Maximal Temporal Period of a Periodic Solution Generated by a One-Dimensional Cellular Automaton

Janko Gravner
Xiaochen Liu

Department of Mathematics
University of California, Davis
1 Shields Avenue
Davis, CA 95616, USA

One-dimensional cellular automata evolutions with both temporal and spatial periodicity are studied. The main objective is to investigate the longest temporal periods among all two-neighbor rules, with a fixed spatial period σ and number of states n. When $\sigma = 2$, 3, 4 or 6, and the rules are restricted to be additive, the longest period can be expressed as the exponent of the multiplicative group of an appropriate ring. Non-additive rules are also constructed with temporal period on the same order as the trivial upper bound n^{σ}. Experimental results, open problems and possible extensions of the results are also discussed.

Keywords: cellular automaton; exponent of a multiplicative group; periodic solution

1. Introduction

We continue our study of periodic solutions of one-dimensional n-state cellular automata (CAs) from [1–3]. In those papers, we assumed a fixed spatial period σ and discussed the temporal periods for randomly selected rules. In the present paper, we instead investigate the analogous extremal questions.

We refer to elements of $\mathbb{Z}$ as *sites*, and, for a fixed $n \geq 2$, to elements of $\mathbb{Z}_n = \{0, 1, \ldots n-1\}$ as *states* or *colors*. A (one-dimensional) *spatial configuration* is a coloring of sites, that is, a map $\xi : \mathbb{Z} \to \mathbb{Z}_n$. A one-dimensional cellular automaton (CA) is a spatially and temporally discrete dynamical system of evolving spatial configurations ξ_t, $t \in \mathbb{Z}_+ = \{0, 1, \ldots\}$. In general, the dynamics of such CAs are determined by a *neighborhood* $N \subset \mathbb{Z}$ of $r \geq 1$ sites and by its (*local*) *rule*, which is a function $f : \mathbb{Z}_n^r \to \mathbb{Z}_n$. In this paper, as in [1], we assume the simplest nontrivial case when $r = 2$ and $N = \{-1, 0\}$. Thus, the spatial configuration updates from ξ_t to ξ_{t+1} using a rule

https://doi.org/10.25088/ComplexSystems.30.3.239

$f : \mathbb{Z}_n^2 \to \mathbb{Z}_n$ as follows:

$$\xi_{t+1}(x) = f\big(\xi_t(x-1), \xi_t(x)\big),$$

for all $x \in \mathbb{Z}$. We sometimes write $c_0\underline{c_1} \mapsto c_2$ instead of $f(c_0, c_1) = c_2$. A rule f is *additive* if it commutes with sitewise addition modulo n or, equivalently, if there exist $a, b \in \mathbb{Z}_n$ so that $f(c_0, c_1) = \mathrm{bc}_0 + ac_1 \bmod n$, for all $c_0, c_1 \in \mathbb{Z}_n$. Once ξ_0 is specified, the rule determines the CA *trajectory* $\xi_0, \xi_1, \ldots$, which we also identify with its spacetime assignment $\mathbb{Z} \times \mathbb{Z}_+ \to \mathbb{Z}_n$, given by $(x, t) \mapsto \xi_t(x)$.

We focus on CAs whose trajectories are periodic in both directions. We call a spatial configuration ξ *periodic* if $\xi(x) = \xi(x + \sigma)$, for all $x \in \mathbb{Z}$ and a $\sigma > 0$. If σ is the smallest such number, we call σ the *spatial period* of ξ. It is clear that, if ξ_t is periodic with period σ, then ξ_{t+1} is also periodic with a period that divides σ. Observe also that, if ξ_0 is periodic with period σ, we may view the evolution of the CA as the sequence of colorings of $\{0, 1, \ldots, \sigma - 1\}$, with periodic boundary, as in [4]. If, for some ℓ, ξ_ℓ is periodic with period σ, and $\tau \geq 1$ is the smallest integer such that $\xi_{\ell+\tau} = \xi_\ell$, then we call ξ_ℓ a *periodic solution* (PS) of rule f, with *temporal period* τ and spatial period σ. We can specify a particular PS by any σ contiguous states $\xi_j(x)\xi_j(x+1)\ldots\xi_j(x+\sigma-1)$, for any $x \in \mathbb{Z}$ and $\ell \leq j < \ell + \tau$. See Figure 1 for an example. In this figure, $n = 3$ and f is the additive rule given by $f(c_0, c_1) = c_0 + c_1$ for all $c_0, c_1 \in \mathbb{Z}_3$. This PS has spatial period $\sigma = 4$ and temporal period $\tau = 8$, and can be specified by any $\sigma = 4$ contiguous states, say 2101. The temporal period $\tau = 8$ is the largest of all additive rules with $\sigma = 4$ and $n = 3$.

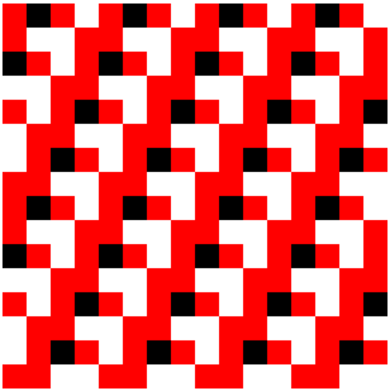

Figure 1. A $16 \times 16 = 4\sigma \times 2\tau$ piece of trajectory of a PS of a three-state additive rule. States 0, 1 and 2 are represented by white, red and black cells, respectively. The time axis is oriented downward, as is customary.

For an n-state rule f and $\sigma \geq 1$, we let $X_{\sigma,n}(f)$ and $Y_{\sigma,n}(f)$ be, respectively, the largest and smallest temporal periods of PS, with spatial period σ, of the rule f. When f is selected uniformly at random, $X_{\sigma,n}$ and $Y_{\sigma,n}$ become random variables, which we investigated in [1, 2]. In [1], we proved that the smallest temporal period $Y_{\sigma,n}$ converges in distribution to a nontrivial limit, as $n \to \infty$; in particular, it is stochastically bounded. By contrast, the longest temporal period $X_{\sigma,n}$ is expected to be on the order of $n^{\sigma/2}$. We prove this in [2] in the more general r-neighbor setting, but for our methods to work, we are forced to assume that $\sigma \leq r$. Then, $X_{\sigma,n} / n^{\sigma/2}$ converges in distribution to a nontrivial limit, as $n \to \infty$. The case $\sigma > r$ is still open, even in our present case $r = 2$.

Instead of their typical size, this paper explores the extremal values of quantities $X_{\sigma,n}(f)$ and $Y_{\sigma,n}(f)$. It is clear that $\min_f Y_{\sigma,n}(f) = \min_f X_{\sigma,n}(f) = 1$, as the minima are attained by the identity n-state rule, that is, the rule f given by $f(c_0, c_1) = c_1$, for all $c_0, c_1 \in \mathbb{Z}_n$. We therefore focus on

$$\max_f Y_{\sigma,n}(f) \text{ and } \max_f X_{\sigma,n}(f), \tag{1}$$

the largest among the shortest and longest temporal periods of a PS with spatial period σ and n states. Let $T(\sigma, n)$ be the number of aperiodic length-σ words from alphabet $\mathbb{Z}_n$, that is, words that cannot be written as repetition of a subword. Then it is clear that, for all n-state rules f, $1 \leq Y_{\sigma,n}(f) \leq X_{\sigma,n}(f) \leq T(\sigma, n)$. We also have the following counting result.

Lemma 1. The number of aperiodic length-σ words from alphabet $\mathbb{Z}_n$ is

$$T(\sigma, n) = \sum_{d|\sigma} n^d \mu\left(\frac{\sigma}{d}\right) = \begin{cases} n^\sigma - n^{\sigma/2} + o\left(n^{\sigma/2}\right), & \text{if } \sigma \text{ is even} \\ n^\sigma + o\left(n^{\sigma/2}\right), & \text{if } \sigma \text{ is odd,} \end{cases}$$

where $\mu(\cdot)$ is the Möbius function.

Proof. See [5]. □

For $\sigma = 1$ and any n, it is easy to find a rule f with $Y_{1,n}(f) = X_{1,n}(f) = n = T(1, n)$; for example, any rule f satisfying $f(a, a) = \phi(a)$, where ϕ is any permutation on $\mathbb{Z}_n$ of order n, would do. For $\sigma = 2$, viewing evolution on $\{0, 1\}$ with periodic boundary, a unique CA with temporal period $\binom{n}{2}$ goes through all length-2 configurations ab, with $a < b \in \mathbb{Z}_n$. For instance, when $n = 3$, the evolution

$$\begin{array}{cc} 0 & 1 \\ 0 & 2 \\ 1 & 2 \end{array}$$

defines a rule with $0\underline{1} \mapsto 2$, $1\underline{0} \mapsto 0$, $0\underline{2} \mapsto 2$, $2\underline{0} \mapsto 1$, $1\underline{2} \mapsto 1$ and $2\underline{1} \mapsto 0$. Switching the last two values of f extends the PS to

$$\begin{array}{cc} 0 & 1 \\ 0 & 2 \\ 1 & 2 \\ 1 & 0 \\ 2 & 0 \\ 2 & 1, \end{array}$$

which has temporal period $6 = 3^2 - 3 = T(2, 3)$. It is clear that this construction works for all n and gives $Y_{2,n}(f) = X_{2,n}(f) = n^2 - n = T(2, n)$.

Even for $\sigma \geq 3$, it is not obvious what the extremal values of equation (1) are, whether they are equal, or whether the upper bound $T(3, n)$ can always be attained. One of our main results is that $\max_f Y_{\sigma,n}(f) = \Theta(n^\sigma)$, matching the order of $T(\sigma, n)$ given by Lemma 1.

Theorem 1. Fix an arbitrary $\sigma > 0$. For $n \geq N(\sigma)$, there exists an n-state CA rule f such that $X_{\sigma,n}(f) = Y_{\sigma,n}(f) \geq C(\sigma) n^\sigma$, where $N(\sigma)$ and $C(\sigma)$ are constants depending only on σ.

To alleviate the difficulties in computing the extremal quantities of equation (1), we may try to restrict the set of rules f. The most natural such restrictions are the additive rules, which exploit the algebraic structure of the states and enable the use of algebraic tools [4, 6, 7]. We denote by $\mathcal{A}_n$ the set of n-state additive rules and let

$$\pi_\sigma(n) = \max_{f \in \mathcal{A}_n} X_{\sigma,n}(f).$$

It follows from [4] that $\pi_\sigma(n) \leq n^{\sigma-1}$ (see Corollary 1), and therefore by Theorem 1 the maximal period of additive rules is at least by one power of n smaller than that of non-additive rules. Furthermore, for $\pi_\sigma(n)$ and $\sigma \in \{2, 3, 4, 6\}$, we are able to give an explicit formula for $\pi_\sigma(n)$. Let $\lambda_\sigma(n)$ be the exponents of multiplicative group of $\mathbb{Z}_n$ when $\sigma = 2$, Eisenstein integers modulo n when $\sigma = 3$ and Gaussian integers modulo n when $\sigma = 4$. Then π_σ is related to λ_σ as follows.

Theorem 2. For $\sigma = 2, 3$, $\pi_\sigma(n) = \lambda_\sigma(\sigma n)$, for all $n \geq 2$. Moreover, $\pi_4(2) = 4$ and $\pi_4(n) = \lambda_4(n)$, for all $n \geq 3$. Finally, $\pi_6(n) = \lambda_3(6n)$, for all $n \geq 2$.

This theorem and Lemmas 2–5 give the promised explicit expressions for the four $\pi_\sigma(n)$. It is tempting to conjecture that a variant of Theorem 2 holds for all σ, with a suitable definition of λ_σ for Kummer ring $\mathbb{Z}_n(\zeta)$, where ζ is the σ^{th} root of unity. However, this remains unclear, as ζ is quadratic only for $\sigma = 3, 4, 6$, and this fact plays a crucial role in our arguments.

We now give a brief review of the previous literature on large temporal periods of PS. The foundational work on the temporal periods of additive CAs is certainly [4]. Various recursive relations and upper bounds given in this paper are very useful, and indeed are utilized in the proof of Theorem 2 in Section 2. Like the present paper, [4], and its notable successors such as [6, 7], study CAs on finite intervals with periodic boundary. This choice is important, as results with other types of boundaries yield substantially different results. For example, [8] investigates the maximal length of temporal periods of binary CAs under null boundary condition and demonstrates that the maximal length $2^\sigma - 1$ can be obtained by additive rules, for any $\sigma > 0$. In [9], the authors address the same question for non-additive CAs and show that the maximal length can also be obtained, if the rule is allowed to be nonuniform among sites. Works that investigate additive rules and their temporal periods also include [10–12] and [13]. In conclusion, we refer to the book [14] for the wider context and extensive discussion on topics related to those addressed in this paper.

The rest of the paper is organized as follows. In Section 2 we address additive rules and prove Theorem 2. We relegate a result on multiplicative group structure of Eisenstein numbers modulo n, which is needed for $\sigma = 3, 6$, to the Appendix. In Section 3, we prove Theorem 1 through explicit construction. Finally, in Section 4, we present several simulation results and propose a number of resulting conjectures.

2. Longest Temporal Periods of Additive Rules

In this section, we investigate the longest temporal period that an additive rule is able to generate, for a fixed spatial period σ.

2.1 Definitions and Preliminary Results

We write a configuration ξ_t on the integer interval $[0, \sigma - 1]$ with periodic boundary as $c_0^{(t)} c_1^{(t)} \ldots c_{\sigma-1}^{(t)}$, where $c_j^{(t)} \in \mathbb{Z}_n$, for

$j = 0, 1, \ldots, \sigma - 1$, or, equivalently, by the polynomial of degree $\sigma - 1$ [4]

$$L^{(t)}(x) = \sum_{j=0}^{\sigma-1} c_j^{(t)} x^j.$$

An additive rule f such that $f(c_0, c_1) = bc_0 + ac_1$, for $a, b \in \mathbb{Z}_n$ is characterized by the polynomial $T(x) = a + bx$, and its evolution as polynomial multiplication:

$$L^{(t+1)}(x) = T(x) L^{(t)}(x),$$

in the quotient ring of polynomials $\mathbb{Z}_n[x]$ modulo the ideal generated by the polynomial $x^\sigma - 1$, to implement the periodic boundary condition. In this section, we will use $T(x)$, for some fixed a and b, to specify an additive CA, in place of the rule f.

As a result, a PS generated by the additive rule $T(x) = a + bx$ with temporal period τ and spatial period σ satisfies

$$T^\tau(x) L^{(\ell)}(x) = L^{(\ell)}(x), \ \text{in} \mathbb{Z}_n[x] \big/ \left(x^\sigma - 1\right).$$

We are interested in the longest temporal period with a fixed spatial period σ. For general CAs, this task requires the examination of the longest cycle in the configuration directed graph [2], which encapsulates information from all initial configurations. For linear rules, however, the following simple proposition from [4] reduces the set of relevant initial configurations to a singleton.

Proposition 1. (Lemma 3.4 in [4]) Fix an additive CA and a $\sigma \geq 1$. The temporal period of any PS with the spatial period σ divides the temporal period resulting from the initial configuration $10^{\sigma-1}$ (1 followed by $\sigma - 1$ 0s), represented by the constant polynomial 1.

Therefore, we may define the longest temporal period $\Pi_\sigma(a, b; n)$ of an additive rule $T(x) = a + bx$, as the smallest k, such that

$$(a + bx)^{k+\ell} = (a + bx)^\ell, \ \text{in} \mathbb{Z}_n[x] \big/ \left(x^\sigma - 1\right),$$

for some $\ell \geq 0$. We will refer to $\Pi_\sigma(a, b; n)$ as simply the *period* of $T(x)$. The largest period is thus

$$\pi_\sigma(n) = \max_{a,b \in \mathbb{Z}_n} \Pi_\sigma(a, b; n).$$

We use the standard notation $\mathbb{Z}_n[i]$ (where $i = \sqrt{-1}$) and $\mathbb{Z}_n[\omega]$ (where $\omega = e^{2\pi i/3}$) for Gaussian integers modulo n and Eisenstein integers modulo n.

For a finite ring R with unity, we denote by $R^\times$ its multiplicative group, define the (multiplicative) *order* $\operatorname{ord}(x)$ for any $x \in R$ to be the smallest integer k so that $x^k = 1$ if $x \in R^\times$, and let $\mathrm{ord}(x) = 1$ otherwise. Note that this is the standard definition when $x \in R^\times$. Recall that

$$\begin{aligned}\mathbb{Z}_n^\times &= \{a : \gcd(a, n) = 1\},\\ \mathbb{Z}_n[i]^\times &= \{a + bi : a, b \in \mathbb{Z}_n, \gcd(a^2 + b^2, n) = 1\},\\ \mathbb{Z}_n[\omega]^\times &= \{a + b\omega : a, b \in \mathbb{Z}_n, \gcd(a^2 + b^2 - ab, n) = 1\}.\end{aligned}$$

Then we define

$$\begin{aligned}\Lambda_2(a, b; n) &= \mathrm{ord}\,(a + b) \text{ in } \mathbb{Z}_n,\\ \Lambda_3(a, b; n) &= \mathrm{ord}\,(a + b\,\omega) \text{ in } \mathbb{Z}_n\,[\omega],\\ \Lambda_4(a, b; n) &= \mathrm{ord}\,(a + b\,i) \text{ in } \mathbb{Z}_n[i].\end{aligned} \tag{2}$$

Furthermore, we let

$$\lambda_\sigma(n) = \max_{a,b \in \mathbb{Z}_n} \Lambda_\sigma(a, b; n),$$

for $\sigma = 2$, 3 and 4, be the exponents of the multiplicative groups $\mathbb{Z}_n^\times$, $\mathbb{Z}_n[\omega]^\times$ and $\mathbb{Z}_n[i]^\times$. In Section 2.2, we obtain explicit formulas for $\lambda_\sigma(n)$ for these three σ.

In the following, we will use p and $p_1, p_2 \ldots$ to denote prime numbers; for an arbitrary n, we write its prime decomposition as $n = p_1^{m_1} \ldots p_k^{m_k}$ or as $n = 2^{m_2} 3^{m_3} \ldots p^{m_p}$. When $p \nmid \sigma$, we use $\mathrm{ord}_\sigma(p)$ to denote the order of p in $\mathbb{Z}_\sigma$. We now list several useful results from [4].

Proposition 2. (Lemma 4.3 in [4]) If $p \mid \sigma$, then

$$\Pi_\sigma(a, b; p) \mid p\Pi_{\sigma/p}(a, b; p).$$

Proposition 3. (Theorem 4.1 and (B.8) in [4]) If $p \nmid \sigma$ and $\sigma \geq 2$, then

$$\Pi_\sigma(a, b; p) \mid \left(p^{\mathrm{ord}_\sigma(p)} - 1\right)$$

and $\mathrm{ord}_\sigma(p) \leq \sigma - 1$. Furthermore, $\Pi_1(a, b; p) \mid (p - 1)$.

Proposition 4. (Theorem 4.4 in [4]) For $n = p_1^{m_1} \ldots p_k^{m_k}$, we have

$$\Pi_\sigma(a, b; n) = \mathrm{lcm}\left(\Pi_\sigma\left(a, b; p_1^{m_1}\right), \ldots, \Pi_\sigma\left(a, b; p_k^{m_k}\right)\right).$$

Proposition 5. (Theorem 4.5 in [4]) Let $m \geq 2$ be an integer. Then $\Pi_\sigma(a, b; p^m)$ either equals $p\Pi_\sigma(a, b; p^{m-1})$ or $\Pi_\sigma(a, b; p^{m-1})$.

As a consequence of the above results, we obtain the following upper bound.

Corollary 1. Let $\sigma \geq 2$, then $\max_{f \in \mathcal{A}_n} X_{\sigma,n}(f) \leq n^{\sigma-1}$, for all $n \in \mathbb{N}$.

Proof. Let $n = p_1^{m_1} \ldots p_k^{m_k}$ be the prime decomposition of n. For every $j = 1, \ldots, k$ write $\sigma = p_j^{n_j} \sigma_j$, where $n_j \geq 0$ and σ_j is such that $p_j \nmid \sigma_j$. Let $\epsilon_j = 1$ if $\sigma_j = 1$, and $\epsilon_j = 0$ otherwise. For any $a, b \in \mathbb{Z}_n$,

$$\begin{aligned}\Pi_\sigma(a, b; n) &= \operatorname{lcm}\left(\Pi_\sigma\left(a, b; p_1^{m_1}\right), \ldots, \Pi_\sigma\left(a, b; p_k^{m_k}\right)\right) \quad (\text{Proposition } 4)\\ &\leq \prod_{j=1}^{k} p_j^{m_j-1} \Pi_\sigma\left(a, b; p_j\right) \quad (\text{Proposition } 5)\\ &\leq \prod_{j=1}^{k} p_j^{m_j+n_j+\sigma_j-2} \left(p_j - 1\right)^{\epsilon_j} \quad (\text{Propositions 2 and 3})\\ &\leq \prod_{j=1}^{k} p_j^{m_j(\sigma-1)} = n^{\sigma-1},\end{aligned}$$

provided that the inequality

$$m_j + n_j + \sigma_j - 2 \leq m_j\left(p_j^{n_j} \sigma_j - 1\right) \tag{3}$$

holds when either $\sigma_j \geq 2$ or $p_j = 2$, and the inequality

$$m_j + n_j + \sigma_j - 1 \leq m_j\left(p_j^{n_j} \sigma_j - 1\right) \tag{4}$$

holds when $\sigma_j = 1$ and $p_j \geq 3$.

Note that $\sigma_j = 1$ implies that $n_j \geq 1$. Next, observe that $p_j^{n_j} \geq 2^{n_j} \geq n_j + 1$. Assume first that $\sigma_j \geq 2$. Then we have $m_j p_j^{n_j} \sigma_j \geq m_j\left(n_j + 1\right)\sigma_j \geq n_j \sigma_j + 2m_j$. Moreover, if $n_j \geq 1$, then $n_j \sigma_j - n_j - \sigma_j + 1 = \left(n_j - 1\right)\left(\sigma_j - 1\right) \geq 0$ and so equation (3) holds. If $n_j = 0$, then equation (3) reduces to $\sigma_j - 2 \leq m_j\left(\sigma_j - 2\right)$, which again holds. Next we assume that $\sigma_j = 1$ and $p_j = 2$. Then equation (3) follows from $m_j + n_j - 1 \leq m_j n_j$. Finally, assume that $\sigma_j = 1$ and $p_j \geq 3$. Then the inequality (4) follows from $n_j \leq 3^{n_j} - 2$. The equalities (3) and (4) are thus established and the proof completed. □

2.2 Exponents of the Multiplicative Groups

In this section, we find formulas for $\lambda_\sigma(n)$, $\sigma = 2$, 3 and 4, that is, the exponents of multiplicative groups $\mathbb{Z}_n^\times$, $\mathbb{Z}_n[\omega]^\times$ and $\mathbb{Z}_n[i]^\times$.

Lemma 2. For $\sigma = 2$, 3 and 4,

$$\lambda_\sigma(n) = \operatorname{lcm}\left(\lambda_\sigma\left(p_1^{m_1}\right), \ldots, \lambda_\sigma\left(p_k^{m_k}\right)\right).$$

Proof. By the Chinese Remainder Theorem, $\mathbb{Z}_n^\times$ (resp., $\mathbb{Z}_n[\omega]^\times$, $\mathbb{Z}_n[i]^\times$) is isomorphic to the direct product of the k groups $\mathbb{Z}^\times_{p_j^{m_j}}$ (resp., $\mathbb{Z}_{p_j^{m_j}}[\omega]^\times$, $\mathbb{Z}_{p_j^{m_j}}[i]^\times$), $j = 1, \ldots, k$. □

To find $\lambda_\sigma(n)$, it therefore suffices to find the formulas for $\lambda_\sigma(p^m)$ for prime p. For $\sigma = 2$, λ_2 is known as the Carmichael function, which is given by the following explicit formula.

Lemma 3. For $m \geq 1$ and p prime,

$$\lambda_2(p^m) = \begin{cases} 2^{m-1}, & \text{if } p = 2 \text{ and } m \leq 2 \\ 2^{m-2}, & \text{if } p = 2 \text{ and } m \geq 3 \\ p^{m-1}(p-1), & \text{if } p > 2. \end{cases}$$

Proof. See [15]. □

The results for λ_3 and λ_4 follow from the classification of the two multiplicative groups. For $\mathbb{Z}_{p^m}[i]^\times$, this task was accomplished in [16], while for $\mathbb{Z}_{p^m}[\omega]^\times$ we relegate the similar argument to the Appendix.

Lemma 4. For $m \geq 1$ and p prime,

$$\lambda_3(p^m) = \begin{cases} 6, & \text{if } p = 3 \text{ and } m = 1 \\ 2 \cdot 3^{m-1}, & \text{if } p = 3 \text{ and } m \geq 2 \\ p^{m-1}(p-1), & \text{if } p = 1 \bmod 3 \\ p^{m-1}(p^2-1), & \text{if } p = 2 \bmod 3. \end{cases}$$

Proof. The claim follows from Theorem 3 in the Appendix. □

Lemma 5. For $m \geq 1$ and p prime,

$$\lambda_4(p^m) = \begin{cases} 2^m, & \text{if } p = 2 \text{ and } m \leq 2 \\ 2^{m-1}, & \text{if } p = 2 \text{ and } m \geq 3 \\ p^{m-1}(p-1), & \text{if } p = 1 \bmod 4 \\ p^{m-1}(p^2-1), & \text{if } p = 3 \bmod 4. \end{cases}$$

Proof. By [16], we have

$$\mathbb{Z}_p[i]^\times \cong \begin{cases} \mathbb{Z}_2, & \text{if } p = 2 \\ \mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1}, & \text{if } p = 1 \bmod 4 \\ \mathbb{Z}_{p^2-1}, & \text{if } p = 3 \bmod 4 \end{cases}$$

and

$$\mathbb{Z}_{p^m}[i]^\times \cong \begin{cases} \mathbb{Z}_{p^{m-1}} \times \mathbb{Z}_{p^{m-2}} \times \mathbb{Z}_4, & \text{if } p = 2 \text{ and } m \geq 2 \\ \mathbb{Z}_{p^{m-1}} \times \mathbb{Z}_{p^{m-1}} \times \mathbb{Z}_p[i]^\times, & \text{if } p \neq 2. \end{cases}$$

The claim follows. □

2.3 Explicit Formulas for Configurations at Time *t*

The next lemma makes the connection between the CA evolution and the integer rings apparent.

Lemma 6. For $\sigma = 2$, in $\mathbb{Z}_n[x] / (x^2 - 1)$,

$$(a + bx)^t = \frac{1}{2}\left[(a+b)^t + (a-b)^t\right] + \frac{1}{2}\left[(a+b)^t - (a-b)^t\right]x. \tag{5}$$

For $\sigma = 3$, in $\mathbb{Z}_n[x] / (x^3 - 1)$,

$$\begin{aligned}(a + bx)^t = {} & \frac{1}{3}\left[(a+b)^t + (a+b\omega)^t + (a+b\omega^2)^t\right] + \\ & \frac{1}{3}\left[(a+b)^t + \omega^2(a+b\omega)^t + \omega(a+b\omega^2)^t\right]x + \\ & \frac{1}{3}\left[(a+b)^t + \omega(a+b\omega)^t + \omega^2(a+b\omega^2)^t\right]x^2.\end{aligned} \tag{6}$$

For $\sigma = 4$, in $\mathbb{Z}_n[x] / (x^4 - 1)$,

$$\begin{aligned}(a + bx)^t = {} & \frac{1}{4}\left[(a+b)^t + (a-b)^t + (a+bi)^t + (a-bi)^t\right] + \\ & \frac{1}{4}\left[(a+b)^t - (a-b)^t + i(a+bi)^t - i(a-bi)^t\right]x + \\ & \frac{1}{4}\left[(a+b)^t + (a-b)^t - (a+bi)^t - (a-bi)^t\right]x^2 + \\ & \frac{1}{4}\left[(a+b)^t - (a-b)^t - i(a+bi)^t + i(a-bi)^t\right]x^3.\end{aligned} \tag{7}$$

For $\sigma = 6$, in $\mathbb{Z}_n[x] / (x^6 - 1)$,

$$
\begin{aligned}
(a+bx)^t = {} & \frac{1}{6}\big[(a+b)^t + (a-b)^t + (a+b\omega)^t + \\
& \quad (a+b\omega^2)^t + (a-b\omega)^t + (a-b\omega^2)^t\big] \\
& + \frac{1}{6}\big[(a+b)^t - (a-b)^t + \omega^2(a+b\omega)^t + \omega \\
& \quad (a+b\omega^2)^t - \omega^2(a-b\omega)^t - \omega(a-b\omega^2)^t\big]x \\
& + \frac{1}{6}\big[(a+b)^t + (a-b)^t + \omega(a+b\omega)^t + \omega^2 \\
& \quad (a+b\omega^2)^t + \omega(a-b\omega)^t + \omega^2(a-b\omega^2)^t\big]x^2 \\
& + \frac{1}{6}\big[(a+b)^t - (a-b)^t + (a+b\omega)^t + \\
& \quad (a+b\omega^2)^t - (a-b\omega)^t - (a-b\omega^2)^t\big]x^3 \\
& + \frac{1}{6}\big[(a+b)^t + (a-b)^t + \omega^2(a+b\omega)^t + \omega \\
& \quad (a+b\omega^2)^t + \omega^2(a-b\omega)^t + \omega(a-b\omega^2)^t\big]x^4 \\
& + \frac{1}{6}\big[(a+b)^t - (a-b)^t + \omega(a+b\omega)^t + \omega^2 \\
& \quad (a+b\omega^2)^t - \omega(a-b\omega)^t - \omega^2(a-b\omega^2)^t\big]x^5.
\end{aligned}
\tag{8}
$$

To clarify, say, the formula for $\sigma = 6$, the expression in each square bracket is evaluated in $\mathbb{Z}[\omega]$ first (without the reduction modulo n), then the result, which must be in $6\mathbb{Z}$, is divided by 6, and finally is reduced modulo n.

Proof. This follows from diagonalization of circulant matrices; see, for example, [17]. □

2.4 The Upper Bounds

In this subsection we prove the upper bounds in Theorem 2.

Lemma 7. For $n \geq 2$, $\pi_\sigma(n) \leq \lambda_\sigma(\sigma n)$ for $\sigma = 2, 3$ and $\pi_6(n) \leq \lambda_3(6n)$. Moreover, for $n \geq 3$, $\pi_4(n) \leq \lambda_4(n)$.

Proof. We will show that, in all cases, $\Pi_\sigma(a, b; n)$ divides the corresponding upper bound for all $a, b \in \mathbb{Z}_n$. Assume that $p \nmid \sigma$, which automatically holds when $p \geq 5$. In this case, we claim that

$$\Pi_\sigma(a, b; p^m) \mid \lambda_\sigma(p^m), \tag{9}$$

which is clearly enough. By Propositions 5 and 3,

$$\Pi_\sigma(a, b; p^m) \mid p^{m-1}\big(p^{\operatorname{ord}_\sigma(p)} - 1\big).$$

As $\operatorname{ord}_2(p) = 1$, $\operatorname{ord}_3(p) = 1$ when $p \bmod 3 = 1$ and $\operatorname{ord}_3(p) = 2$ when $p \bmod 3 = 2$, and $\operatorname{ord}_4(p) = 1$ when $p \bmod 4 = 1$ and $\operatorname{ord}_4(p) = 2$ when $p \bmod 4 = 3$, Lemmas 3–5 imply equation (9).

We now consider each σ separately. Write $n = 2^{m_2} 3^{m_3} \ldots p^{m_p}$.

We begin with $\sigma = 2$. Note that equation (9) holds for $p = 3$, and we next consider powers of 2. For $m = 1$ and $m = 2$, it can be directly verified that $\Pi_2(a, b; 2^m) \mid 2$. For $m \geq 3$, by Proposition 5,

$$\Pi_2(a, b; 2^m) \mid 2^{m-2} \Pi_2(a, b; 2^2),$$

and then $\Pi_2(a, b; 2^m) \mid 2^{m-1}$. Therefore

$$\Pi_2(a, b; 2^m) \mid \lambda_2(2^{m+1}),$$

which, together with equation (9) and Proposition 4, implies that

$$\Pi_2(a, b; n) \mid \operatorname{lcm}(\lambda_2(2^{m_2+1}), \ldots, \lambda_2(p^{m_p})) = \lambda_2(2n),$$

by Lemma 2.

We continue with $\sigma = 3$. Now, equation (9) holds for $p = 2$ and we need to consider powers of 3. A direct verification shows that $\Pi_3(a, b; 3) \mid 6$. For $m \geq 2$, $\Pi_3(a, b; 3^m) \mid 3^{m-1} \Pi_3(a, b; 3)$ and so $\Pi_3(a, b; 3^m) \mid 2 \cdot 3^m$. By Lemma 4,

$$\Pi_3(a, b; 3^m) \mid \lambda_3(3^{m+1})$$

and again equation (9), Proposition 4, and Lemma 2 imply that $\Pi_3(a, b; 3^m) \mid \lambda_3(3n)$.

Next in line is $\sigma = 4$. This time, a direct verification (by computer) shows that $\Pi_4(a, b; 2)$, $\Pi_4(a, b; 2^2)$ and $\Pi_4(a, b; 2^3)$ all divide 4. For $m \geq 3$, we then have $\Pi_4(a, b; 2^m) \mid 2^{m-3} \Pi_4(a, b; 2^3)$, thus $\Pi_4(a, b; 2^m) \mid 2^{m-1}$. Now, if $n = 2^{m_2} 3^{m_3} \ldots p^{m_p}$ and $m_2 \geq 2$ or $m_2 = 0$, the result follows similarly as for $\sigma = 2$ or $\sigma = 3$. If $m_2 = 1$,

$$\Pi_4(a, b; 2 \cdot 3^{m_3} \ldots p^{m_p}) \mid \operatorname{lcm}(4, \lambda_4(3^{m_3}), \ldots, \lambda_4(p^{m_p})).$$

But

$$\begin{aligned} \operatorname{lcm}(4, \lambda_4(3^{m_3}), \ldots, \lambda_4(p^{m_p})) &= \operatorname{lcm}(2, \lambda_4(3^{m_3}), \ldots, \lambda_4(p^{m_p})) \\ &= \operatorname{lcm}(\lambda_4(2), \lambda_4(3^{m_3}), \ldots, \lambda_4(p^{m_p})) \\ &= \lambda_4(n), \end{aligned}$$

as long as one of the exponents $m_3, \ldots, m_p$ is nonzero, that is, when $n \geq 3$. The desired divisibility therefore holds.

Finally, we deal with $\sigma = 6$. This time, a similar argument shows that $\Pi_6(a, b; 2^{m_2}) \mid 3 \cdot 2^{m_2}$ and $\Pi_6(a, b; 3^{m_3}) \mid 2 \cdot 3^{m_3}$, for all

$m_2, m_3 \geq 1$. So, $\Pi_6(a, b; n)$ divides

$$\begin{aligned}&\operatorname{lcm}\left(3 \cdot 2^{m_2}, 2 \cdot 3^{m_3}, \ldots, \lambda_3\left(p^{m_p}\right)\right) = \\ &\quad \operatorname{lcm}\left(\lambda_3\left(2 \cdot 2^{m_2}\right), \lambda_3\left(3 \cdot 3^{m_3}\right), \ldots, \lambda_3\left(p^{m_p}\right)\right) = \lambda_3(6n).\end{aligned}$$

The desired divisibility is thus established in all cases. □

2.5 The Lower Bounds

Lemma 8. If n has prime decomposition $n = p_1^{m_1} \ldots p_k^{m_k}$, then, for any σ,

$$\operatorname{lcm}\left(\pi_\sigma\left(p_1^{m_1}\right), \ldots, \pi_\sigma\left(p_k^{m_k}\right)\right) \leq \pi_\sigma(n). \tag{10}$$

Proof. We identify $\mathbb{Z}_n$ by

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{m_1}} \times \ldots \times \mathbb{Z}_{p_k^{m_k}}.$$

For the CA rule in the j^{th} coordinate, we find $a_j, b_j \in \mathbb{Z}_{p_j^{m_j}}$ such that $\Pi_\sigma\left(a_j, b_j; p_j^{m_j}\right) = \pi_\sigma\left(p_j^{m_j}\right)$. Then a configuration repeats if and only if all k coordinates simultaneously repeat. □

As a consequence of Lemma 8, it suffices to consider the cases when $n = p^m$. In each case below, our strategy is to find an $a, b \in \mathbb{Z}_{p^m}$ for which the dynamics never reduces the spatial period and such that $\Pi_\sigma(a, b; p^m)$ equals the upper bound given by Lemma 7.

Lemma 9. For $\sigma = 2$, we have $\pi_2(p^m) = \lambda_2(2p^m)$.

Proof. We first prove that $a - b \in \mathbb{Z}_{p^m}^\times$ implies that the spatial period never reduces. Indeed, such a reduction means that the coefficients of 1 and x in equation (5) agree at some time $t \geq 1$, and then their difference $(a - b)^t$ must vanish in $\mathbb{Z}_{p^m}$, a contradiction.

We now assume that $p \geq 3$. By definition of λ_2, we can select a and b such that $\Lambda_2(a, -b; p^m) = \lambda_2(p^m)$; in particular, $a - b \in \mathbb{Z}_{p^m}^\times$. Let $k = \Pi_2(a, -b; p^m)$. Then, for some $\ell \geq 0$, $(a - bx)^{k+\ell} = (a - bx)^\ell$ in $\mathbb{Z}_{p^m}[x] / (x^2 - 1)$. If we replace x by any number $c \in \mathbb{Z}_{p^m}$ that satisfies $c^2 - 1 = 0 \operatorname{mod} p^m$, we get an equality in $\mathbb{Z}_{p^m}$, so we can substitute $x = 1$ to get $(a - b)^{k+\ell} = (a - b)^\ell \bmod p^m$. As $a - b$ is invertible in $\mathbb{Z}_{p^m}$, $(a - b)^k = 1 \bmod p^m$. We conclude that $\lambda_2(p^m) \leq \Pi_2(a, -b; p^m) \leq \pi_2(p^m)$. As the spatial period does not reduce, the desired conclusion follows from the equality $\lambda_2(p^m) = \lambda_2(2p^m)$ and Lemma 7.

Finally, we assume that $p = 2$. In this case, we need to prove that $\pi_2(2^m) = \lambda_2(2^{m+1})$. A direct verification shows that $\pi_2(2) = \pi_2(4) = 2$, so we may assume that $m \geq 3$, in which case $\lambda_2(2^{m+1}) = 2^{m-1}$. Pick a $c \in \mathbb{Z}_{2^{m+1}}^{\times}$ whose order equals $\lambda_2(2^{m+1})$. This is an odd number. Let $b = (c-1)/2$ and $a = b+1$, so that $a+b = c$ and $a-b = 1$. Clearly $b \leq 2^m - 1$, but then also $a \leq 2^m - 1$, as otherwise $c = 2^{m+1} - 1$, which has order 2. It then follows from equation (5) that $(a+bx)^{2^{m-1}} = 1$ in $\mathbb{Z}_{2^m}[x]/(x^2-1)$. Moreover, the coefficient of x in $(a+bx)^{2^{m-2}}$ cannot vanish in $\mathbb{Z}_{2^m}$, as otherwise $c^{2^{m-2}} = 1 \bmod 2^{m+1}$. It follows that $\Pi_2(a, b; 2^m) = 2^{m-1}$. □

Lemma 10. For $\sigma = 3$, we have $\pi_3(p^m) = \lambda_3(3p^m)$.

Proof. We first show that, provided $a + b\omega \in \mathbb{Z}_{p^m}[\omega]^{\times}$, spatial period does not reduce. Indeed, if the spatial period reduces to 1 at time $t \geq 1$, then from equation (6)

$$\frac{1}{3}\begin{bmatrix} B & A \\ A & B \end{bmatrix}\begin{bmatrix} (a+b\omega)^t \\ (a-b\omega)^t \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \text{ in } \mathbb{Z}_{p^m}[\omega],$$

where $A = 1 - \omega$ and $B = 1 - \omega^2$. This implies that $(a+b\omega)^t = 0$ in $\mathbb{Z}_{p^m}[\omega]$, a contradiction.

This time, we first assume that $p \neq 3$ and select a and b such that $\Lambda_3(a, b; p^m) = \lambda_3(p^m)$. Then, if $k = \Pi_3(a, b; p^m)$, we have $(a+bx)^{k+\ell} = (a+bx)^{\ell}$, in $\mathbb{Z}_{p^m}[x]/(x^3-1)$, for some ℓ. As $\omega^3 = 1$, we may replace x with ω to get $(a+b\omega)^k = 1$ in $\mathbb{Z}_{p^m}[\omega]$. As a result, $\lambda_3(p^m) \leq \Pi_3(a, b; p^m)$. As the spatial period does not reduce, the desired conclusion follows from $\lambda_3(p^m) = \lambda_3(3p^m)$ and Lemma 7.

It remains to consider $p = 3$. By direct verification, $\pi_3(3) = 6$, and we assume $m \geq 2$ from now on. Select $a = b = 1$. By Proposition 5, $\Pi_3(1, 1; 3^m) = 2 \cdot 3^{m'}$, for some $m' \in [1, m]$. Also, $(1+x)^{2\cdot 3^m} = 1$ in $\mathbb{Z}_{3^m}[x]/(x^3-1)$, which can be easily verified by equation (6) using $(1+\omega)^2 = \omega$, $(1+\omega^2)^2 = \omega^2$, and the fact, easily verified by induction, that $2^{2\cdot 3^m} = 1 \bmod 3^{m+1}$. So, it suffices to show that $(1+x)^{2\cdot 3^{m-1}} \neq 1$ in $\mathbb{Z}_{3^m}[x]/(x^3-1)$, and for this we verify that the constant term in equation (6) does not equal 1, that is,

$$(1+1)^{2\cdot 3^{m-1}} + (1+\omega)^{2\cdot 3^{m-1}} + (1+\omega^2)^{2\cdot 3^{m-1}} \neq 3 \text{ in } \mathbb{Z}_{3^{m+1}}[\omega].$$

Indeed, in $\mathbb{Z}_{3^{m+1}}[\omega]$, $\left(1+\omega\right)^{2\cdot 3^{m-1}} = \left(1+\omega^2\right)^{2\cdot 3^{m-1}} = 1$ and, again by induction, $2^{2\cdot 3^{m-1}} = 3^m + 1$. □

Lemma 11. For $\sigma = 4$, we have $\pi_4(p^m) = \lambda_4(p^m)$.

Proof. For any p, select a and b such that $\Lambda_4\left(a, b; p^m\right) = \lambda_4(p^m)$. Then if $k = \Pi_4\left(a, b; p^m\right)$, we have $\left(a + bx\right)^{k+\ell} = \left(a + bx\right)^{\ell}$, in $\mathbb{Z}_{p^m}[x] \big/ \left(x^4 - 1\right)$, for some ℓ. Replacing x with i, we have $\left(a + bi\right)^k = 1$ in $\mathbb{Z}_{p^m}[i]$. As a result, $\lambda_4(p^m) \le \Pi_4\left(a, b; p^m\right)$. Thus we only need to verify that the spatial period does not reduce. If it does, then for some t, by equation (7),

$$\frac{1}{2}\begin{bmatrix} 1 & 1 \\ i & -i \end{bmatrix}\begin{bmatrix} \left(a+bi\right)^t \\ \left(a-bi\right)^t \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \text{in } \mathbb{Z}_{p^m}[i],$$

implying that $\left(a + bi\right)^t = 0$ in $\mathbb{Z}_{p^m}[i]$, a contradiction with $a + bi \in \mathbb{Z}_{p^m}[i]^{\times}$. □

Lemma 12. Assume that $\sigma = 6$, $n = p^m$, and that one of these two conditions on a and b is satisfied: $p \ne 3$ and $a + b\omega$ is invertible $\mathbb{Z}_{p^m}[\omega]$; or $p = 3$, $m \ge 2$, $a = 1$ and $b = 2$. Then the spatial period of $\left(a + bx\right)^t$ is 6 for all $t \ge 0$.

Proof. If the period reduces to 2, then by equation (8),

$$\frac{1}{6}\begin{bmatrix} A & B & A & B \\ B & A & B & A \\ -B & -A & B & A \\ A & B & -A & -B \end{bmatrix}\begin{bmatrix} \left(a+b\omega\right)^t \\ \left(a+b\omega^2\right)^t \\ \left(a-b\omega\right)^t \\ \left(a-b\omega^2\right)^t \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \text{in } \mathbb{Z}_{p^m}[\omega],$$

where $A = 1 - \omega$ and $B = 1 - \omega^2$. Multiply rows, in order, by A, $-B$, B, A and add. Using $B^2 - A^2 = 3\left(2\omega + 1\right)$, we get that $\left(1 + 2\omega\right)\left(a + b\omega\right)^t = 0$ in $\mathbb{Z}_{p^m}[\omega]$. Multiplying instead by A, $-B$, $-B$, $-A$ gives $\left(1 + 2\omega\right)\left(a - b\omega\right)^t = 0$ in $\mathbb{Z}_{p^m}[\omega]$. If $p \ne 3$, then $1 + 2\omega \in \mathbb{Z}_{p^m}[\omega]^{\times}$ and so $\left(a + b\omega\right)^t = 0$, a contradiction. Assume now that $p = 3$. Then we use the fact that Eisenstein norm $\left|1 - 2\omega\right| = 7$, and so the norm of the product $\left|\left(1 + 2\omega\right)\left(1 - 2\omega\right)^t\right| = 3 \cdot 7^t$, which is not divisible by 3^m if $m \ge 2$, and so $\left(1 + 2\omega\right)\left(1 - 2\omega\right)^t$ is nonzero in $\mathbb{Z}_{3^m}[\omega]$.

We next show that the spatial period does not reduce to 3. If it does, then by equation (8),

$$\frac{1}{3}\begin{bmatrix} 1 & 1 & 1 \\ 1 & \omega^2 & \omega \\ 1 & \omega & \omega^2 \end{bmatrix}\begin{bmatrix} (a-b)^t \\ (a-b\omega)^t \\ (a-b\omega^2)^t \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \text{ in } \mathbb{Z}_{p^m}[\omega].$$

From this, we get that

$$(a-b)^t = (a-b\omega)^t = (a-b\omega^2)^t = 0 \text{ in } \mathbb{Z}_{p^m}[\omega]. \tag{11}$$

Assume $p \neq 3$ first. Then, equation (11) implies that neither $a-b$ nor $a-b\omega$ is invertible in $\mathbb{Z}_{p^m}[\omega]$, and thus p must divide $a-b$ and the norm a^2+b^2+ab. Then $3ab = (a^2+b^2+ab)-(a-b)^2$ is also divisible by p, and then so is ab. This implies that $p \mid (a^2+b^2-ab)$, and so $a+b\omega$ is not invertible, a contradiction. If $p=3$, then equation (11) is not satisfied for $a=1$, $b=2$, as $(a-b)^t$ cannot vanish. □

Lemma 13. For $\sigma = 6$, we have $\pi_6(p^m) = \lambda_3(6p^m)$.

Proof. Assume first that $p \geq 5$. Select any a and b such that

$$\Lambda_3(a, b; p^m) = \lambda_3(p^m) = \lambda_3(6p^m).$$

Then, if $k = \Pi_6(a, b; p^m)$, $(a+bx)^{k+\ell} = (a+bx)^\ell$, in $\mathbb{Z}_{p^m}[x] / (x^6-1)$, for some ℓ. Replacing x with ω, we have $(a+b\omega)^k = 1$, thus $\lambda_3(p^m) \leq \Pi_6(a, b; p^m)$.

Next in line is $p=2$. The claim is that $\pi_6(2^m) = 3 \cdot 2^m$. We may assume that $m \geq 3$, after a direct verification for $m = 1, 2$. By Theorem 2, $\Pi_6(1, 1; 2^m) = 3 \cdot 2^{m'}$, for some $m' \in [1, m]$. Therefore, it suffices to show that there are infinitely many ℓ for which the equality

$$(1+x)^{3\cdot 2^{m-1}+\ell} = (1+x)^\ell, \text{ in } \mathbb{Z}_{2^m}[x] / (x^6-1),$$

is *not* satisfied. A necessary condition for this equality is that the constant terms in equation (8) for both sides agree, which yields

$$\begin{aligned} \frac{1}{6}\Big[& 2^\ell\big(2^{3\cdot 2^{m-1}}-1\big) + (1+\omega)^\ell\Big((1+\omega)^{3\cdot 2^{m-1}}-1\Big) + (1+\omega^2)^\ell \\ & \Big((1+\omega^2)^{3\cdot 2^{m-1}}-1\Big) + (1-\omega)^\ell\Big((1-\omega)^{3\cdot 2^{m-1}}-1\Big) + \\ & (1-\omega^2)^\ell\Big((1-\omega^2)^{3\cdot 2^{m-1}}-1\Big)\Big] = 0 \bmod 2^m. \end{aligned}$$

As $1+\omega = -\omega^2$, $1+\omega^2 = -\omega$, the second and third terms vanish. The first term vanishes for large enough ℓ. Moreover, as $(1-\omega)^2 = -3\omega$ and $(1-\omega^2)^2 = -3\omega^2$, $(1-\omega)^{3\cdot 2^{m-1}} =$

$\left(1-\omega^2\right)^{3\cdot 2^{m-1}} = 3^{3\cdot 2^{m-2}}$, for $m \geq 3$. We obtain the necessary condition

$$\left(1-\omega\right)^{\ell}\left[1+\left(1+\omega\right)^{\ell}\right]\left(3^{3\cdot 2^{m-2}}-1\right) = 0 \bmod 3\cdot 2^{m+1}. \tag{12}$$

If $\ell = 1 \bmod 12$, then $\left(1-\omega\right)^{\ell}$ is a power of 3 times $\left(1-\omega\right)$ and $\left(1+\omega\right)^{\ell} = -\omega^2$. By a simple induction argument, $3^{3\cdot 2^{m-2}} - 1 = 2^m \bmod 2^{m+1}$. Then, if $\ell = 1 \bmod 12$, equation (12) reduces to $3^{\ell'}\cdot 2^m = 0 \bmod 3\cdot 2^{m+1}$, for some $\ell' \geq 1$, which is clearly false. This completes the proof for $p = 2$.

Finally, we deal with $p = 3$. We aim to prove $\pi_6\left(3^m\right) = 2\cdot 3^m$, and we will accomplish this by establishing the claim that $\Pi\left(1, 2; 3^m\right) = 2\cdot 3^m$. We may, again, assume $m \geq 3$. Similarly to the previous case, it suffices to show that

$$\left(1+2x\right)^{2\cdot 3^{m-1}+\ell} = \left(1+2x\right)^{\ell}, \text{ in } \mathbb{Z}_{3^m}[x] \,/\, \left(x^6-1\right), \tag{13}$$

fails to hold for infinitely many ℓ, and we will assume that ℓ is large enough and $18\,|\ell$. As before, we show the constant terms in equation (8) do not match. If they do, this expression needs to vanish modulo $2\cdot 3^{m+1}$:

$$\begin{aligned}
&\left(1+2\right)^{\ell}\left[\left(1+2\right)^{2\cdot 3^{m-1}}-1\right]+\left(1-2\right)^{\ell}\left[\left(1-2\right)^{2\cdot 3^{m-1}}-1\right]+\\
&\quad\left(1+2\omega\right)^{\ell}\left[\left(1+2\omega\right)^{2\cdot 3^{m-1}}-1\right]+\\
&\quad\left(1+2\omega^2\right)^{\ell}\left[\left(1+2\omega^2\right)^{2\cdot 3^{m-1}}-1\right]+\left(1-2\omega\right)^{\ell}\Big[\\
&\qquad\left(1-2\omega\right)^{2\cdot 3^{m-1}}-1\Big]\left(1-2\omega^2\right)^{\ell}\left[\left(1-2\omega^2\right)^{2\cdot 3^{m-1}}-1\right].
\end{aligned} \tag{14}$$

As $\left(1+2\omega\right)^2 = \left(1+2\omega^2\right)^2 = -3$, the first four terms all vanish when ℓ is large enough. For the fifth and sixth term, we first observe that

$$\begin{aligned}
&\left(1-2\omega\right)^{\ell} = \left[\left(1-\omega\right)-\omega\right]^{\ell} =\\
&\quad(-\omega)^{\ell}+\sum_{j=1}^{\ell}\binom{\ell}{j}\left(1-\omega\right)^{j}(-\omega)^{\ell-j} = 1 \text{ in } \mathbb{Z}_9[\omega].
\end{aligned} \tag{15}$$

By a similar calculation, $\left(1-2\omega^2\right)^{\ell}=1$ in $\mathbb{Z}_9[\omega]$. Next, we have

$$\begin{aligned}\left(1-2\omega\right)^{2\cdot 3^{m-1}}-1 &= \left[\left(1-\omega\right)-\omega\right]^{2\cdot 3^{m-1}}-1\\ &= -1+(-\omega)^{2\cdot 3^{m-1}}+\\ &\quad 2\cdot 3^{m-1}\left(1-\omega\right)(-\omega)^{2\cdot 3^{m-1}-1}+\\ &\quad \tfrac{1}{2}2\cdot 3^{m-1}\left(2\cdot 3^{m-1}-1\right)\left(1-\omega\right)^2\\ &\qquad (-\omega)^{2\cdot 3^{m-1}-2}+\tfrac{1}{2\cdot 3}2\cdot 3^{m-1}\left(2\cdot 3^{m-1}-1\right)\\ &\qquad \left(2\cdot 3^{m-1}-2\right)\ \left(1-\omega\right)^3(-\omega)^{2\cdot 3^{m-1}-3}+\\ &\quad \textstyle\sum_{j=4}^{2\cdot 3^{m-1}}\displaystyle\binom{2\cdot 3^{m-1}}{j}\left(1-\omega\right)^j(-\omega)^{2\cdot 3^{m-1}-j}\\ &= 2\cdot 3^{m-1}\left(1-\omega\right)\left(-\omega^2\right)-\\ &\quad 3^m\left(2\cdot 3^{m-1}-1\right)\omega^2+3^{m-1}\left(2\cdot 3^{m-1}-1\right)\\ &\qquad \left(2\cdot 3^{m-1}-2\right)\omega\left(1-\omega\right)\text{ in }\mathbb{Z}_{3^{m+1}}[\omega].\end{aligned} \tag{16}$$

Similarly,

$$\begin{aligned}&\left(1-2\omega^2\right)^{2\cdot 3^{m-1}}-1=\\ &\quad 2\cdot 3^{m-1}\left(1-\omega^2\right)(-\omega)-3^m\left(2\cdot 3^{m-1}-1\right)\omega+\\ &\qquad 3^{m-1}\left(2\cdot 3^{m-1}-1\right)\left(2\cdot 3^{m-1}-2\right)\omega\left(\omega-1\right)\text{ in }\mathbb{Z}_{3^{m+1}}[\omega].\end{aligned} \tag{17}$$

Combining equations (15) through (17), we conclude that equation (14) equals $3^m \bmod 3^{m+1}$. (We need $m\geq 3$ to ensure $3^{m+1}\mid 3^{m-1}\cdot 3^{m-1}$, so that we can ignore products of powers of 3.) Therefore equation (13) does not hold, which concludes the proof for $p=3$.

We also need that the spatial period is not reduced in considered cases, which are all covered by Lemma 12. □

Proof. (Proof of Theorem 2) The desired claims are established by Lemmas 7–11 and Lemma 13. □

3. Periodic Solution with Long Temporal Periods in Non-additive Rules

In this section, we prove Theorem 1, by two explicit constructions. Our first rule resembles a car odometer and is similar to others that have previously appeared in the literature, see [18]. We view this as the most natural design, which also gives explicit constants $C(\sigma)$ and $N(\sigma)$, although the second construction based on prime partition is much shorter.

3.1 The Odometer Rule

For a fixed integer $k \geq 2$, we define the state space

$$\mathcal{S} = \mathbb{Z}_k \times \{\leftarrow, \circ\} \times \{*, \circ\} \times \{E, \circ\},$$

which has cardinality $2^3 k$. We call these four coordinates the *number*, *particle*, *asterisk* and *end* coordinate, respectively. In words, each of the symbols $\leftarrow$, $*$ and E can be present at a site in addition to a number, and $\circ$ signifies its absence. We use abbreviations such as $(5, \leftarrow, *, E) = \overleftarrow{{}_E 5^*}$, $(5, \leftarrow, \circ, \circ) = \overleftarrow{5}$ and $(5, \circ, \circ, \circ) = 5$. To be consistent with the car odometer interpretation, we construct a *right-sided* rule. That is

$$\xi_{t+1}(x) = f\big(\xi_t(x), \xi_t(x+1)\big),$$

or $\underline{\xi_t(x)}\xi_t(x+1) \mapsto \xi_{t+1}(x)$. Clearly, such a rule may be transformed to our standard left-sided one by a vertical reflection.

The rule is described in the following 14 assignments, in which I, J represent numbers in $\mathbb{Z}_k$ and addition is modulo k; i, j represent elements in $\mathbb{Z}_k \backslash \{k-1\}$ and $\diamond$ stands for any state in $\mathcal{S}$:

1. $\underline{I}\overleftarrow{i^*} \mapsto \overleftarrow{I}$
2. $\underline{I}\overleftarrow{J} \mapsto \overleftarrow{I}$
3. $\underline{I}\overleftarrow{(k-1)^*} \mapsto \overleftarrow{I^*}$
4. $\overleftarrow{\underline{I}^*} \diamond \mapsto (I+1)$
5. $\overleftarrow{\underline{I}} \diamond \mapsto I$
6. $\overleftarrow{\underline{I}_E(k-1)} \mapsto \overleftarrow{I^*}$
7. $\overleftarrow{\underline{{}_E i}} \diamond \mapsto \overleftarrow{{}_E(i+1)}$
8. $\overleftarrow{\underline{{}_E(k-1)}} \diamond \mapsto_E 0$
9. $\underline{{}_E I}\overleftarrow{J^*} \mapsto \overleftarrow{{}_E 0}$
10. $\underline{{}_E I}\overleftarrow{J} \mapsto \overleftarrow{{}_E 0}$
11. $\underline{I}J \mapsto I$
12. $\underline{{}_E I}J \mapsto_E I$
13. $\underline{I}_E J \mapsto I$
14. $\underline{I}\overleftarrow{{}_E j} \mapsto I$

In all cases not covered, the rule leaves the current state unchanged: $\underline{c_0}c_1 \mapsto c_0$. We view the rule on $[0, \sigma - 1]$ with periodic boundary, that is, within one spatial period of the PS.

Our construction simulates the dynamics of an odometer on the number coordinate. The three auxiliary coordinates are needed for the update rule to be a CA. We now give a less formal description. The end position indicator E marks the right end of our interval with periodic boundary. Hence, there has to be exactly one E and it is designed so that it does not appear or disappear (see assignments 7–10 and 12–14). The $\leftarrow$ is a left-moving particle (assignments 1–10), marking the site on which the number coordinate may add 1 in the next step. The number marked by an E adds 1 if its site also contains a particle, that is, its particle coordinate is an $\leftarrow$ (assignments 7 and 8), and updates to 0 when an $\leftarrow$ is to its right (assignments 9 and 10). The number coordinates not marked by an E add 1 if and only if the asterisk coordinate is $*$ (see assignments 4 and 5). The symbol $*$ plays the role of carry in addition and can appear and disappear: it appears if the E position has number $k - 1$, then it moves along with the particle (see assignment 6) if its number coordinate is $k - 1$ (see assignment 3), and disappears if there is no carry (see 1) or if it arrives to the E position (see 9).

Any rule with the 14 given *odometer assignments* is called an *odometer* CA and generates a PS of temporal period at least k^σ, called *odometer* PS. This shows that $\max_f X_{\sigma,8k}(f) \geq k^\sigma$. To give an example, let $L = 00\ldots\overleftarrow{{}_E0}$ be the configuration consisting of $(\sigma - 1)$ 0s and a $\overleftarrow{{}_E0}$. When $\sigma = 3$, $k = 10$, then the PS is given in Table 1, where the relevant assignments are given in the parentheses. The PS has temporal period $1199 > 10^3 = k^\sigma$. We summarize the result of this section, which provides the best lower bound we have on $\max_f X_{\sigma,n}(f)$.

Proposition 6. There exists a CA rule f so that $X_{\sigma,}(f) \geq \lfloor n / 8 \rfloor^\sigma$.

The shortcoming of this construction is that it does not ensure that $Y_{\sigma,n}(f) = \Theta(n^\sigma)$, as the odometer rule, as it stands, has other PS with much shorter temporal periods. For example, in the CAs from Table 1, the configuration 123 is fixed due to the assignment 11, and so it generates a PS with temporal period 1. We provide the remedy in the next subsection.

3.2 The Odometer Rule with Automata

To prevent short temporal periods, we need to extend the state space. The strategy is to introduce a second layer to each state, which encodes two finite automata that determine whether a configuration is legitimate, that is, either itself or one of its updates is included in the odometer PS. A legitimate configuration will generate the PS with long temporal period, while an illegitimate one will eventually end up in a spatially constant configuration.

0	0	$\overleftarrow{{}_{E}0}$	
0	0	$\overleftarrow{{}_{E}1}$	(11, 14, 7)
	$\vdots$		
0	0	$\overleftarrow{{}_{E}9}$	(11, 14, 7)
0	$\overleftarrow{0^*}$	${}_{E}0$	(11, 6, 8)
$\overleftarrow{0}$	1	${}_{E}0$	(1, 4, 12)
0	1	$\overleftarrow{{}_{E}0}$	(5, 13, 10)
0	1	$\overleftarrow{{}_{E}1}$	(11, 14, 7)
	$\vdots$		
0	9	$\overleftarrow{{}_{E}9}$	(11, 14, 7)
0	$\overleftarrow{9^*}$	${}_{E}0$	(11, 6, 8)
$\overleftarrow{0^*}$	0	${}_{E}0$	(3, 4, 12)
1	0	$\overleftarrow{{}_{E}0}$	(4, 13, 9)
	$\vdots$		
9	9	$\overleftarrow{{}_{E}9}$	(11, 14, 7)
9	$\overleftarrow{9^*}$	${}_{E}0$	(11, 6, 8)
$\overleftarrow{9^*}$	0	${}_{E}0$	(3, 4, 12)
0	0	$\overleftarrow{{}_{E}0}$	(4, 13, 9).

Table 1. An odometer PS for $\sigma = 3$, $k = 10$.

Definition 1. Consider the state space $\mathbb{Z}_k \times \{\leftarrow, \circ\} \times \{*, \circ\} \times \{E, \circ\} \times \mathcal{A}$ of the odometer CA, where $\mathcal{A}$ is any finite set. A configuration on $[0, \sigma - 1]$ is legitimate if the following three conditions are satisfied: (1) there is exactly one site that contains an $\leftarrow$; (2) there is exactly one site that contains an E; (3) if a site contains $*$, then this site contains an $\leftarrow$ but does not contain an E.

Lemma 14. Any odometer rule starting from any legitimate configuration eventually enters the odometer PS.

Proof.

Case 1. An inductive argument shows that any legitimate configuration in the form of $a_0 \ldots \overleftarrow{{}_{E}a_{\sigma-1}}$ generates the odometer PS.

Case 2. Suppose that a legitimate configuration does not contain an $*$ and thus is of the form $a_0 \ldots \overleftarrow{a_j} \ldots {}_E a_{\sigma-1}$. Then by assignments 2 and 5, the ← moves left until $\overleftarrow{a_0} \ldots {}_E a_{\sigma-1}$ and then updates to $a_0 \ldots \overleftarrow{{}_E 0}$ because of assignments 5 and 10, reducing to Case 1.

Case 3. A legitimate configuration $a_0 \ldots \overleftarrow{a_j^*} \ldots {}_E a_{\sigma-1}$, $a_j < k-1$ updates to $a_0 \ldots \overleftarrow{a_{j-1}} (a_j + 1) \ldots {}_E a_{\sigma-1}$ because of assignments 1 and 4, or to $a_0 \ldots \overleftarrow{{}_E a_{\sigma-1}}$, reducing to either Case 2 or Case 1.

Case 4. A legitimate configuration $a_0 \ldots \overleftarrow{(k-1)^*} \ldots {}_E a_{\sigma-1}$ (with the ← at position j) becomes $a_0 \ldots \overleftarrow{a_{j-1}^*} 0 \ldots {}_E a_{\sigma-1}$, which is reduced to Case 3 when $a_{j-1} < k-1$. If $a_{j-1} = k-1$, repeated updates eventually reduce to Case 3 or Case 1. □

We now define the augmented state space for our two-layer construction of the *odometer rule with automata*:

$$\mathcal{S}_A = (\mathbb{Z}_k \times \{ \leftarrow, \circ\} \times \{ *, \circ\} \times \{E, \circ\} \times \mathcal{E} \times \mathcal{A}) \bigcup \{T\},$$

where

$$\mathcal{E} = \{(0, 0), (1, 0), \ldots, (\sigma-1, 0), (1, 1), (2, 1), \ldots, (\sigma-1, 1), T_1\}$$

comprises states of a finite automaton, called END-READER; and $\mathcal{A} = \{0, 1, \ldots, \sigma, T_2\}$ comprises states of another finite automaton, called ARROW-READER; and T is the special terminator state that erases the configuration once it appears. We regard the first four components—those from the odometer rule—as the first layer of a state, and the two automata components as the second layer.

We proceed to specify the rule. The first layer updates according to the previous odometer assignments. In addition, we include the assignment

- $\underline{(I, \circ, *, \circ)}s \mapsto T$ and $\underline{(I, \circ, *, E)}s \mapsto T$ for all $s \in \mathcal{S}_A$.

That is, if the first layer of a state contains an $*$ but not an ←, the state updates to T. Such an update will happen in any configuration that is illegitimate due to having an $*$ but not an ←.

The next assignment spells out the role of T_1, T_2 and T:

- For any site x, if either x or $x+1$ is in the state T or at least one of the second layers of x, $x+1$ contains a T_1 or a T_2, then x updates its state to T.

A configuration that contains a T_1, a T_2 or a T is called *terminated*. Any terminated configuration will eventually update to the constant configuration consisting of all T, thus reducing the spatial period to 1.

The transition function δ_E of the finite automaton END-READER= $\left(\mathcal{E}, \{E, \circ\}, \delta_E, (i, j), T_1\right)$ reads the end coordinate and is given in Figure 2; its initial state (i, j) can be any state in $\mathcal{E}$. From time t to time $t+1$, an END-READER at position x reads the state on its first layer, updates its state according to δ_E, then "moves" to $x-1$. This left shift of the entire END-READER configuration is allowed, as we are constructing a right-sided rule. According to the odometer assignments, the E position in a configuration does not appear or disappear and does not move. As a result, the END-READER counts the number of Es.

Lemma 15. Every configuration with zero or at least two sites containing an E will be terminated for any initial state of the END-READER. Conversely, starting from a configuration whose first layer is $= 00\ldots\overleftarrow{{}_E0}$, no END-READER ever reaches T_1 unless it starts there.

Proof. Start with a configuration with zero or two more states that contain an E. Suppose that it is never terminated by the END-READER. Then there is a time t and a position x such that the state of the END-READER is $\left(0, 0\right)$, as it is clear from Figure 2. Within σ time steps from t, the END-READER transitions to T_1. The converse result is also clear from Figure 2. □

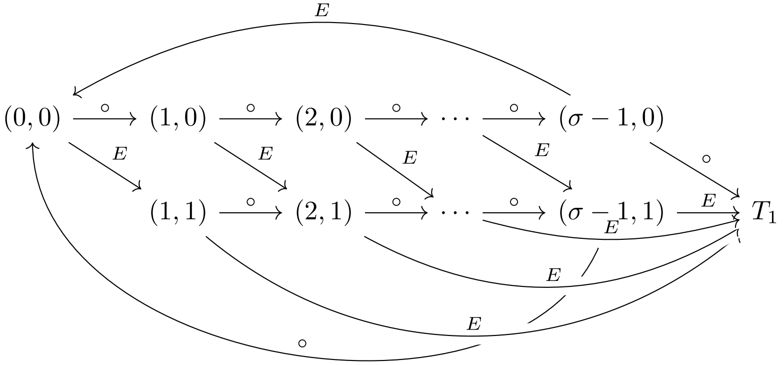

Figure 2. The transition function δ_E for END-READER.

We also need to terminate illegitimate configurations with zero or at least two arrows. First, a configuration with two or more arrows can be handled by adding the following assignment:

- $\underline{s_1}s_2 \mapsto T$, for all $s_1, s_2 \in \mathcal{S}_A$ such that s_1, s_2 both contain an ←.

Lemma 16. Assume $k > \sigma$. Let L be a configuration that is never terminated by the END-READER and such that at least two states of L contain an ←. Then L will be eventually terminated.

Proof. Since L is not terminated by the END-READER, there is exactly one state of L that contains E. Assume that the two states with $\leftarrow$ are not adjacent, as otherwise the configuration is terminated immediately. Note that the arrow at the E position stays there for k updates and other arrows move left at every update. As $k > \sigma$, two arrows will eventually be adjacent. □

Due to Lemma 16, it suffices to enlist a finite automaton whose mission is to terminate configurations with no $\leftarrow$. This automaton is the ARROW-READER that reads the particle and end coordinates and is given by $\left(\mathcal{A}, \{\leftarrow, \circ\}\times\{E, \circ\}, \delta_A, (i, j), T_2\right)$, where the transition function δ_A is described in Figure 3 and its initial state is any state in $\mathcal{A}$. From time t to time $t+1$, an ARROW-READER at site x updates its state according to δ_A and stays at the same position x. According to the odometer assignments, an $\leftarrow$ must appear at the E position within σ updates if there is at least one $\leftarrow$. Hence, the ARROW-READER terminates a configuration that fails this condition. The effect of this automaton is summarized in the following lemma.

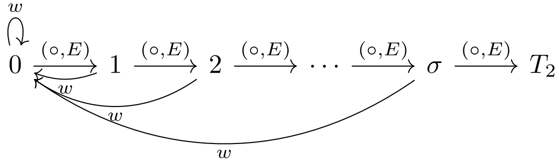

Figure 3. The transition function δ_A of the ARROW-READER. Here w is any symbol in $\{\leftarrow, \circ\}\times\{E, \circ\}\setminus\{(\circ, E)\}$.

Lemma 17. Every configuration with no $\leftarrow$ is eventually terminated for any initial state of the ARROW-READER. Conversely, starting from a configuration whose first layer is $00\ldots{}_{E}\overleftarrow{0}$, no ARROW-READER ever reaches T_2 unless it starts there.

The next proposition provides our first proof of Theorem 1.

Proposition 7. Let $S(\sigma) = 16\sigma(\sigma+2)$. For the rule f defined in this subsection, we have $X_{\sigma,}(f) = Y_{\sigma,n}(f) \geq \lfloor n / S(\sigma)\rfloor^{\sigma}$ for $n \geq (\sigma+2)S(\sigma)+1$.

Proof. Observe that $\left|\mathcal{S}_A\right| = S(\sigma)\cdot k+1$. For a number of states n, let $k = \lfloor (n-1) / S(\sigma)\rfloor$. Encode the odometer rule with automata on $S(\sigma)\cdot k+1$ states, and make any leftover states immediately transition to T. Let $L \in \mathcal{S}_A^{\sigma}$ be a configuration where its first layer is $00\ldots{}_{E}\overleftarrow{0}$; on the second layer, the END-READERs are at state $(0, 0)$ and the ARROW-READERs are at state 0. Then the configuration is not terminated by either END-READER or ARROW-READER, by Lemmas 15 and 17. Then the global configuration restricted on the first layer is the one of odometer CA, which has temporal period at least k^{σ}. Therefore, $X_{\sigma,n}(f) \geq k^{\sigma} = \lfloor n / S(\sigma) \rfloor^{\sigma}$.

Furthermore, note that any illegitimate configuration in $\mathcal{S}_A^{\sigma}$, as well as any configuration not in $\mathcal{S}_A^{\sigma}$, will eventually produce the constant configuration of all Ts with spatial period 1, by Lemmas 15–17. Furthermore, any legitimate configuration on the first layer will eventually update to a configuration whose first layer is in the odometer PS (by Lemma 14), and will never be terminated by the second layer that is not already in one of the terminator states (by Lemmas 15 and 17). Therefore, $Y_{\sigma,n}(f) = X_{\sigma,n}(f)$. □

3.3 The Prime Partition Rule

We begin with a simple consequence of the prime number theorem.

Lemma 18. For an arbitrary $\sigma > 0$, and for large enough n, there are σ primes $p_0, \ldots, p_{\sigma-1} \in \left[\frac{n-1}{2\sigma}, \frac{n-1}{\sigma}\right]$.

Assume that n is large enough so that Lemma 18 holds. Find disjoint sets $P_0, \ldots, P_{\sigma-1} \subset \mathbb{Z}_n \backslash \{0\}$ such that ${}_j| = p_j$, for $j = 0, \ldots, \sigma - 1$. This can be achieved since $p_0 + \cdots + p_{\sigma-1} \leq n - 1$. The state $0 \in \mathbb{Z}_n \backslash (P_0 \cup \ldots \cup P_{\sigma-1})$ will play the role of the terminator. Let $\phi_j : P_j \to P_j$ be a cyclic permutation of the p_j states. Keeping the right-sided convention from Section 3, we define the CA rule f as follows:

$$f(s, s') = \begin{cases} \phi_j(s) & \text{if } s \in P_j \text{ and } s' \in P_{(j+1) \bmod \sigma} \text{ for} \\ & \quad \text{some } j \in \{0, \ldots, \sigma - 1\} \\ 0 & \text{otherwise.} \end{cases}$$

Proposition 8. For f as just defined, we have $X_{\sigma,}(f) = Y_{\sigma,}(f)$ and $\liminf_{n \to \infty} n^{-\sigma} Y_{\sigma,}(f) \geq (2\sigma)^{-\sigma}$.

Proof. Call a configuration $s_0 s_1 \ldots s_{\sigma-1}$ *regular* if there exists an ℓ so that $s_j \in P_{(j+\ell) \bmod \sigma}$, $j = 0, \ldots, \sigma - 1$. To show that $X_{\sigma,n}(f) \geq (n-1)^{\sigma} / (2\sigma)^{\sigma}$, run the rule starting from any regular configuration. Such a configuration appears again for the first time after $p_0 p_1 \ldots p_{\sigma-1} \geq (n-1)^{\sigma} / (2\sigma)^{\sigma}$ updates. To show that $Y_{\sigma,n}(f) = X_{\sigma,n}(f)$, observe that any nonregular initial configuration eventually ends up in the constant configuration of all 0. □

4. Discussion and Open Problems

In this paper, we continue our study of the shortest and the longest temporal periods of a periodic solution (PS) for a fixed spatial period σ. While we are able to construct a rule whose longest temporal period grows as n^σ for large n, more precise results remain elusive even for $\sigma = 3$. We start our discussion with this case.

We call an n-state rule that has a PS with spatial period σ and temporal period $T(\sigma, n)$ a *maximum cycle length* (MCL) rule. For $\sigma = 3$, our computations demonstrate that an MCL rule exists for $n \leq 20$. More precisely, the number of MCL rules is 1 for $n = 2$ (out of 2^4 rules), 12 for $n = 3$ (out of 3^9 rules) and 732 for $n = 4$ (out of 4^{16} rules). These numbers match the first three terms of the sequence

$$\begin{gathered}(-1)^k 7^{2k} E_{2k}\left(\frac{3}{7}\right), \ k = 0, 1, 2, 3, \\ \ldots = 1, 12, 732, 109\,332, \ldots,\end{gathered} \tag{18}$$

where E_n are the Euler polynomials. Unfortunately, it is hard to traverse all of the $5^{25} \approx 2.98\times 10^{17}$ 5-state rules to count the number of MCL ones, so we merely state an open question.

Question 1. Assume $\sigma = 3$. Does there exist an MCL rule for any number of states $n \geq 2$? If so, is the number of MCL rules given by equation (18) for all n, or is the connection just a curious coincidence for $n \leq 4$?

If $X_{\sigma,n}(f) = T(\sigma, n)$, then automatically

$$Y_{\sigma,n}(f) = X_{\sigma,n}(f) = T(\sigma, n),$$

as the PS goes through all configurations with number of states n and spatial period σ. However, for $\sigma \geq 4$, an MCL may not exist, as demonstrated for $n = 3$ by Table 2, and therefore the maxima of $X_{\sigma,n}$ and $Y_{\sigma,n}$ may differ. This motivates our next question.

Question 2. What is the asymptotic behavior of $\max_f X_{\sigma,3}(f)$ as σ grows? Or of $\max_f X_{\sigma,}(f)$ for an arbitrary fixed n? Making n large first, what is the asymptotic behavior of

$$\liminf_{n\to\infty} n^{-\sigma} \max_f X_{\sigma,}(f)$$

for large σ? (See Proposition 6 for an exponentially small lower bound.) The same questions can be posed for $Y_{\sigma,}$ (for which Propositions 7 and 8 provide even smaller lower bounds).

σ	$\max_f X_{\sigma,3}(f)$	N_X	$\max_f Y_{\sigma,3}(f)$	N_Y	$T(\sigma, 3)$
1	3	1458	3	1458	3
2	6	216	6	216	6
3	24	12	24	12	24
4	40	12	32	72	72
5	120	2	120	2	240
6	111	6	84	42	696
7	1967	12	546	2	2184
8	904	12	896	24	6480
9	9207	12	1809	12	19656
10	10490	6	410	12	58800

Table 2. Maximal temporal period for $n = 3$ and spatial periods $\sigma \leq 10$. We also give N_X, and N_Y, the numbers of rules that realize the respective maxima.

To discuss the relation between $X_{\sigma,n}$ and $Y_{\sigma,n}$ for additive rules, let $\rho_\sigma(n) = \max_{f \in A_n} Y_{\sigma,n}(f)$. As it is clear from Table 3, $\pi_\sigma(n)$ and $\rho_\sigma(n)$ may differ, even for $\sigma = 2$ or 3. This suggests our next question.

Question 3. Fix a $\sigma \geq 2$. Is there an explicit formula for $\rho_\sigma(n)$, in terms of n, at least for small σ? Can one characterize n for which $\pi_\sigma(n) = \rho_\sigma(n)$?

n	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$\rho_2(n)$	2	2	2	4	2	6	2	2	4	10	2	12	6	4	2	16	2	18	4
$\pi_2(n)$	2	2	2	4	2	6	4	6	4	10	2	12	6	4	8	16	6	18	4
$\rho_3(n)$	3	6	3	24	6	6	3	6	24	120	6	12	6	24	3	288	6	18	24
$\pi_3(n)$	3	6	6	24	6	6	12	18	24	120	6	12	6	24	24	288	18	18	24

Table 3. Maximum of shortest and longest temporal periods of additive rules, for $\sigma = 2$, 3 and $n = 2, \ldots, 20$.

For a prime power p^m, we define the function $\mathrm{ub}_\sigma(p^m)$ to be the upper bound obtained from Propositions 2, 3 and 5. That is, $\mathrm{ub}_1(p) = p - 1$; $\mathrm{ub}_\sigma(p) = p^{\mathrm{ord}_\sigma(p)} - 1 \nmid \sigma \geq 2$; $\mathrm{ub}_\sigma(p) = p^k \cdot \mathrm{ub}_{\sigma/p^k}(p)$ if $k \geq 1$ is the largest power of p dividing σ; and $\mathrm{ub}_\sigma(p^m) = p \cdot \pi_\sigma\left(p^{m-1}\right)$ if $m \geq 2$. It is common that $\pi_\sigma(p^m) = \mathrm{ub}_\sigma(p^m)$, most notably for $\sigma = 5$.

Question 4. Is it true that, for all prime powers p^m, we have $\pi_5(p^m) = \mathrm{ub}_5(p^m)$?

We have checked that there are no counterexamples to the "yes" answer on Question 4 for all p^m such that $p \leq 50$ and $\mathrm{ub}_5(p^m) \leq 10^5$. As counterexamples should be harder to come by for larger p (more a and b to choose from) and for larger m (less chance for $\Pi\left(a, b; p^m\right)$ to be equal to $\Pi\left(a, b; p^{m-1}\right)$), we conjecture that the answer to Question 4 is indeed affirmative. We also remark that, if this conjecture holds, there is an explicit formula for $\pi_5(n)$ for all n, due to Lemma 8 and Proposition 4.

It is not always true that $\pi_\sigma(p^m) = \mathrm{ub}_\sigma(p^m)$. Table 4 contains a list of examples of inequality we have found for $\sigma \leq 50$. One hint that the table offers is easy to prove and we do so in the next proposition.

σ	2	4	7	8	11	13	14	16
p^m	2^2	$2^{2\to3}$	3	$2^{2\to4}$	2	2	3	$2^{2\to5}$
$\pi_\sigma(p^m)$	2	4	364	8	341	819	364	16
$\mathrm{ub}_\sigma(p^m)$	4	8	728	16	1023	4095	728	32

σ	21	22	26	32	42	44
p^m	3	2	2	$2^{2\to6}$	3	2
$\pi_\sigma(p^m)$	1092	682	1638	32	1092	1364
$\mathrm{ub}_\sigma(p^m)$	2184	2046	8190	64	2184	4092

Table 4. Examples with $\pi(p^m) < \mathrm{ub}(p^m)$. An arrow indicates a range of powers.

Proposition 9. Assume that $\sigma = 2^k$, $k \geq 1$. Then $\pi_\sigma\left(2^m\right) = 2^k$ for all $m \leq k + 1$, but $\pi_\sigma\left(2^{k+2}\right) = 2^{k+1}$.

Proof. When $n = 2$, $\left(1 + x\right)^{2^k} = 1 + x^{2^k} = 0$ in $\mathbb{Z}_2[x] / \left(x^\sigma - 1\right)$. This implies that, for any m, when a and b are both odd, all states are eventually divisible by 2, and then by additivity $\left(a + bx\right)^t = 0$ for large enough t. Clearly the same is true when a and b are both even. If a is odd and b is even,

$$\left(a+bx\right)^{2^k}=a^{2^k}=1 \text{ in } \mathbb{Z}_{2^{k+1}}[x]\big/\left(x^{\sigma}-1\right),$$

and the same conclusion holds if a is even and b is odd. This shows that $\pi_{\sigma}\left(2^m\right)\leq 2^k$ for $m\leq k+1$. As clearly $\Pi_{\sigma}\left(0,\,1;\,2^m\right)=\sigma=2^k$, we get $\pi_{\sigma}\left(2^m\right)=2^k$.

By the same argument, $\left(a+bx\right)^{2^{k+1}}=1$ in $\mathbb{Z}_{2^{k+2}}[x]\big/\left(x^{\sigma}-1\right)$, for all a and b. Moreover, it is easy to check that $\left(1+2x\right)^{2^k}=1+2^{k+1}x+2^{k+1}x^2\neq 1$ in $\mathbb{Z}_{2^{k+2}}[x]\big/\left(x^{\sigma}-1\right)$, proving the last claim. □

Call a prime p *persistent* if $\pi_{\sigma}(p)<\text{ub}_{\sigma}(p)$ for infinitely many σ. We conclude with a few questions suggested by Table 4.

Question 5. (1) Is either 2 or 3 persistent? (2) Are there infinitely many primes p such that $\pi_{\sigma}(p)<\text{ub}_{\sigma}(p)$ for some σ? (3) Is 2 the only prime with $\pi_{\sigma}(p^m)<\text{ub}_{\sigma}(p^m)$ for some $m\geq 2$?

Acknowledgments

Both authors were partially supported by the NSF grant DMS-1513340. J. Gravner was also supported in part by the Slovenian Research Agency (research program P1-0285). The authors thank Jingyang Shu for useful conversations, in particular for pointing out the sequence of equation (18).

Appendix

In this appendix, we determine the structure of the multiplicative group of Eisenstein integers modulo n, that is, the group

$$\mathbb{Z}_n[\omega]^{\times}=\left\{a+b\omega\in\mathbb{Z}_n[\omega]:a^2+b^2-ab\in\mathbb{Z}_n^{\times}\right\},$$

where $\omega=e^{2\pi i/3}$.

While our arguments are similar to those in [16] on Gaussian integers modulo n, we are aware of no reference that directly implies Theorem 3, so we provide a sketch of the proof.

Lemma A.1.

1. Let $p\geq 3$ be a prime number and a be an integer not divisible by p. Then $x^2=a \bmod p$ either has no solutions or exactly two solutions.

2. Let $p\geq 5$ be a prime number. The number -3 is a quadratic residue modulo p if and only if $p=1 \bmod 6$.

Proof. See [16] for the proof of part 1. For part 2, see [19, Exercise 9, p. 109]. □

Lemma A.2. Let p be a prime.

1. If $p = 3$, then $\mathbb{Z}_p[\omega]^\times \cong \mathbb{Z}_6$.
2. If $p = 1 \bmod 6$, then $\mathbb{Z}_p[\omega]^\times \cong \mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1}$.
3. If $p = 5 \bmod 6$, then $\mathbb{Z}_p[\omega]^\times \cong \mathbb{Z}_{p^2-1}$.

Proof. To prove part 1, observe that the group $\mathbb{Z}_3[\omega]^\times$ is Abelian, and $\left|\mathbb{Z}_3[\omega]^\times\right| = 6$, so $\mathbb{Z}_3[\omega]^\times \cong \mathbb{Z}_6$.

To prove part 2, first note that then the equation $x^2 - x + 1 = 0 \bmod p$ is equivalent to $(2x-1)^2 = -3 \bmod p$. By Lemma 19, the equation $y^2 = -3 \bmod p$, where $y = 2x - 1$ has two solutions $y = \pm q$. We next find the cardinality of $\mathbb{Z}_p[\omega]^\times$. Assume that $a + b\omega \notin \mathbb{Z}_p[\omega]^\times$, so that $a^2 + b^2 - ab = 0 \bmod p$. If $a \neq 0 \bmod p$, then $(a^{-1}b)^2 - (a^{-1}b) = -1 \bmod p$ and so $2a^{-1}b - 1 = \pm q \bmod p$. So, $b = 2^{-1}a(\pm q + 1)$. In particular, for a fixed nonzero a, there are two possible values for b such that $a + b\omega \notin \mathbb{Z}_p[\omega]^\times$, proving that $\left|\mathbb{Z}_p[\omega]^\times\right| = (p-1)^2$.

As $\mathbb{Z}_p^\times \cong \mathbb{Z}_{p-1}$, it suffices to show that there is an isomorphism

$$\psi : \mathbb{Z}_p[\omega]^\times \to \mathbb{Z}_p^\times \times \mathbb{Z}_p^\times.$$

It is routine to check that ψ, defined by $\psi(a + b\omega) = (a - 2^{-1}b(q+1), a - 2^{-1}b(-q+1))$, is an injective homomorphism, hence it is an isomorphism by equality of cardinalities.

To prove part 3, note that $\mathbb{Z}_p[\omega]$ has p^2 elements, so it suffices to show that $\mathbb{Z}_p[\omega]$ is a field, as the multiplicative group of any field is cyclic. Assume again that $a + b\omega \notin \mathbb{Z}_p[\omega]^\times$, so that $a^2 + b^2 - \mathrm{ab} = 0 \bmod p$. If $a \neq 0 \bmod p$, then $(a^{-1}b)^2 - (a^{-1}b) = -1 \bmod p$. By Lemma 19, the equation $x^2 - x + 1 = 0 \bmod p$, or equivalently $(2x-1)^2 = -3 \bmod p$, has no solution, as $p = 5 \bmod 6$. We conclude that $a = 0 \bmod p$, and similarly $b = 0 \bmod p$, so $\mathbb{Z}_p[\omega]$ is a field. □

Lemma A.3. For a prime $p \geq 3$ and $m \geq 2$,

$$\mathbb{Z}_{p^m}[\omega]^\times \cong \mathbb{Z}_{p^{m-1}} \times \mathbb{Z}_{p^{m-1}} \times \mathbb{Z}_p[\omega]^\times.$$

Proof. The proof is analogous to that for Theorem 7 in [16]. □

Lemma A.4. For $m \geq 1$, $\mathbb{Z}_{2^m}[\omega]^\times$ is classified as follows: $\mathbb{Z}_2[\omega]^\times \cong \mathbb{Z}_3$, $\mathbb{Z}_{2^2}[\omega]^\times \cong \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, and, for $m \geq 3$,

$$\mathbb{Z}_{2^m}[\omega]^\times \cong \mathbb{Z}_3 \times \mathbb{Z}_{2^{m-1}} \times \mathbb{Z}_{2^{m-2}} \times \mathbb{Z}_2.$$

Proof. The multiplicative group $\mathbb{Z}_2[\omega]^\times$ is Abelian with three elements, so $\mathbb{Z}_2[\omega]^\times \cong \mathbb{Z}_3$. Assume that $m \geq 2$. Write $H = \mathbb{Z}_{2^m}[\omega]^\times$. The elements of the group H are of the form $(1+2k_1)+2k_2\omega$, $2k_1+(1+2k_2)\omega$ and $(1+2k_1)+(1+2k_2)\omega$ for $0 \leq k_1, k_2 \leq 2^{m-1}-1$, so the number of them is $2^{m-1}2^{m-1}3 = 3 \times 2^{2m-2}$. Furthermore (see proof of Theorem 7 in [16]), each element in H has order at most $3 \cdot 2^{m-1}$, and by verifying that $(1+3\omega)^{3 \cdot 2^{m-2}} \neq 1$ in $\mathbb{Z}_{2^m}[\omega]$ and $(1+3\omega)^{2^{m-1}} \neq 1$ in $\mathbb{Z}_{2^m}[\omega]$, we see that there exists an element with order exactly $3 \cdot 2^{m-1}$. As a consequence, $H \cong \mathbb{Z}_3 \times \mathbb{Z}_{2^{m-1}} \times \prod_{j=1}^r \mathbb{Z}_{2^{e_j}}$, where $e_j \geq 1$ and $\sum_{j=1}^r e_j = m-1$. When $m = 2$, the result follows immediately, so we assume $m \geq 3$ from now on.

We claim that $r = 2$. Since each factor, except $\mathbb{Z}_3$, is cyclic of order at least two, each contains exactly one subgroup of order two. So, H has 2^{r+1} solutions to the equation $(a+b\omega)^2 = 1 \bmod 2^m$, which is equivalent to

$$\begin{cases} a^2 - b^2 = 1 \bmod 2^m \\ 2ab - b^2 = 0 \bmod 2^m. \end{cases}$$

This system has no solution unless a is odd and b is even, so we write $a = 2k_1 + 1$ and $b = 2k_2$ and obtain

$$\begin{cases} k_1^2 + k_1 - k_2^2 = 0 \bmod 2^{m-2} \\ (2k_1 + 1 - k_2)k_2 = 0 \bmod 2^{m-2}. \end{cases}$$

From the first equation, k_2 is even, so $2k_1 + 1 - k_2$ has an inverse and then $k_2 = 0 \bmod 2^{m-2}$, so $k_2 = 0$ or 2^{m-2}. Now $k_1(k_1+1) = 0 \bmod 2^{m-2}$. If k_1 is odd, then $k_1 + 1 = 0 \bmod 2^{m-2}$ implies $a = 2^{m-1} - 1$ or $a = 2^m - 1$; if k_1 is even, then $k_1 = 0 \bmod 2^{m-2}$ implies $a = 0$ or $a = 2^{m-1} + 1$. So, the original system has eight solutions, $2^{r+1} = 8$ and $r = 2$.

We now have $H \cong \mathbb{Z}_3 \times \mathbb{Z}_{2^{m-1}} \times \mathbb{Z}_{2^{e_1}} \times \mathbb{Z}_{2^{e_2}}$, where $e_1 + e_2 = m - 1$ and $e_1 \geq e_2$. Now, the result follows for $m = 3$ and 4, so we assume $m \geq 5$. Then, we claim that $e_2 = 1$ and $e_1 = m - 2$. Assume, to the contrary, that $e_2 \geq 2$. Then each factor, except $\mathbb{Z}_3$, has exactly one subgroup of order four, giving $4^3 = 64$ elements of order at most four in the direct product. However, we will show that H has at most 32 solutions to the equation $x^4 = 1$, which will establish our claim and end the proof. To this end, suppose $(a + b\omega)^4 = 1$ for some $a + b\omega \in \mathbb{Z}_{2^m}[\omega]$. Then

$$\begin{cases} a^4 - 6a^2b^2 + 4ab^3 = 1 \bmod 2^m \\ b\left(4a^3 - 6a^2b^2 + b^3\right) = 0 \bmod 2^m. \end{cases}$$

This system has no solutions unless b is even and a is odd, so write $a = 2k_1 + 1$ and $b = 2k_2$, $0 \leq k_1, k_2 \leq 2^{m-1} - 1$. Then the system becomes

$$\begin{cases} k_1(k_1+1)\left(2k_1^2 + 2k_1 + 1\right) - 3(2k_1+1)^2k_2^2 + 4(2k_2+1)k_2 = 0 \bmod 2^{m-3} \\ k_2\left[(2k_1+1)^3 - 6(2k_1+1)^2k_2^2 + 2k_2^3\right] = 0 \bmod 2^{m-3}. \end{cases}$$

The factor in square brackets and $2k_1^2 + 2k_1 + 1$ are odd, reducing the system to

$$\begin{cases} k_1(k_1+1) = 0 \bmod 2^{m-3} \\ k_2 = 0 \bmod 2^{m-3}, \end{cases}$$

which has at most 32 solutions. □

We conclude by summarizing Lemmas 20–22.

Theorem 3. We have

$$\mathbb{Z}_p[\omega]^\times \cong \begin{cases} \mathbb{Z}_6, & \text{if } p = 3 \\ \mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1}, & \text{if } p = 1 \bmod 3 \\ \mathbb{Z}_{p^2-1} & \text{if } p = 2 \bmod 3 \end{cases}$$

and

$$\mathbb{Z}_{p^m}[\omega]^\times \cong \begin{cases} \mathbb{Z}_{p^{m-1}} \times \mathbb{Z}_{p^{m-2}} \times \mathbb{Z}_6, & \text{if } p = 2 \text{ and } m \geq 2 \\ \mathbb{Z}_{p^{m-1}} \times \mathbb{Z}_{p^{m-1}} \times \mathbb{Z}_p[\omega]^\times, & \text{if } p \neq 2. \end{cases}$$

References

[1] J. Gravner and X. Liu, "Periodic Solutions of One-Dimensional Cellular Automata with Random Rules." arxiv.org/abs/1909.06913.

[2] J. Gravner and X. Liu, "One-Dimensional Cellular Automata with Random Rules: Longest Temporal Period of a Periodic Solution." arxiv.org/abs/1909.06914.

[3] J. Gravner and X. Liu, "Weakly Robust Periodic Solutions of One-Dimensional Cellular Automata with Random Rules." arxiv.org/abs/2008.03815.

[4] O. Martin, A. M. Odlyzko and S. Wolfram, "Algebraic Properties of Cellular Automata," *Communications in Mathematical Physics*, **93**(2), 1984 pp. 219–258. doi:10.1007/BF01223745.

[5] K. Cattell, F. Ruskey, J. Sawada, M. Serra and C. R. Miers, "Fast Algorithms to Generate Necklaces, Unlabeled Necklaces, and Irreducible Polynomials over GF(2)," *Journal of Algorithms*, **37**(2), 2000 pp. 267–282. doi:10.1006/jagm.2000.1108.

[6] E. Jen, "Cylindrical Cellular Automata," *Communications in Mathematical Physics*, **118**(4), 1988 pp. 569–590. doi:10.1007/BF01221109.

[7] E. Jen, "Linear Cellular Automata and Recurring Sequences in Finite Fields," *Communications in Mathematical Physics*, **119**(1), 1988 pp. 13–28. doi:10.1007/BF01218258.

[8] T. Chang, I. Song, J. Bae and K. S. Kim, "Maximum Length Cellular Automaton Sequences and Its Application," *Signal Processing*, **56**(2), 1997 pp. 199–203. doi:10.1016/S0165-1684(97)00017-0.

[9] S. Adak, S. Mukherjee and S. Das, "Do There Exist Non-linear Maximal Length Cellular Automata? A Study," in *International Conference on Cellular Automata, ACRI 2018* (G. Mauri, S. El Yacoubi, A. Dennunzio, K. Nishinari and L. Manzoni eds.), Cham, Switzerland: Springer, 2018 pp. 289–297. doi:10.1007/978-3-319-99813-8_26.

[10] P.-h. Guan and Y. He, "Exact Results for Deterministic Cellular Automata with Additive Rules," *Journal of Statistical Physics*, **43**(3), 1986 pp. 463–478. doi:10.1007/BF01020648.

[11] W. Pries, A. Thanailakis and C. Card, "Group Properties of Cellular Automata and VLSI Applications," *IEEE Transactions on Computers*, **35**(12), 1986 pp. 1013–1024. doi:10.1109/TC.1986.1676709.

[12] D. M. Thomas, J. G. Stevens and S. Lettieri, "Characteristic and Minimal Polynomials of Linear Cellular Automata," *The Rocky Mountain Journal of Mathematics*, **36**(3), 2006 pp. 1077–1092. doi:10.1216/rmjm/1181069447.

[13] M. Misiurewicz, J. G. Stevens and D. M. Thomas, "Iterations of Linear Maps over Finite Fields," *Linear Algebra and Its Applications*, **413**(1), 2006 pp. 218–234. doi:10.1016/j.laa.2005.09.002.

[14] S. Wolfram, *A New Kind of Science*, Champaign, IL: Wolfram Media, Inc., 2002.

[15] R. D. Carmichael, "Note on a New Number Theory Function," *Bulletin of the American Mathematical Society*, **16**(5), 1910 pp. 232–238. doi:10.1090/S0002-9904-1910-01892-9.

[16] A. A. Allan, M. J. Dunne, J. R. Jack, J. C. Lynd and H. W. Ellingsen, "Classification of the Group of Units in the Gaussian Integers Modulo *N*," *Pi Mu Epsilon Journal*, **12**(9), 2008 pp. 513–519. www.jstor.org/stable/24345265.

[17] P. J. Davis, *Circulant Matrices*, New York: Wiley, 1979.

[18] E. M. Coven and R. Yassawi, "Embedding Odometers in Cellular Automata," *Fundamenta Mathematicae*, **206**, 2009 pp. 131–138. doi:10.4064/fm206-0-8.

[19] W. J. LeVeque, *Fundamentals of Number Theory*, Dover ed., New York: Dover, 1996.