\end{bmatrix}, \begin{bmatrix}0\\3\\4\end{bmatrix}, \begin{bmatrix}3\\4\\3\end{bmatrix}, \begin{bmatrix}4\\3\\4\end{bmatrix}, \begin{bmatrix}3\\4\\0\end{bmatrix}, \begin{bmatrix}4\\0\\1\end{bmatrix} \right\},$$

$$H_5 = \left\{ \begin{bmatrix}0\\1\\4\end{bmatrix}, \begin{bmatrix}1\\4\\2\end{bmatrix}, \begin{bmatrix}4\\2\\2\end{bmatrix}, \begin{bmatrix}2\\2\\0\end{bmatrix}, \begin{bmatrix}2\\0\\2\end{bmatrix}, \begin{bmatrix}0\\2\\3\end{bmatrix}, \begin{bmatrix}2\\3\\4\end{bmatrix}, \begin{bmatrix}3\\4\\4\end{bmatrix}, \begin{bmatrix}4\\4\\0\end{bmatrix}, \begin{bmatrix}4\\0\\4\end{bmatrix}, \begin{bmatrix}0\\4\\1\end{bmatrix}, \begin{bmatrix}4\\1\\3\end{bmatrix}, \begin{bmatrix}1\\3\\3\end{bmatrix}, \begin{bmatrix}3\\3\\0\end{bmatrix}, \begin{bmatrix}3\\0\\3\end{bmatrix}, \begin{bmatrix}0\\3\\2\end{bmatrix}, \begin{bmatrix}3\\2\\1\end{bmatrix}, \begin{bmatrix}2\\1\\1\end{bmatrix}, \begin{bmatrix}1\\1\\0\end{bmatrix}, \begin{bmatrix}1\\0\\1\end{bmatrix} \right\},$$

$$H_6 = \left\{ \begin{bmatrix}1\\1\\1\end{bmatrix}, \begin{bmatrix}1\\1\\2\end{bmatrix}, \begin{bmatrix}1\\2\\3\end{bmatrix}, \begin{bmatrix}2\\3\\2\end{bmatrix}, \begin{bmatrix}3\\2\\2\end{bmatrix}, \begin{bmatrix}2\\2\\2\end{bmatrix}, \begin{bmatrix}2\\2\\4\end{bmatrix}, \begin{bmatrix}2\\4\\1\end{bmatrix}, \begin{bmatrix}4\\1\\4\end{bmatrix}, \begin{bmatrix}1\\4\\4\end{bmatrix}, \begin{bmatrix}4\\4\\4\end{bmatrix}, \begin{bmatrix}4\\4\\3\end{bmatrix}, \begin{bmatrix}4\\3\\2\end{bmatrix}, \begin{bmatrix}3\\2\\3\end{bmatrix}, \begin{bmatrix}2\\3\\3\end{bmatrix}, \begin{bmatrix}3\\3\\3\end{bmatrix}, \begin{bmatrix}3\\3\\1\end{bmatrix}, \begin{bmatrix}3\\1\\4\end{bmatrix}, \begin{bmatrix}1\\4\\1\end{bmatrix}, \begin{bmatrix}4\\1\\1\end{bmatrix} \right\},$$

$$H_7 = \left\{ \begin{bmatrix}1\\1\\3\end{bmatrix}, \begin{bmatrix}1\\3\\4\end{bmatrix}, \begin{bmatrix}3\\4\\1\end{bmatrix}, \begin{bmatrix}4\\1\\2\end{bmatrix}, \begin{bmatrix}1\\2\\2\end{bmatrix}, \begin{bmatrix}2\\2\\1\end{bmatrix}, \begin{bmatrix}2\\1\\3\end{bmatrix}, \begin{bmatrix}1\\3\\2\end{bmatrix}, \begin{bmatrix}3\\2\\4\end{bmatrix}, \begin{bmatrix}2\\4\\4\end{bmatrix}, \begin{bmatrix}4\\4\\2\end{bmatrix}, \begin{bmatrix}4\\2\\1\end{bmatrix}, \begin{bmatrix}2\\1\\4\end{bmatrix}, \begin{bmatrix}1\\4\\3\end{bmatrix}, \begin{bmatrix}4\\3\\3\end{bmatrix}, \begin{bmatrix}3\\3\\4\end{bmatrix}, \begin{bmatrix}3\\4\\2\end{bmatrix}, \begin{bmatrix}4\\2\\3\end{bmatrix}, \begin{bmatrix}2\\3\\1\end{bmatrix}, \begin{bmatrix}3\\1\\1\end{bmatrix} \right\},$$

$$H_8 = \left\{ \begin{bmatrix}1\\2\\4\end{bmatrix}, \begin{bmatrix}2\\4\\3\end{bmatrix}, \begin{bmatrix}4\\3\\1\end{bmatrix}, \begin{bmatrix}3\\1\\2\end{bmatrix} \right\}.$$

Note that the first row of H_4 corresponds to the sequence in Example 1.1.

To further study the structure of the transitive G-sets, we turn to the eigenvalues and eigenvectors associated with the matrix A. By inspection, it is easy to see that the rank of $xI - A$ is n or $n-1$. If $\lambda \in Z_p$ is a root of the characteristic polynomial $C(x) = \det(xI - A) = x^n - a_{n-1}x^{n-1} - \cdots - a_1 x - a_0$, then it can be verified that $\begin{bmatrix}1\\ \lambda\\ \lambda^2\\ .\\ .\\ .\\ \lambda^{n-1}\end{bmatrix}$ is an eigenvector of A and the dimension of the eigenspace corresponding to λ is one. Write E_λ for this eigenspace and note that

$$E_\lambda = \left\{ \begin{bmatrix}0\\0\\0\\.\\.\\.\\0\end{bmatrix}, \begin{bmatrix}1\\ \lambda\\ \lambda^2\\ .\\ .\\ .\\ \lambda^{n-1}\end{bmatrix}, \begin{bmatrix}2\\ 2\lambda\\ 2\lambda^2\\ .\\ .\\ .\\ 2\lambda^{n-1}\end{bmatrix}, \begin{bmatrix}3\\ 3\lambda\\ 3\lambda^2\\ .\\ .\\ .\\ 3\lambda^{n-1}\end{bmatrix}, \ldots, \begin{bmatrix}(p-1)\\ (p-1)\lambda\\ (p-1)\lambda^2\\ .\\ .\\ .\\ (p-1)\lambda^{n-1}\end{bmatrix} \right\}.$$

It is easy to check that $\left\{ \begin{bmatrix}0\\0\\.\\.\\.\\0\end{bmatrix} \right\}$ will always be a transitive G-set under the action of G on $(Z_p)^n$. It is also easy to see that if a transitive G-set contains an eigenvector, all the other vectors in that transitive G-set must also be eigenvectors. Therefore, for any transitive G-set, there are three mutually exclusive possibilities:

(1) it is the transitive G-set $\left\{ \begin{bmatrix} 0 \\ 0 \\ \cdot \\ \cdot \\ \cdot \\ 0 \end{bmatrix} \right\}$,
(2) it consists entirely of eigenvectors,
(3) it consists entirely of nonzero noneigenvectors.

In Example 2.1, the characteristic polynomial $C(x) = (x-2)^3$. So $\lambda = 2$ is the only eigenvalue and the eigenspace is

$$H_1 \cup H_8 = E_2 = \left\{ \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \\ 4 \end{bmatrix}, \begin{bmatrix} 2 \\ 4 \\ 3 \end{bmatrix}, \begin{bmatrix} 3 \\ 1 \\ 2 \end{bmatrix}, \begin{bmatrix} 4 \\ 3 \\ 1 \end{bmatrix} \right\}.$$

3. The Case $C(x) = (x - \lambda)^n$

Throughout this section assume that

$$C(x) = x^n - a_{n-1}x^{n-1} - \cdots - a_1 x - a_0 = (x - \lambda)^n$$

for some $\lambda \in Z_p - \{0\}$.

Definition 3.1. *Let J be the elementary Jordan matrix associated with C (see* [3, p. 359]*). So*

$$J = \begin{bmatrix} \lambda & 1 & 0 & \dots & 0 \\ 0 & \lambda & 1 & \ddots & 0 \\ 0 & 0 & \lambda & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & 1 \\ 0 & 0 & 0 & \dots & \lambda \end{bmatrix}.$$

Theorem 3.2. *For all $i \in \{0, 1, \dots\}$,*

$$J^i = \begin{bmatrix} \lambda^i & \binom{i}{1}\lambda^{i-1} & \binom{i}{2}\lambda^{i-2} & \binom{i}{3}\lambda^{i-3} & \dots & \binom{i}{n-1}\lambda^{i-(n-1)} \\ 0 & \lambda^i & \binom{i}{1}\lambda^{i-1} & \binom{i}{2}\lambda^{i-2} & \dots & \binom{i}{n-2}\lambda^{i-(n-2)} \\ 0 & 0 & \lambda^i & \binom{i}{1}\lambda^{i-1} & \dots & \binom{i}{n-3}\lambda^{i-(n-3)} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & \lambda^i \end{bmatrix}.$$

In particular, if k is the smallest power of p such that $n \le p^k$, then

$$J^{\alpha p^k} = \begin{bmatrix} \lambda^{\alpha p^k} & 0 & 0 & \dots & 0 \\ 0 & \lambda^{\alpha p^k} & 0 & \dots & 0 \\ 0 & 0 & \lambda^{\alpha p^k} & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & \lambda^{\alpha p^k} \end{bmatrix} = \begin{bmatrix} \lambda^{\alpha} & 0 & 0 & \dots & 0 \\ 0 & \lambda^{\alpha} & 0 & \dots & 0 \\ 0 & 0 & \lambda^{\alpha} & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & \lambda^{\alpha} \end{bmatrix}$$

and the order of J is $p^k|\lambda|$, where $|\lambda|$ is the order of the unit λ in the group Z_p.

Proof. The result follows from Lucas' Theorem [2], since if $i = p^j$, then $\binom{i}{1}, \binom{i}{2}, \binom{i}{3}, \dots, \binom{i}{n-1}$, are all equal to 0 modulo p if and only if $n \le p^j$. □

Theorem 3.3. *Let $\mathbf{v} \in (Z_p)^n$. There are three mutually exclusive possibilities for the transitive G-set containing $\mathbf{v}$:*

(1) *it is a transitive G-set of size one, consisting of only* $\left\{ \begin{bmatrix} 0 \\ 0 \\ \cdot \\ \cdot \\ \cdot \\ 0 \end{bmatrix} \right\}$,
(2) *it consists entirely of eigenvectors of A and has size $|\lambda|$,*
(3) *it consists entirely of nonzero noneigenvectors of A and has size $p^i|\lambda|$, for some $i \in \{1, \dots, k\}$, where k is the smallest power of p for which $n \le p^k$.*

Proof. Let

$$G' = \left\{ J^i \mid 0 \le i \ \le p^k|\lambda| - 1 \right\}.$$

Since J and A are similar matrices, that is $AP = PJ$ for some invertible matrix P, it is enough to show that the corresponding statement is true for the transitive G'-set containing $\mathbf{w} = P^{-1}(\mathbf{v})$. Assume that $J^i(\mathbf{w}) = \mathbf{w}$, for some positive integer i. Then $\mathbf{w}$ is an eigenvector of J^i with eigenvalue 1. By Theorem 3.2, the only eigenvalue of J^i is λ^i. Thus, $\lambda^i = 1$ and so $|\lambda|$ divides i.

In the first case, we have $\mathbf{v} = \mathbf{w} = \mathbf{0}$ so clearly the corresponding G'-set has size one.

For the second case, assume $\mathbf{v}$ is an eigenvector of A, so $A\mathbf{v} = \lambda\mathbf{v}$. Then $P^{-1}(A\mathbf{v}) = P^{-1}(\lambda\mathbf{v})$. Since A and J are similar, $J\mathbf{w} = \lambda\mathbf{w}$. Thus $\mathbf{w}$ is an eigenvector of J with eigenvalue λ. This implies that $J^{|\lambda|}\mathbf{w} = \lambda^{|\lambda|}\mathbf{w} = \mathbf{w}$. So $J^{|\lambda|}\mathbf{w} = \mathbf{w}$ and no smaller positive power of J can fix $\mathbf{w}$ because we know from the paragraph above that $|\lambda|$ would have to divide such a positive power.

Finally, let $\mathbf{v}$ be a nonzero noneigenvector of A. By an argument similar to the one in the paragraph above, $\mathbf{w}$ is a nonzero noneigenvector of J. If $J^i\mathbf{w} = \mathbf{w}$, we know from the first paragraph that there exists $j \in \{1, 2, 3, \ldots\}$ such that $i = j|\lambda|$. By Theorem 3.2, $J^{p^k|\lambda|}$ is the identity, so the size of the transitive G'-set containing $\mathbf{w}$ divides $p^k|\lambda|$ (and has a factor of $|\lambda|$), in other words, j divides p^k. Assume by way of contradiction that $j = 1$. Applying Theorem 3.2 we see that

$$J^{|\lambda|} = \begin{bmatrix} \lambda^{|\lambda|} & \binom{|\lambda|}{1}\lambda^{|\lambda|-1} & * & \ldots & * \\ 0 & \lambda^{|\lambda|} & \binom{|\lambda|}{1}\lambda^{|\lambda|-1} & \ldots & * \\ 0 & 0 & \lambda^{|\lambda|} & \ldots & * \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & \lambda^{|\lambda|} \end{bmatrix}.$$

But this matrix equals

$$\begin{bmatrix} 1 & |\lambda|\lambda^{-1} & * & \ldots & * \\ 0 & 1 & |\lambda|\lambda^{-1} & \ldots & * \\ 0 & 0 & 1 & \ldots & * \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \end{bmatrix}.$$

Since $|\lambda|\lambda^{-1}$ is nonzero, it is easy to see that the null space of the matrix $J^{|\lambda|} - 1I$ is one dimensional. We have already shown that the eigenspace of A, namely E_λ has cardinality p. So $P^{-1}(E_\lambda)$ is the complete one dimensional eigenspace of J with eigenvalue λ. Thus, $P^{-1}(E_\lambda)$ is the complete one dimensional eigenspace of $J^{|\lambda|}$ with eigenvalue $\lambda^{|\lambda|} = 1$. This contradicts the fact that $\mathbf{w}$ is a nonzero noneigenvector of J with $J^{|\lambda|}(\mathbf{w}) = \mathbf{w}$. Hence, j does not equal 1. This completes the proof. $\square$

We note that the G-sets corresponding to nonzero noneigenvectors may have different sizes. Let $C(x) = (x-2)^5$ and

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 2 & 1 & 2 & 2 & 1 \end{bmatrix},$$

taken over Z_3. The G-set associated with $\begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 2 \end{bmatrix}$ has size $6 = 3^1 \cdot 2$, while the G-set associated with $\begin{bmatrix} 0 \\ 2 \\ 1 \\ 0 \\ 0 \end{bmatrix}$ has size $18 = 3^2 \cdot 2$.

Theorem 3.4. *Let* $\mathbf{w} \in (Z_p)^n$. *Then for all* $i, \alpha \in \{0, 1, \ldots\}$,

$$J^{i+\alpha p^k}(\mathbf{w}) = \lambda^\alpha \cdot J^i(\mathbf{w}),$$

where k *is the smallest power of* p *for which* $n \leq p^k$.

Proof. By Theorem 3.2, $J^{\alpha p^k}(\mathbf{w}) = \lambda^\alpha \mathbf{w}$. Thus, $J^{i+\alpha p^k}(\mathbf{w}) = J^i J^{\alpha p^k}(\mathbf{w}) = J^i(\lambda^\alpha(\mathbf{w})) = \lambda^\alpha \cdot J^i(\mathbf{w})$. □

Definition 3.5. *If* $\mathbf{v} = \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix}$ *is a vector, then* $\pi_1(\mathbf{v}) = v_1$.

By examining the Jordan form J of A, we have obtained results for the sizes of the G'-sets corresponding to J. This gives us information about cardinality of the G-sets corresponding to A and periods of the related sequences. These results hold for any invertible matrix P with $AP = PJ$. Next we will construct a specific matrix P, with the property that $\pi_1(A^i\mathbf{v}) = \pi_1(J^i(P^{-1}\mathbf{v}))$, for all $i \in \{0, 1, \ldots\}$.

Lemma 3.6. *Given* $i \in \{1, \ldots, n-1\}$, *write* $C^{(i)}(x)$ *or* $\dfrac{d^i}{dx^i}C(x)$ *for the ith (formal) derivative of the polynomial* $C(x)$. *Then* $C^{(i)}(x)$ *evaluated at* λ *equals zero.*

Proof. See Lemma 6.10, [3, p. 161]. □

Lemma 3.7. *Given* $i \in \{1, \ldots, n-1\}$, $\frac{1}{i!} \cdot \frac{d^i}{dx^i}\Big|_{x=\lambda} (x^n - C(x)) = \binom{n}{i}\lambda^{n-i}$.

Proof. By the previous lemma, we know that $C^{(i)}(\lambda) = \frac{d^i}{dx^i}\Big|_{x=\lambda} C(x) = 0$.

Thus,

$$\frac{1}{i!} \cdot \frac{d^i}{dx^i}\bigg|_{x=\lambda} (x^n - C(x)) = \frac{1}{i!} \cdot \frac{d^i}{dx^i}\bigg|_{x=\lambda} x^n = \frac{1}{i!}\frac{n!}{(n-i)!}\lambda^{n-i} = \binom{n}{i}\lambda^{n-i}.$$

□

For the remainder of this section we will use a specific invertible matrix P.

Definition 3.8. *Let $P = [p_{ij}]$ be the $n \times n$ matrix*

$$\begin{bmatrix} 1 & 0 & 0 & 0 & \cdots & 0 & 0 \\ \lambda & 1 & 0 & 0 & \cdots & 0 & 0 \\ \lambda^2 & 2\lambda & 1 & 0 & \cdots & 0 & 0 \\ \lambda^3 & 3\lambda^2 & 3\lambda & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \lambda^{n-2} & \binom{n-2}{1}\lambda^{n-3} & \binom{n-2}{2}\lambda^{n-4} & \binom{n-2}{3}\lambda^{n-5} & \cdots & 1 & 0 \\ \lambda^{n-1} & \binom{n-1}{1}\lambda^{n-2} & \binom{n-1}{2}\lambda^{n-3} & \binom{n-1}{3}\lambda^{n-4} & \cdots & \binom{n-1}{n-2}\lambda^1 & 1 \end{bmatrix}.$$

Here, $p_{ij} = \binom{i-1}{j-1}\lambda^{i-j}$.

Lemma 3.9. *P is invertible and $P^{-1} =$*

$$\begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ -\lambda & 1 & 0 & \cdots & 0 & 0 \\ \lambda^2 & -2\lambda & 1 & \cdots & 0 & 0 \\ -\lambda^3 & 3\lambda^2 & -3\lambda & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ (-\lambda)^{n-2} & \binom{n-2}{1}(-\lambda)^{n-3} & \binom{n-2}{2}(-\lambda)^{n-4} & \cdots & 1 & 0 \\ (-\lambda)^{n-1} & \binom{n-1}{1}(-\lambda)^{n-2} & \binom{n-1}{2}(-\lambda)^{n-3} & \cdots & \binom{n-1}{n-2}(-\lambda)^1 & 1 \end{bmatrix}.$$

Proof. This is easily checked. □

Theorem 3.10. *$AP = PJ$.*

Proof. First we consider the product PJ. If $i \in \{1, \ldots, n\}$, then the dot product of the ith row of P and the first column of J is λ^i. If $j \in \{2, \ldots, n\}$, then the dot product of the ith row of P and the jth column of J is

$$\lambda \cdot \binom{i-1}{j-1}\lambda^{i-j} + \binom{i-1}{j-2}\lambda^{i-j+1} = \left(\binom{i-1}{j-1} + \binom{i-1}{j-2}\right) \cdot \lambda^{i-j+1}.$$

By Pascal's Identity, this reduces to $\binom{i}{j-1}\lambda^{i-j+1}$. So

$$PJ = \begin{bmatrix} \lambda & 1 & 0 & 0 & \dots & 0 & 0 \\ \lambda^2 & 2\lambda & 1 & 0 & \dots & 0 & 0 \\ \lambda^3 & 3\lambda^2 & 3\lambda & 1 & \dots & 0 & 0 \\ \lambda^4 & 4\lambda^3 & 6\lambda^2 & 4\lambda & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \dots & 0 & 0 \\ \lambda^{n-1} & \binom{n-1}{1}\lambda^{n-2} & \binom{n-1}{2}\lambda^{n-3} & \binom{n-1}{3}\lambda^{n-4} & \dots & 1 & 0 \\ \lambda^n & \binom{n}{1}\lambda^{n-1} & \binom{n}{2}\lambda^{n-2} & \binom{n}{3}\lambda^{n-3} & \dots & \binom{n}{n-2}\lambda^2 & n\lambda \end{bmatrix}.$$

Next we consider the product AP. If $i \in \{1, \dots, n-1\}$ and $j \in \{1, \dots, n\}$, then the dot product of the ith row of A and the jth column of P is the $i+1, j$th entry of P, i.e. $\binom{i}{j-1}\lambda^{i-j+1}$. So
$AP =$

$$\begin{bmatrix} \lambda & 1 & 0 & 0 & 0 & \dots & 0 & 0 \\ \lambda^2 & 2\lambda & 1 & 0 & 0 & \dots & 0 & 0 \\ \lambda^3 & 3\lambda^2 & 3\lambda & 1 & 0 & \dots & 0 & 0 \\ \lambda^4 & 4\lambda^3 & 6\lambda^2 & 4\lambda & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \dots & 0 & 0 \\ \lambda^{n-1} & \binom{n-1}{1}\lambda^{n-2} & \binom{n-1}{2}\lambda^{n-3} & \binom{n-1}{3}\lambda^{n-4} & \binom{n-1}{4}\lambda^{n-5} & \dots & 1 & 0 \\ * & * & * & * & * & \dots & * & * \end{bmatrix}.$$

All that remains is to show that the last row of AP and PJ are equal. The dot product of the nth row of A and the jth column of P is

$$\begin{aligned} & a_{j-1}p_{jj} + \dots + a_{n-1}p_{nj} \\ &= a_{j-1}\binom{j-1}{j-1}\lambda^0 + a_j\binom{j}{j-1}\lambda^1 + \dots + a_{n-1}\binom{n-1}{j-1}\lambda^{n-j} \\ &= \frac{1}{(j-1)!} \cdot \left(a_{j-1}\frac{(j-1)!}{0!}\lambda^0 + a_j\frac{(j)!}{1!}\lambda^1 + \dots + a_{n-1}\frac{(n-1)!}{(n-j)!}\lambda^{n-j} \right) \\ &= \frac{1}{(j-1)!} \cdot \frac{d^{j-1}}{dx^{j-1}}\bigg|_{x=\lambda} \left(a_0 + a_1x^1 + a_2x^2 + \dots + a_{n-1}x^{n-1} \right) \\ &= \frac{1}{(j-1)!} \cdot \frac{d^{j-1}}{dx^{j-1}}\bigg|_{x=\lambda} (x^n - C(x)). \end{aligned}$$

But by Lemma 3.7, this equals $\binom{n}{j-1}\lambda^{n-j+1}$. This is precisely the entry in the last row, jth column of PJ. Thus, $AP = PJ$. □

Theorem 3.11. *For all* $i \in \{0, 1, \dots\}$ *and* $\mathbf{v} \in (Z_p)^n$, $J^i(P^{-1}\mathbf{v}) = P^{-1}(A^i\mathbf{v})$ *and* $\pi_1(A^i\mathbf{v}) = \pi_1(J^i(P^{-1}\mathbf{v}))$.

Proof. By Theorem 3.10,

$$\begin{aligned} J^i(P^{-1}\mathbf{v}) &= (P^{-1}AP)^i(P^{-1}\mathbf{v})) \\ &= (P^{-1}A^iP)(P^{-1}\mathbf{v}) \\ &= P^{-1}(A^i\mathbf{v}). \end{aligned}$$

By Lemma 3.9, the first row of P^{-1} is $(1, 0, 0, \ldots, 0)$, so clearly $\pi_1(A^i\mathbf{v}) = \pi_1(P^{-1}(A^i\mathbf{v}))$. □

Corollary 3.12. *As mentioned earlier, a sequence $\{S_i\}$ that is generated by A can be described by $S_i = \pi_1(A^i\mathbf{v})$, for some $\mathbf{v} \in (Z_p)^n$. Consequently, $\{S_i\}$ is uniformly distributed if and only if the elements $\pi_1\left(J^i(P^{-1}\mathbf{v})\right)$ are uniformly distributed.*

Example 3.13. *If A is the matrix from Example 2.1, then $\lambda = 2, J = \begin{bmatrix} 2 & 1 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{bmatrix}, P = \begin{bmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 4 & 4 & 1 \end{bmatrix}$, and $P^{-1} = \begin{bmatrix} 1 & 0 & 0 \\ 3 & 1 & 0 \\ 4 & 1 & 1 \end{bmatrix}$. Now let $\mathbf{w} = P^{-1}(\mathbf{v})$, where $\mathbf{v} = \begin{bmatrix} 0 \\ 1 \\ 3 \end{bmatrix}$, the initial conditions of the sequence in Example 1.1. The G'-set corresponding to $\mathbf{w}$ is*

$$K = \left\{ \begin{bmatrix} 0 \\ 1 \\ 4 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 3 \end{bmatrix}, \begin{bmatrix} 3 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 2 \end{bmatrix}, \begin{bmatrix} 3 \\ 4 \\ 4 \end{bmatrix}, \begin{bmatrix} 0 \\ 2 \\ 3 \end{bmatrix}, \begin{bmatrix} 2 \\ 2 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 2 \end{bmatrix}, \begin{bmatrix} 2 \\ 2 \\ 4 \end{bmatrix}, \begin{bmatrix} 1 \\ 3 \\ 3 \end{bmatrix}, \right.$$
$$\left. \begin{bmatrix} 0 \\ 4 \\ 1 \end{bmatrix}, \begin{bmatrix} 4 \\ 4 \\ 2 \end{bmatrix}, \begin{bmatrix} 2 \\ 0 \\ 4 \end{bmatrix}, \begin{bmatrix} 4 \\ 4 \\ 3 \end{bmatrix}, \begin{bmatrix} 2 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 3 \\ 2 \end{bmatrix}, \begin{bmatrix} 3 \\ 3 \\ 4 \end{bmatrix}, \begin{bmatrix} 4 \\ 0 \\ 3 \end{bmatrix}, \begin{bmatrix} 3 \\ 3 \\ 1 \end{bmatrix}, \begin{bmatrix} 4 \\ 2 \\ 2 \end{bmatrix} \right\}.$$

Note that the sequence in Example 1.1 is the first row of both K and H_4 of Example 2.1.

Finally, we observe that Theorem 3.2 can be generalized to the case where

$$C(x) = (x - \lambda_1)^{n_1}(x - \lambda_2)^{n_2} \cdots (x - \lambda_t)^{n_t}$$

over Z_p. The corresponding Jordan forms will consist of blocks of elementary Jordan matrices (see Definition 3.1) for each λ_i. Applying Theorem 3.2 to each block, we see that the order of A is equal to the least common multiple of the orders of the elementary Jordan blocks. The distribution properties for second order recurrences over Z_p are well-known [5]. As seen in Example 2.1, not all G-sets corresponding to nonzero noneigenvectors are uniformly distributed. A general characterization of the distribution properties of third order recurrences appears in [4] and partial results for higher order linear recurrences are discussed in [7]. To the best of our knowledge, general criteria for the distribution properties of nth order linear recurrences are not known for large n.

References

[1] M. Artin, *Algebra*, Prentice Hall, New Jersey, 1991.
[2] N. J. Fine, *Binomial coefficients modulo a prime*, The American Mathematical Monthly, **54.10**, Part 1 (1947), 589–592.
[3] T. Hungerford, *Algebra*, Springer, New York, 1974.
[4] M. J. Knight and W. A. Webb, *Uniform distribution of third order linear recurrence sequences*, Acta Arithmetica, **36** (1980), 6–20.
[5] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and Their Applications*, Cambridge University Press, Cambridge, 1986.
[6] T. McKenzie, S. Overbay, and R. Ray, *G-sets and linear recurrences modulo primes*, Missouri Journal of Mathematical Sciences, **21.1** (2013), 27–36.
[7] H. Niederreiter and J.-S. Shiue, *Equidistribution of linear recurring sequences in finite fields*, Indagationes Mathematicae, **80** (1977), 397–405.

MSC2010: 11B50

Key words and phrases: matrix groups, linear recurrences over Z_p

Department of Mathematics, Gonzaga University, Spokane, WA
E-mail address: mckenzie@gonzaga.edu

Department of Mathematics, Gonzaga University, Spokane, WA
E-mail address: overbay@gonzaga.edu

Department of Mathematics, Gonzaga University, Spokane, WA
E-mail address: rayr@gonzaga.edu