Complex Systems **3** (1989) 599–614

Period Multiplying Operators on Integer Sequences Modulo A Prime

Burton Voorhees
Athabasca University, Box 10,000,
Athabasca, Alberta TOG 2RO, Canada

Abstract. We study properties of operators defined on the space $E^+(p)$ of right half-infinite sequences with entries chosen from Z_p where p is prime. The operators in question allow solution of the problem of finding predecessor states for certain cellular automata evolutions and they can be thought of as discrete integration with respect to sequence index.

These operators are self-accumulating, not solipsistic, and have no dense orbits. In addition, they exhibit a period-multiplying property. Many of these results are derived from properties of Pascal's triangle modulo p which are presented in an appendix.

1. Introduction

Let $E^+(p)$ be the space of right half-infinite sequences with entries chosen from $\mathbf{Z}_p$, where p is prime. A cellular automation defined on $E^+(p)$ can be represented as a mapping $Q : E^+(p) \rightarrow E^+(p)$ where Q is an operator determined by the automation rule [1]. The automation is denoted $(Q, E^+(p))$. The predecessor problem for such a cellular automaton is to determine for any given $\beta \in E^+(p)$ the set of solutions to the equation $Q(\mu) = \beta$. Voorhees [2] has solved this problem for the class of linear operators defined by $D_{(y,z)} = yI + z\sigma$ and $D^-_{(x,y)} = yI + x\sigma^{-1}$ where σ and σ^{-1} are respectively the left and right shifts on $E^+(p)$ and the coefficients x, y, and z are in $\mathbf{Z}_p$. This solution involves an operator $B_{(b,r)} : E^+(p) \rightarrow E^+(p)$ defined, for b, r in $\mathbf{Z}_p$, μ in $E^+(p)$, by

$$[B_{(b,r)}(\mu)]_i = \sum_{j=1}^{i} [b(p-r)]^{i-j} \mu_j \tag{1.1}$$

where the notation β_i denotes the ith entry in the sequence β. Solution of the equations $D_{(r,s)}(\mu) = \beta$ and $D^-_{(r,s)}(\mu) = \beta$ are given by theorem 1.

Theorem 1. *1. The general solution of* $D_{(r,s)}(\mu) = \beta$ *is*

$$\mu = \mu_1 \beta_{(b,r)}(\alpha_1) + bB_{(b,r)}\sigma^{-1}(\beta). \tag{1.2}$$

where α_1 *has first term equal to one and all other terms zero,* $bs \equiv 1 \bmod (p)$*, and* $0 \leq \mu_1 < p$ *is an "initial" or "boundary" condition.*

2. Let $0 < b, c, t, r, s < p$ *and let these numbers be chosen so that* $cr \equiv 1$ *and* $s + b(p-t)r \equiv 0 \bmod (p)$*. Then* $cB_{(b,t)}$ *is the unique inverse of* $D^{-}_{(r,s)}$*.*

It was also found that the family of operators $B_{(b,r)}$ exhibited an interesting period-multiplying property, as will be discussed in section 2 of this paper, and in a well-defined sense can be thought of as integration with respect to sequence index.

The main purpose of this paper is to demonstrate that these "discrete integrals" are self-accumulating but not solipsistic and have no dense orbits in $E^+(p)$. In fact, it will turn out that they define a foliation of $E^+(p)$ into infinite "strings" of states. Many of the proofs presented will depend on number theoretic properties of Pascal's triangle modulo p. Derivation of these properties is presented in the appendix.

2. Period multiplication

Let $\mu \in E^+(p)$ be periodic with period n. Then, under certain circumstances, $B_{(b,r)}(\mu)$ will have period kn where the multiplication factor k can be determined.

Theorem 2. *Let* μ *have period* n *in* $E^+(p)$*.*

1. *If* $[B_{(b,r)}(\mu)]_n \equiv 0 \bmod (p)$ *then* $B_{(b,r)}(\mu)$ *also has period* n*.*
2. *If* $[B_{(b,r)}(\mu)]_n \not\equiv 0 \bmod (p)$ *there exists a smallest integer* $k \leq p$ *such that* $[B_{(b,r)}(\mu)]_{kn} \equiv 0 \bmod (p)$*, and* $B_{(b,r)}(\mu)$ *has period* kn*.*

Proof. By (1.1), $[B_{(b,r)}(\mu)]_{n+1} = b(p-r)[B_{(b,r)}(\mu)]_n + \mu_{n+1}$. If μ has period n and $[B_{(b,r)}(\mu)]_n \equiv 0 \bmod (p)$, then $[B_{(b,r)}(\mu)]_{n+1} = \mu_{n+1} = \mu_1 = [B_{(b,r)}(\mu)]_1$ and part (1) follows from the iterative form of (1.1).

Suppose that $[B_{(b,r)}(\mu)]_n \not\equiv 0 \bmod (p)$. Setting $b(p-r) = x$ and making use of the periodicity of μ, (1.1) yields

$$[B_{(b,r)}(\mu)]_{kn} = \tag{2.1}$$
$$(1 + x^n + x^{2n} + \ldots + x^{(k-1)n})(x^{n-1}\mu_1 + x^{n-1}\mu_2 + \ldots + \mu_n)$$

But x^n is between 1 and $p-1$. Hence, by standard theorems of number theory (e.g., [3]) there is a smallest positive integer k such that $(x^n)^k \equiv 1 \bmod (p)$.

In this case x^n is said to have order k modulo $p (\mathrm{ord}_p(x^n) = k)$. Choose the k in (2.1) to be the order modulo p of x^n. Then

$$\begin{aligned} x^n + x^{2n} + \ \ldots \ + x^{(k-1)n} + x^{kn} &= 1 + x^n + x^{2n} + \ldots + x^{(k-1)n} \\ &= x^n(1 + x^n + \ldots + x^{(k-1)n}). \end{aligned}$$

Hence $(x^n - 1)(1 + x^n + \ldots + x^{(k-1)n}) \equiv 0 \bmod (p)$. If $x^n \not\equiv 1 \bmod (p)$ the term $1 + x^n + \ldots + x^{(k-1)n} = 0$ and by (2.1) $[B_{(b,r)}(\mu)]_{kn} \equiv 0 \bmod (p)$. If $x^n \equiv 1 \bmod (p)$ then $1 + X^n + \ldots + x^{(k-1)n} = k$ and we choose $k = p$ to obtain $[B_{(b,r)}(\mu)]_{pn} \equiv 0 \bmod (p)$.

Now the same argument used to prove part (1) yields the result that $B_{(b,r)}(\mu)$ has period kn.

The next theorem indicates that iteration of $B_{(b,r)}$ will eventually multiply the period of every periodic sequence in $E^+(p)$, even if it does not do so initially:

Theorem 3. *Let μ have period n, $[B_{(b,r)}(\mu)]_n \equiv 0 \bmod (p)$, and μ_m be the first nonzero term of the sequence μ. Then there exists an $s \leq n - m$ such that $[B^s_{(b,r)}(\mu)]_n \not\equiv 0 \bmod (p)$.*

Proof. Taking $x = b(p - r)$ and applying (2.1) with $[B_{(b,r)}(\mu)]_n \equiv 0 \bmod (p)$

$$[B^2_{(b,r)}(\mu)]_n = x[B^2_{(b,r)}(\mu)]_{n-1} + [B_{(b,r)}(\mu)]_n = x[B^2_{(b,r)}(\mu)]_{n-1}$$

If $[B^2_{(b,r)}(\mu)]_n \not\equiv 0 \bmod (p)$, we are done with $s = 2$. Therefore, suppose that $[B^2_{(b,r)}(\mu)]_n \equiv 0 \bmod (p)$. Since $x \not\equiv 0$, this requires that $[B^2_{(b,r)}(\mu)]_{n-1} \equiv 0 \bmod (p)$. Now, from (2.1),

$$\begin{aligned} [B^3_{(b,r)}(\mu)]_n &= x[B^3_{(b,r)}(\mu)]_{n-1} + [B^2_{(b,r)}(\mu)]_n = x[B^3_{(b,r)}(\mu)]_{n-1} \\ &= x[x[B^3_{(b,r)}(\mu)]_{n-2} + [B^2_{(b,r)}(\mu)_{n-1}] \\ &= x^2[B^3_{(b,r)}(\mu)]_{n-2} \end{aligned}$$

and again if $[B^3_{(b,r)}(\mu)]_n \equiv 0 \bmod (p)$. We are done with $s = 3$. Therefore, take $[B^3_{(b,r)}(\mu)]_m \equiv 0 \bmod (p)$. This, however, requires

$[B^3_{(b,r)}(\mu)]_{n-2} \equiv 0 \bmod (p)$. Clearly this process can be continued and, if we are allowed to require that $[B^s_{(b,r)}(\mu)]_n \equiv 0 \bmod (p)$ for all s, indicates that for some value of s all of the first n terms of $[B^2_{(b,r)}(\mu)]_n$ must become 0. On the other hand, let μ_m be the first nonzero term of the sequence μ. By equation (2.1) $[B^s_{(b,r)}(\mu)]_m = \mu_m$ for all s, and hence is never zero. Therefore, to avoid contradiction, there must be an $s \leq n - m$ such that $[B^s_{(b,r)}(\mu)]_n \equiv 0 \bmod (p)$.

3. Properties of $B_{(b,r)}$

A metric can be defined on the space $E^+(p)$ as follows. Let $\emptyset : E^+(p) \to [0,1]$ be defined by

$$\emptyset(\mu) = \sum_{j=1}^{\infty} \mu_j / p^j \tag{3.1}$$

Lemma 1. *The function $\emptyset$ defined by (3.1) is a norm on $E^+(p)$.*

Proof. Clearly $\emptyset(\mu) \geq 0$ and equals zero if and only if $\mu = \mathbf{0}$ where $\mathbf{0}$ is the sequence consisting entirely of zeros. Thus, it is only necessary to demonstrate that $\emptyset(\mu + \beta) \leq \emptyset(\mu) + \emptyset(\beta)$. But addition in $E^+(p)$ is always term by term modulo p. Therefore

$$\emptyset(\mu) + \emptyset(\beta) = \emptyset(\mu + \beta) + \sum_{j=1}^{\infty} \delta(\mu_j, \beta_j)/p^j \tag{3.2}$$

where

$$\delta(\mu_j, \beta_j) = \begin{cases} 0 & \mu_j + \beta_j < p \\ p & \mu_j + \beta_j \geq p \end{cases}$$

and the final term of (3.2) is nonnegative.

A metric on $E^+(p)$ is now defined by the formula

$$g(\mu, \beta) = \emptyset(|\mu - \beta|) \tag{3.3}$$

with $|\mu - \beta|_i = |\mu_i - \beta_i|$. The remainder of this section is concerned with deduction of properties of the operators $B_{(b,r)}$ with respect to the topology induced on $E^+(p)$ by the metric g. The major tool in this will be an expression for $B^k_{(b,r)}$ in terms of entries in Pascal's triangle modulo p:

Theorem 4. *Let μ be in $E^+(p)$ and write $x = b(p-r)$. Then*

$$[B^k_{(b,r)}(\mu)]_i = \sum_{j=1}^{i} \Pi_{i-j+1}^{(k+i-j)} x^{i-j} \mu_j \tag{3.4}$$

where $\Pi_i^{(k)}$ is the ith entry in the kth row of Pascal's triangle modulo p.

Remark. The coefficients in (3.4) are the first i terms in the kth diagonal of the mod(p) Pascal triangle.

Proof. Since $\Pi_{i-j+1}^{(1+i-j)} = 1$ for all $i, j (i \geq j)$ equation (1.1) indicates that the claim is true for $k = 1$. The remainder of the proof will proceed by induction. Assume the theorem is true for k. Then by (1.1) and the induction hypothesis,

$$\begin{aligned} [B^{k+1}_{(b,r)}(\mu)]_i &= [B_{(b,r)}(B^k_{(b,r)}(\mu))]_i = \sum_{j=1}^{i} x^{i-j} [B^k_{(b,r)}(\mu)]_j \\ &= \sum_{j=1}^{i} \sum_{d=1}^{j} \Pi_{j-d+1}^{(k+j-d)} x^{i-d} \mu_d \end{aligned} \tag{3.5}$$

Rearranging terms in (3.5) by grouping coefficients of μ_d yields

$$[B_{(b,r)}^{k+1}(\mu)]_i = \sum_{j=1}^{i} \left[\sum_{s=0}^{i-j} \Pi_{s+1}^{(k+s)} \right] x^{i-j} \mu_j \tag{3.6}$$

but by lemma 8 of the

$$\sum_{s=0}^{i-j} \Pi_{s+1}^{(k+s)} = \Pi_{i-j+1}^{(k+1+i-j)}$$

hence (3.6) is identical to (3.4) with k replaced by $k+1$ and the theorem is proved.

The first question asked of the operators $B_{(b,r)}$ is whether or not they have cycles. The next theorem answers this in the negative.

Theorem 5. *$B_{(b,r)} : E^+(p) \to E^+(p)$ has no cycles other than the trivial cycle* $\mathbf{0}$.

Proof. Suppose that there is a $k > 0$ and a nonzero μ in $E^+(p)$ such that $B_{(b,r)}^k(\mu) = \mu$. Then, for all i

$$(p-1)\mu_i + \sum_{j=1}^{i} \Pi_{i-j+1}^{(k+i-j)} x^{i-j} \mu_j \equiv 0 \bmod (p) \tag{3.7}$$

Let μ_s be the first nonzero term of the sequence μ. Expansion of (3.7) dropping terms which sum to zero modulo p, yields the hierarchy of equations

$$\begin{aligned}
&\Pi_2^{(k+1)} x^{i-s} \mu_s = 0 \\
&\Pi_2^{(k+1)} x^{i-s-1} \mu_{s+1} + \Pi_3^{i-s} \mu_s = 0 \\
&\Pi_2^{(k+1)} x^{i-s-2} \mu_{s+2} + \Pi_3^{(k+2)} x^{i-s-1} \mu_{s+1} + \Pi_4^{(k+3)} x^{i-s} \mu_s = 0 \\
&\text{etc.}
\end{aligned} \tag{3.8}$$

Since μ_s, $x \neq 0$ the first equation of (3.8) requires that $\Pi_2^{(k+1)} = 0$. Substitution of this into the second equation yields the requirement that $\Pi_3^{(k+2)} = 0$. Continuation of this process indicates that $\Pi_{j+1}^{(k+j)} = 0$ for all $j > 0$. However, these coefficients are drawn from the kth diagonal of the mod (p) Pascal triangle and no diagonal of this triangle consists entirely of zeros after the leading one. Hence, (3.7) can never be satisfied for all i and the theorem is true.

Proof of theorem 5 is based on the nonexistence in the mod(p) Pascal triangle of a diagonal consisting only of zeros following the leading one. This triangle does, however, contain diagonals which are mostly zeros. Thus, although $B_{(b,r)}$ has no cycles and is therefore not periodic, it can be shown to be "almost periodic" in the sense of being self-accumulating, i.e., every iterate of $B_{(b,r)}$ is an accumulation point for further iterates.

Theorem 6. *For all $k, s \geq 0$ and for all μ in $E^+(p)$*

$$g(B^k_{(b,r)}(\mu), B^{k+p^s}_{(b,r)}(\mu)) \leq [\sum_{j=1}^{p^5} p^j]^{-1} \tag{3.9}$$

Proof. It is sufficient to prove the theorem for $k = 0$. In this case consider the sequence $\xi = \mu - B^{p^s}_{(b,r)}(\mu)$ which can be shown to have components

$$\xi_i = \sum_{j=1}^{i-1} \Pi^{(p^s+1-j)}_{i-j+1} x^{i-j} \mu_j$$

The coefficients in the sum are the first i entries of the p^s diagonal of the mod(p) Pascal triangle, with the first entry excluded (since the sum is only to $i-1$). Thus, by lemma 6 of the appendix these coefficients are all zero for $i \leq p^s$. Indeed,

$$\Pi^{(p^s+i-j)}_{i-j+1} = \begin{cases} 1 & i-j = 0, p^s, p^{2s}, \ldots \\ 0 & \text{otherwise} \end{cases}$$

so the values of i giving nonzero contributions to ξ_i are $i = mp^s + 1, m \geq 1$. The maximum possible value of ξ_i is $p-1$. Hence

$$\begin{aligned} g(\mu, B^p_{(b,r)}(\mu)) &= \sum_{i=1}^{\infty} \xi_i / p^i \leq \sum_{i=1}^{\infty} (p-1)/p^{ip^s+1} \\ &= [(p-1)/p] \sum_{i=1}^{\infty} p^{-is} \end{aligned}$$

The final sum on the right is just $1/(p^s-1)$, which can be written as $[(p-1)(p^{s-1}+P^{s-2}+\ldots+1)]^{-1}$. Multiplication by $(p-1)/p$ now yields the desired result.

The content of this theorem can be summarized by saying that with respect to the topology induced on $E^+(p)$ by the metric g, the operators $B_{(b,r)}$ are self-accumulating. That is, under iteration of $B_{(b,r)}$ the sequence $[B^k_{(b,r)}(\mu)]$ eventually returns to arbitrarily small neighborhoods of its previous iterates. The next question is whether or not these operators are solipsistic—that is, does $[B^k_{(b,r)}(\mu) | 0 \leq k < \infty]$ exhaust all of the accumulation points of $B_{(b,r)}$? The answer to this question is not quite. Let μ_q be the first nonzero term of a sequence μ and consider

$$|\mu - B^{p^s-1}(\beta)|_i = |(\mu_i - \beta_i) - \sum_{j=1}^{i-1} \Pi^{(p^s+i-j-1)}_{i-j+1} x^{i-j} \beta_j| \tag{3.10}$$

From lemma 7 of the appendix, the $(p-1)-st$ diagonal of the mod (p) Pascal triangle is periodic, with first term 1, second term $p-1$, followed by p^s-2 zeros. Setting the right side of (3.10) to zero for all $i \leq p^s$ yields

$$\sum_{j=1}^{m} \Pi^{(p^s+i-j-1)}_{i-j+1} x^{i-j} \beta_j = 0 \quad m < q$$

$$\mu_q = \beta_q \tag{3.11}$$

$$\mu_{q+m} = \beta_{q+m} + (p-1)x\beta_{q+m-1} \quad q+m \leq p^s.$$

The first of these equations requires that $\beta_i = 0$ for $i \leq q$. Define

$$[D_{(r,s)}(\mu)]_i = \begin{cases} \mu_1 & i = 1 \\ \mu_1 + s\mu_{i-1} & \text{otherwise} \end{cases} \tag{3.12}$$

Noting that $(p-1)x = b(p-1)(p-r) = br \bmod (p)$, the right-hand side of the first p^s terms in equations (3.11) are just the components of $D^-_{(1,br)}(\beta)$. Additional terms will enter for $i > p^s$, but this does not alter the desired result.

Theorem 7. *For every μ in $E^+(p)$ $g(D^-_{(1,br)}(\mu), B^{p^s-1}_{(b,r)}(\mu)) \leq p^{-(p^s-1)}$. Thus, $D^-_{(1,br)}(\mu)$ is an accumulation point of $B_{(b,r)}$ iterated on μ.*

By direct computation using (1.1) and (3.12)

$$D^-_{(1,br)}B_{(b,r)} = B_{(b,r)}D^-_{(1,br)} = 1.$$

Hence, $D^-_{(1,br)}$ and $B_{(b,r)}$ are inverses of each other. This yields a proof that the $B_{(b,r)}$ are not solipsistic:

Theorem 8. *Let $D^-_{(1,br)}$ and $B_{(b,r)}$ be as above, with $s < 0$ and a sequence μ given. There does not exist an integer $k > 0$ such that $B^k_{(b,r)}(\mu) = [D^-_{(1,br)}]^s(\mu)$.*

Proof. Suppose that such a k existed. Then $B^{k+s}_{(b,r)}(\mu) = \mu$. By theorem 5, however, $B_{(b,r)}$ has no nontrivial cycles.

By theorem 7 it is possible to write

$$D^-_{(1,br)}(\mu) = B^{p^s-1}_{(b,r)}(\mu) + \beta$$

with $\beta_i = 0$ for $i \leq p^s$. Thus, by (3.12) $[D^-_{(1,br)}(\mu)]_i = 0$ for $i \leq p^s$. Since $D^-_{(1,br)}$ is the inverse of $B_{(b,r)}$ there is a generalization of theorem 7:

Theorem 9. *For all $k < p^s$ and every $\mu g((D^-)^k_{(1,br)}(\mu), B^{p^s-k}_{(b,r)}(\mu)) \leq p^{-(p^s-1)}$.*

We now show that $B_{(b,r)}$ has no dense orbits. Define a partition of $E^+(p)$ by $E^+(p)$ by $E^+_q = [\mu \text{in} E^+(p) | \mu_i = 0$ if $i < q; \mu_q \neq 0]$. By (1.1) $B_{(b,r)} : E^+_q \to E^+_q$ so no orbit of $B_{(b,r)}$ can be dense in $E^+(p)$. Indeed, if μ is in E^+_q and $\mu\prime$ is in E^+_s with $s < q$ then $g(\mu, B^k_{(b,r)}(\mu\prime)) > p^{-q}$. For all $k, \emptyset(B^k_{(b,r)}(\mu))$ is contained in the interval $[p^{-(q-1)}, p^{-q}]$ and the diagram of figure 1 commutes.

In other words, $E^+(p) = \bigcup_{q=1}^{\infty} E^+_q$ defines a stratification of $E^+(p)$ with respect to $\emptyset$ which is preserved under $B_{(b,r)}$. (We might call this the Zeno stratification—as above, so below.) The remaining question is whether or not $B_{(b,r)}$ might possess orbits which are dense in one of the E^+_q.

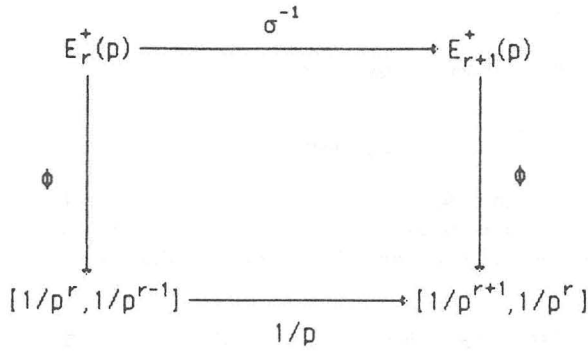

Figure 1: Stratified mapping to the unit interval.

Theorem 10. *No orbit of $B_{(b,r)} : E_q^+ \to E_q^+$ is dense in E_q^+ for any q.*

Proof. It is sufficient to prove the theorem for E_1^+. Suppose that μ is an element of E_1^+ such that the orbit $[B^k_{(b,r)}(\mu)|0 \leq k < \infty]$ is dense in E_1^+. Then, for any given $\beta, \beta\prime$ in E_1^+, and for all $N < \infty$, there will be integers k, m (dependent on N) such that

$$g(\beta, B^k_{(b,r)}(\mu)) < p^{-N} \quad \text{and} \quad g(\beta\prime, B^m_{(b,r)}(\mu)) < p^{-N} \tag{3.13}$$

Without loss of generality assume that k, m are the smallest integers for which this occurs for a fixed N, and $k \leq m$. (3.13) requires that

$$|\beta - B^k_{(b,r)}(\mu)|_i = |\beta\prime - B^m_{(b,r)}(\mu)|_i = 0 \quad \forall i \leq N$$

Thus, it must be possible to simultaneously satisfy the sets of equations

$$\begin{aligned} \beta_i &= \sum_{j=1}^{i} \Pi_{i-j+1}^{(k+1-j)} x^{i-j} \mu_j \\ & \\ i &\leq N \\ & \\ \beta\prime_i &= \sum_{j=1}^{i} \Pi_{i-j+1}^{(m+i-j)} x^{i-j} \mu_j \end{aligned} \tag{3.14}$$

Addition of these equations yields, for $i \leq N$

$$(\beta_i + \beta\prime_i) = \sum_{j=1}^{i} \left[\Pi_{i-j+1}^{(k+i-j)} + \Pi_{i-j+1}^{(m+i-j)} \right] x^{i-j} \mu_j \tag{3.15}$$

which can be written in matrix form as

$$\Psi = \Gamma x^{(k,m)} \tag{3.16}$$

where Ψ and $x^{(k,m)}$ are column vectors in $\mathbf{Z}_p^N$ with jth components given by $\beta_j + \beta\prime_j$ and $\Pi_j^{(k+j-1)} + \Pi_j^{(m+j-1)}$ respectively, and Γ is the NxN matrix

$$\Gamma = \begin{bmatrix} \mu_1 & 0 & 0 & 0 & 0 \\ \mu_2 & x\mu_1 & 0 & 0 & 0 \\ \mu_3 & x\mu_2 & x^2\mu_1 & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \mu_N & x\mu_{N-1} & x^2\mu_{N-2} & x^3\mu_{N-3} & x^{N-1}\mu_1 \end{bmatrix} \tag{3.17}$$

$\mathrm{Det}(\Gamma) = x^{N(N-1)/2}\mu_1^N \neq 0$ since $\mu_1 = 1$, hence Γ^{-1} exists and (3.16) has a unique solution

$$x^{(k,m)} = \Gamma^{-1}\Psi. \tag{3.18}$$

Now suppose that $\Psi \to \Psi + \Psi^*$. This will change the solution of (3.18), say to $X^* = X^{(k,m)} + \Gamma^{-1}\Psi^*$. In general, however, it is not true that X^* can be written as the sum of the first N terms of two diagonals of the mod(p) Pascal triangle. To see that this is so, let q be such that $p^{q-1} < N \leq p^q$. Then, for $i \leq p^q$, the first N terms of the $(i + p^q)$th diagonal of the mod(p) Pascal triangle equal the first N terms of the ith diagonal. Thus, the number of possible distinct combinations of the first N terms of diagonals of this triangle, taken two at a time, is given by $p^q(p^q - 1)/2$. However, Ψ^* is arbitrary, except that $\Psi_1^* = 0$. Hence, there are $p^{N-1} = p^{p^q-1}$ possible choices for Ψ^*, and N can always be chosen large enough that this is greater than $p^q(p^q - 1)/2$. (For example, the choice of N such that $q < (p^q - 1)/2$ is sufficient.) Thus, no μ can have a dense orbit under iteration of B.

4. $B_{(b,r)}$ as discrete integration

The operators $D_{(r,s)}$ and $D^-_{(r,s)}$ can be considered as discrete derivatives with respect to the sequence index, via an analogy to the Taylor formula $f(x) = f(a) + (x - a)f\prime(a)$. The analogy is

$$\mu_{i+1} = (p - r)\mu_i + b[D_{(r,s)}(\mu)]_i$$

$$\mu_{i+1} = (p - r)\mu_i + b[D^-_{(r,s)}(\mu)]_{i+1}$$

where $bs \equiv 1 \bmod (p)$. The equation $D^-_{(r,s)}(\mu) = \beta$ can be directly "integrated" since the inverse of $D^-_{(r,s)}$ is $bB_{(b,r)}$ so that $\mu = bB_{(b,r)}(\beta)$. The equation $D_{(r,s)}(\mu) = \beta$ can also be "integrated" via theorem 1. Thus the operators $B_{(b,r)}$ are analogues to discrete integration with respect to sequence index.

Restricting consideration to $p = 2, B_{(1,1)} \equiv B$ is closely related to two operators studied by Rogers and Weiss [4,5].

$A = \sigma B$ (Accumulator operator)
$T = \sigma + [\sigma, B]$ (Twisted-shift operator).

In order to derive formulas for powers of these operators we need the following:

Lemma 2. $B\sigma^r = \sigma^r B + BP_1 \sum_{s=0}^{r-1} \sigma^s$

where $P_1(\mu) = \mu_1 \alpha_1$.

Proof. This is true for $r = 1$ and we proceed by induction. Assuming (4.1) is true for r then

$$\begin{aligned} B\sigma^{r+1} &= B\sigma^r\sigma = \sigma^r B\sigma + BP_1 \sum_{s=1}^{r} \sigma^s \\ &= \sigma^{r+1}B + \sigma^r BP_1 + BP_1 \sum_{s=1}^{r} \sigma^s \end{aligned}$$

which yields the desired result since for any $r, \sigma^r BP_1 = BP_1$.

Making use of equation (4.1) together with lemma 2, an induction argument also proves:

Theorem 11. *With A and T defined as above*

$$\begin{aligned} T^k &= \sigma^k + B\sigma^{k-1}P_k \qquad (4.2) \\ A^k &= \sum_{r=1}^{k} \sigma^r B^r Z_{k-r} \end{aligned}$$

where the Z_r are defined recursively by

$$Z_0 = 1, \quad Z_r = P_1 \sum_{s=1}^{r} \sum_{q=0}^{r-s} \sigma^q B^{r-s+1} Z_{s-1}$$

5. Discussion

This paper has introduced a family of operators $B_{(b,r)} : E^+ \to E^+$ which have been interpreted as discrete integrals with respect to sequence index. Properties of these operators have been determined: they are self-accumulating, not solipsistic, and have a period-multiplying property. In terms of application, these operators are significant in solution of the problem of determining predecessor states for certain cellular automata evolutions [2]. They have also been found useful in studies of arithmetic properties of the mapping $D : [0,1] \to [0,1]$ defined in terms of the operator $D : E^+ \to E^+$ and the mapping (3.1) by $D(\emptyset(\mu)) = \emptyset(D(\mu))$ [6]. Although conceptually and mathematically simple, this family of operators is found, at least in the $p = 2$ case, to have a direct relation to other more complicated operators such as Rogers and Weiss's twisted-shift and accumulator operators.

Appendix A. The mod(p) Pascal triangle

Several of the proofs given in section 3 of this paper are based on properties of Pascal's triangle reduced modulo p, and the coefficients in expansions of powers of the operators studied in this paper are drawn from this triangle. The properties of the mod(p) Pascal triangle which are important for the present paper are derived in this appendix. Many of the results presented here are due to Long [7].

Long has proved an elegant structural theorem for the mod(p) Pascal triangle. For p prime let k, n, and m be integers with $0 \leq k \leq n$ and $1 \leq m$. Let $\Delta_{n,k}$ denote the triangle

$$\begin{array}{ccccc} & & \binom{np^m}{kp^m} & & \\ & \cdot & & \cdot & \\ \cdot & & & & \cdot \\ \binom{np^m+p^m-1}{kp^m} & \cdots\cdots & & \cdots\cdots & \binom{np^m+p^m-1}{kp^m+p^m-1} \end{array}$$

Theorem 12. *(Long, [7])* $\Delta_{n,k}$ *defined above is the triangle*

$$\begin{array}{ccccc} & & \binom{n\ 0}{k\ 0} & & \\ & \binom{n\ 1}{k\ 0} & & \binom{n\ 1}{k\ 1} & \\ \cdot & & & & \cdot \\ & \cdot & & \cdot & \\ \cdot & & & & \cdot \\ \binom{n\ p^m-1}{k\ 0} & \cdots\cdots & & \cdots\cdots & \binom{n\ p^m-1}{k\ p^m-1} \end{array}$$

with all products reduced modulo p. Further,

$$\Delta_{n,k} + \Delta_{n,k+1} = \Delta_{n+1,k+1}$$

where the addition is element-wise modulo p. Finally, every element in Pascal's triangle and not in one of the $\Delta_{n,k}$ *is congruent to* 0 *modulo p.*

Proof of this theorem is contained in Long's paper. The triangles $\Delta_{n,k}$ are in one-to-one correspondence with the residues $0, 1, 2, \ldots, p-1$ so that

the triangle of triangles:

$$\Delta_{0,0}$$

$$\Delta_{1,0} \quad \Delta_{1,1}$$

$$\Delta_{2,0} \quad \Delta_{2,1} \quad \Delta_{2,2}$$

$$\cdots\cdots\cdots\cdots$$

is isomorphic to the mod(p) Pascal triangle. This leads to the basic self-similarity property for the mod(p) Pascal's triangle: "If we repeatedly iterate this process by mapping the triangles $\Delta_{n,k}$ onto the residues it follows that, modulo p, Pascal's triangle is a triangle that contains a Pascal's triangle of triangles, that in turn contain a Pascal's triangle of triangles, ..., *ad infinitum*" (from [7], author's italics).

It also turns out that the entries of Pascal's triangle not contained in any of the $\Delta_{n,k}$ form inverted triangles of the form

$$\begin{bmatrix} np^m \\ kp^m + 1 \end{bmatrix} \quad \cdots\cdots\cdots\cdots \quad \begin{bmatrix} np^m \\ kp^m + p^m + 1 \end{bmatrix}$$

$$\begin{bmatrix} np^m + p^m - 2 \\ kp^m + p^m - 1 \end{bmatrix}$$

Every element of these inverted triangles is congruent to 0 modulo p.

Figure 2 shows the first 33 rows of the mod(2) Pascal triangle, illustrating Long's results.

What is of particular interest for this paper are the locations of the inverted triangles of zeros, and the self-similar property which follows from Long's results. In particular, these results indicate that inverted triangles of zeros will be based only on rows k such that $(k-1)|p$. Further, if $k = p^s + 1$ then there will be one such inverted triangle with base length $p^s - 1$. That is, the $p^s + 1$ row of the mod(p) Pascal triangle consists of an initial and final one separated by $p^s - 1$ zeros. The general pattern of self-similarity for the mod(p) Pascal triangle is indicated in figure 3 below:

Lemma 3. *Let A_s be the* mod (p) *Pascal triangle truncated at row p^s. Then A_s consists of $p(p+1)/2$ upright triangles isomorphic to A_{s-1} and $p(p-1)/2$ inverted triangles of zeros having base length $p^{s-1} - 1$. These last are the largest inverted triangles of zeros contained in A_s. The upright triangles have the numerical form mA_{s-1} with $1 \leq m < p$.*

Proof. The upright triangles are the $\Delta_{i,j}$ defined by Long. Since the triangle of these triangles is isomorphic to Pascal's triangle mod (p) the number of upright triangles isomorphic to A_{s-1} is the same as the number of elements

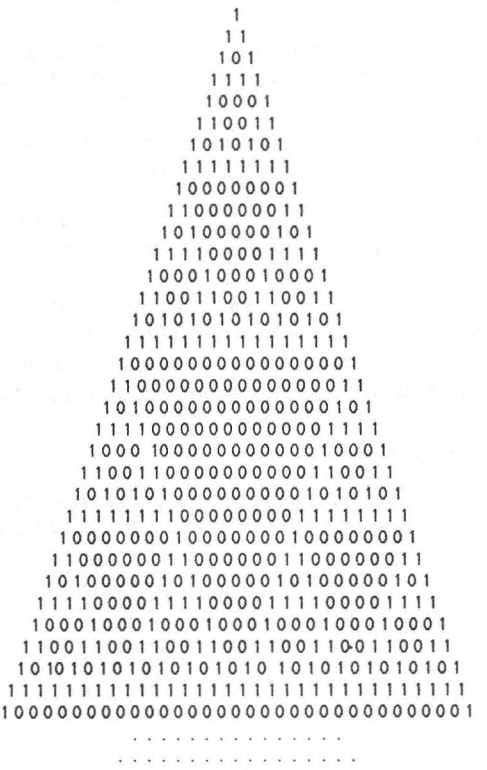

Figure 2: Pascal's triangle modulo 2.

in the first p rows of this triangle and this is just the sum of the first p integers, that is, $p(p+1)/2$. The inverted triangles of zeros fall between the upright triangles so that the number of these is just the sum of the first $p-1$ integers, that is, $p(p-1)/2$.

On the basis of this lemma, it is possible to count the number of inverted triangles of zeros of any size which are contained in A_s. That is, there are $p(p-1)/2$ with the maximum base of $p^{s-1}-1$. Each of the upright triangles has the form mA_{s-1}. But, A_{s-1} contains $p(p+1)/2$ triangles isomorphic to A_{s-2} and $p(p-1)/2$ inverted triangles of zeros with base length $p^{s-2}-1$. Thus, there are $p^2(p^2-1)/4$ of these inverted triangles and a total of $p^2(p+1)^2$ triangles isomorphic to A_{s-2}. Continuation of this yields

Lemma 4. *A_s contains $2^{-d}p^d(p+1)^d$ upright triangles isomorphic to A_{s-d} and $2^{-d}p^d(p+1)^{d-1}(p-1)$ inverted triangles of zeros with base length $p^{s-d}-1$, where $1 \leq d \leq s-1$.*

It is also possible to specify which rows of A_s the inverted triangles are based on and how many are based on each of these rows.

Lemma 5. *For $1 \leq d \leq s-1$ there are m_d inverted triangles of base length $p^{s-d}-1$ based on row $m_d p^{s-d}+1$ with $1 \leq m_d \leq p^d - 1$ and point p^q not a divisor of m_d for any $q < d$.*

There are also some formulas relating to properties of diagonals of the mod(p) *Pascal triangle which can be derived from:*

Lemma 6. *The p^s diagonal of the* mod(p) *Pascal triangle is periodic with period p^s. The first p^s terms consist of a leading one followed by $p^s - 1$ zeros.*

Proof. The first term of every diagonal of Pascal's triangle is 1. However, there is an inverted triangle of zeros with base length $p^s - 1$ based on row $p^s + 1$ and the next $p^s - 1$ terms of the p^s diagonal lie along a side of this triangle. Periodicity follows from the self-similarity properties of the Pascal triangle modulo p.

With a similar argument we prove:

Lemma 7. *The $p^s - 1$ diagonal of Pascal's triangle modulo p has period p^s and consists of a leading one followed by $p-1$, followed by a total of $p^s - 2$ zeros.*

Finally, any element of the mod(p) *Pascal triangle can be written as a sum of elements along a diagonal.*

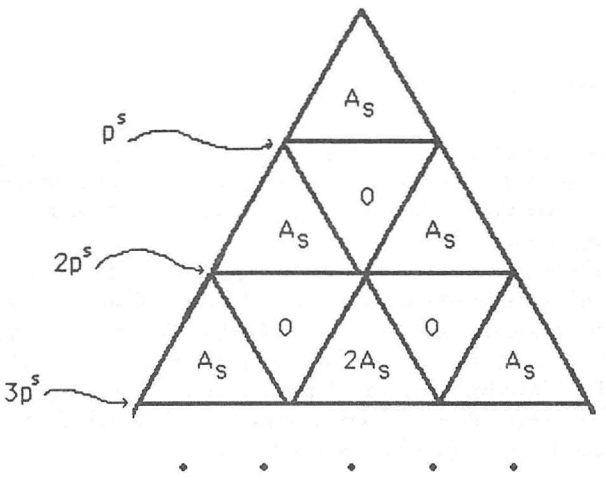

Figure 3: Self-similarity pattern for Pascal's Triangle modulo p. Indicated triangle continues to row p^{s+1} and this defines A_{s+1}.

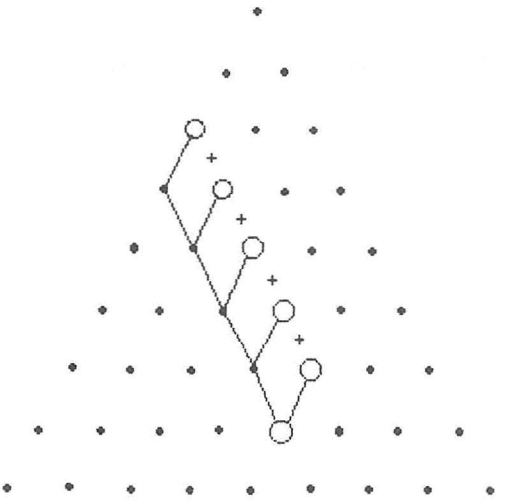

Figure 4: Backward decomposition from an element of Pascal's triangle.

Lemma 8. $\Pi_i^{(k+i+1)} = \sum_{j=0}^{i} \Pi_{j+1}^{(k+j)}$

Proof. An analytic proof follows directly from the addition rule for Pascal's triangle, noting that $\Pi_1^{(k)} = \Pi_1^{(r)} = 1$ for all k, r. The essence of this proof, however, is most easily conveyed through consideration of figure 4.

The given entry marked by the lowest circle is the sum of the two entries immediately above it, and this property propagates back to the initial diagonal which consists entirely of ones.

References

[1] B. Voorhees, "Cellular automata, Pascal's triangle, and generation of order," *Physica*, **31D** (1988) 135–140.

[2] B. Voorhees, "Predecessor states for certain additive cellular automata," *Communications in Mathematical Physics*, **117** (1988) 431–439.

[3] K.H. Rosen, *Elementary Number Theory and Its Applications* (Addison-Wesley, Reading, MA, 1984) 232.

[4] T.D. Rogers and A. Weiss, "Proceedings of 1986 University of Toronto Conference on Oscillations, Bifurcation, and Chaos," to appear.

[5] T.D. Rogers, private communication.

[6] B. Voorhees, "Geometry and arithmetic of a simple cellular automata," preprint.

[7] C.T. Long, "Pascal's triangle modulo p," *Fibonacci Quarterly*, **19** (1981) 458–463.