

σ -Automata and Chebyshev-Polynomials

KLAUS SUTNER

Carnegie Mellon University

Pittsburgh, PA 15213

sutner@cs.cmu.edu

<http://www.cs.cmu.edu/~sutner>

Abstract

A σ -automaton is an additive, binary cellular automaton on a graph. For product graphs such as a grids and cylinders, reversibility and periodicity properties of the corresponding σ -automaton can be expressed in terms of a binary version of Chebyshev polynomials. We will give a detailed analysis of the divisibility properties of these polynomials and apply our results to the study of σ -automata.

1 Introduction

A σ -automaton is a simple, non-uniform, binary cellular automaton on a directed graph. These automata were first studied by Lindenmayer in [8], and later in [1, 10, 13, 14, 2]. Briefly, a σ -automaton consists of a directed graph $G = \langle V, E \rangle$ together with a global rule given by

$$\sigma(X)(v) := \sum_{u \in N(v)} X(u) \bmod 2.$$

Here $X : V \rightarrow \{0, 1\}$ is a *pattern* or *configuration* of the automaton and $N(v)$ denotes the open neighborhood $\{u \in V \mid (u, v) \in E\}$ of vertex v . If the underlying graph is not obvious from context we will write σ_G or $\sigma(G)$ for emphasis. Note that rule σ is well-defined for any locally finite graph. For example, the σ -automaton on the undirected biinfinite path P_∞ is none other than the standard linear CA with rule number 90, see [16]. As usual, we interpret an undirected edge as a pair of opposite directed edges. A closely related class of automata is obtained by modifying rule σ to rule σ^+ : the summation is now over the closed neighborhood $N^+(v) = N(v) \cup \{v\}$. Alternatively, one can think of attaching self-loops to all nodes in the graph. On P_∞ , rule σ^+ corresponds to the linear CA with rule number 150. As observed by Fredkin, both rules have the property that any finite configuration (i.e., a configuration with finite support) will reproduce itself after a sufficient number of iterations.

There is a peculiar difference between σ -automata and σ^+ -automata with respect to their reversibility properties on simple product graphs such as n by m grids, cylinders and tori. For σ -automata, there is a simple characterization of reversibility in terms of the parameters n and m . For example, the n by m grid under rule σ is reversible iff $n + 1$ and $m + 1$ are coprime. No such characterizations are known for σ^+ -automata and it appears difficult to determine reversibility by means other than brute force calculation. The purpose of this paper is to trace the source of these difficulties to determining the position of irreducible polynomials over the 2-element field in a certain canonical enumeration (π_n) of polynomials associated with σ/σ^+ -automata on product graphs. For σ -automata, it suffices to deal with π -polynomials directly, but for σ^+ -automata one has to consider the images of the irreducible factors of these polynomials under the involution $x \mapsto x + 1$. It appears that this involution alters the position of an irreducible polynomial in a rather complicated fashion, and is responsible for the erratic behavior of σ^+ -automata.

The dynamics of a σ -automaton on a graph G can be summarized conveniently by the *state transition diagram* $\mathcal{T}(G)$, also referred to as the *phase space* of the automaton, a directed graph whose vertex set is \mathcal{C}_G , the collection of all patterns over G , and whose edges are of the form $(X, \sigma(X))$. For our discussion, it is helpful to interpret the pattern space \mathcal{C}_G as a vector space over the two-element field F_2 . From the definitions, it follows that both rules σ and $\sigma^+ = \sigma + id$ are linear endomorphisms of these pattern spaces. Over undirected graphs the rules are also self-adjoint, a property that was used in [14, 13] to analyze the phase space of these automata. Due to the linearity of rule σ , the structure is fairly simple: every vertex has out-degree 1 and in-degree either 0 or corank of σ_G , since the predecessors of a vertex form an affine subspace of the pattern space \mathcal{C}_G . The diagram thus consists of cycles and trees which are anchored on these cycles. In particular, for finite graphs G , the σ -automaton over G is reversible iff the diagram is a disjoint union of cycles. The same comments apply to σ^+ -automata. A detailed analysis of the state transition diagrams of rules σ and σ^+ on undirected cycles, as well as higher dimensional analogues, can be found in [10].

We write $d(G)$ for the corank of $\sigma_G : \mathcal{C} \rightarrow \mathcal{C}$, and likewise $d^+(G)$ for rule σ^+ . If the graph G is

given explicitly, say, as an adjacency matrix, then it is trivial to determine the corank of the linear maps σ and σ^+ over \mathcal{C} in time polynomial in the size of G . However, one is usually interested in parameterized families of graphs, such as grids, cylinders, tori and so forth. For these graphs, there is a natural succinct representation in terms of their defining parameters. For example, an n by m grid can be specified in $\log n + \log m$ bits. Therefore, one would like to determine the crucial properties of a σ -automaton or σ^+ -automaton in time polynomial in the size of the succinct representation. For example, the σ -automaton on an m by n grid $P_{m,n}$ has kernel dimension

$$d(P_{m,n}) = \gcd(m+1, n+1) - 1,$$

and therefore the automaton is reversible iff $m+1$ and $n+1$ are coprime; a property that is easily tested in time polynomial in the size of n and m . Similar characterizations exist for cylinders $C_m \times P_n$ and tori $C_m \times C_n$, see [13]. As we already mentioned, no comparable simple characterization are known for the corresponding σ^+ -automata.

In this paper we will focus on determining the reversibility of σ^+ -automata on product graphs of the form $G = H \times P$ where P is a path or a cycle. Let us write P_n and C_n for the undirected path and cycle of length n , respectively, and $P_{m,n} = P_m \times P_n$ for m by n grids. For product graphs $G = H \times P_n$ it is demonstrated in [13] that

$$d(G) = \text{cork } \pi_{n+1}(\sigma(H)),$$

where π_i is a binary version of the Chebyshev polynomials of the second kind. More precisely, $\pi_0 = 0$ and π_i is a polynomial defined by

$$\pi_i(x) := U_{i-1}(x/2) \bmod 2.$$

Alternatively, the generating function G of the sequence (π_i) is given by

$$G(z) = \frac{z}{z^2 + xz + 1}$$

For our purposes, the most convenient representation of these polynomials is in terms of a homogeneous second order recurrence over $F_2[x]$:

$$\pi_{n+2} = x \cdot \pi_{n+1} + \pi_n$$

with initial conditions $\pi_0 = 0$, $\pi_1 = 1$. Note that second order recurrences similar to the last one can also be used to construct reversible cellular automata, a trick going back to Fredkin, see for example [15]. The reversibility of the recurrence in the sense that $\pi_n = x \pi_{n+1} + \pi_{n+2}$ will be important later.

In their recent paper [2], Barua and Ramakrishnan show that m by n grids under rule σ^+ are reversible iff the two polynomials $\pi_{m+1}(x)$ and $\pi_{n+1}(1+x)$ are coprime. We will extend their results to show that

$$d^+(P_{m,n}) = \deg \gcd(\pi_{m+1}(x), \pi_{n+1}(1+x)).$$

Moreover, it can be seen that π_{m+1} is the minimal polynomial of the linear map $\sigma(P_m)$. Thus, the reversibility of σ^+ -automata on grids depends on divisibility properties of polynomials, rather than integers as for σ -automata. In fact, reversibility of σ -automata can also be expressed in terms of π -polynomials: $\gcd(m+1, n+1) - 1$ is none other than the degree of $\gcd(\pi_{m+1}, \pi_{n+1}) = \pi_{\gcd(m+1, n+1)}$. Extensions of these results to higher-dimensional automata can be found in the forthcoming [3].

In order to shed some light on reversibility conditions, we will study the divisibility properties of π -polynomials in some detail. As it turns out, for odd n , π_n can be written as a product $\pi_n = \prod_{d|n} \rho_d$ where ρ_d is the square of a product of certain irreducible polynomials, referred to as the *critical factors* of π_n . A similar representation can be found for even n . In our setting, it is crucial that every irreducible polynomial τ occurs as a factor of some π -polynomial. Hence, we can define the *depth* of τ to be the least n such that τ divides π_n . We will show that the depth d of τ divides $2^k \pm 1$, where k is the degree of τ . In fact, the degree of τ turns out to be the suborder of 2 in the multiplicative group \mathbb{Z}_d^* . Hence, the depth of τ is bounded by $2^k + 1$ where k is the degree of τ . As we will see, this bound is tight.

Note that as a consequence of the characterization of the degree in terms of the suborder of 2, all irreducible polynomials of the same depth must have the same degree; but not conversely. This turns out to be the major obstacle in generalizing the description of the kernel dimension in grids under rule σ to rule σ^+ . The involution $x \mapsto 1 + x$ changes the depth of the irreducible factors of π_{n+1} in a rather complicated fashion, see the table 2 in the appendix for the depth values of irreducible polynomials of degree 8. Consequently, there appears to be no easy way to compute the GCD of two polynomials $\pi_{m+1}(x)$ and $\pi_{n+1}(1+x)$.

The reader may also wish to compare these polynomials to another variation of binary Chebyshev polynomials discussed in [4] on page 118. The inductive definition there takes the form $\rho_n = \rho_{n-1} + x\rho_{n-2}$. Many of the divisibility properties of the π -polynomials are shared by the ρ -polynomials.

Binary Chebyshev polynomials are also useful in the study of automata on infinite grids of the form $H_\infty := H \times P_\infty$. We can think of the σ -automaton H_∞ as an additive one-dimensional cellular automaton of width 3 over the alphabet $\{0, 1\}^{V(H)}$, where $V(H)$ denotes the vertex set of H . One can easily show that $d(H_\infty) = 2 \cdot d(H)$. As it turns out, all patterns in the kernel of $\sigma(H_\infty)$ are periodic. We denote the maximal period of any kernel pattern by $\text{per}(H)$ and likewise by $\text{per}^+(H)$ for σ^+ -automata. Computing the period of a σ -automaton with $H = P_m$ is easy: it is always equal to $2m + 2$. For the analogous σ^+ -automata, on the other hand, periods and weak periods are much harder to describe and we can only give a somewhat indirect description in terms of the depth function mentioned above.

More precisely, define the *weak period* $\text{wper}(H)$ of H to be the least p such that $\pi_p(\sigma(H)) = 0$; $\text{wper}^+(H)$ is defined analogously. It is easy to see that $\text{per}(H) = \text{wper}(H)$ or $\text{per}(H) = 2 \text{wper}(H)$. In particular for σ -automata with $H = P_m$ we have $\text{per}(P_m) = 2(m + 1) = 2 \text{wper}(P_m)$. Barua and Ramakrishnan verify a conjecture from [13] which states that

$$\text{wper}^+(P_{2^k-1}) = 3 \cdot 2^{k-1}$$

for all k . We will show that $\text{per}^+(P_{2^k-1}) = 3 \cdot 2^k$. In fact, the last assertion is a simple corollary to theorem 3.1 below, which shows how to express the periods of paths P_m under rule σ^+ in terms of the depth function.

This paper is organized as follows. In section 2 we introduce π -polynomials in $F_2[x]$ and determine their basic divisibility properties. In the next section, we consider related shift register sequences over F_q . In particular we will show that every irreducible polynomial occurs as a factor of one of the π -polynomials. We also obtain simple representations of these shift register sequences. The next section deals with linear operators of the form $\pi_n(\sigma(P_m))$ and shows how to compute their coranks. We then apply these results to the problem of determining the reversibility of the σ -automaton on $P_{m,n}$ in section 5. In section 6 we briefly indicate how our results can be generalized to σ -automata

on cylinders. The last section concludes with a few open problems. The appendix contains tables of the π -polynomials (or rather: their essential irreducible factors, see below) up to π_{51} , their counterparts under the involution $x \mapsto 1 + x$ on $F_2[x]$, and their depths.

Background information from linear algebra and the theory of finite fields can be found in, say, [6], [11] or [7]. The second and third reference and Berlekamp's classic text on coding theory [4] both contain a careful discussion of the relationship between shift registers and finite fields.

2 Binary Chebyshev Polynomials

Consider the sequence of π -polynomials π_n , $n \geq 0$, over $F_2[x]$ given by $\pi_0 = 0$ and

$$\pi_i(x) := U_{i-1}(x/2) \bmod 2,$$

where U_n denotes the n -th Chebyshev polynomial of the second kind. A little calculation shows that

$$\pi_n(x) = \sum_i \binom{n+i}{2i+1} x^i \bmod 2.$$

Thus, the coefficients of the π -polynomials are closely related to the well-known pattern of binomial coefficients modulo 2. Figure 1 below shows a plot of the first 100 π -polynomials.

By Lucas' theorem [9], $\binom{x}{y} \bmod 2 = \prod \binom{x_i}{y_i} \bmod 2$, where x_i is the i -th digit in the binary expansion of x , and likewise for y . Thus, the coefficients of π_n can be computed in constant time, at least for machine sized integers n . This representation can be used to establish proposition 2.1 below, but the necessary calculations are rather tedious. For example, one can see that $\pi_{2^k} = x^{2^k-1}$.

For our purposes, the most useful representation of π -polynomials is in terms of a second order homogeneous recurrence over $F_2[x]$:

$$\begin{aligned} \pi_0 &= 0, \\ \pi_1 &= 1, \\ \pi_n &= x \cdot \pi_{n-1} + \pi_{n-2}. \end{aligned} \tag{1}$$

As mentioned earlier, the recurrence is reversible in the sense that $\pi_{n-2} = x \pi_{n-1} + \pi_n$. We will also have occasion to study the same recurrence over other algebraic structures such as finite fields F_{2^k} and endomorphism rings $End(\mathcal{C})$ where \mathcal{C} is a finite vector space over F_2 . Note that the reversibility of equation (1) is preserved over these structures, and therefore the corresponding sequences must all be periodic. For the time being, though, we only consider polynomials over F_2 .

We hasten to point out that the numbering of the polynomials differs from the one used in [13] and [2]; the polynomials there begin with $\pi_0 = 1$ (i.e., in the old numbering $\pi_i(x) = U_i(x/2) \bmod 2$). As it turns out, the current numbering makes it easier to state some of the divisibility properties.

Our interest in these polynomials in connection with σ -automata comes from the fact that for product graphs $G = H \times P_n$, every pattern X in the kernel of σ_G is already completely determined by its first row $X_1 = \text{row}_1(X)$. Here we assume that patterns are represented by m by n matrices over F_2 , where m is the cardinality of H . The partial patterns are given by $X_i = \pi_i(X_1)$, and the complete pattern (X_1, X_2, \dots, X_n) lies in the kernel of σ_G iff $\pi_{n+1}(\sigma_H)(X_1) = 0$. In particular, σ_G is reversible iff the map $\pi_{n+1}(\sigma_H)$ is injective.

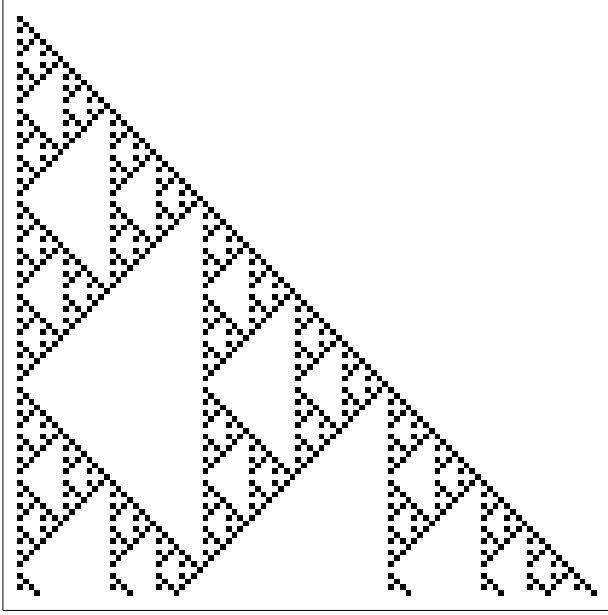


Figure 1: A plot of the coefficients of the first 100 π -polynomials. A box indicates a 1, and a blank a 0. The low-order terms are on the left.

The basic divisibility properties of binary Chebyshev polynomials are shared by a whole class of recurrences over $F[x]$. In fact, the following proposition holds in any Euclidean domain; see also [2] for a direct proof for π -polynomials.

Proposition 2.1 *Let $a, b \in F[x]$ be coprime, where F is an arbitrary finite field. Define a sequence (τ_n) in $F[x]$ by $\tau_0 = 0$, $\tau_1 = 1$, and $\tau_n = a \cdot \tau_{n-1} + b \cdot \tau_{n-2}$, for all $n \geq 2$. Then*

$$\begin{aligned} \tau_p &= \tau_{q+1}\tau_{p-q} + b \cdot \tau_q\tau_{p-q-1}, \\ \gcd(\tau_n, \tau_m) &= \tau_{\gcd(n,m)}, \\ \tau_{2^k n} &= a^{2^k - 1} \tau_n^{2^k}, \\ \tau_{2n+1} &= \tau_{n+1}^2 + b \cdot \tau_n^2. \end{aligned}$$

where $p \geq q + 1$.

The proofs are straightforward by induction and will be omitted. Note that for the binary Chebyshev polynomials we have $a = x$ and $b = 1$, so that the last two equations can also be written as

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

Also note that as a consequence of the second equation, $m \mid n \iff \pi_m \mid \pi_n$.

2.1 Factoring π -Polynomials

From the last proposition, it is trivial to determine the GCD of π -polynomials. As we will show in section 5, in connection with σ^+ -automata it is necessary to compute GCDs of the form $\gcd(\pi_i(x), \pi_j(x+1))$. To this end, we will now determine how π -polynomials factor into irreducible components. We will see later that indeed all irreducible polynomials over F_2 occur as factors of some π -polynomial. For the time being, note that except for $\tau = x = \pi_2$, all irreducible factors τ must first occur at odd levels by proposition 2.1. Furthermore, since π_{2n+1} is a square by the same corollary, all irreducible factors in π_{2n+1} must occur at least squared. Define the *depth* of an irreducible polynomial $\tau \in F_2[x]$ to be

$$\text{dep}(\tau) := \min(n \mid \tau \text{ divides } \pi_n),$$

whenever such an n exists, and let

$$\rho_n := \prod_{\text{dep}(\tau)=n} \tau^2$$

be the squared product of all irreducible factors that occur at level n for the first time. For the sake of completeness, let $\rho_1 = \pi_1 = 1$. We will refer to ρ_n as the *critical term* of π_n . Note that ρ_n may be a product of squares of irreducible factors; e.g., $\rho_{17} = (1 + x + x^4)^2 (1 + x + x^2 + x^3 + x^4)^2$.

The remainder of this section is devoted to a proof of the following characterization of the π -polynomials in terms of their irreducible factors. Let ϕ denote Euler's totient function.

Theorem 2.1 *For all positive $n = 2^k p$, where p is odd,*

$$\pi_n(x) = x^{2^k-1} \prod_{d|p} \rho_d^{2^k}(x) = x^{2^k-1} \prod_{d|p} \rho_d(x^{2^k}).$$

Furthermore, $\deg \rho_d = \phi(d)$ unless $d = 1$.

Möbius inversion allows one to compute the critical factors in terms of the π -polynomials: $\rho_n = \prod_{d|n} \pi_{n/d}^{\mu(d)}$, again for all odd numbers n , where μ denotes the Möbius function.

Proof. (Of theorem 2.1.)

The first step is to show that whenever a critical term ρ_d divides a π -polynomial π_n , then all of π_d also divides ρ_n .

Claim 1: Let τ be an irreducible factor of depth d . Then $\tau \mid \pi_n$ implies that $\pi_d \mid \pi_n$.

If $\tau \mid \pi_n$, then, by the last proposition, $\tau \mid \gcd(\pi_d, \pi_n) = \pi_{\gcd(d,n)}$. But then, by the definition of depth, $d \leq \gcd(n, d)$, and it follows that indeed $d = \gcd(d, n)$, whence $\pi_d \mid \pi_n$.

As a consequence, $\rho_d \mid \pi_n$ iff $d \mid n$. It follows that every π -polynomial π_n is a product of powers of terms ρ_d where $d > 1$ ranges over the divisors of n , and it remains to determine the exponents. For even n we can use proposition 2.1 to reduce the problem of finding a decomposition for π_n to the problem of finding a decomposition for π_p where $n = 2^k p$, p odd. Thus, we only have to show that $\text{mult}_{\rho_d}(\pi_p) = 1$ for p odd, $d > 1$. Here $\text{mult}_a(b) := \max(i \mid a^i \text{ divides } b)$ denotes the multiplicity of a in b . To this end, write $\Delta_n := \pi_{n+1} + \pi_n$ so that $\pi_{2n+1} = \Delta^2$. We have to show that the polynomials Δ_n contain no square factors.

Claim 2: The polynomials Δ_n are square-free, for all n .

It suffices to prove that polynomial Δ_n and its formal derivative Δ'_n are coprime, for all n . Here is the argument for n even, the odd case is entirely similar. For $n = 2m$,

$$\Delta'_n = \pi'_{n+1} + \pi'_n = \pi'_n = \pi_m^2.$$

Now suppose τ is an irreducible factor dividing both Δ_n and Δ'_n . Then τ divides π_m and therefore π_n . But then τ must also divide π_{n+1} , and, by the last proposition, $\text{dep } \tau$ divides both n and $n+1$. Thus, $\text{dep } \tau = 1$, $\tau = 1$, and we are done.

To complete the proof of the theorem it now remains to verify that the degree of ρ_n is $\phi(n)$, for all odd $n > 1$, the case $n = 2$ being trivial. We have already seen that $\pi_n = \prod_{d|n} \rho_d$ for odd n . By induction we get

$$\deg \rho_n = n - 1 - \sum_{d|n, 1 < d < n} \rho_d = n - 1 - \sum_{d|n, 1 < d < n} \phi(d) = \phi(n),$$

since $\sum_{d|n} \phi(d) = n$. □

As an example of theorem 2.1, we consider π_{300} . We have the factorization

$$\begin{aligned} \pi_{300} = & x^3 (1+x)^8 (1+x+x^2)^8 (1+x^3+x^4)^8 \\ & (1+x+x^2+x^3+x^5+x^6+x^{10})^8 (1+x^3+x^4+x^5+x^9+x^{12}+x^{13}+x^{15}+x^{20})^8 \end{aligned}$$

where the irreducible terms are associated with divisors 2, 3, 5, 15, 25, and 75, respectively. All critical factors are squares of just one irreducible term in this case.

3 The Depth of an Irreducible Polynomial

We now show that all irreducible polynomials over F_2 occur as factors of some π -polynomial, so that the depth function from the last section is indeed well-defined for all irreducible polynomials. To this end, consider $\tau \in F_2[x]$ irreducible of degree k . Set $q := 2^k$ and let α be a root of τ in the splitting field F_q . Substituting, we obtain a sequence $s_i := \pi_i(\alpha)$ in F_q given by the second order homogeneous recurrence

$$s_{n+2} = \alpha s_{n+1} + s_n \tag{2}$$

with initial conditions $s_0 = 0$, $s_1 = 1$. Thus, (s_i) is a feedback shift register sequence or linear recurrent sequence, see [4] and [7] for a wealth of background information. We will frequently use results from these sources without further mention. Since the coefficient of s_n in the recurrence is 1, the sequence must be periodic. By our choice of initial conditions, our sequence is the impulse response sequence associated with recurrence (2), and therefore maximizes the period of all such sequences. Needless to say, the period of sequence (2) is none other than the depth d of polynomial τ : $0 = s_d = \pi(\alpha) \in F_q \simeq F_2[x]/(\tau)$. Thus we have the following lemma.

Lemma 3.1 *Every irreducible polynomial in $F_2[x]$ occurs as a factor of some π -polynomial.*

Note that the basic building block of the sequence is a palindrome: $s_i = s_{d-i}$ for all $0 \leq i \leq d$. To obtain more information about the depth of an irreducible polynomial over F_2 , consider the companion matrix of recurrence (1). Over F_q , the companion matrix takes the form $\begin{pmatrix} 0 & 1 \\ 1 & \alpha \end{pmatrix}$, and the depth of τ must be a divisor of the order of A in $\text{GL}(2; F_q)$. The latter is well-known to be $q(q-1)(q^2-1)$. In fact, one can obtain a slightly stronger result: the order of A is a divisor of $2\text{lcm}(q-1, q+1)$, see [12].

Since we can rule out the factor 2, the depth of an irreducible polynomial must actually be a divisor of $q-1$ or $q+1$. To determine which irreducible polynomials give rise to depths dividing $q-1$ and which have depth dividing $q+1$, consider the characteristic polynomial of recurrence (2):

$$f(z) := z^2 + \alpha z + 1 \in F_q[z]. \quad (3)$$

We have chosen z as the indeterminate to avoid confusion with the irreducible polynomial $\tau(x)$.

In the splitting field of f we can obtain the following simple representation of the shift register sequence (s_n) . Since f is an affine polynomial, its roots form an affine subspace of the splitting field. In this case, it is easy to see that the roots must have the form β_1 and $\beta_2 = \alpha + \beta_1 = 1/\beta_1$. If f splits over F_q , then the shift register sequence (s_i) can be represented thus, see [7]:

$$s_n = (\beta_1^n + \beta_2^n)/\alpha. \quad (4)$$

It follows immediately that the period of (s_i) , and thus the depth of τ , the order of β_1 , and in particular a divisor of $q-1$, the order of the multiplicative subgroup of F_q .

Suppose, on the other hand, that f is irreducible over F_q . Then f splits over F_{q^2} , and the shift register sequence can be represented in the form $s_n = \theta\beta_1^n + (\theta\beta_1^n)^q$ where β_1 is a root of f and θ an element of F_{q^2} . Note that the sum is the trace of $\theta\beta_1^n$ from F_{q^2} to F_q and the conjugate β_1^q is none other than the second root $\beta_2 = 1/\beta_1$. A little calculation shows that $\theta = 1/\alpha \in F_q$, so that the representation from equation (4) still holds. Hence, the depth of τ is the order of β_1 in the multiplicative subgroup of F_{q^2} , and, since $\beta_1^q = 1/\beta_1$, a divisor of $q+1$.

Given τ , it is easy to check whether f splits over F_q .

Lemma 3.2 *The characteristic polynomial of recurrence (2) is irreducible over F_q iff the linear term in τ is 0.*

Proof. Let f be the characteristic polynomial as in equation (3). By the characteristic 2 version of Stickelberger's theorem, see [4], f has two irreducible factors iff the trace of $1/\alpha$ is 0. Lastly, the absolute trace over F_q of $1/\alpha$ is the coefficient of x^{k-1} in the minimal polynomial of $1/\alpha$, which is none other than the coefficient of x in the reciprocal polynomial τ . \square

We note in passing that one can find a reasonably explicit description of the roots of the characteristic polynomial f in the case where f splits over F_q . Consider any element $\theta \in F_q$ such that $\text{Tr } \theta = 1$ and let $\gamma := 1/\alpha^2$. Define

$$\beta' := \sum_{i=1}^{m-1} \theta^{2^i} \sum_{j=0}^{i-1} \gamma^{2^j}$$

Then $\alpha\beta'$ is a root of f , as one can verify via a simple calculation. In particular for m odd we can choose $\theta = 1$, so that

$$\alpha(\alpha^{-4} + \alpha^{-16} + \dots + \alpha^{-2^{m-1}})$$

is a root of f .

It remains to pin down the relationship between the degree of an irreducible polynomial and its depth a little more carefully. Recall that the *suborder* of 2 in the multiplicative group \mathbb{Z}_n^* , n odd, is defined as $\text{sord}_n(2) = \min(i \mid 2^i \equiv \pm 1 \pmod{n})$. Clearly, $\text{sord}_n(2)$ is either the same as the standard order of 2 in \mathbb{Z}_n^* , or half that value. We will show that degree of an irreducible polynomial is the suborder of 2 in \mathbb{Z}_d^* , where d is the depth of the polynomial.

Theorem 3.1 *Let $\tau \in F_2[x]$ be an irreducible polynomial of degree k and d its depth. Letting $q = 2^k$, d divides $q - 1$ iff the linear term in τ vanishes, and $q + 1$ otherwise. In either case, k is the suborder of 2 in the multiplicative group \mathbb{Z}_d^* .*

Proof. The first claim of the theorem follows immediately from the last lemma and the preceding comments. Letting $l := \text{sord}_d(2)$, we conclude that $l \leq k$.

Setting $r := 2^l$, a simple induction shows that

$$\begin{aligned}\pi_{r-1} &= \sum_{1 \leq i \leq l} x^{r-2^i} \\ \pi_{r+1} &= \pi_{r-1} + x^r.\end{aligned}$$

We will need the following technical claim.

Claim: Let $K \subseteq L \subseteq M$ be a tower of finite fields where $K = F_2$, $L = F_{2^l}$ and $M = F_q$. Let b be an element of M such that $\text{Tr}_K^L b = c \in K$. Then $b \in L$.

To verify the claim, consider the Frobenius homomorphism $h(z) = z^2$ of L/K . Thus,

$$c = \text{Tr}_K^L b = \sum_{0 \leq i < l} h^i(b).$$

Applying h we obtain

$$h(c) = c = \sum_{1 \leq i \leq l} h^i(b).$$

Adding, we find $b = b^{2^l}$. But then b must lie in L , the fixed field of h^l , the Frobenius homomorphism of M over L .

We can now establish the second part of the theorem as follows. Suppose for the sake of a contradiction that $l = \text{sord}_d(2) < k$. As before, we write α rather than x to denote a root of τ in the splitting field F_q .

First assume that d divides $2^l - 1$. It is easy to see that l must then divide k . Hence, F_{2^l} is a subfield of F_q . Then

$$0 = s_{2^l-1} = \sum_{1 \leq i \leq l} \alpha^{2^l-2^i} = \alpha^{2^l} \sum_{1 \leq i \leq l} (1/\alpha)^{2^i}.$$

Thus, the trace of $1/\alpha$ from F_{2^l} to F_2 is 0. From the claim, it follows that $1/\alpha$ lies in the proper subfield F_{2^l} , therefore α lies in the same subfield, and we have the desired contradiction.

It remains to deal with the situation $d \mid 2^l + 1$ for some $l < k$. In this case, $0 = s_{2^l+1} = s_{2^l-1} + \alpha^{2^l}$. Hence, $0 = \alpha^{2^l}(1 + \sum_{1 \leq i \leq l} (1/\alpha)^{2^i})$ and again we obtain a contradiction via our claim. \square

As a consequence of the last theorem, all irreducible factors of a critical factor ρ_n must have the same degree. Furthermore, all linear terms must have the same coefficient. Since ρ_n has degree $\phi(n)$, the number of irreducible factors in ρ_n is $\phi(n)/(2 \text{sord}_n(2))$. The relation $\deg \tau = \text{sord}_{\text{dep } \tau}(2)$ leaves an exponential range of possibilities for the depth of an irreducible polynomial. The only bounds immediately available are $2k + 1 \leq \text{dep } \tau \leq 2^k + 1$ where k is the degree of τ . The upper bound is tight. It appears that for each d such that $\text{sord}_d(2) = k$ there exists an irreducible polynomial of degree k whose depth is d . For example, table 3 in the appendix shows all 30 irreducible polynomials of degree 8 and their depths. The possible choices for d are 51, 85, 255 and 257 in this case.

4 The Minimal Polynomial of $\sigma(P_m)$

We now return to the discussion of σ -automata over product graphs $G = H \times P_n$. Let \mathcal{C} be the pattern space of H and let f be any endomorphism of \mathcal{C} as an F_2 vector space. Then the map $F_2[x] \rightarrow \text{End}(\mathcal{C})$, $x \mapsto f$, is a homomorphism into a finite ring. Hence, the sequence $(\pi_i(f))$ is periodic. We are here interested in the case $f = \sigma(P_m)$ or $f = \sigma^+(P_m)$. To lighten notation, we write S_m for $\sigma(P_m)$ and $S_m^+ = S_m + id$ for $\sigma^+(P_m)$. The following basic properties of $\pi_n(S_m)$ are obvious from our previous discussion.

Proposition 4.1 *For all $n \geq m \geq 1$ we have the following basic symmetry properties:*

$$\begin{aligned} \text{cork } \pi_{n+1}(S_m) &= \text{cork } \pi_{m+1}(S_n), \\ \text{cork } \pi_{n+1}(S_m) &= \text{cork } \pi_{(n+1)-(m+1)}(S_m) \\ &= \text{cork } \pi_{\text{gcd}(n+1, m+1)}(S_m). \end{aligned}$$

The crucial connection between binary Chebyshev polynomials and rule σ on paths is the fact that the minimal polynomial of $\sigma(P_m)$ is π_{m+1} . Using a geometric argument, it is shown in [13] that π_{m+1} is an annihilator of S_m . As pointed out in [2], this fact follows immediately from the Caley-Hamilton theorem since π_{m+1} is none other than the characteristic polynomial of S_m . We will now show that π_{m+1} is indeed the minimal polynomial of S_m .

For the proof of minimality, it is convenient to use the following notation system for vectors in $v \in F_2^m$. Let $\{1, 2, \dots, m\}$ be the standard basis and write correspondingly for any non-zero vector v : $v = v[1] + v[2] + \dots + v[k]$, where $1 \leq v[1] < v[2] < \dots < v[k] \leq m$. We will refer to k as the length of v .

Lemma 4.1 *π_{m+1} is the minimal polynomial of S_m .*

Proof. From the preceding discussion, it suffices to show that no polynomial of degree $d < m$ annihilates S_m . To see this, note that $S_m^i(1) = v[1] + v[2] + \dots + v[r] + (i+1)$ for all $0 \leq i < m$: S_m is the sum of a right and a left shift with fixed boundary conditions. But then, for any polynomial τ of degree $d < m$, we have $\tau(S_m)(1) = v[1] + v[2] + \dots + v[r] + d \neq 0$, since the contribution of the leading term cannot be canceled by lower order terms. \square

The critical terms of π_{m+1} are coprime by definition, hence we have the following fact.

Proposition 4.2 *Let $m + 1 = 2^k p$ where p is odd. Then*

$$m = \text{cork } \pi_{m+1}(S_m) = \text{cork } x^{2^k-1}(S_m) + \sum_{d|p} \text{cork } \rho_d^{2^k}(S_m).$$

Lemma 4.2 *Let τ be any polynomial of degree d where $1 \leq d \leq m$. Then $\text{cork } \tau(S_m) \leq \text{deg } \tau$.*

Proof. Suppose that v_1, \dots, v_d is a collection of linearly independent elements of the kernel of $\tau(S_m)$. As in lemma 4.1, it follows that $1 \leq v_i[1] \leq d$ for all $i = 1, \dots, d$. From linear algebra, we obtain a new basis v'_1, \dots, v'_d such that $v'_i[1] = i$, and $d < v'_i[2] \leq m$ or the length of v'_i is only 1.

Now suppose u is a kernel element not contained in the linear hull of v'_1, \dots, v'_d . Then there is a linear combination w of v'_1, \dots, v'_d such that $(u + w)[1] > d$. But then, by the standard argument, $\tau(S_m)(u + v) \neq 0$, contradiction. \square

Lemma 4.3 *For any factor τ of π_{m+1} , we have $\text{cork } \tau(S_m) = \text{deg } \tau$.*

Proof. First note that it suffices to establish the claim for factors $\tau = \tau_0^e$ where τ_0 is irreducible, since corank is additive on orthogonal factors. So let $m + 1 = 2^k p$ where p is odd. From proposition 4.2 and lemma 4.2 we have

$$\begin{aligned} m &= \text{cork } x^{2^k-1}(S_m) + \sum_{d|p} \sum_{\text{dep } \tau=d} \text{cork } \tau^{2^{k+1}}(S_m) \\ &\leq 2^k - 1 + 2^k \sum_{d|p} \phi(d) = m. \end{aligned}$$

Hence, equality holds everywhere and we have $\text{cork } x^{2^k-1}(S_m) = 2^k - 1$ and $\text{cork } \tau^{2^{k+1}}(S_m) = 2^k \text{deg } \tau$. For the sake of simplicity we will only consider the irreducible terms $\tau \neq x$, the argument for x is entirely similar.

So suppose τ is any irreducible factor of π_{m+1} and write $f := \tau(S_m)$ to lighten notation. It follows from linear algebra that $\text{cork } f^j \leq j \text{cork } f$ for all j . But then $\text{cork } f^j = j \text{cork } f = j \text{deg } \tau$ for all $j \leq 2^{k+1}$, as required. \square

Since P_m is undirected, the map $f = \tau(S_m)$ in the last proof is self-adjoint. It follows that $\text{cork } f^2 = 2 \text{cork } f$ iff $\ker f \subseteq \text{rg } f = (\ker f)^\perp$, and likewise for higher powers of f . This will be used again in theorem 5.2.

We can now determine the corank of any map $\tau(S_m)$ in terms of the GCD of τ and the minimal polynomial of S_m .

Theorem 4.1 *Let τ be an arbitrary polynomial in $F_2[x]$. Then*

$$\text{cork } \tau(S_m) = \text{deg } \gcd(\tau, \pi_{m+1}). \tag{5}$$

Proof. We will first show that factors of τ that are orthogonal to π_{m+1} do not contribute to the corank of $\tau(S_m)$.

Claim 1: $\text{cork } \tau(S_m) = 0$ iff τ and π_{m+1} are coprime.

First suppose that τ and π_{m+1} have a nontrivial common factor τ_0 . Then, by the last lemma, $\text{cork } \tau(S_m) \geq \tau_0(S_m) = \deg \tau_0 > 0$. On the other hand, suppose that τ and π_{m+1} are coprime. Since $\tau\pi_{m+1}$ is an annihilator of S_m we have $m = \text{cork } \tau\pi_{m+1}(S_m) = \text{cork } \tau(S_m) + \text{cork } \pi_{m+1}(S_m)$. But the last term is m , so that $\text{cork } \tau(S_m) = 0$, as required.

It follows from claim 1 that the corank of $\tau(S_m)$ is the same as the corank of $\prod \delta^e(S_m)$ where the product is over all irreducible divisors δ of π_{m+1} , and $e = \text{mult}_\delta(\tau)$. By orthogonality, $\text{cork } \tau(S_m) = \sum \text{cork } \delta^e(S_m)$.

Claim 2: For all irreducible divisors δ of π_{m+1} : $\text{cork } \delta^e(S_m) = \min(e, \text{mult}_\delta(\tau)) \deg \delta$.

As in the last lemma, write $f := \delta(S_m)$. We have already shown that $\text{cork } \delta^e(S_m) = e \deg \delta$ as long as $e \leq e_0 := \text{mult}_\delta(\tau)$. For $e \geq e_0$ we have $m = \text{cork } \delta^e(S_m) + \text{cork } \theta(S_m)$ where $\theta := \pi_{m+1}/\delta^{e_0}$. But then $\text{cork } \delta^e(S_m) = e_0 \deg \delta$ and we are done.

By the second claim, $\text{cork } \tau(S_m) = \sum_\delta \min(\text{mult}_\delta(\tau), \text{mult}_\delta(\pi_{m+1})) \deg \delta = \deg \gcd(\tau, \pi_{m+1})$. This completes the proof of the theorem. \square

Since π_{m+1} is the minimal polynomial of S_m , we can decompose the pattern space F_2^m of P_m into a direct sum of subspaces E_i , associated with the invariant factors of π_{m+1} . For example, if $m = 2p$ is even, the invariant factors take the form $(\tau_1 \dots \tau_r)(S_m)$ and $(\tau_1 \dots \tau_r)^2(S_m)$. The invariant subspace of the first map has dimension p and consists of all symmetric patterns X such that $X(p+1) = 0$. As a $F_2[x]$ -submodule, it is generated by the pattern $1 + m$. For $m+1 = 2^k p$ we have symmetric patterns associated with $\pi_{(m+1)/2}(S_m)$, double symmetric ones associated with $\pi_{(m+1)/4}(S_m)$, and so forth. Invariant subspaces will be used in the proof of theorem 5.2 below.

5 π^+ -Polynomials

The last theorem gives a complete characterization of the coranks of a σ -automata on a grid. Indeed, the description of the corank of $S_{n,m}$ in [13, 2] can be rephrased as follows:

$$d^+(P_{n,m}) = \deg \pi_{n+1}(S_m) = \deg \gcd(\pi_{n+1}, \pi_{m+1}) = \deg \pi_{\gcd(n+1, m+1)} = \gcd(n+1, m+1) - 1.$$

In order to extend this result to σ^+ -automata, first note the following basic symmetry properties.

Proposition 5.1

$$\begin{aligned} \text{cork } S_{n,m}^+ &= \text{cork } \pi_{n+1}(S_m^+) = \text{cork } \pi_{m+1}(S_n^+) \\ &= \text{cork } \pi_{n+1}^+(S_m) = \text{cork } \pi_{m+1}^+(S_n). \end{aligned}$$

Here $\pi_n^+(x) := \pi_n(1+x)$. It is advantageous to consider π_n^+ as the result of applying the endomorphism $F_2[x] \rightarrow F_2[x]$ induced by $x \mapsto 1+x$ to π_n . In keeping with previous notation, we will write τ^+ for the image of polynomial τ under this map. Now $+$ is an involution, so the π^+ -polynomials inherit the divisibility properties of the π -polynomials. For example, $\pi_m^+ | \pi_n^+$ iff $m | n$. Moreover, all irreducible polynomials occur as factors of some π^+ -polynomial. We can think of the involution

$+$ as acting on the endomorphism ring $\text{End}(\mathcal{C})$: $\sigma^+ = \sigma + id$. Hence, it follows from lemma 4.1 that π_{m+1}^+ is the minimal polynomial of S_m^+ :

$$\tau^+(S_m^+) = \tau^+(S_m + id) = \tau^+(1 + x)(S_m) = \tau^{++}(S_m) = \tau(S_m).$$

Theorem 4.1 allows one to determine the corank of $S_{n,m}^+$ as follows.

Theorem 5.1 *For all positive n and m :*

$$d^+(P_{n,m}) = \deg \gcd(\pi_{n+1}^+, \pi_{m+1}) = \deg \gcd(\pi_{n+1}, \pi_{m+1}^+).$$

Proof. Since the second claim follows from the first by symmetry, it suffices to prove the first equation. But $\text{cork } S_{n,m}^+ = \text{cork } \pi_{n+1}^+(S_m) = \deg \gcd(\pi_{n+1}^+, \pi_{m+1})$, by the last theorem, and we are done. \square

For a few special values of n and m one can determine $d^+(P_{n,m})$ completely from theorem 5.1, see also theorem 4.6 of [2].

Corollary 5.1 *For $m + 1 = 2^k$ and $n + 1 = 2^l p$, p odd, we have*

$$d^+(P_{n,m}) = \begin{cases} 0 & \text{if } 3 \nmid n + 1, \\ 2^{l+1} & \text{if } l < k - 1, \\ 2^k - 1 & \text{otherwise.} \end{cases}$$

Corollary 5.2 *For $m + 1 = 2^k \cdot 3$ and $n + 1 = 2^l p$, p odd, we have*

$$d^+(P_{n,m}) = \begin{cases} 0 & \text{if } 2, 3 \nmid n + 1, \\ 2^l - 1 & \text{if } l \leq k + 1, 3 \nmid n + 1 \\ 2^{k+1} & \text{if } l > k + 1, 3 \nmid n + 1 \\ 3 \cdot 2^l - 1 & \text{if } l + 1 < k, 3 \mid n + 1 \\ 2^l - 1 + 2^k - 1 & \text{if } k - 1 \leq l \leq k + 1, 3 \mid n + 1 \\ 3 \cdot 2^k - 1 & \text{if } l \geq k + 2, 3 \mid n + 1 \end{cases}$$

In general, though, there seems to be no simple way to determine GCDs of the π^+ -polynomials and π -polynomials as a function of the parameters m and n .

5.1 Reversible Grids

Consider the somewhat easier problem of determining all reversible σ^+ -automata on an m by n grid where m is fixed. As we have seen, reversibility of the σ^+ -automaton on $P_{m,n} = P_m \times P_n$ is equivalent to π_{m+1}^+ being coprime to π_{n+1} . The latter condition can be expressed as a divisibility condition on $n + 1$.

Lemma 5.1 *Fix $m \geq 1$. Then there are positive integers t_1, \dots, t_r such that the σ^+ -automaton on $P_{m,n}$, $n \geq m$, is reversible iff t_i does not divide $n + 1$, for all $i = 1, \dots, r$.*

Proof. As usual, write $m + 1 = 2^k p$ where p is odd and let $q = 2^k$. Then

$$\pi_{m+1} = x^{q-1} \prod_{1 \leq i \leq r} \tau_i^{2q}$$

for certain irreducible polynomials τ_1, \dots, τ_r . Set $\tau_0 := x$ and let $t_i := \text{dep } \tau_i^+$ for $i = 0, \dots, r$. Then the σ^+ -automaton on $P_{m,n}$ is reversible iff t_i does not divide $n + 1$, for all $i = 0, \dots, r$.

To see this, first assume that $\sigma^+(P_{m,n})$ is reversible. Then, by the last theorem, π_{m+1}^+ must divide π_{n+1} . Therefore τ_i^+ divides π_{n+1} and, by claim 1 in the proof of theorem 2.1, π_{t_i} must divide π_{n+1} . By proposition 2.1, t_i divides $n + 1$, as required.

On the other hand, suppose that none of the t_i divides $n + 1$, for $i = 0, \dots, r$. But then none of the τ_i^+ divides π_{n+1} either and we must have $\text{gcd}(\pi_{n+1}^+, \pi_{m+1}) = 1$. Hence $\sigma^+(P_{m,n})$ is reversible and we are done. \square

5.2 Periodicity Properties of Grids

We now turn to linear cellular automata of the form $G = H \times P_\infty$ where the local rule is given by rule σ^+ and the alphabet is $F_2^V(H)$. Using the same extension argument as in [13], it is not hard to see that $d^+(G) = 2d^+(H)$. It follows that the global map of G is injective iff the $\sigma^+(H)$ is injective; furthermore, the global map is always open. By an argument similar to the one in lemma 3.1, we can see that all kernel patterns are periodic and the periods are uniformly bounded. Denote the maximal period of the σ^+ -automaton G by $\text{per}^+(H)$. In order to determine $\text{per}^+(H)$, suppose X is a kernel pattern $\sigma^+(G)$ of period p such that $X_0 = 0$. Then the partial configuration (X_1, \dots, X_{p-1}) is clearly in the kernel of $\sigma^+(H \times P_{p-1})$.

This leads to the following definition. Suppose H is a graph on m points. A σ^+ -automaton on $H \times P_n$ is *totally irreversible* if $d^+(H \times P_n) = m$. Hence, in a totally irreversible automaton $\pi_{n+1}^+(\sigma(H)) = 0$. Note that whenever $\pi_p^+(\sigma(H)) = 0$, it follows from the symmetry of equation (1) that

$$\pi_{p-i}(\sigma(H)) = \pi_{p+i}(\sigma(H)), \text{ for all } 0 \leq i \leq p.$$

Thus, any kernel pattern on the infinite cellular automaton G must consist of identical blocks of length $p - 1$, possibly reversed, and separated by 0-patterns. The pattern is symmetric with respect to each of these 0-patterns. This suggests to define the *weak period* of H under σ^+ , in symbols $\text{wper}^+(H)$, to be the least $p > 0$ such that $H \times P_p$ is totally irreversible.

It follows that $\pi_p^+(\sigma(H)) = 0$ iff p is a multiple of $\text{per}^+(H)$ iff the minimal polynomial of $\sigma(H)$ divides π_p^+ . Specifically, if H is a path, it follows that

$$\text{wper}^+(P_m) = \min(n \mid \pi_{m+1}^+ \text{ divides } \pi_{n+1}).$$

The basic properties of the period and weak period are expressed in the next proposition.

Proposition 5.2 *For all graphs H we have:*

- $\text{per}^+(H) = \text{wper}^+(H)$ or $\text{per}^+(H) = 2 \text{wper}^+(H)$.
- If $\text{per}^+(H)$ is odd, then $\text{per}^+(H) = \text{wper}^+(H)$.
- If $\text{per}^+(H) = 2p$ is even, then $\pi_p(\sigma^+(H))(X)$ lies in the kernel of $\sigma^+(H)$, for all patterns X .

Proof.

It is clear that $\text{wper}^+(H) \mid \text{per}^+(H)$, so suppose $p := \text{wper}^+(H) < \text{per}^+(H)$. Then by the symmetry of equation (1) we have $\pi_{p-i}(\sigma(H)) = \pi_{p+i}(\sigma(H))$ for all $0 \leq i \leq p$. In particular, $\pi_{2p}(\sigma(H)) = 0$

and $\pi_{2p-1}(\sigma(H)) = id$. But then $\pi_{2p+1}(\sigma(H)) = id$ and we are done with the first claim. The second claim follows immediately from the first.

For the third claim note that $0 = \pi_{2p}^+(S_m) = ((1+x)\pi_p^+)(S_m) = S_m^+(\pi_p(S_m^+))$. \square

Returning to paths, we can describe the period of P_m under rule σ^+ as follows. First, define the following analogue to the depth function

$$\text{dep}^+(\tau) := \min(i \mid \tau \text{ divides } \pi_i^+),$$

where τ is irreducible. Of course, $\text{dep}^+(\tau) = \text{dep}(\tau^+)$ since F is an involution. Second, to simplify the statement of the next theorem, let us adopt Knuth's convention to write $[\varphi]$ for the boolean value, interpreted as 0 or 1, of any predicate φ , see [5].

Theorem 5.2 *Let $m+1 = 2^k p$ where p is odd and set*

$$D := \text{lcm}(\text{dep}^+(\tau) \mid \tau \mid \pi_{m+1}, \tau \neq x, 1+x, \tau \text{ irreducible}).$$

Here we assume $D = 1$ if no such factor τ exists. Then

$$\text{wper}^+(P_m) = \begin{cases} 2^k \cdot 3 & \text{if } p = 1, \\ 2^{k+2[3|m+1]} \text{lcm}(D, 3^{[2|m+1]}) & \text{otherwise.} \end{cases} \quad (6)$$

Moreover, $\text{per}^+(P_m) = \text{wper}^+(P_m)$ iff $3 \mid m+1$, and $\text{per}^+(P_m) = 2 \text{wper}^+(P_m)$ otherwise.

Proof. To determine the weak period of S_m^+ we have to find the least $n > 0$ such that π_n annihilates S_m^+ . Equivalently, π_n^+ must annihilate S_m . Since π_{m+1} is the minimal polynomial of S_m , it follows that π_{m+1} must divide π_n^+ , or, equivalently, π_{m+1}^+ must divide π_n .

As we have seen,

$$\pi_{m+1} = x^{2^k-1} \cdot \left((1+x)^{2^{k+1}} \right) \cdot \prod \tau^{2^{k+1}}$$

where the product is over all irreducible $\tau \neq x, 1+x$ that divide π_p and the parenthesized middle term only occurs if $3 \mid p$. Hence,

$$\pi_{m+1}^+ = (1+x)^{2^k-1} \cdot \left(x^{2^{k+1}} \right) \cdot \prod \tau^{+2^{k+1}}.$$

A straightforward, if tedious, calculation now shows that $\text{wper}(\sigma(P_m))$ has the form as claimed in the theorem.

It remains to show that $\text{wper}^+(P_m) = \text{per}^+(P_m)$ iff $3 \mid m+1$. First, suppose that $3 \mid m+1$. Then the weak period of m must be even, say, $2p$. A little calculation shows that $\text{cork } \pi_p(S_m^+) = \text{deg gcd}(\pi_p, \pi_{m+1}^+) = \pi_{m+1}^+/x = m-1$. Hence, the range of $\pi_p(S_m^+)$ is one-dimensional. Now the kernel of S_m^+ is $Z := 1 + 2 + 4 + 5 + \dots + (m-1) + m$ and it is easy to see that $\sum_i Z \times \{2i+1\}$ is a pattern in the kernel of $\sigma(P_m \times P_{2p-1})$. But then the range of $\pi_p(S_m^+)$ is the kernel of S_m^+ . It now follows immediately from the symmetry of equation (1) that $\pi_{p-1}(S_m^+) = \pi_{p+i}(S_m^+)$ for all $i = 0, \dots, p$. In particular, $id = \pi_1(S_m^+) = \pi_{2p-1}(S_m^+)$, whence the period of m is $2p$.

The second case, $3 \nmid m+1$, requires a slightly more complicated argument. Note, though, that as long as the period of m is even, say, $2p$, we can proceed as in the previous case: the range of $\pi_p(S_m^+)$ must be the kernel of S_m^+ , which is trivial since 3 does not divide $m+1$. Thus, the weak period of m must be p .

Hence, it suffices to show that P_m cannot have odd period. So suppose for the sake of a contradiction that $\text{per}^+(P_m) = 2p + 1$ is odd. It follows that the weak period of m must agree with the full period. From the first part of the theorem, neither 2 nor 3 can divide $m + 1$ and we must have $\pi_p = (\tau_1 \dots \tau_r)^2$, where all the τ_i are irreducible polynomials and different from x and $1 + x$. We can enumerate these irreducible factors in such a way that $\pi_{m+1} = (\tau_1^+ \dots \tau_s^+)^2$ for some $s \leq r$. We will write $\tau := \tau_1 \dots \tau_s$ and $f := \tau(S_m^+)$. Thus, $f^2 = \tau^2(S_m^+) = \tau^{+2}(S_m) = \pi_{m+1}(S_m) = 0$. We will now show that the invariant subspaces corresponding to f and f^2 are the symmetric patterns in F_2^m , and the asymmetric patterns, respectively. More information on orthogonal subspaces in connection with σ -automata can be found in [13, 14].

Claim 1: $F_2^m = E_1 \oplus E_2$ where E_1 is the kernel of $f = \tau(S_m^+)$. Then E_1 consists precisely of all symmetric patterns in F_2^m and has dimension $m/2$.

It is clear from the definition that E_1 is closed under reversal and also closed under S_m^+ . Furthermore, E_1 is self-orthogonal. To see this, note that $f^2 = 0$, whence $\ker f \subseteq \text{rg } f = (\ker f)^\perp$, where the last equality follows from the self-adjointness of f . It follows that E contains only symmetric patterns. For suppose $X = X[1] + X[2] + \dots + X[k]$ is a pattern in E . k must be even, by orthogonality. Since every basis vector except for 1 and m maps to an odd-cardinality pattern under S_m^+ it follows that $X[1] + X[k] = m + 1$. Otherwise, the orbit of X under S_m^+ would contain an odd-cardinality pattern. Repeating the argument for $X + X[1] + X[k]$ shows that X is symmetric. The degree of τ is $m/2$, and it follows by theorem 4.1 that the dimension of E is also $m/2$. Our claim follows.

Let us write \mathcal{Z} for the kernel of $\sigma(P_{m,2p})$. We will think of these patterns as m by $2p$ matrices over F_2 . Let $V := \{\text{row}_1(K) \mid K \in \mathcal{Z}\} \subseteq F_2^{2p}$ be the subspace consisting of the top rows of patterns in \mathcal{Z} .

Claim 2: $V = V_1 \oplus V_2$ where $V_1 = \ker \tau(S_{2p})$ contains precisely all the symmetric patterns in V . Moreover, $\text{col}_1(K) \in E_1$ iff $\text{row}_1(K) \in V_1$.

For the proof of the second claim, it is best to write the action of $\sigma(P_{m,2p})$ on any two-dimensional kernel pattern K as a matrix equation

$$S_m^+ \cdot K + K \cdot S_{2p} = 0.$$

It follows immediately that

$$\tau(S_m^+) \cdot K + K \cdot \tau(S_{2p}) = 0.$$

Since the subspaces $E_1 \subseteq F_2^m$ and $V_1 \subseteq F_2^{2p}$ are both closed under S_m and S_{2p} , respectively, we have, for any two-dimensional pattern K in \mathcal{Z} : $\tau(S_m^+)$ annihilates the first column of K iff $\tau(S_m^+)$ annihilates all columns of K iff $\tau(S_{2p})$ annihilates all rows of K iff $\tau^+(S_{2p}^+)$ annihilates all rows of K iff $\tau^+(S_{2p}^+)$ annihilates the first row of K . In other words, $\text{col}_1(K)$ lies in E_1 iff $\text{row}_1(K)$ lies in V_1 .

We can now repeat the argument of claim 1 for the map $g = \tau(S_m^+) : V \rightarrow V$. To see that every symmetric pattern in V must lie in V_1 note that $\ker g = (\ker g)^\perp$: every symmetric pattern is orthogonal to the kernel, and therefore an element of it.

From claims 1 and 2, we can write \mathcal{Z} as a direct sum $\mathcal{Z}_1 \oplus \mathcal{Z}_2$, where both spaces have dimension $m/2$. Moreover, \mathcal{Z}_1 consists of all patterns that have symmetric columns, or, equivalently, symmetric rows. In particular, there are $2^{m/2}$ patterns in \mathcal{Z} whose rows fail to be symmetric. It follows that the period of m must be larger than $\text{wper}(m)$ and we have $\text{per}(m) = 2 \text{wper}(m)$, as desired. \square

The analogue of the following corollary for weak periods was conjectured in [13] and first proved in [2].

Corollary 5.3 *For all $k \geq 0$: $\text{per}^+(2^k - 1) = 3 \cdot 2^k$.*

6 Cylinders

In this section we will briefly show how to adapt our results for σ -automata on grids to σ -automata on cylinders of the form $C_m \times P_n$. First, we have to determine the minimal polynomial for the maps $\sigma(C_m)$.

Lemma 6.1 *The minimal polynomial of $\sigma(C_m)$ is $x \pi_{m/2}$ if m is even, and $x \sqrt{\pi_m}$ for m odd.*

Proof. Consider the case where $m = 2m_0$ is even. Since $\sigma(C_m)$ commutes with the shift, we have to determine the non-trivial polynomial π of lowest degree such that $\pi(\sigma(C_m))(m) = 0$, where m denotes a one-point pattern, as in section 4. Note that $X := \sigma(C_m)(m) = 1 + (m - 1)$ because of the cyclic boundary conditions. Furthermore, since m is even, every pattern $X^t = \sigma(C_m)^t(X)$, $t \geq 1$, has the properties $X^t(m_0) = X^t(m) = 0$ and is symmetric with respect to m_0 . Hence, we can simulate the evolution of pattern X on the σ -automaton C_m on the σ -automaton P_{m-1} . Since the patterns on the second automaton are all symmetric, it follows from 5.2 that the the least degree polynomial π such that $\pi(\sigma(C_m))(X) = 0$ is none other than $\pi_{m/2}$.

The argument for m odd is entirely similar and will be omitted. □

It is now straightforward to establish the analogue of lemma 5.1 and characterize the reversible and totally irreversible cylinders. For example, for odd m , all those cylinders $C_m \times P_n$ are reversible for which n is also odd but $\text{gcd}(m, n + 1) = 1$.

Note, though, there is a slight complication in computing the coranks of rule σ on a cylinder. The degree of the minimal polynomial of $\sigma(C_m)$ is $(m + 1)/2$ or $m/2$, depending on whether m is odd or even. Thus, the arguments of lemmata 4.1 and 4.2 have to be adjusted. In particular, for even m , the corank of $\tau(\sigma(C_m))$ is $2 \deg \tau$ for all divisors τ of the minimal polynomial $x \pi_{m/2}$. For odd m , the corank of $\tau(\sigma(C_m))$ is $2 \deg \tau$ for all divisors τ of $\sqrt{\pi_{m/2}}$, but $1 + 2 \deg \tau$ for $(x\tau)(\sigma(C_m))$.

The following table shows the degree of $\text{gcd}(\pi, \pi_{n+1})$, where π is the minimal polynomial of $\sigma(C_m)$, as well as the coranks of $\sigma(C_m \times P_n)$. We write $k = \text{mult}_2(m)$ and $l = \text{mult}_2(n + 1)$.

degree	corank	
$1/2(\text{gcd}(m, n + 1) - 1)$	$\text{gcd}(m, n + 1) - 1$	$0 = k = l,$
$1/2(\text{gcd}(m, n + 1) - 1) + 1$	$\text{gcd}(m, n + 1)$	$0 = k < l,$
$1/2 \text{gcd}(m, n + 1)$	$\text{gcd}(m, n + 1)$	$0 < k \leq l,$
$\text{gcd}(m, n + 1) - 1$	$2(\text{gcd}(m, n + 1) - 1)$	$l < k.$

The weak period as well as the full period of rule σ on C_m is m for m even, and $2m$ for m odd.

To determine the weak and full period of rule σ^+ on cylinders, we have to compute the depth of τ^+ , where τ is an irreducible factor of the minimal polynomial of $\sigma(C_m)$. Note that x is always such a factor, hence the weak period of rule σ^+ on a cylinder must always be divisible by three, the depth of $x^+ = 1 + x$.

Using the same notation as in theorem 5.2, we have for $m = 2^k p$, p odd,

$$\text{wper}^+(C_m) = \begin{cases} 2^{[3^m]} \text{lcm}(3, D) & \text{if } k = 0, \\ 2^{k-1+2[3^m]} \text{lcm}(3, D) & \text{otherwise.} \end{cases} \quad (7)$$

Also, for cylinders the periods are determined thus: $\text{per}^+(C_m) = 2 \text{wper}^+(C_m)$ iff $m \equiv 2, 4 \pmod{6}$, and $\text{per}^+(C_m) = \text{wper}^+(C_m)$ otherwise.

7 Open Problems

We conclude by stating a few open problems about the dynamics of binary σ^+ -automata that can be expressed in terms of Chebyshev polynomials.

Reversible Squares

As far as squares are concerned, it follows from our results that in order for the m by m grid to be reversible under rule σ^+ we must have $6 \nmid m+1$ and for all odd $e > 3$ such that $e \mid m+1$ and $\tau \mid \rho_e$ irreducible: $\text{dep}(\tau^+) \nmid m+1$. Is there a simple algorithm to test the second property? Are there any totally irreversible squares other than 4×4 ? Equivalently, is there any $m > 4$ such that $\pi_{m+1} = \pi_{m+1}^+$? We suspect that the answer to the last question is no.

Computing Depth and Period

Lastly, the most interesting question in connection with binary Chebyshev polynomials is whether there is an algorithm to compute the depth of an irreducible polynomial τ over F_2 , other than the obvious brute-force approach. In particular, is there an algorithm which is polynomial in the degree of τ ? Note that the depth of many irreducible polynomials realizes the upper bound $2^{\text{deg } \tau} \pm 1$, so that one cannot enumerate in polynomial time all π -polynomials that are potential multiples of τ . Is it the case that for each d such that $\text{sord}_d(2) = k$ there exists an irreducible polynomial of degree k depth is d ? What is the distribution of these polynomials for the possible choices of d ? See table 3 in the appendix for a complete listing of the depths of all irreducible polynomials τ of degree 8 as well as their counterparts τ^+ .

An obviously related problem is the computation of periods $\text{per}^+(m)$. Note, though, that there might be an alternative approach to computing periods that does not use the depth function.

References

- [1] B. Andrasfai. Cellular automata in trees. In *Finite and Infinite Sets*, volume 37, pages 35–45. Colloquia Mathematica Societatis Janos Bolyai, Eger, Hungary, 1981.
- [2] R. Barua and S. Ramakrishnan. σ -game, σ^+ -game, and two-dimensional cellular automata. *Theoretical Computer Science*, 154(2):349–366, 1996.
- [3] P. Sarkar and R. Barua. Multidimensional σ -automata, π -polynomials and generalized S -matrices. To appear.
- [4] E. R. Berlekamp. *Algebraic Coding Theory*. McGraw-Hill, 1968.
- [5] R. L. Graham, D. E. Knuth, and O. Patashnik. *Concrete Mathematics: A Foundation for Computer Science*. Addison-Wesley, 1988.
- [6] T. W. Hungerford. *Algebra*. Springer-Verlag, 1974.
- [7] R. Lidl and H. Niederreiter. *Finite Fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, 1984.
- [8] A. Lindenmayer. Mathematical models for cellular interactions in development. *Journal of Theoretical Biology*, 18:280–299, 1968.
- [9] M. E. Lucas. Sur les congruences des nombres Euleriennes et des coefficients différentiels des fonctions trigonométrique, suivant un module premier. *Bull. Soc. Math. France*, 6:49–54, 1878.
- [10] O. Martin, A. M. Odlyzko, and S. Wolfram. Algebraic properties of cellular automata. *Commun. Math. Phys.*, 93:219–258, 1984.
- [11] R. J. McEliece. *Finite Fields for Computer Scientists and Engineers*. Kluwer, 1987.
- [12] I. Niven. Fermat’s theorem for matrices. *Duke Math. J.*, 15:823–826, 1948.
- [13] K. Sutner. On σ -automata. *Complex Systems*, 2(1):1–28, 1988.
- [14] K. Sutner. Linear cellular automata and the Garden-of-Eden. *Mathematical Intelligencer*, 11(2):49–53, 1989.
- [15] T. Toffoli and Margolus. Injective cellular automata. *Physica D*, 45(1–3):386–395, 1990.
- [16] S. Wolfram. *Theory and Applications of Cellular Automata*. World Scientific, 1986.

8 Appendix

The first table below contains all the critical factors ρ_e for $e \leq 51$ and the second shows the images of the irreducible factors τ of ρ_e under the involution $x^+ = 1 + x$. The second column in this table gives the depth of τ^+ . A dash indicates a value larger than 2000.

From the table, we can calculate the periods $\text{per}^+(P_m)$ and $\text{per}^+(C_m)$ for some values of m . For example, $\text{per}^+(P_{20}) = 2^2 \text{lcm}(9, 65) = 2340$. By contrast, $\text{per}^+(P_{40}) = 2 \cdot \text{lcm}(1025, 1023) = 2097150$.

Lastly, in table three, the depth of all irreducible polynomials of degree 8 are shown. Note that all d such that $\text{sord}_d(2) = 8$ occur ($d = 51, 85, 255, 257$). Those irreducibles whose roots α give rise to a reducible characteristic polynomial $f(z) = z^2 + \alpha z + z$ of the linear recurrence sequence (s_i) have depths dividing 255, and the ones for which f splits only over F_{q^2} all have depth 257, since the latter is a Fermat prime.

e	ρ_e
2	x
3	$1 + x$
5	$1 + x + x^2$
7	$1 + x^2 + x^3$
9	$1 + x + x^3$
11	$1 + x + x^2 + x^4 + x^5$
13	$1 + x + x^4 + x^5 + x^6$
15	$1 + x^3 + x^4$
17	$1 + x + x^4$ $1 + x + x^2 + x^3 + x^4$
19	$1 + x + x^4 + x^5 + x^6 + x^8 + x^9$
21	$1 + x^5 + x^6$
23	$1 + x^2 + x^3 + x^4 + x^8 + x^{10} + x^{11}$
25	$1 + x + x^2 + x^3 + x^5 + x^6 + x^{10}$
27	$1 + x + x^5 + x^7 + x^9$
29	$1 + x + x^8 + x^9 + x^{12} + x^{13} + x^{14}$
31	$1 + x^2 + x^5$ $1 + x^3 + x^5$ $1 + x^2 + x^3 + x^4 + x^5$
33	$1 + x + x^2 + x^3 + x^5$ $1 + x + x^3 + x^4 + x^5$
35	$1 + x^5 + x^6 + x^7 + x^9 + x^{11} + x^{12}$
37	$1 + x + x^2 + x^8 + x^9 + x^{10} + x^{12} + x^{13} + x^{16} + x^{17} + x^{18}$
39	$1 + x^3 + x^4 + x^5 + x^6 + x^7 + x^8 + x^{11} + x^{12}$
41	$1 + x + x^3 + x^4 + x^7 + x^8 + x^{10}$ $1 + x + x^4 + x^9 + x^{10}$
43	$1 + x + x^7$ $1 + x + x^2 + x^3 + x^4 + x^5 + x^7$ $1 + x + x^2 + x^4 + x^5 + x^6 + x^7$
45	$1 + x^3 + x^4 + x^5 + x^7 + x^9 + x^{12}$
47	$1 + x^4 + x^6 + x^7 + x^8 + x^{16} + x^{20} + x^{22} + x^{23}$
49	$1 + x^2 + x^3 + x^7 + x^9 + x^{10} + x^{11} + x^{14} + x^{17} + x^{19} + x^{21}$
51	$1 + x^2 + x^3 + x^4 + x^8$ $1 + x^2 + x^3 + x^7 + x^8$

Table 1: The critical factors ρ_e for $e \leq 51$.

e	depth	ρ_e^+
2	3	$1 + x$
3	2	x
5	5	$1 + x + x^2$
7	9	$1 + x + x^3$
9	7	$1 + x^2 + x^3$
11	31	$1 + x^2 + x^5$
13	63	$1 + x^2 + x^4 + x^5 + x^6$
15	17	$1 + x + x^2 + x^3 + x^4$
17	17	$1 + x + x^4$
	15	$1 + x^3 + x^4$
19	513	$1 + x + x^2 + x^4 + x^5 + x^6 + x^9$
21	65	$1 + x + x^2 + x^5 + x^6$
23	–	$1 + x^4 + x^8 + x^9 + x^{11}$
25	1025	$1 + x + x^3 + x^5 + x^6 + x^8 + x^{10}$
27	511	$1 + x^2 + x^3 + x^6 + x^7 + x^8 + x^9$
29	–	$1 + x + x^2 + x^4 + x^5 + x^6 + x^8 + x^{10} + x^{12} + x^{13} + x^{14}$
31	11	$1 + x + x^2 + x^4 + x^5$
	31	$1 + x^2 + x^3 + x^4 + x^5$
	31	$1 + x^3 + x^5$
33	33	$1 + x + x^3 + x^4 + x^5$
	33	$1 + x + x^2 + x^3 + x^5$
35	455	$1 + x^2 + x^7 + x^8 + x^{10} + x^{11} + x^{12}$
37	–	$1 + x^2 + x^5 + x^8 + x^{10} + x^{13} + x^{16} + x^{17} + x^{18}$
39	585	$1 + x^3 + x^4 + x^7 + x^8 + x^9 + x^{10} + x^{11} + x^{12}$
41	1025	$1 + x + x^2 + x^5 + x^6 + x^7 + x^{10}$
	1023	$1 + x^2 + x^4 + x^9 + x^{10}$
43	127	$1 + x^2 + x^3 + x^4 + x^5 + x^6 + x^7$
	127	$1 + x^2 + x^4 + x^6 + x^7$
	129	$1 + x + x^2 + x^3 + x^7$
45	1365	$1 + x^6 + x^7 + x^9 + x^{12}$
47	–	$1 + x^8 + x^{17} + x^{19} + x^{20} + x^{21} + x^{23}$
49	–	$1 + x + x^2 + x^4 + x^7 + x^{10} + x^{11} + x^{12} + x^{14} + x^{16} + x^{17} + x^{18} + x^{19} + x^{20} + x^{21}$
51	257	$1 + x + x^3 + x^4 + x^8$
	85	$1 + x^2 + x^4 + x^5 + x^6 + x^7 + x^8$

Table 2: The irreducible polynomials τ^+ where τ divides a critical factor ρ_e for $e \leq 51$. The second column shows the depth of τ^+ (a dash indicates a value larger than 2000).

number	image	depth	irreducible polynomial
1	17	257	$1 + x + x^3 + x^4 + x^8$
2	12	51	$1 + x^2 + x^3 + x^4 + x^8$
3	15	257	$1 + x + x^3 + x^5 + x^8$
4	29	255	$1 + x^2 + x^3 + x^5 + x^8$
5	13	255	$1 + x^3 + x^4 + x^5 + x^8$
6	10	257	$1 + x + x^2 + x^3 + x^4 + x^5 + x^8$
7	16	255	$1 + x^2 + x^3 + x^6 + x^8$
8	23	257	$1 + x + x^2 + x^3 + x^4 + x^6 + x^8$
9	9	257	$1 + x + x^5 + x^6 + x^8$
10	6	255	$1 + x^2 + x^5 + x^6 + x^8$
11	28	255	$1 + x^3 + x^5 + x^6 + x^8$
12	2	85	$1 + x^4 + x^5 + x^6 + x^8$
13	5	257	$1 + x + x^2 + x^4 + x^5 + x^6 + x^8$
14	24	257	$1 + x + x^3 + x^4 + x^5 + x^6 + x^8$
15	3	257	$1 + x + x^2 + x^7 + x^8$
16	7	257	$1 + x + x^3 + x^7 + x^8$
17	1	51	$1 + x^2 + x^3 + x^7 + x^8$
18	19	257	$1 + x + x^2 + x^3 + x^4 + x^7 + x^8$
19	18	257	$1 + x + x^5 + x^7 + x^8$
20	21	85	$1 + x^3 + x^5 + x^7 + x^8$
21	20	255	$1 + x^4 + x^5 + x^7 + x^8$
22	22	255	$1 + x^2 + x^3 + x^4 + x^5 + x^7 + x^8$
23	8	257	$1 + x + x^6 + x^7 + x^8$
24	14	257	$1 + x + x^2 + x^3 + x^6 + x^7 + x^8$
25	30	257	$1 + x + x^2 + x^4 + x^6 + x^7 + x^8$
26	27	85	$1 + x^2 + x^3 + x^4 + x^6 + x^7 + x^8$
27	26	257	$1 + x + x^2 + x^5 + x^6 + x^7 + x^8$
28	11	257	$1 + x + x^4 + x^5 + x^6 + x^7 + x^8$
29	4	85	$1 + x^2 + x^4 + x^5 + x^6 + x^7 + x^8$
30	25	255	$1 + x^3 + x^4 + x^5 + x^6 + x^7 + x^8$

Table 3: The depths of all irreducible binary polynomials τ of degree 8. The image column gives the index of τ^+ with respect to the numbering in the first column. All polynomials of the form $1 + x + \dots + x^8$ have depth 257.