TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 339, Number 1, September 1993

PERIODIC SEEDED ARRAYS AND AUTOMORPHISMS OF THE SHIFT

EZRA BROWN

ABSTRACT. The automorphism group $\mathrm{Aut}(\Sigma_2)$ of the full 2-shift is conjectured to be generated by the shift and involutions. We approach this problem by studying a certain family of automorphisms whose order was unknown, but which we show to be finite and for which we find factorizations as products of involutions. The result of this investigation is the explicit construction of a subgroup $\mathscr{H}$ of $\mathrm{Aut}(\Sigma_2)$; $\mathscr{H}$ is generated by certain involutions g_n, and turns out to have a number of curious properties. For example, g_n and g_k commute unless n and k are consecutive integers, the order of $g_{n+k} \circ \cdots \circ g_k$ is independent of k, and $\mathscr{H}$ contains elements of all orders. The investigation is aided by the development of results about certain new types of arrays of 0's and 1's called periodic seeded arrays, as well as the use of Boyle and Krieger's work on return numbers and periodic points.

1. INTRODUCTION

Let $S_1 = \{0, 1\}$; let S_n be the set of n-long sequences of 0's and 1's. Each element of S_n will be called an n-block, or merely a block. Let S be the set of all doubly infinite sequences of 0's and 1's, indexed by the integers; we may also view S as the doubly infinite product of copies of S_1.

Under the product topology, S is a metric space homeomorphic to the Cantor discontinuum. The *shift operator* σ is the mapping of S onto itself defined by

$$(\sigma(x))_n = x_{n+1},$$

for any sequence $x \in S$. The pair (S, σ) is called the *shift dynamical system* over $\{0, 1\}$, or the 2-*shift*, and is often designated by Σ_2.

An *endomorphism* of Σ_2 is any mapping from S to S that is continuous and commutes with the shift operator; an *automorphism* of Σ_2 is an endomorphism that is 1-1 and onto. An *n-block map* is a mapping from S_n to S_1; a *block map* is an n-block map for some n. Every block map induces an endomorphism of Σ_2 as follows: if f is an n-block map, define $f_\infty : S \to S$ by

$$(f_\infty(x))_k = f(x_k, \ldots, x_{k+n-1}),$$

Received by the editors May 22, 1991.
1991 *Mathematics Subject Classification.* Primary 54H20; Secondary 20B27, 58F20, 05B20.
Key words and phrases. Block maps, shift dynamical system, automorphism group, symbolic dynamics, 0-1 arrays, periodic points.

where $x = (x_k)$. By a theorem of Curtis, Hedlund, and Lyndon [H, Theorem 3.4], the endomorphisms of Σ_2 are precisely those maps of the form $\sigma^r \circ f_\infty$, where f is a block map and σ^r denotes the rth iterate of σ under composition. Hence, one way to study the endomorphisms and automorphisms of the 2-shift is via the properties of block maps.

A convenient way to represent block maps is by means of polynomial functions; a straightforward counting argument reveals a one-to-one correspondence between the set $\mathscr{F}_n$ of n-block maps and the set of polynomial functions (also called Boolean polynomials) in n variables over $\mathbb{Z}_2$. If we define the block maps f and g to be equal provided $f_\infty = g_\infty$, then $\mathscr{F}_n \subset \mathscr{F}_{n+1}$. Now define addition and multiplication on $\mathscr{F} = \bigcup_n \mathscr{F}$ as follows; if $f \in \mathscr{F}_n$ and $g \in \mathscr{F}_m$, then define $f + g$, $f \cdot g \in \mathscr{F}_M$, where $M = \max\{m, n\}$ by

$$(f + g)(x_1 \cdots x_M) = f(x_1 \cdots x_n) + g(x_1 \cdots x_m),$$
$$(f \cdot g)(x_1 \cdots x_M) = f(x_1 \cdots x_n) \cdot g(x_1 \cdots x_m).$$

Under this equality and these operations, $(\mathscr{F}, +, \cdot)$ is a commutative ring with identity in which $(f + g)_\infty = f_\infty + g_\infty$ and $(f \cdot g)_\infty = f_\infty \cdot g_\infty$.

We may also define composition of block maps in the following way. Suppose $f \in \mathscr{F}_n$ and $g \in \mathscr{F}_m$; if we put $y_k = g(x_k \cdots x_{k+m-1})$, then $y = (y_k) = (g(x_k \cdots x_{k+m-1})) = g_\infty(x)$, where $x = (x_k)$. Thus, $f_\infty(y) = f_\infty \circ g_\infty(x)$. We now define $f \circ g \in \mathscr{F}_{m+n-1}$ by

$$f \circ g(x_1 \cdots x_{n+m-1}) = f(g(x_1 \cdots x_m), \ldots, g(x_n \cdots x_{n+m-1})).$$

It follows that $(f \circ g)_\infty = f_\infty \circ g_\infty$, where the left side is a composition of block maps and the right side is a composition of endomorphisms of Σ_2. In addition, if f is a block map, let us define f^k by $f^1 = f$ and $f^{k+1} = f^k \circ f$ for $k \geq 1$. Since composition of block maps is associative, it follows that powers of f commute.

2. The problem at hand

Much is known about the structure of $\mathrm{Aut}(\Sigma_2)$, the group of automorphisms of Σ_2. For example, $\mathrm{Aut}(\Sigma_2)$ is countable and contains a copy of every finite group [H], and its center consists of the powers of the shift [R]. Several authors [CHR, R1–R5 and Ry] have studied conditions under which endomorphisms of the 2-shift commute, and there is an explicit construction (see [Br]) of a subgroup of $\mathrm{Aut}(\Sigma_2)$ generated by infinitely many commuting involutions.

But open questions about $\mathrm{Aut}(\Sigma_2)$ abound; in particular, it is now known whether $\mathrm{Aut}(\Sigma_2)$ is generated by the shift operator and involutions. We began our study of this question with an example due to Lee Neuwirth.

Let us write $\overline{x}$ to mean the complement $x+1$ of the variable x, and consider the block map $F_5 \in \mathscr{F}_5$, defined by

$$F_5(x_1 \cdots x_5) = x_4 + x_5(\overline{x}_3 + x_1\overline{x}_2x_4 + \overline{x}_1\overline{x}_2\overline{x}_3).$$

According to Neuwirth [N], if $f \in \mathscr{F}_5$ induces an automorphism of Σ_2, then either f_∞ is an involution modulo the shift, or $f = F_5$; moreover, the order of $(F_5)_\infty$ modulo the shift was unknown. Hence there was some interest in studying F_5. A fairly laborious calculation showed that

$$F_5^2(x_1 \cdots x_9) = x_7 + x_4\overline{x}_5\overline{x}_6x_8 + x_5\overline{x}_6\overline{x}_7x_9 + x_5\overline{x}_6x_8x_9,$$

and

$$F_5^3(x_1 \cdots x_{13}) = x_{10} + x_8\overline{x}_9x_{11}\overline{x}_{12};$$

it easily followed that $F_5^6(x_1 \cdots x_{25}) = x_{19}$, and so $(F_5^6)_\infty = \sigma^{18}$. Thus, $\sigma^{-3} \circ (F_5)_\infty$ is an automorphism of order 6, so that modulo the shift, $(F_5)_\infty$ has finite order. Unfortunately, there was no obvious factorization of $\sigma^{-3} \circ (F_5)_\infty$ as a product of involutions.

Now F_5 is part of an infinite family of inductively defined block maps (whence the subscript 5), all of which were thought to induce automorphisms of finite order modulo the shift [N]. However, since

$$\begin{aligned} F_6 &= x_5 + x_6(\overline{F}_5 + \overline{x}_1\overline{x}_2\overline{x}_3\overline{x}_4) \\ &= x_5 + x_6(\overline{x}_4 + x_5(\overline{x}_3 + x_1\overline{x}_2x_4 + \overline{x}_1\overline{x}_2\overline{x}_3) + \overline{x}_1\overline{x}_2\overline{x}_3\overline{x}_4), \end{aligned}$$

and since the F_n grew steadily more complicated with n, it seemed as if the only way to attack the problem lay in writing a computer program to do composition of block maps. Progress in this direction went slowly, and frustration with pesky programs and recalcitrant compilers mounted. In desperation, we returned to the paper-and-pencil approach, and finally proved that F_6 induces an automorphism of order 12 modulo the shift. Along the way, we obtained the representations of F_n that are Theorems 3.1 and 3.2 of this paper, the latter being essentially a factorization of $\sigma^{-(n-2)} \circ (F_n)_\infty$ into a product of involutions.

The key to our early progress, however, was Lemma 3.3, which says that composing F_n with the block map $x_1\overline{x}_2$ merely shifts the latter. We soon saw the general pattern and conjectured that

$$F_n^{\operatorname{lcm}(1,2,\ldots,n-2)} = T^{(n-2)\operatorname{lcm}(1,2,\ldots,n-2)},$$

where $T(x_1x_2) = x_2$ satisfies $T_\infty = \sigma$. A proof of this conjecture came only after much streamlining of notation, observing the role played by certain arrays of 0's and 1's we call periodic seeded arrays, and applying some of the fine work Boyle and Krieger did on return numbers and periodic points in shifts of finite type (see [BK]).

The result of this investigation is the explicit construction of a subgroup $\mathscr{H}$ of $\operatorname{Aut}(\Sigma_2)$, containing the automorphism $(F_n)_\infty$ and having a number of curious properties. For example, $\mathscr{H}$ is generated by the shift, the complement map $c(x_1) = \overline{x}_1$ and by infinitely many involutions g_n for $n = 4, 5, \ldots$; it turns out that g_n commutes with g_k if and only if $n - k \neq \pm 1$. Furthermore, for fixed n, the order of the element $g_{n+r} \circ \cdots \circ g_{5+r} \circ g_{4+r}$ is finite and independent of r, while the maps $c \circ g_n \circ \cdots \circ g_4$ all have infinite order. Finally, $\mathscr{H}$ contains automorphisms of all finite orders.

3. The maps F_n and automorphisms of the shift

Definitions: For $n \geq 1$, define $F_n \in \mathscr{F}_n$ as follows:

$F_1 = 1$, $F_2 = x_1$, and $F_n = x_{n-1} + x_n(\overline{F}_{n-1} + \overline{x}_1 \cdots \overline{x}_{n-2})$ for $n \geq 3$.

Thus,

$$\begin{aligned} F_3 &= x_2, \\ F_4 &= x_3 + x_1\overline{x}_2x_4, \\ F_5 &= x_4 + x_1\overline{x}_2(x_3x_4 + \overline{x}_3\overline{x}_4)x_5 + x_2\overline{x}_3x_5, \quad \text{etc.} \end{aligned}$$

For $n \geq 4$, define $f_n \in \mathscr{F}_n$ by

$$f_n = x_{n-1} + x_1 \left(\prod_{k=2}^{n-2} \overline{x}_k \right) x_n .$$

Define T, G_n, and g_n by

$$T(x_1 x_2) = x_2 , \quad G_n = \sigma^{-(n-2)} \circ (F_n)_\infty , \quad \text{and} \quad g_n = \sigma^{-(n-2)} \circ (f_n)_\infty .$$

Note that $T = F_3$ and $T_\infty = \sigma$; hence, $G_n = (T^{-(n-2)} \circ (F_n))_\infty$, and G_n and g_n are all endomorphisms of Σ_2. It turns out that the g_n are all involutions, and that

$$G_n = g_n \circ g_{n-1} \circ \cdots \circ g_4 \quad \text{for } n \geq 4 ;$$

hence, the G_n are automorphisms of Σ_2. Although it is not at all obvious that the G_n have finite order, we will show that the order $o(G_n)$ of G_n is equal to $\operatorname{lcm}(1, 2, \ldots, n-2)$, where lcm denotes the least common multiple. Our strategy is to prove that $\operatorname{lcm}(1, 2, \ldots, n-2)$ is the smallest positive power of F_n that is equal to a power of the shift block map T. For, if $f^r = T^{kr}$, and if r is the least such integer for which this is true, then $(T^{-k} \circ f)_\infty$ is an automorphism of Σ_2 of order r.

If a and b are integers, write $a|b$ to mean that a is a divisor of b. Our first result, Theorem 3.1, gives a representation of F_n which we will use to prove that

$$F_n^{\operatorname{lcm}(1,2,\ldots,n-2)} = T^{(n-2)\operatorname{lcm}(1,2,\ldots,n-2)} .$$

From this it will follow that $o(G_n) | \operatorname{lcm}(1, 2, \ldots, n-2)$.

But first, let us simplify the notation. We will write k to stand for x_k; thus, F_4 looks like $3 + 1\overline{2}4$. To avoid confusion, we will use $\mathbf{I}$ to stand for the number 1; thus, $4 + \mathbf{I}$ means $x_4 + 1$, or $\overline{x}_4$. If j and k are integers with $j \leq k$, define $\Delta(j, k)$ by

$$\Delta(j, k) = j(j+1)\cdots k + \overline{j}(\overline{j+1})\cdots\overline{k} .$$

Note that $\Delta(k, k) = k + \overline{k} = \mathbf{I}$.

Theorem 3.1. *If $n \geq 4$, then*

$$F_n = (n-1) + \sum_{j=1}^{n-3} j(\overline{j+1})\Delta(j+2, n-1)n .$$

Proof. If $n = 4$, then

$$F_4 = 3 + 1\overline{2}4 = 3 + 1\overline{2}(3 + \overline{3})4 = 3 + \sum_{j=1}^{1} j(\overline{j+1})\Delta(j+2, 3)4 ,$$

as claimed. Now assume that the theorem is true for $4 \le k \le n$. Then:

$$\begin{aligned}
F_{n+1} &= n + (n+1)(\overline{F}_n + \overline{1}\,\overline{2}\cdots\overline{n-1}) \\
&= n + \left(\overline{n-1} + \sum_{n=1}^{n-3} j(\overline{j+1})\Delta(j+2, n-1)n\right)(n+1) + \overline{1}\,\overline{2}\cdots\overline{n-1}(n+1) \\
&= n + \sum_{j=1}^{n-3} j(\overline{j+1})\Delta(j+2, n-1)n(n+1) \\
&\quad + \overline{n-1}(n+1) + \overline{1}\,\overline{2}\cdots\overline{n-1}(n+1) \\
&\quad + 2\overline{3}\cdots\overline{n-1}(n+1) + \cdots + \overline{n-1}(n+1) \\
&= n + \sum_{j=1}^{n-3} j(\overline{j+1})(\overline{j+2}\cdots\overline{n-1}n(n+1) + (j+2)\cdots(n-1)n(n+1) \\
&\qquad\qquad + j(\overline{j+1})\cdots\overline{n-1}(n+1)) \\
&\quad + (n-2)\overline{n-1}(n+1) \\
&= n + \sum_{j=1}^{n-2} j(\overline{j+1})\Delta(j+2, n)(n+1).
\end{aligned}$$

The theorem follows by induction.

Theorem 3.2 gives a representation of F_n which we will use to prove that $o(G_n)$ is divisible by $\operatorname{lcm}(1, 2, \ldots, n-2)$.

Theorem 3.2. *If* $n \ge 4$, *then*

$$f_n \circ f_{n-1} \circ \cdots \circ f_4 = T^{\binom{n-2}{2}-1} \circ F_n.$$

The proof follows from a series of technical lemmas.

Lemma 3.3. *If* $n \ge 4$, *then* $1\overline{2} \circ F_n = T^{n-2} \circ 1\overline{2} = (n-1)\overline{n}$.

Proof. By Theorem 3.1,

$$\begin{aligned}
1\overline{2} \circ F_n &= 1\overline{2} \circ \left((n-1) + \sum_{j=1}^{n-3} j(\overline{j+1})\Delta(j+2, n-1)n\right) \\
&= ((n-1) + 1\overline{2}\Delta(3, n-1)n + 2\overline{3}\Delta(4, n-1)n + \cdots + (n-3)\overline{n-2}n) \\
&\quad \circ (\overline{n} + 2\overline{3}\Delta(4, n)(n+1) + 3\overline{4}\Delta(5, n)(n+1) + \cdots + (n-2)\overline{n-1}(n+1)).
\end{aligned}$$

Using the fact that $k \cdot \overline{k} = 0$, we see that the term $1\overline{2}\Delta(3, n-1)n$ cancels all terms in the second factor, and if $j > 1$, then $j(\overline{j+1})\Delta(j+2, n-1)n$ cancels all of those terms except for $j(\overline{j+1})\Delta(j+2, n)(n+1)$. From this, the

commutativity of multiplication and the fact that $k \cdot k = k$, we find that

$$\begin{aligned}
1\overline{2} \circ F_n &= (n-1)\left(\overline{n} + \sum_{j=2}^{n-2} j(\overline{j+1})\Delta(j+2, n)(n+1)\right) \\
&\quad + \sum_{j=2}^{n-3} j(\overline{j+1})\Delta(j+2, n-1)n\Delta(j+2, n)(n+1) \\
&= (n-1)\left(\overline{n} + \sum_{j=2}^{n-3} j(\overline{j+1})(j+2)\cdots n(n+1)\right) \\
&\quad + \sum_{j=2}^{n-3} j(\overline{j+1})((j+2)\cdots(n-1) + \overline{j+2}\cdots\overline{n-1}) \\
&\quad \times ((j+2)\cdots n + \overline{j+2}\cdots\overline{n})n(n+1) \\
&= (n-1)\left(\overline{n} + \sum_{j=2}^{n-3} j(\overline{j+1})(j+2)\cdots n(n+1)\right) \\
&\quad + \sum_{j=2}^{n-3} j(\overline{j+1})((j+2)\cdots(n-1))n(n+1), \quad \text{as all other terms cancel} \\
&= (n-1)\overline{n} + \sum_{j=2}^{n-3} j(\overline{j+1})(j+2)\cdots n(n+1) \\
&\quad + \sum_{j=2}^{n-3} j(\overline{j+1})((j+2)\cdots n)(n+1) \\
&= (n-1)\overline{n},
\end{aligned}$$

and we are done.

Lemma 3.4. (a) *If* $j < m \leq k$, *then* $(n-1)\overline{m}\Delta(j, k) = 0$.
(b) *If* $j \leq k \leq m \leq n$, *then* $\Delta(j, m)\Delta(k, n) = \Delta(j, n)$.
(c) *If* $2 \leq k \leq n-1$, *then* $1\overline{2}\cdots\overline{k} \circ F_n = (n-1)\overline{n}\Delta(n+1, n+k-1)$.

Proof. (a)

$$(m-1)\overline{m}\Delta(j, k) = (n-1)\overline{m}(j\cdots(m-1)m\cdots + \overline{j}\cdots\overline{m-1}\overline{m}\cdots) = 0,$$

since $(m-1)\cdot\overline{m-1} = m\cdot\overline{m} = 0$.
(b)

$$\begin{aligned}
\Delta(j, m)\Delta(k, n) &= (j(j+1)\cdots k\cdots m + \overline{j}(\overline{j+1})\cdots\overline{k}\cdots\overline{m}) \\
&\quad \cdot (k(k+1)\cdots m\cdots n + \overline{k}(\overline{k+1})\cdots\overline{m}\cdots\overline{n}) \\
&= (j(j+1)\cdots n + \overline{j}(\overline{j+1})\cdots\overline{n}) \\
&= \Delta(j, n),
\end{aligned}$$

since all the other terms cancel.

(c) Using Lemma 3.3 and parts (a) and (b), we find that

$$\begin{aligned}1\overline{2}\,\overline{3}\circ F_n &= (n-1)\overline{n}(\overline{n+1}+3\overline{4}\Delta(5,n+1)(n+2)\\ &\qquad +\cdots+(n-2)\overline{n-1}\Delta(n,n+1)(n+2)+(n-1)\overline{n}(n+2))\\ &= (n-1)\overline{n}(\overline{n+1}+(n-1)\overline{n}(n+2))\\ &= (n-1)\overline{n}(\overline{n+1}+(n+2))=(n-1)\overline{n}(\Delta(n+1,n+2));\end{aligned}$$

assuming that $1\overline{2}\cdots\overline{k-1}\circ F_n=(n-1)\overline{n}\Delta(n+1,n+k-2)$, we have that

$$\begin{aligned}1\overline{2}\cdots\overline{k-1}k\circ F_n &= (n-1)\overline{n}\Delta(n+1,n+k-2)\\ &\quad\times\left(\overline{n+k-2}+\sum_{j=k}^{n+k-4} j(\overline{j+1})\Delta(j+2,n+k-2)(n+k-1)\right)\\ &= (n-1)\overline{n}\Delta(n+1,n+k-2)(\overline{n+k-2}+(n+k-1))\\ &= (n-1)\overline{n}\Delta(n+1,n+k-1),\qquad \text{all other terms cancelling.}\end{aligned}$$

Lemma 3.5. $f_{n+1}\circ F_n = T^{n-1}\circ F_{n+1}$.

Proof.

$$\begin{aligned}f_{n+1}\circ F_n &= (n+1\overline{2}\cdots\overline{n-1}(n+1))\circ F_n\\ &= T^{n-1}\left((n-1)+\sum_{j=1}^{n-3} j(\overline{j+1})\Delta(j+2,n-1)n\right)\\ &\quad+(n-1)\overline{n}\Delta(n+1,2n-2)\cdot T^n\circ(F_n)\\ &= \left((2n-2)+\sum_{j=1}^{n-3}(n+j-1)\overline{n+j}\Delta(n+j+1,2n-2)(2n-1)\right)\\ &\quad+(n-1)\overline{n}\Delta(n+1,2n-2)\\ &\quad\times\left((2n-1)+\sum_{j=1}^{n-3}(n+j)\overline{n+j+1}\Delta(n+j+2,2n-1)2n\right).\end{aligned}$$

But by previous results, the last summand collapses to

$$(n-1)\overline{n}\Delta(n+1,2n-2)(2n-1).$$

Hence

$$\begin{aligned}f_{n+1}\circ F_n &= (2n-2)+\sum_{j=1}^{n-3}((n+j-1)\overline{n+j}\Delta(n+j+1,2n-2)(2n-1)\\ &\qquad+(n-1)\overline{n}\Delta(n+1,2n-2)(2n-1))\\ &= (2n-2)+\sum_{j=1}^{n-2}(n+j-1)\overline{n+j}\Delta(n+j+1,2n-2)(2n-1)\\ &= T^{n-2}\circ F_{n+1},\end{aligned}$$

and we are done.

Proof of Theorem 3.2. First, the theorem holds for $n = 4$, since $f_4 = F_4 = 3 + 1\overline{24}$ and $\binom{n-2}{2} - 1 = 1 - 1 = 0$. Assume the theorem holds for some $n = k \geq 4$. Since $T_\infty = \sigma$, T commutes with every block map. Then by Lemma 3.5,

$$\begin{aligned} f_{n+1} \circ f_n \circ \cdots \circ f_4 &= f_{n+1} \circ T^{\binom{n-2}{2}-1} \circ F_n \\ &= T^{\binom{n-2}{2}-1} \circ T^{n-2} \circ F_{n+1} = T^{\binom{n-2}{2}-1} \circ F_{n+1}, \end{aligned}$$

and the proof follows by induction.

Corollary 3.6. *Let* $n \geq 4$. *Then* $G_n = g_n \circ g_{n-1} \circ \cdots \circ g_4$.

Proof. Note that

$$\begin{aligned} g_n \circ \cdots \circ g_4 &= \sigma^{-(n-2+n-3+\cdots+2)} \circ (f_n \circ \cdots \circ f_4)_\infty \\ &= \sigma^{-\left(\binom{n-1}{2}-1\right)} \circ (f_n \circ \cdots \circ f_4)_\infty \\ &= \sigma^{-\left(n-2+\binom{n-2}{2}-1\right)} \circ (f_n \circ \cdots \circ f_4)_\infty \\ &= \sigma^{-(n-2)} \circ (F_n)_\infty = G_n. \end{aligned}$$

4. Powers of F_n

Computing powers of F_n under composition of block maps requires some more notation. For $j < m < n$, define

$$[j, m, n] = j(\overline{j+1}) \cdots \overline{m}(m+1) \cdots n;$$

thus,

$$[j, m, n] = T^{j-1} \circ [1, m-j+1, n-j+1],$$

and

$$\begin{aligned} F_n &= (n-1) + \sum_{j=1}^{n-3} j(\overline{j+1})\Delta(j+2, n-1)n \\ &= (n-1) + \sum_{j=1}^{n-3}([j, j+1, n] + [j, n-1, n]). \end{aligned}$$

Let us compute $F_n^2 = F_n \circ F_n$; we find that

$$\begin{aligned} F_n^2 &= T^{n-2} \circ F_n + \left(\sum_{j=1}^{n-3}([j, j+1, n] + [j, n-1, n])\right) \circ F_n \\ &= T^{2(n-2)} + \sum_{j=1}^{n-3} T^{n-2} \circ ([j, j+1, n] + [j, n-1, n]) \\ &\quad + \sum_{j=1}^{n-3}([j, j+1, n] + [j, n-1, n]) \circ F_n. \end{aligned}$$

The following theorem describes how $[1, k, r]$ composes with F_n, and will allow us to calculate powers of F_n easily.

Theorem 4.1. *If* $2 \le k < r \le n$, *then*

$$\begin{aligned} T^{-(n-2)} \circ [1, k, r] \circ F_n &= [1, k+1, r], \quad \text{if } k+1 < r, \\ &= [1, 2, r], \quad \text{if } k+1 = r = n, \\ &= [1, 2, r] + [1, 2, r+1] + [1, r, r+1], \\ &\qquad \text{if } k+1 = r < n. \end{aligned}$$

Proof. Using Lemma 3.4(c), we see that

$$\begin{aligned} [1, k, k+1] \circ F_n &= 1\overline{2} \cdots \overline{k}(k+1) \circ F_n \\ &= (n-1)\overline{n}\Delta(n+1, n+k-1) \cdot (k+1) \circ F_n \\ &= (n-1)\overline{n}\Delta(n+1, n+k-1) \\ &\quad \times \left((n+k-1) + \sum_{j=1}^{n-3} (j+k)(\overline{j+k+1}) \right. \\ &\qquad \left. \times \Delta(j+k+2, n+k-1)(n+k)_{j=1}^{n-3} \right). \end{aligned}$$

First, suppose $k \le n-2$. If $k \le n-3$, then $(n-1)\overline{n}$ cancels the term

$$(j+k)(\overline{j+k+1})\Delta(j+k+2, n+k-1)(n+k)$$

for $j = 1, \ldots, n-k-2$ or $j = n-k$, and $\Delta(n+1, n+k-1)$ cancels this term for $j \ge n-k+1$. If $k = n-2$, then $(n-1)\overline{n}$ cancels this term for $j = 2$, and $\Delta(n+1, 2n-3)$ cancels this term for $j \ge 3$. Hence if $k+1 < n$, then

$$\begin{aligned} [1, k, k+1] \circ F_n &= (n-1)\overline{n}\Delta(n+1, n+k-1) \\ &\quad \times ((n+k-1) + (n-1)\overline{n}\Delta(n+1, n+k-1)(n+k)) \\ &= (n-1)\overline{n}\Delta(n+1, n+k-1)((n+k-1+(n+k)) \\ &= (n-1)\overline{n}((n+1) \cdots (n+k-1))((n+k-1) + (n+k))(n+k) \\ &\quad + (\overline{n+1}) \cdots (\overline{n+k-1})(n+k) \\ &= T^{n-2} \circ ([1, 2, k+1] + [1, 2, k+2] + [1, k+1, k+2]). \end{aligned}$$

Thus, if $k+2 \le r \le n$, then

$$\begin{aligned} [1, k, r] \circ F_n &= ([1, k, k+1] \circ F_n) \cdot ((k+2) \cdots r) \circ F_n \\ &= T^{n-2} \circ (n-1)\overline{n}\Delta(n+1, n+k-1) \\ &\quad \times ((n+k-1) + (n+k))((k+2) \cdots r) \circ F_n. \end{aligned}$$

Now

$$(k+2) \circ F_n = (n+k) + \sum_{j=1}^{n-3} (j+k+1)(\overline{j+k+2})\Delta(j+k+3, n+k)(n+k+1);$$

when we multiply this expression by $((n+k-1)+(n+k))$, all of the terms inside the summation either are cancelled or appear twice. Hence,

$$((n+k-1)+(n+k)) \cdot ((k+2) \circ F_n) = ((n+k-1)+(n+k))(n+k).$$

A straightforward induction argument shows that

$$((n+k-1)+(n+k))\cdot((k+2)\cdots r)\circ F_n$$
$$=((n+k-1)+(n+k))((n+k)(n+k+1)\cdots(n+r-2)),$$

and so,

$$[1,k,r]\circ F_n=(n-1)\overline{n}\Delta(n+1,n+k-1)((n+k-1)+(n+k))\prod_{s=k}^{r-2}(n+s)$$
$$=(n-1)\overline{n}(\overline{n+1})\cdots(\overline{n+k-1})(n+k)\cdots(n+r-2)$$
(as all other terms cancel)
$$=T^{n-2}\circ[1,k+1,r],$$

as claimed.

Finally, we consider the case $k+1=r=n$; by Lemma 3.4(c), we have that

$$[1,n-1,n]\circ F_n=1\overline{2}\cdots\overline{n}\circ F_n$$
$$=((n-1)\overline{n}\Delta(n+1,2n-2))\cdot(n\circ F_n)$$
$$=(n-1)\overline{n}\Delta(n+1,2n-2)$$
$$\times\left((2n-2)+\sum_{j=1}^{n-3}(j+n-1)\overline{j+n}\Delta(j+n+1,2n-2)(2n-1)\right).$$

But for $1\le j\le n-3$,

$$\Delta(n+1,2n-2)(j+n-1)\overline{j+n}=0.$$

Hence,

$$[1,n-1,n]\circ F_n=(n-1)\overline{n}\Delta(n+1,2n-2)(2n-2)$$
$$=(n-1)\overline{n}(n+1)\cdots(2n-2)$$
$$=T^{n-2}\circ[1,2,n],$$

as claimed.

In order to streamline the computation of powers of F_n, we need some more notation: for $r\le n$ and k a positive integer, define $\langle 1,r;n\rangle^k$ by

$$\langle 1,r;n\rangle=[1,2,r]+[1,r-1,r],$$

and

$$\langle 1,r;n\rangle^{k+1}=T^{k(n-2)}\circ([1,2,r]+[1,r-1,r])+\langle 1,r;n\rangle^k\circ F_n,\qquad\text{for } k\ge 1.$$

Lemma 4.2. (a)

$$F_n=T^{n-2}+\sum_{r=4}^{n}T^{n-r}\circ\langle 1,r;n\rangle,$$

(b)

$$F_n^2=T^{2(n-2)}+\sum_{r=4}^{n}T^{n-r}\circ\langle 1,r;n\rangle^2,$$

(c)

$$F_n^k=T^{k(n-2)}+\sum_{r=4}^{n}T^{n-r}\circ\langle 1,r;n\rangle^k.$$

Proof. (a) Since

$$[j, j+1, n]+[j, n-1, n] = T^{j-1} \circ ([1, 2, n-j+1]+[1, n-j, n-j+1]),$$

it follows that if we put $r = n - j + 1$ and reverse the order of summation, we find that

$$\begin{aligned} F_n &= (n-1) + \sum_{j=1}^{n-3}([j, j+1, n]+[j, n-1, n]) \\ &= T^{n-2} + \sum_{j=1}^{n-3} T^{j-1}([1, 2, n-j+1]+[1, n-j, n-j+1]) \\ &= T^{n-2} + \sum_{r=4}^{n} T^{n-r} \circ ([1, 2, r]+[1, r-1, r]) \\ &= T^{n-2} + \sum_{r=4}^{n} T^{n-r} \circ \langle 1, r; n\rangle . \end{aligned}$$

(b) Because composition of block maps is left distributive over both addition and multiplication—i.e., $(f+g)\circ h = (f\circ h)+(g\circ h)$ and $(f\cdot g)\circ h = (f\circ h)\cdot(g\circ h)$ for all block maps f, g, and h—we have that

$$\begin{aligned} F_n^2 &= \left(T^{n-2} + \sum_{r=4}^{n} T^{n-r} \circ \langle 1, r; n\rangle\right) \circ F_n \\ &= T^{2(n-2)} + \sum_{r=4}^{n} T^{n-r} \circ T^{n-2} \circ \langle 1, r; n\rangle \\ &\quad + \left(\sum_{r=4}^{n} T^{n-r} \circ \langle 1, r; n\rangle\right) \circ F_n \\ &= T^{2(n-2)} + \sum_{r=4}^{n} T^{n-r}(T^{n-2} \circ \langle 1, r; n\rangle + \langle 1, r; n\rangle) \circ F_n \\ &= T^{2(n-2)} + \sum_{r=4}^{n} T^{n-r} \circ \langle 1, r; n\rangle^2 . \end{aligned}$$

(c) This follows from (b) and induction.

Define the order $o(\langle 1, r; n\rangle)$ of $\langle 1, r; n\rangle$ to be the least positive integer k for which $\langle 1, r; n\rangle^k = 0$, provided such an integer exists. (The context will reveal whether o refers to the order of an array or to the order of a group element.)

Lemma 4.3. *If N is a positive integer divisible by $o(\langle 1, r; n\rangle)$ for $4 \le r \le n$, then $F_n^N = T^{N(n-2)}$ and $o(G_n)|N$.*

Proof. By the previous lemma,

$$F_n^N = T^{N(n-2)} + \sum_{r=4}^{n} T^{n-r} \circ \langle 1, r; n\rangle^N .$$

But if $o(\langle 1, r; n\rangle)$ divides N, then the above sum is a sum of zeros; hence $F_n^N = T^{N(n-2)}$. By earlier work, it then follows that $o(G_n)|N$.

We are now ready to transform the problem to an analogous one involving arrays of 0's and 1's.

5. Periodic seeded arrays

Let $a > 0$ and $b \geq 0$ be integers. An $(a, a+b)$ *(seeded) array with seed* $\mathbf{s}$ is a rectangular array $\{a, a+b; \mathbf{s}\}$ of cells containing 0's and 1's. The array contains b *sections* number $a+1$ through $a+b$, with section $a+k$ containing $a+k$ rows. Above row 1 of section 1 is the *seed row*, which consists of repeated occurrences of an a-block $\mathbf{s} = s_1 s_2 \cdots s_a$ called the *seed*. The seed row is fixed throughout the discussion of a particular array; the rules of generation do not apply to the cells in the seed row. We identify cells with three letters: cell $(i, j; a+k)$ is in the ith column of section $a+k$.

Note: if $b = 0$, then the array $\{a, a; \mathbf{s}\}$ consists solely of the seed row generated by $\mathbf{s}$.

We generate $\{a, a+b; \mathbf{s}\}$ inductively as follows:

1. Column 1 consists of all zeros. Having filled all cells in column j:
2. If there is a 1 in the jth column of the seed row, place a 1 in each of cells $(1, j+1; a+1)$ and $(a+1, j+1; a+1)$.
3. If cell $(i, j; a+k)$ contains a 1, and $i \neq a+k$, then place a 1 in cell $(i+1, j+1; a+k)$.
4. If cell $(a+k, j; a+k)$ contains a 1, place a 1 in each of cells $(1, j+1; a+k)$, $(1, j+1; a+k+1)$ and $(a+k+1, j+k; a+k+1)$. However, if $k = b$ (i.e., the cell is in the last row of the entire array), place a 1 in cell $(1, j+1; a+b)$.
5. If the application of rules 2, 3, and 4, put two 1's in a cell and add them modulo 2.
6. Place a 0 in all cells in column $j+1$ unaffected by the preceding rules.

We often identify the contents of a cell with a cell itself; to say that $(i, j; a+k) = 1$ means that there is a 1 in cell $(i, j; a+k)$.

The *period* $\mathscr{P}(\{a, a+b; \mathbf{s}\})$ of $\{a, a+b; \mathbf{s}\}$ is defined to be the least positive integer p such that for all i, j, and k, $(i, j; a+k) = (i, j+p; a+k)$, and we use the same notation to denote the period of a seed $\mathbf{s}$. Finally, if B is a k-block, let us denote the nk-block consisting of n repeated occurrences of B by B^n. In particular, 1^n (resp., 0^n) is the n-block consisting of all 1's (resp., all 0's).

Theorem 5.1. *Suppose that* $\mathscr{P}(\{r-2, n-2; 1^{r-3}0\}) \equiv 0 \pmod{r-2}$. *Then* $o(\langle 1, r; n\rangle) = \mathscr{P}(\{r-2, n-2; 1^{r-3}0\})$.

Proof. Let us construct a table in which columns represent powers of $\langle 1, r; n\rangle$ and in which rows represent terms of the form $[1, j, m]$, where $2 \leq j \leq m-1$ and $r \leq m \leq n$. Let us place a 1 or a 0 in a cell according as the term of that row does or does not appear as a summand (multiplied by the appropriate power of T) in the power of $\langle 1, r; n\rangle$ of that column. Theorem 4.1 describes the rules for filling the cells.

Figure 1 illustrates this procedure for $r = 4$ and $n = 6$.

The rules from Theorem 4.1 imply that we have an initial section corresponding to the terms $[1, 2, r], \ldots, [1, r-1, r]$ which is periodic with period $r-2$ and such that for $1 \leq j \leq r-3$, there is a 1 in rows j and $r-2$, while column $r-2$ is all zeros. Hence, row $r-2$ consists of periodic occurrences of $r^{r-3}0$.

$\langle 1, 4; 6\rangle^k$

k:	1	2	3	4	5	6	7	8	9	10	11	12
$[1, j, m]$												
$[1, 2, 4]$	1	0	1	0	1	0	1	0	1	0	1	0
$[1, 3, 4]$	1	0	1	0	1	0	1	0	1	0	1	0
$[1, 2, 5]$	0	1	1	1	0	0	1	1	1	0	0	0
$[1, 3, 5]$	0	0	1	1	1	0	0	1	1	1	0	0
$[1, 4, 5]$	0	1	0	0	1	0	0	1	0	0	1	0
$[1, 2, 6]$	0	0	1	1	0	1	0	1	1	0	0	0
$[1, 3, 6]$	0	0	0	1	1	0	1	0	1	1	0	0
$[1, 4, 6]$	0	0	0	0	1	1	0	1	0	1	1	0
$[1, 5, 6]$	0	0	1	0	0	0	1	0	0	0	1	0

FIGURE 1

The rest of the table fills in according to Theorem 4.1, which corresponds exactly to the rules for filling in the cells of a seeded array. In fact, we may regard row $r-2$ as a seed—namely, the seed $1^{r-3}0$—for an $(r-2, n-2)$ seeded array in which the jth cell in row $[1, i+1, r+k]$ is labeled $(i, j; r+k-2)$. (After that initial section, the first column in the array proper consists of all zeros.)

Hence, the least positive power k for which $\langle 1, r; n\rangle^k = 0$ will be equal to the least positive k such that all entries in the kth column of the array, *including the entry in the seed row*, are all zero. This is equal to $\mathscr{P}(\{r-2, n-2; r^{r-3}0\})$, if we know that $\mathscr{P}(\{r-2, n-2; 1^{r-3}0\})$ is divisible by $r-2$. But this was assumed to be the case, and so we are done.

Theorem 5.2. *Suppose that* $n \geq 4$ *is an integer; suppose that, for* $4 \leq r \leq n$,

$$\mathscr{P}(\{r-2, n-2; 1^{r-3}0\}) \equiv 0 \pmod{r-2}.$$

Then

$$o(G_n) \mid \operatorname{lcm}(\{\mathscr{P}(\{r-2, n-2; 1^{r-3}0\}) : 4 \leq r \leq n\}).$$

Proof. This follows immediately from Theorem 5.1 and Lemma 4.3.

The next result is the key to understanding the periodicity of these seeded arrays.

Theorem 5.3. (a) *If* $\{a, a+1; \mathbf{s}\}$ *is a seeded array, then row* $a+1$ *consists of repeated occurrences of the* $(a+1)$*-block* $0\mathbf{s}$.

(b) *If* $\{a, a+b; \mathbf{s}\}$ *is a seeded array, then for* $1 \leq k \leq b$, *the* $(a+k)$*th row of section* $a+k$ *consists of repeated occurrences of the* $(a+k)$*-block* $0^k\mathbf{s}$.

(c) *If* $s_a = 0$, *then* $\mathscr{P}(\{a, a+1; \mathbf{s}\}) \mid \operatorname{lcm}(\mathscr{P}(\mathbf{s}), \mathscr{P}(0\mathbf{s}))$.

Proof. (a) Let $\mathbf{s} = s_1 s_2 \cdots s_a$ be the seed for the seed row of an $\{a, a+1\}$ seeded array. Since there is only one section, let us identify the cells by row and column only, i.e., put $(i, j) = (i, j; a+1)$.

Suppose $s_m = 1$. Since the seed row is periodic, we have that $s_{m+ka} = 1$ for $k \geq 0$. The following table lists the cell positions containing 1's which result from $s_{m+ka} = 1$ in the seed row:

Note that the rules apply independently to different occurrences of a 1 among the first m elements of the seed row. Hence, if $1 \leq m \leq a$ and $s_m = 1$, then

Row	Apply	Place 1 in these columns
1	Rule 2	$m+1,\ a+m+1,\ 2a+m+1,\ 3a+m+1,\ldots$
$a+1$	Rule 2	$m+1,\ a+m+1,\ 2a+m+1,\ 3a+m+1,\ldots$
$i,\ 2\le i\le a$	Rule 3	$m+i,\ a+m+1,\ 2a+m+i,\ 3a+m+1,\ldots$
$a+1$	Rule 3	$a+m+1,\ 2a+m+1,\ 3a+m+1,\ldots$
$a+1$	Rule 5	$m+1$ (1's from Rules 2 and 3 add mod 2). Then:
1	Rule 4	$m+2,\ a+1+m+2,\ 2(a+1)+m+2,\ldots$
$i,\ 2\le i\le a$	Rule 3	$m+1+i,\ a+1+m+1+i,\ 2(a+1)+m+1+i,$
$a+1$	Rule 3	$\ldots a+1+m+1,\ 2(a+1)+m+1,\ldots.$

the array contains 1's in cells $(a+1,\ k(a+1)+m+1)$, for $k\ge 0$, and by Rule 6, all other cells in row $a+1$ contain zeros. That is,

$$(a+1,\ j)=\begin{cases}0, & \text{if } j\equiv 1 \pmod{a+1},\\ s_m, & \text{if } j=k(a+1)+m+1,\ k\ge 0,\ \text{and } 1\le m\le a,\end{cases}$$

and it follows that row $a+1$ consists of repeated occurrences of the $(a+1)$-block **0s**, as claimed.

(b) Part (a) takes care of the case $k=1$. Inductively, if row $a+k$ of section $a+k$ consists of repeated occurrences of $0^k\mathbf{s}$, then we may regard this row, together with section $a+k+1$, as the seeded array $\{a+k,\ a+k+1;\ 0^k\mathbf{s}\}$. But then, by part (a), the last row consists of repeated occurrences of $00^k\mathbf{s}$, which is just $0^{k+1}\mathbf{s}$, and the result follows by induction.

(c) We prove this if the periods of the seed row and row $a+1$ are a and $a+1$, respectively; for shorter periods, the argument is similar.

Now the net result of applying the rules is that for $1\le i\le a$,

(1) The third row of the table reveals that the ith row of the array has a 1 in each of the following columns: $m+i,\ a+m+i,\ldots,(a-1)a+m+i,\ a^2+m+i,\ (a+1)a+m+i,\ldots$; and

(2) The seventh row of the table reveals that the ith row of the array has a 1 in each of the following columns: $m+i+1,\ a+1+m+i+1,\ldots,\ (a-1)(a+1)+m+i-1,\ a(a+1)+m+i+1,\ldots$.

However, since $a^2+m+i=(a-1)(a+1)+m+i+1$, those two 1's add to 0 mod 2, and so column $a+m+i$ has a 0 in row i. Hence, for $1\le i\le a$, row i has no 1 between columns $(a-1)a+m+i$ and $(a+1)a+m+i$. So the only way for there to be a 1 in column $a(a+1)$ is either (i) if $(a-1)a+m+i=a(a+1)$ for $1\le i\le a$ and $1\le m\le a$ or (ii) if cell $(a+1,\ a(a+1))$ has a 1. If (i) is true, then $m=i=a$ and $s_a=1$; if (ii) is true, then $s_a=1$. By hypothesis, $s_a=0$, so column $a(a+1)$ consists entirely of zeros, including the seed row. As a result, column $a(a+1)+1$ is identical to column 1, and so $(i,\ j)=(i,\ j+a(a+1))$ for all i and j. We conclude that $\mathscr{P}(\{a,\ a+1;\ \mathbf{s}\})\,|\,a(a+1)$.

An analogous argument for the general case shows that $\mathscr{P}(\{a,\ a+1;\ \mathbf{s}\})$ is a factor of $\operatorname{lcm}(\mathscr{P}(s),\ \mathscr{P}(0\mathbf{s}))$. We are done.

Lemma 5.4. $(\mathscr{P}(1^{a-1}0),\ \mathscr{P}(01^{a-1}0))=1,\ \mathscr{P}(\{a,\ a+1;\ 1^{a-1}0\})\equiv 0 \pmod{a}$.

Proof. For, the a-block $1^{a-1}0$ clearly has period a and the period of the $(a+1)$-block $01^{a-1}0$ divides $a+1$; hence, these two periods are relatively

prime. Finally, since $s_a = 0$, it follows from Theorem 5.3(c) that

$$a | \mathscr{P}(\{a, a+1; 1^{a-1}0\}).$$

Lemma 5.5. *If* $s_a = 0$, *then*

$$\mathscr{P}(\{a, a+b; \mathbf{s}\}) | \operatorname{lcm}(\mathscr{P}(\{a, a+b-1; \mathbf{s}\}), \mathscr{P}(\{0^b, \mathbf{s}\})).$$

Proof. We proceed by induction on b. If $b = 1$, then the array $\{a, a+\mathbf{s}\}$ is just the seed row generated by $\mathbf{s}$, whose period is $\mathscr{P}(\mathbf{s})$; by Theorem 5.3(c), $\mathscr{P}(\{a, a+1; \mathbf{s}\})$ is a factor of $\operatorname{lcm}(\mathscr{P}(\{a, a; \mathbf{s}\}), \mathscr{P}(0\mathbf{s}))$.

Assume that the theorem is true for $b \geq 1$, and consider the array $\{a, a+b+1; \mathbf{s}\}$. By Theorem 5.3(b), row $a+b$ of section $a+b$ consists of periodic occurrences of $0^b\mathbf{s}$, and it is the seed row for the array $\{a+b, a+b+1; 0^b\mathbf{s}\}$. By Theorem 5.3(c), the period of $\{a+b, a+b+1; 0^b\mathbf{s}\}$ divides $\operatorname{lcm}(\mathscr{P}(0^b\mathbf{s}), \mathscr{P}(0^{b+1}; \mathbf{s}))$. But $\{a, a+b+1; \mathbf{s}\}$ repeats precisely when both $\{a, a+b; \mathbf{s}\}$ and $\{a+b, a+b+1; 0^b\mathbf{s}\}$ repeat. Since $\mathscr{P}(0^b\mathbf{s})$ is a factor of both of these, and since $\mathscr{P}(0^{b+1}\mathbf{s})$ is a factor of $\mathscr{P}(\{a+b, a+b+1; 0^b\mathbf{s}\})$, it follows that $\mathscr{P}(\{a, a+b+1; \mathbf{s}\})$ divides $\operatorname{lcm}(\mathscr{P}(\{a, a+b; \mathbf{s}\}), \mathscr{P}(\{0^{b+1}\mathbf{s}\}))$. We are done.

Lemma 5.6. *If* $s_a = 0$, *then* $\mathscr{P}(\{a, a+b; \mathbf{s}\}) | \operatorname{lcm}(a, a+1, \ldots, a+b)$.

Proof. By the proof of Lemma 5.5,

$$\mathscr{P}(\{a, a+b; \mathbf{s}\}) | \operatorname{lcm}(\{\mathscr{P}(0^k\mathbf{s}) : 0 \leq k \leq b\}).$$

The lemma follows when we note that for $0 \leq k \leq b$, $\mathscr{P}(0^k\mathbf{s}) | a+k$.

Lemma 5.7. *If* $4 \leq r \leq n$, *then*

$$\mathscr{P}(\{r-2, n-2; 1^{r-3}0\}) | \operatorname{lcm}(r-2, \ldots, n-2).$$

Proof. This is an immediate consequence of Lemma 5.6.

Theorem 5.8. *Let* $n \geq 4$. *Then*:

(a) $o(G_n) | \operatorname{lcm}(1, 2, \ldots, n-2)$.

(b) $F_n^{\operatorname{lcm}(2,3,\ldots,n-2)} = T^{(n-2)\operatorname{lcm}(2,3,\ldots,n-2)}$.

Proof. (a) Let $4 \leq r \leq n$. Then $\mathscr{P}(1^{r-3}0) = r-2$, so that by the proof of Lemma 5.5, $r-2 | \mathscr{P}(\{r-2, n-2; a^{r-3}0\})$. By Theorem 5.2, it follows that

$$o(G_n) | \operatorname{lcm}(\{\mathscr{P}(\{r-2, n-2; 1^{r-3}0\}) : 4 \leq r \leq n\}).$$

Call this number M. By Theorem 5.1, $o(\langle 1, r; n\rangle) = \mathscr{P}(\{r-2, n-2; 1^{r-3}0\})$, and so $o(\langle 1, r; n\rangle) | M$ for $4 \leq 4 \leq n$. Hence, by Lemma 5.7,

$$M | \operatorname{lcm}(r-2, \ldots, n-2)$$

for $4 \leq r \leq n$. Thus, $o(G_n) | \operatorname{lcm}(2, 3, \ldots, n-2)$.

(b) Lemma 4.3 implies that $F_n^M = T^{(n-2)M}$; this proves (b), since

$$M | \operatorname{lcm}(2, 3, \ldots, n-2).$$

Theorem 5.8 does not rule out the possibility that $o(G_n)$ is a proper divisor of $\operatorname{lcm}(2, 3, \ldots, n-2)$; in the next section, we rule out that possibility by showing that $o(G_n)$ is divisible by $\operatorname{lcm}(2, 3, \ldots, n-2)$.

6. Periodic points and the order of G_n

In this section, we show that $o(G_n) = \operatorname{lcm}(2, 3, \ldots, n-2)$. The notation is consistent with that of Boyle and Krieger [BK].

A *periodic point* is an element $x = (x_i)$ of Σ_2 such that $x_i = x_{i+k}$ for some $k > 0$ and all integers i; the least such k is called the *period* of x. Let P_n^0 be the set of points of period n; the action of the shift σ partitions P_n^0 into orbits of length n. If f is an automorphism of Σ_2, then we may restrict the domain of f to the set P_n^0. Now if Q is an orbit in P_n^0, so is $f(Q)$, since f commutes with σ; since P_n^0 is a finite set, and since f is 1-1, it follows that f permutes the set $\mathcal{O}_n$ of orbits of P_n^0. Let us call this permutation $\pi_n(f)$.

Lemma 6.1. *If $\pi_n(f)$ has a cycle of length l, and f is an automorphism of finite order, then $l|o(f)$.*

Proof. It is known [BK, p. 127] that the restriction of f to P_n^0 is a homomorphism of the automorphism group $\mathrm{Aut}(\Sigma_2)$ of Σ_2 onto the symmetric group of $\mathcal{O}_n$. Hence $o(\pi_n(f))|o(f)$; thus, the length of any cycle of $\pi_n(f)$ also divides $o(f)$.

We now consider the restriction of G_n to P_k^0, for $3 \le k \le n-1$. If k is a positive integer, and B is a k-block, write $[B]_k$ to indicate the element of P_k^0 consisting of repetitions of the block B. We will omit the subscript when the block length is clear from the context. Let J_k be the orbit in $\mathcal{O}_k$ of the periodic point $[0^{k-1}1]_k$.

Lemma 6.2. *Let r, s, and t be positive integers. Then*

(a)
$$g_r([0^s1^t]_{s+t}) = [0^{s-1}1^{t+1}]_{s+t}, \quad \text{if } s = r-2,$$

(b)
$$g_r([0^s1^t]_{s+t}) = [0^{s+1}1^{t-1}]_{s+t}, \quad \text{if } s = r-3,$$

(c)
$$g_r([0^s1^t]_{s+t}) = [0^s1^t]_{s+t}, \quad \text{otherwise}.$$

Proof. From the definitions, we see that

$$\begin{aligned} g_r(x_1 \cdots x_r) &= T^{-(r-2)} \circ (x_{r-1} + x_1\overline{x}_2 \cdots \overline{x}_{r-2}x_r) \\ &= x_1 + x_{3-r}\overline{x}_{2-r} \cdots \overline{x}_0 x_2 \\ &= \overline{x}_1, \quad \text{if } x_{3-r} = x_2 = 1 \text{ and } x_{2-r} = \cdots = x_0 = 0 \\ &= x_1, \quad \text{otherwise}. \end{aligned}$$

Hence, if $x \in \Sigma_2$, then g_r complements x_j if and only if x_j is preceded by the block 10^{r-3} and followed by a 1; otherwise, g_r leaves x_j alone. Thus, the only way that the periodic point $[0^s1^t]_{s+t}$ can be altered by g_r is if it contains the block $10^{r-2}1$ or the block $10^{r-3}11$. This happens if and only if $s = r-2$ or $s = r-3$. If $s = r-2$, then

$$[0^s1^t] = \cdots 1^t0^{r+2}1^t0^{r+2}1^t \cdots,$$

so that

$$g_r([0^s1^t]) = \cdots 1^t0^{r+1}11^t0^{r+1}11^t \cdots = [0^{r+1}1^{t+1}] = [0^{s-1}1^{t+1}],$$

as claimed. Likewise, if $s = r-3$, then $g_r([0^s1^t]) = [0^{s+1}1^{t-1}]$. For all other values of r and s, g_r leaves $[0^s1^t]$ unchanged.

Lemma 6.3. *Suppose* $1 \le i \le m-2 \le n-3$. *Then*:
(a) $G_n([0^{m-i}1^i]_m) = [0^{m-i-1}1^{i+1}]_m$.
(b) $G_n([01^{m-1}]_m) = [0^{m-1}1]_m$.

Proof. (a) Let $1 \le i \le m-2 \le n-1$. Now

$$G_n = g_n \circ \cdots \circ g_{m-i+2} \circ \cdots \circ g_4 .$$

Hence, by Lemma 6.2(a),

$$g_{m-i+1} \circ \cdots \circ g_4([0^{m-i}1^i]_m) = [0^{m-i}0^i]_m ,$$
$$g_{m-i+2}([0^{m-i}0^i]_m) = [0^{m-i-1}0^{i+1}]_m , \text{ and}$$
$$g_n \circ \cdots \circ g_{m-i+3}([0^{m-i-1}0^{i+1}]_m) = [0^{m-i-1}0^{i+1}]_m .$$

Thus, $G_n([0^{m-i}1^i]_m) = [0^{m-i-1}1^{i+1}]_m$, as claimed.
(b) By Lemma 6.2(b) and (c).

$$g_4([01^{m-1}]_m) = [0^2 1^{m-2}]_m ,$$
$$g_5([0^2 1^{m-2}]_m) = [0^3 1^{m-3}]_m , \ldots ,$$
$$g_{m+1}([0^{m-2}1^2]_m) = [0^{m-1}1]_m) ,$$
$$g_r([0^{m-1}1]_m) = [0^{m-1}1]_m \quad \text{for } m+1 \le r \le n ;$$

hence, it follows that $G_n([01^{m-1}]_m) = [0^{m-1}1]_m$.

Lemma 6.4. *Let* $\pi_m(G_n)$ *be the permutation induced by the automorphism* G_n *on* $\mathscr{O}_m$. *If* $3 \le m \le n-1$, *then* $[0^{m-1}1]_m$ *is in a cycle of* $\pi_m(G_n)$ *of length* $m-1$.

Proof. Repeated applications of Lemma 6.3(a) reveal that

$$G_n([0^{m-1}1]_m) = [0^{m-2}1^2]_m , \; G_n^2([0^{m-1}1]_m) = [0^{m-3}1^3]_n , \ldots ,$$
$$G_n^{m-2}([0^{m-1}1]_m) = [01^{m-1}]_m ;$$

then by Lemma 6.3(b),

$$G_n^{m-1}([0^{m-1}1]_m) = [0^{m-1}1]_m .$$

Hence, $([0^{m-1}1]_m , [0^{m-2}1^2]_m , , \ldots , [01^{m-1}]_m)$ is a cycle of $\pi_m(G_n)$ of length $m-1$.

Corollary 6.5. $\operatorname{lcm}(2, 3, \ldots, n-2) | o(G_n)$.

Proof. Let $3 \le m \le n-1$. By Lemma 6.4, $\pi_m(G_n)$ contains a cycle of length $m-1$. Hence, by Lemma 6.1, $o(G_n)$ is divisible by $m-1$, and so by $\operatorname{lcm}(2, 3, \ldots, n-2)$.

Theorem 6.6. *Let* $n \ge 4$; *then* $o(G_n) = \operatorname{lcm}(2, 3, \ldots, n-2)$.

Proof. This follows from Corollary 6.5 and Theorem 5.8(a).

We note that we may generalize the results of §§3–6 in the following way. For $n \ge 4$ and $r \ge 0$, define the block map $F_{n,r}$ and the automorphism $G_{n,r}$ by

$$F_{n,r} = (n+r-1) + \sum_{j=1}^{n-3} j(\overline{j+1}) \cdots (\overline{j+r+1}) \Delta(j+r+2, n+r-1)(n+r) ,$$

$$G_{n,r} = \sigma^{-(n+r-2)} \circ F_{n,r} .$$

Using the techniques of the previous section, we can show that the order of $G_{n,r}$ is independent of r.

Theorem 6.7. *Let* $n \geq 4$ *and* $r \geq 0$. *Then*:
(a) $G_{n,r} = g_{n+r} \circ g_{n-1+r} \circ \cdots \circ g_{4+r}$.
(b) *For all* r *and fixed* n, $o(G_{n,r}) = \operatorname{lcm}(2, 3, \ldots, n-2)$.

The proof is somewhat messier than that of Theorem 6.6, but it follows the same lines, and so is limited.

7. Return numbers and the order of $\overline{G}_n$

In this section, we show that, whereas each G_n has finite order, composing G_n with the complementation map produces an automorphism of infinite order. We turn once again to the work of Boyle and Krieger [BK].

Let $f \in \operatorname{Aut}(\Sigma_2)$, and let $\pi_n(f)$ be the permutation induced by f on $\mathscr{O}_n$, the orbits of periodic points of least period n. For each orbit $Q \in \mathscr{O}_n$, choose a fixed but arbitrary periodic point $x_Q \in Q$. If Q is in a cycle $C(Q)$ of $\pi_n(f)$ of length d, then $f^d(x_Q) \in Q$. Since

$$Q = (x_Q, \sigma(x_Q), \ldots, \sigma^{d-1}(x_Q)),$$

it follows that $f^d(x_Q) = \sigma^r(x_Q)$, for some unique r such that $0 \leq r < d$. This integer r is called the *return number* of f for the cycle $C(Q)$.

Lemma 7.1. *Let* $f \in \operatorname{Aut}(\Sigma_2)$ *be of finite order* k. *If* r *is a return number of* f *for a cycle of orbits of points of period* n, *then* $kr \equiv 0 \pmod{n}$.

Proof. This is essentially Boyle and Krieger's Proposition 1.4 [BK, p. 130].

Theorem 7.2. *Let* $c(x) = \overline{x}$ *be the complementation automorphism. Then for all* $n \geq 4$, $c \circ G_n = \overline{G}_n$ *is an automorphism of infinite order.*

Proof. Let N be any positive integer such that $2N + 1 \geq n$ and such that $(2N + 1, n) = 1$. Let x be the periodic point $[(10)^N 1]_{2N+1}$. Now $G_n = g_n \circ \cdots \circ g_4$; it is easy to check that g_k leaves x fixed and unshifted if $k \geq 5$, but that $g_4(x) = [(10)^N 0]_{2N+1}$. Hence, $G_n(x) = [(10)^N 0]_{2N+1}$, and so

$$\overline{G}_n(x) = [(01)^N 1]_{2N+1} = [0(10)^{N-1}11]_{2N+1} = \sigma([(10)^N 1]_{2N+1}) = \sigma(x).$$

Hence, $\overline{G}_n$ has return number $r = 1$ on an orbit of points of period $2N + 1$. If $o(\overline{G}_n) = k$, then by Lemma 7.1, $k = kr \equiv 0 \pmod{2N + 1}$. But since N is arbitrary (although $2N + 1$ is relatively prime to n), it follows that $k = 0$, contrary to the assumption that k is the order of a nonidentity automorphism of Σ_2. Hence, $\overline{G}_n$ has infinite order for all $n \geq 4$.

Remark. A key step in the preceding proof is that if $k \geq 5$, then the maps g_k fix all periodic points $[(10)^N 1]_{2N+1}$ for N sufficiently large. Thus, with only very slight changes in the proof, we may generalize Theorem 7.2 as follows:

Theorem 7.3. *Let* $c(x) = \overline{x}$ *be the complementation automorphism. Let* F *be any automorphism of* Σ_2 *that fixes the periodic points* $[(10)^N 1]_{2N+1}$ *for all sufficiently large* N. *Then* $c \circ F \circ g_4 = \overline{F} \circ g_4$ *is an automorphism of* Σ_2 *of infinite order.*

8. The subgroup $\mathscr{K}$ and its properties

In this section, we define the subgroup $\mathscr{K}$ of $\operatorname{Aut}(\Sigma_2)$ and summarize its properties. First, we show that g_n and g_k commute, except when $n = k \pm 1$.

Lemma 8.1. *Let* $n, k \geq 4$. *Then*:
(a) $f_n \circ f_k = f_k \circ f_n$ *if and only if* $|n-k| \neq \pm 1$.
(b) $f_n^2 = T^{2n-4}$.

Proof. (a) Since $f_n = (n-1) + 1\overline{2}\cdots\overline{(n-2)}n$, a straightforward computation shows that

$$\begin{aligned} f_n \circ f_k = {} & (n+k-3) + (n-1)\overline{n}\cdots\overline{(n+k-4)}(n+k-2) \\ & + (k-1)\overline{k}\cdots\overline{(k+n-4)}(k+n-2) \\ & + ((k-1)\overline{k}\cdots\overline{(k+n-5)}(k+n-3) \\ & \quad \times (n-2)\overline{(n-1)}\cdots\overline{(n+k-5)}(n+k-3)(n+k-2)). \end{aligned}$$

Note that the last product is equal to zero if and only if $n \neq k+1$. Since the rest of the expression is symmetric in n and k, this implies that f_n commutes with f_k whenever $|n-k| \neq 1$. Finally, by the previous statement, it is clear that $f_n \circ f_{n-1} \neq f_{n-1} \circ f_n$.

(b) Note that if $n = k$, then everything cancels in the previous expression except for the term $(n+n-3) = (2n-3) = T^{2n-4}$. Hence $f^n = T^{2n-4}$.

Corollary 8.2. *Let* $n, k \geq 4$. *Then*:
(a) $g_n \circ g_k = g_k \circ g_n$ *if and only if* $|n-k| \neq \pm 1$.
(b) g_n *is an involution.*

Proof. (a) This follows from Lemma 8.1(a), the definition of g_n and the fact that the shift commutes with all block maps.

(b) Since $g_n = \sigma^{-(n-2)} \circ (f_n)_\infty$, Lemma 8.1(b) implies that

$$g_n^2 = \sigma^{-(2n-4)} \circ (T^{2n-4})_\infty = \sigma^{-(2n-4)+2n-4} = \sigma^0;$$

hence, g_n^2 is the identity map. Since it is clear that g_n is not the identity map, it follows that g_n is an involution.

We may now summarize our results as follows:

Theorem 8.3. *Put*

$$F_1 = 1, \quad F_2 = x_1, \quad \text{and} \quad F_n = x_{n-1} + x_n(\overline{F}_{n-1} + \overline{x}_1 \cdots \overline{x}_{n-2}) \quad \text{for } n \geq 3,$$

$$G_n = \sigma^{-(n-2)} \circ (F_n)_\infty \quad \text{for } n \geq 4,$$

$$f_n = x_{n-1} + x_1 \left(\prod_{k=2}^{n-2} \overline{x}_k \right) x_n,$$

$$g_n = \sigma^{-(n-2)} \circ (f_n)_\infty,$$

$$\mathscr{H} = \langle \{\sigma\} \cup \{c\} \cup \{g_n : n \geq 4\} \rangle.$$

If $n \geq 4$, *then*:
(a) $G_n = g_n \circ g_{n-1} \circ \cdots \circ g_4$.
(b) $(F_n^{\operatorname{lcm}(2,3,\ldots,n-2)})_\infty = \sigma^{(n-2)\operatorname{lcm}(2,3,\ldots,n-2)}$.
(c) $o(G_n) = \operatorname{lcm}(2, 3, \ldots, n-2)$.
(d) $\overline{G}_n$ *is an automorphism of infinite order.*
(e) *For* $r \geq 0$, *put* $G_{n,r} = g_{n+r} \circ g_{n-1+r} \circ \cdots \circ g_{4+r}$; *then*

$$o(G_{n,r}) = \operatorname{lcm}(2, 3, \ldots, n-2).$$

(f) *For* $k \geq 4$, g_n *commutes with* g_k *if and only if* $|n-k| \neq \pm 1$.

(g) g_n *is an involutory automorphism of* Σ_2.
(h) $\mathscr{H}$ *contains automorphisms of all orders.*

Proof. We have already proved all of these results except for (h). So let M be a positive integer. Since $o(G_{M+2}) = \operatorname{lcm}(2, 3, \ldots, M)$, it follows that

$$o(G_{M+2})^{\operatorname{lcm}(2,3,\ldots,M)/M} = M.$$

Hence, $\mathscr{H}$ contains automorphisms of all finite orders. Since σ and $\overline{G}_n$ have infinite order, it follows that $\mathscr{H}$ has automorphisms of all orders.

9. Problems and questions

The work in this paper suggests problems and raises questions in a number of areas. First of all, those interested in combinatorial arrays might pursue further investigations of the structure of seeded arrays. In particular:

Question 9.1. What happens to the periodicity of seeded arrays if we
(a) change the rules for filling the array?
(b) change the modulus (i.e., fill the array mod n instead of mod 2)?

There are other infinite families of block maps, like the maps F_n, whose powers can be described in terms of seeded arrays.

Problem 9.2. Characterize those families of block maps whose powers correspond to the periodic seeded arrays of §5.

Question 9.3. Given a set of rules for filling seeded arrays, is there a corresponding family of block maps whose powers can be described in terms of the given set of rules?

Next, the algebraic and geometric structure of $\mathscr{H}$ and of its subgroups is an area worthy of further study. If no two of $\{n_1, n_2, \ldots, n_k\}$ are consecutive positive integers, then $\langle g_{n_1}, g_{n_2}, \ldots, g_{n_k}\rangle$ is isomorphic to the direct sum of k copies of $\mathbb{Z}_2$. It is easy to show that if $n \geq 4$, then $\langle g_n, g_{n+1}\rangle$ is isomorphic to the dihedral group D_6 of symmetries of the regular hexagon. Other than that, not much is known; there is, however, enough evidence to suggest the following conjecture:

Conjecture 9.4. If $k \geq 0$, and $n_1, \ldots, n_k$ are distinct integers ≥ 4, then the number of nonisomorphic groups of the form $\langle g_{n_1}, \ldots, g_{n_k}\rangle$ is equal to the number $\pi(k)$ of partitions of the integer k.

Problem 9.5. Characterize the finite subgroups of $\mathscr{H}$.

The marker constructions of Hedlund [H] and of Boyle, Lind, and Rudolph [BLR] yield automorphisms of Σ_2 (as well as automorphisms of arbitrary shifts of finite type) which have finite order. To each such automorphism, there corresponds a block map. But deciding whether the endomorphism corresponding to a given block map is an automorphism, or even merely onto, seems to be somewhat more involved. This problem may be tractable for involutions, however: to this end, if $a = 0$ or 1, define $a^1 = a$ and $a^0 = \overline{a}$.

Problem 9.6. Let $\mathscr{B}_{n,k} = b_1 \cdots b_{k-1} b_{k+1} \cdots b_n$, where $b_i = 0$ or 1. Given necessary and sufficient conditions on the block $\mathscr{B}_{n,k}$ for the block map

$$f(x_1 \cdots x_n) = x_k + \prod_{i \neq k} x_i^{b_i}$$

to induce an automorphism of Σ_2 that is an involution modulo the shift.

We note that certain sufficient conditions are known (see [BLR, pp. 74–75]), but that these may not be necessary.

Finally, we begin this study by investigating the following question, which is still unanswered:

Question 9.7. Is $\mathrm{Aut}(\Sigma_2)$ generated by the shift and involutions?

References

[BK] M. Boyle and W. Krieger, *Periodic points and automorphisms of the shift*, Trans. Amer. Math. Soc. **302** (1987), 125–149.

[BLR] M. Boyle, D. Lind, and D. Rudolph, *The automorphism group of a shift of finite type*, Trans. Amer. Math. Soc. **306** (1988), 71–114.

[Br] E. Brown, *Commuting block maps in the shift dynamical system*, submitted.

[CHR] E. M. Coven, G. A. Hedlund, and F. Rhodes, *The commuting block maps problem*, Trans. Amer. Math. Soc. **249** (1979), 113–138.

[H] G. A. Hedlund, *Endomorphisms and automorphisms of the shift dynamical system*, Math. Systems Theory **3** (1969), 320–375.

[N] L. P. Neuwirth, private communication.

[R1] F. Rhodes, *The principal part of a block map*, J. Combin. Theory Ser. A **33** (1982), 48–64.

[R2] ——, *The sums of powers theorem for commuting block maps*, Trans. Amer. Math. Soc. **271** (1982), 225–236.

[R3] ——, *Left cancellation of block maps*, Bull. London Math. Soc. **16** (1984), 19–24.

[R4] ——, *The role of the principal part in factorizing block maps*, Math. Proc. Cambridge Philos. Soc. **96** (1984), 223–235.

[R5] ——, *The enumeration of certain sets of block maps*, J. Combin. Theory Ser. A **45** (1987), 263–276.

[Ry] J. P. Ryan, *The shift and commutativity*, Math. Systems Theory **6** (1972), 82–85.

Department of Mathematics, Virginia Polytechnic Institute and State University, Blacksburg, Virginia 24061-0123

E-mail address: brown@math.vt.edu