Available online at www.sciencedirect.com
SCIENCE DIRECT®
Theoretical Computer Science 320 (2004) 465–483
Theoretical Computer Science
www.elsevier.com/locate/tcs

Chebyshev polynomials over finite fields and reversibility of σ-automata on square grids

Markus Hunziker[a], António Machiavelo[b,1], Jihun Park[c,*]

[a] *Department of Mathematics, University of Georgia, Athens, GA 30602, USA*
[b] *Centro de Matemática da Universidade do Porto, Porto 4169-007, Portugal*
[c] *Department of Mathematics, POSTECH, Pohang, Kyungbuk, 790-784, Republic of Korea*

Received 10 January 2003; received in revised form 1 March 2004; accepted 9 March 2004
Communicated by B. Durand

Abstract

Using number theory on function fields and algebraic number fields, we prove results about Chebyshev polynomials over finite prime fields to investigate reversibility of two-dimensional additive cellular automata on finite square grids. For example, we show that there are infinitely many primitive irreversible additive cellular automata on square grids when the base field has order two or three.
© 2004 Elsevier B.V. All rights reserved.

Keywords: Additive cellular automata; Chebyshev polynomials; Finite fields

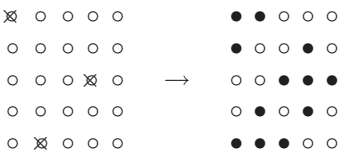
1. Introduction

What got us interested to study Chebyshev polynomials over finite fields was a game commonly known as Lights Out (Copyright Tiger Electronics), which was introduced to the mathematical community by Pelletier and Sutner [12,19,18] and has since then been broadly investigated by many others [1,15,16,20]. In this game, we are given a square array of lights that can be in one of ℓ states, say $\{0,1,2,\ldots,\ell-1\}$. If $\ell=2$ we

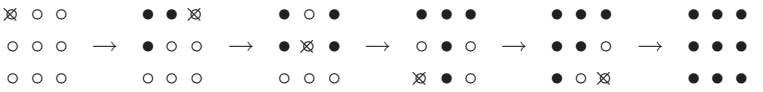
* Corresponding author.
Auckland University of Technology, Private Bag 92006, Auckland, New Zealand.
E-mail address: wlog@postech.ac.kr (J. Park).
[1] Partially supported by Fundação para a Ciência e Tecnologia (FCT) through Centro de Matemática da Universidade do Porto.

0304-3975/$ - see front matter © 2004 Elsevier B.V. All rights reserved.
doi:10.1016/j.tcs.2004.03.031

might think of the possible states as "off" (0) and "on" (1) and similarly, if $\ell = 3$ as "off" (0), "green" (1) and "red" (2). Each light is also a button and pushing that button changes the state of the corresponding light as well as the states of the vertical and horizontal neighbors by adding 1 modulo ℓ. As an example, consider a 5×5 square and suppose that $\ell = 2$. Pressing the buttons with coordinates $(1,1)$, $(3,4)$ and $(5,2)$ will have the following effect on the lights:



The aim in the game is—starting from some initial configuration—to turn all the lights off (all 0's) by pushing (a minimal number of) buttons. If $\ell = 2$ and all lights are initially turned on, then it is always possible—for any size of square—to turn all lights off (this was first discovered by Sutner and presented in [18]; see also [4]). For example,



A first natural question is then the following: given some fixed ℓ (= number of possible states of each light), what are the square arrays for which all lights can be turned off from any initial configuration? This question has a surprising answer in terms of Chebyshev polynomials. Let $F_{n+1}(x) := U_n(x/2)$ be the normalized (monic) Chebyshev polynomial of the second kind of degree n. Suppose that ℓ is prime. Then the $n \times n$ square is reversible (i.e., completely solvable) if and only if the polynomials $F_{n+1}(x)$ and $F_{n+1}(1-x)$ have no common factor mod ℓ. This result was first proved by Sutner [20].[2] The degree shift in the indexing of the Chebyshev polynomials is motivated by the following divisibility property: the polynomial $F_m(x)$ divides $F_n(x)$ if and only if the integer m divides n. For a fixed prime ℓ, we now define a set of natural numbers

$$\mathscr{S}_\ell := \{n \in \mathbb{N} : F_n(x) \text{ and } F_n(1-x) \text{ have a common factor modulo } \ell\}.$$

The divisibility property of the polynomials $F_n(x)$ implies that $\mathscr{S}_\ell$ is a set of multiples, i.e. if $n \in \mathscr{S}_\ell$ then every positive integer multiple of n belongs also to $\mathscr{S}_\ell$. An element $n \in \mathscr{S}_\ell$ is called *primitive* if n is not a positive integer multiple of a smaller element of $\mathscr{S}_\ell$. For $\ell = 2$, the first 26 primitive elements of $\mathscr{S}_\ell$ are:

$$5, 6, 17, 31, 33, 63, 127, 129, 171, 257, 511, 683, 2047, 2731, 2979, 3277,$$
$$3641, 8191\ \ 28197, 43691, 48771, 52429, 61681, 65537, 85489, 131071, \ldots\ .$$

Note that this list includes the Fermat primes 5, 17, 257 and 65537 as well as Mersenne primes 31, 127, 8191, 131071, etc. Goldwasser et al. [5] proved in general that $2^k \pm 1$

[2] Sutner proved the result in the case $\ell = 2$, but his proof immediately generalizes to arbitrary primes ℓ.

belongs to $\mathscr{S}_2$ for $k \geqslant 5$. Even though the set $\mathscr{S}_2$ has been studied by many people such as Barua, Ramakrishnan, Sarkar, and Sutner, it still remains somewhat mysterious. The mystery results from the fact that it requires a huge amount of computation to decide whether an additive cellular automaton on a big size square is reversible or not. What is interesting, but difficult, about the set $\mathscr{S}_\ell$ is that its primitive elements behave like prime numbers.

In this article, we study the polynomials $F_n(x)$ modulo ℓ and in particular, the sets $\mathscr{S}_\ell$, by using number theory in various fields such as function fields, cyclotomic fields and p-adic local fields.

As an application of our techniques we prove that the $(5k-1)\times(5k-1)$ square and the $(6k-1)\times(6k-1)$ square, $k=1,2,\ldots$, are the only squares that are irreversible modulo ℓ for all primes ℓ. We also show that the 1×1 square is the only square that is reversible modulo ℓ for all primes ℓ.

We then consider the question whether the sets $\mathscr{S}_\ell$ contain infinitely many primitive elements. It is conjectured that this question is answered affirmatively for all primes ℓ. For $\ell=2$, it can be answered in the affirmative by using the result of Goldwasser, Klostermeyer and Ware mentioned above. Furthermore, our way to prove the case of $\ell=2$ leads us to another conjecture that for a prime ℓ the positive integers of the form $(\ell^k-1)/(\ell-1)$ belong to $\mathscr{S}_\ell$ (Conjecture 5.3), which is a generalization of that same result of Goldwasser, Klostermeyer and Ware. It turns out that the latter conjecture immediately implies the former one. We prove the conjecture is true for $\ell=2$ and 3. An evidence for Conjecture 5.3 is also provided at the end of the article (Proposition 5.4).

2. Chebyshev polynomials

We first recall the definition of normalized Chebyshev polynomials over the integers and prove some of their properties. Most of this material is standard (see [13]) but we provide some of the proofs to illustrate our function field approach that will play an important role later on. We then study Chebyshev polynomials over finite prime fields in more detail. We will relate these polynomials to additive cellular automata in the next section.

Definition 2.1. We define $F_0(x) := 0$, $F_1(x) := 1$ and for $n > 1$

$$F_n(x) := \det \begin{pmatrix} x & 1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 1 & x & 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & x & 1 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 & x & 1 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 & x \end{pmatrix},$$

where the matrix on the right-hand side is an $(n-1)\times(n-1)$-matrix.

By expanding the determinant above with respect to the first row it follows that the polynomials $F_n(x)$ satisfy the linear recurrence

$$F_n(x) = xF_{n-1}(x) - F_{n-2}(x).$$

The monic polynomials $F_n(x)$ are known as *normalized Chebyshev polynomials of the second kind*. More precisely, for $n \geqslant 1$, $F_n(x) = U_{n-1}(x/2)$, where $U_{n-1}(x)$ is the usual Chebyshev polynomial of the second kind of degree $n-1$. The degree shift in our notation will prove to be useful when we consider divisibility properties. A first example of such a property is the following.

Proposition 2.2. *A polynomial $\tau(x)$ in $\mathbb{Z}[x]$ divides both $F_n(x)$ and $F_m(x)$ if and only if it divides $F_{\gcd(m,n)}(x)$. In particular,*

$$\gcd(F_m(x), F_n(x)) = F_{\gcd(m,n)}(x).$$

Proof. The proof is the same as the proof of the analogous well-known result for Fibonacci numbers and uses Euclid's algorithm. See [8], for example. □

To study the polynomials $F_n(x)$ it is useful to introduce another sequence of polynomials that satisfies the same recurrence relation but whose initial terms are different. We define $G_0(x) := 2$, $G_1(x) := x$ and for $n \geqslant 2$, $G_n(x) := xG_{n-1}(x) - G_{n-2}(x)$. The polynomials $G_n(x)$ are the *normalized Chebyshev polynomials of the first kind*. More precisely, $G_n(x) = 2T_n(x/2)$, where $T_n(x)$ is the usual Chebyshev polynomial of the first kind of degree n.

Before we prove more properties of the Chebyshev polynomials $F_n(x)$ and $G_n(x)$, we give another expression of these polynomials. Let α and β be the two distinct roots of the characteristic polynomial $t^2 - xt + 1$ of the linear recurrence relation that is satisfied by both the $F_n(x)$ and $G_n(x)$. The roots α and β are taken in the algebraic closure of the function field $\mathbb{Q}(x)$. Explicitly, we may write $\alpha = (x + \sqrt{x^2-4})/2$ and $\beta = (x - \sqrt{x^2-4})/2$. Note that we have the identities $\alpha + \beta = x$ and $\alpha\beta = 1$.

Proposition 2.3. *Let α be as above. Then*

$$F_n(x) = \frac{\alpha^n - \alpha^{-n}}{\alpha - \alpha^{-1}} \quad \text{and} \quad G_n(x) = \alpha^n + \alpha^{-n}.$$

Proof. We prove the formula for $F_n(x)$. The proof of the formula for $G_n(x)$ is similar. Put $\tilde{F}_n(x) = (\alpha^n - \alpha^{-n})/(\alpha - \alpha^{-1})$. Clearly, $\tilde{F}_0(x) = 0$ and $\tilde{F}_1(x) = 1$. We claim that for $n \geqslant 2$ we have $\tilde{F}_n(x) = x\tilde{F}_{n-1}(x) - \tilde{F}_{n-2}(x)$. This follows, since $\alpha + \alpha^{-1} = x$, from the identity

$$\frac{\alpha^n - \alpha^{-n}}{\alpha - \alpha^{-1}} = (\alpha + \alpha^{-1}) \frac{\alpha^{n-1} - \alpha^{-(n-1)}}{\alpha - \alpha^{-1}} - \frac{\alpha^{n-2} - \alpha^{-(n-2)}}{\alpha - \alpha^{-1}}.$$

By induction, we then have $\tilde{F}_n(x) = F_n(x)$ for all n. □

Another identity is sometimes useful. The Laurent polynomial $F_n(x+x^{-1})$ in $\mathbb{Z}[x,x^{-1}]$ can be written in the form

$$F_n(x+x^{-1}) = \frac{x^n - x^{-n}}{x - x^{-1}}.$$

This formula is proved in the same way as Proposition 2.3.

Lemma 2.4. *The Chebyshev polynomials $F_n(x)$ and $G_m(x)$ satisfy the following identities*:
(a) $(x^2-4)F_m(x)F_n(x) = G_{m+n}(x) - G_{|m-n|}(x)$,
(b) $F_{mn}(x) = F_m(G_n(x))F_n(x)$.

Proof. By Proposition 2.3 we have

$$\begin{aligned}(\alpha-\alpha^{-1})^2 F_m(x)F_n(x) &= (\alpha^m - \alpha^{-m})(\alpha^n - \alpha^{-n}) \\ &= (\alpha^{m+n} + \alpha^{-m-n}) - (\alpha^{m-n} + \alpha^{-m+n}) \\ &= G_{m+n}(x) - G_{|m-n|}(x).\end{aligned}$$

Since $(\alpha-\alpha^{-1})^2 = (\alpha+\alpha^{-1})^2 - 4 = x^2 - 4$ this shows (a). The proof of (b) is similar. By Proposition 2.3 and the remark following it we have

$$F_m(G_n(x)) = F_m(\alpha^n + \alpha^{-n}) = \frac{\alpha^{mn} - \alpha^{-mn}}{\alpha^n - \alpha^{-n}}.$$

Multiplying this equation by $F_n(x)$ we then get

$$F_m(G_n(x))F_n(x) = \frac{\alpha^{mn} - \alpha^{-mn}}{\alpha^n - \alpha^{-n}} \frac{\alpha^n - \alpha^{-n}}{\alpha - \alpha^{-1}} = \frac{\alpha^{mn} - \alpha^{-mn}}{\alpha - \alpha^{-1}} = F_{mn}(x). \qquad \square$$

In what follows, let ℓ be a fixed prime and let $\mathbb{F}_\ell := \mathbb{Z}/\ell\mathbb{Z}$ be the prime field with ℓ elements.

Definition 2.5. We define $f_n(x)$ in $\mathbb{F}_\ell[x]$ by

$$f_n(x) := F_n(x) \bmod \ell,$$

i.e. $f_n(x)$ is the image of $F_n(x)$ under the natural homomorphism $\mathbb{Z}[x] \to (\mathbb{Z}/\ell\mathbb{Z})[x] = \mathbb{F}_\ell[x]$. Similarly, we define $g_n(x)$ in $\mathbb{F}_\ell[x]$ by $g_n(x) := G_n(x) \bmod \ell$.

It is clear that the properties we have proved so far for the polynomials $F_n(x)$ and $G_n(x)$ are inherited by the polynomials $f_n(x)$ and $g_n(x)$. We also still have the expression in terms of the roots α and β of the characteristic equation. The only difference is that we now take the roots in the algebraic closure of the field of rational functions $\mathbb{F}_\ell(x)$. By abuse of notation we still will again denote the two roots by α and β. As before we have $\alpha+\beta = x$ and $\alpha\beta = 1$.

We now prove some more identities that are specific to the finite field case since they involve the *Frobenius homomorphism*. Recall that if K is a field of characteristic ℓ

then the map $K \to K$ given by $a \mapsto a^\ell$ is a homomorphism, i.e. $(a+b)^\ell = a^\ell + b^\ell$ (and $(ab)^\ell = a^\ell b^\ell$) for all $a, b \in K$. The prime field $\mathbb{F}_\ell \subseteq K$ is fixed under this homomorphism.

Lemma 2.6. *The polynomials $f_n(x)$ have the following properties*:
(a) *$f_m(x)$ divides $f_n(x)$ if and only if m divides n*;
(b) *$f_{\ell^k m}(x) = f_{\ell^k}(x) f_m^{\ell^k}(x)$*;
(c) *$f_{\ell^k}(x) = (x^2-4)^{(\ell^k-1)/2}$; in particular, if $\ell = 2$ then $f_{2^k}(x) = x^{2^k-1}$.*

Proof. Part (a) immediately follows from Proposition 2.2. For parts (b) and (c) we use the expression of $f_n(x)$ in terms of α and $\beta = \alpha^{-1}$. Let K be the quadratic extension of $\mathbb{F}_\ell(x)$ to which α belongs. Then in the field K we have the identity

$$f_{\ell^k m}(x) = \frac{\alpha^{\ell^k m} - \beta^{\ell^k m}}{\alpha - \beta} = \frac{(\alpha^m - \beta^m)^{\ell^k}}{\alpha - \beta} = \left(\frac{\alpha^m - \beta^m}{\alpha - \beta}\right)^{\ell^k} \frac{\alpha^{\ell^k} - \beta^{\ell^k}}{\alpha - \beta}$$
$$= f_m^{\ell^k}(x) \cdot f_{\ell^k}(x).$$

This proves part (b). Similarly, we have

$$f_{\ell^k}(x) = \frac{\alpha^{\ell^k} - \beta^{\ell^k}}{\alpha - \beta} = \frac{(\alpha - \beta)^{\ell^k}}{\alpha - \beta} = (\alpha - \beta)^{\ell^k - 1} = (x^2 - 4)^{(\ell^k - 1)/2}.$$

Here in the last step we used the fact that $(\alpha - \beta)^2 = x^2 - 4$. This proves part (c). □

Proposition 2.7. *For any $k \geqslant 0$,*

$$f_{2^k-1}(x) f_{2^k+1}(x) = (x^{2^k-1} - 1)^2 \quad \text{if } \ell = 2,$$

and similarly

$$f_{(\ell^k-1)/2}(x) f_{(\ell^k+1)/2}(x) = \frac{x^{\ell^k} - x}{x^2 - 4} \quad \text{if } \ell \neq 2.$$

Proof. We give the proof in the case $\ell \neq 2$. The case $\ell = 2$ is similar. By Lemma 2.4(a), we have

$$f_{(\ell^k-1)/2}(x) f_{(\ell^k+1)/2}(x) = \frac{g_{\ell^k}(x) - g_1(x)}{x^2 - 4}.$$

Since $g_{\ell^k}(x) = \alpha^{\ell^k} + \beta^{\ell^k} = (\alpha + \beta)^{\ell^k} = x^{\ell^k}$ and since $g_1(x) = x$ the proposition follows. □

Corollary 2.8. *Every irreducible polynomial $\tau(x)$ in $\mathbb{F}_\ell[x]$ occurs as a factor of some $f_n(x)$. More precisely, suppose $\tau(x)$ has degree k and $\tau(x) \neq x \pm 2$. Then*

$$\tau(x) \text{ divides } \begin{cases} f_{2^k+1}(x) \text{ or } f_{2^k-1}(x) & \text{if } \ell = 2, \\ f_{(\ell^k+1)/2}(x) \text{ or } f_{(\ell^k-1)/2}(x) & \text{if } \ell \neq 2. \end{cases}$$

Moreover, if $\tau(x) = x \pm 2$ then $\tau(x)$ divides $f_\ell(x)$.

Proof. The last assertion immediately follows from Lemma 2.6. For the other assertions, note that the irreducible polynomial $\tau(x)$ of degree k divides $x^{\ell^k}-x$ because the splitting field of $\tau(x)$ over $\mathbb{F}_\ell$ is the field $\mathbb{F}_{\ell^k}$. Proposition 2.7 implies the results. □

Corollary 2.8 tells us that any irreducible polynomial $\tau(x)\in\mathbb{F}_\ell[x]$, which is neither $x+2$ nor $x-2$, divides $f_{(\ell^k+1)/2}(x)$ or $f_{(\ell^k-1)/2}(x)$, where k is the degree of $\tau(x)$. However, it is not clear which one is divided by $\tau(x)$. Since $\gcd((\ell^k-1)/2,(\ell^k+1)/2)=1$, the polynomial $\tau(x)$ cannot divide both. For $\ell=2$ Sutner showed that an irreducible polynomial $\tau(x)\in\mathbb{F}_2[x]$ of degree k divides $f_{2^k-1}(x)$ if $\tau'(0)=0$, and $f_{1^k+1}(x)$ otherwise ([20, Theorem 3.1]). For the case $\ell\neq 2$, unlike the case $\ell=2$, this criterion does not work at all. In what follows we show a numerical criterion for the case $\ell\neq 2$.

From now to the end of this section we assume $\ell\neq 2$. Let $K=\mathbb{F}_\ell(x)$ be the field of rational functions over $\mathbb{F}_\ell$, and consider the quadratic extension $E=K(\alpha)$, of K, where α is one of the roots of $t^2-xt+1\in K[t]$. It is easy to show that the ring of integers $\mathcal{O}_E$ of E is precisely $\mathcal{O}_K[\alpha]$, where $\mathcal{O}_K=\mathbb{F}_\ell[x]$.

Lemma 2.9. *Let $\tau(x)\neq x\pm 2$ be an irreducible polynomial of $\mathbb{F}_\ell[x]$. Then $\tau(x)$ divides $f_n(x)$ in $\mathcal{O}_K$ if and only if it divides $\alpha^{2n}-1$ in $\mathcal{O}_E$.*

Proof. Suppose $\tau(x)$ divides $f_n(x)$ in $\mathcal{O}_K$. Then $\alpha^n-\alpha^{-n}=(\alpha-\alpha^{-1})q\tau(x)$, for some $q\in\mathcal{O}_K$. Therefore, $\tau(x)$ divides $\alpha^{2n}-1$.

Conversely, suppose that $\tau(x)$ divides $\alpha^{2n}-1$ in $\mathcal{O}_E$. Then $\alpha^n-\alpha^{-n}=\alpha^{-n}q\tau(x)$ for some $q\in\mathcal{O}_E$, and hence $f_n(x)=\tau(x)(q\alpha^{-n}(\alpha-\alpha^{-1}))/(x^2-4)$. Since α is a unit in $\mathcal{O}_E$, it follows that $q\alpha^{-n}(\alpha-\alpha^{-1})\in\mathcal{O}_E\cap K=\mathcal{O}_K$. Finally, the assumption that $\tau\neq x\pm 2$ implies the claim. □

From now on, we use the Legendre symbol $(\frac{\cdot}{\cdot})$ and the second power residue symbol $(\frac{\cdot}{\cdot})_2$ (for the details, refer to [14]). Let $\tau\in\mathbb{F}_\ell[x]$ be an irreducible polynomial, and put $d=\deg(\tau)$. Then

$$\alpha^{\ell^d}=\left\{\frac{x+\sqrt{x^2-4}}{2}\right\}^{\ell^d}$$

$$\equiv\frac{x+((x^2-4)/\tau(x))_2\cdot\sqrt{x^2-4}}{2}\pmod{\tau(x)},$$

by the analogue of Fermat's little theorem for rings of polynomials over finite fields (see the corollary to Proposition 1.8 in [14]). Therefore

$$\alpha^{\ell^d}\equiv\begin{cases}\alpha\pmod{\tau(x)} & \text{if } \left(\dfrac{x^2-4}{\tau(x)}\right)_2=1,\\ \alpha^{-1}\pmod{\tau(x)} & \text{if } \left(\dfrac{x^2-4}{\tau(x)}\right)_2=-1.\end{cases}$$

The reciprocity law for $\mathbb{F}_\ell[x]$ (see [14, Theorems 3.3 and 3.5]) now implies that

$$\left(\frac{x^2-4}{\tau(x)}\right)_2 = \left(\frac{\tau(x)}{x^2-4}\right)_2 = \left(\frac{\tau(x)}{x-2}\right)_2 \left(\frac{\tau(x)}{x+2}\right)_2 = \left(\frac{\tau(2)\tau(-2)}{\ell}\right)$$

by Proposition 3.2 in [14].

This together with the lemma above gives the following:

Proposition 2.10. *Suppose that $\ell \neq 2$ and let $\tau(x) \neq x \pm 2$ be an irreducible polynomial of degree k in $\mathbb{F}_\ell[x]$. Then we have*

$$\tau(x) | f_{\frac{\ell^k-\varepsilon}{2}}(x), \quad \text{where } \varepsilon = \left(\frac{\tau(2)\tau(-2)}{\ell}\right).$$

So far we considered irreducible factors of Chebyshev polynomials. Next it is natural to ask what their multiplicities are. This question is answered by the following:

Proposition 2.11. *If $\ell = 2$ and n is odd, then $f_n(x)$ is the square of a square-free polynomial. If $\ell \neq 2$ and ℓ does not divide n, then $f_n(x)$ is square-free.*

Proof. We will prove the result in the case $\ell \neq 2$. The case $\ell = 2$ was done by Sutner [20]. The proof of the case $\ell \neq 2$ is different from that of the case $\ell = 2$.

Suppose that $\ell \neq 2$ and that n is not divisible by ℓ. We have to check that $\gcd(f_n(x), f_n'(x)) = 1$. To compute $f_n'(x)$, we work in the quadratic extension $\mathbb{F}_\ell(x)(\alpha)$ of $\mathbb{F}_\ell(x)$ to which α and β belong. We note that the derivative on $\mathbb{F}_\ell(x)$ uniquely extends to a derivation on the quadratic extension $\mathbb{F}_\ell(x)(\alpha)$. (Explicitly, in the case $\ell \neq 2$, α and β are $(x \pm \sqrt{x^2-4})/2$ and the derivatives α' and β' are given by the usual formulas.) The identities $\alpha + \beta = x$ and $\alpha\beta = 1$ imply that

$$\alpha' + \beta' = 1 \quad \text{and} \quad \alpha'\beta + \alpha\beta' = 0.$$

Using these relations it is easy to get that

$$(x^2-4) f_n'(x) = n g_n(x) - x f_n(x).$$

It then follows that $\gcd(f_n(x), f_n'(x))$ divides $\gcd(f_n(x), g_n(x))$. On the other hand, one has

$$g_n(x)^2 - (x^2-4) f_n(x)^2 = 4,$$

which can again be easily obtained by Proposition 2.3. This implies $\gcd(f_n(x), g_n(x)) = 1$, since $\ell \neq 2$. Therefore $\gcd(f_n(x), f_n'(x)) = 1$. □

Remark. Using this proposition we can easily generalize Theorem 2.1 in [20] to the case $\ell \neq 2$.

3. Additive cellular automata

We recall Sutner's definition of a σ-automaton on a graph [19,20].

Definition 3.1. Let $G=(V,E)$ be a graph. We define an additive cellular automaton on G with configuration space $\mathscr{C}_G := \{X : V \to \mathbb{F}_\ell\}$ by the global rule $\sigma_G : \mathscr{C}_G \to \mathscr{C}_G$ given by

$$\sigma_G(X)(v) = \sum_{u \in N(v)} X(u),$$

where $N(v) := \{u \in V : \{u,v\} \in E\} \cup \{v\}$ is the neighborhood of v.

Remark. A natural variant of a σ-automaton on G is obtained by taking, instead of the neighborhood $N(v) = N^+(v) := \{u \in V : \{u,v\} \in E\} \cup \{v\}$, the deleted neighborhood $N^-(v) := \{u \in V : \{u,v\} \in E\}$. The two different notions of σ-automata are sometimes referred to as σ^+- and σ^--automata, respectively. Here, we only consider σ^+-automata since questions about reversibility of σ^--automata on square grids turn out to be trivial.

Note that σ_G is a $\mathbb{F}_\ell$-linear endomorphism of the configuration space $\mathscr{C}_G$. In what follows we will identify σ_G with its matrix relative to the canonical basis $\{e_v : v \in V\}$, where $e_v : V \to \mathbb{F}_\ell$ is defined by $e_v(u) = \delta_{uv}$. When the graph G is a parallelotope, i.e. $G = P_{m_1} \square \cdots \square P_{m_d}$, where P_n denotes the path with n vertices and $\square$ denotes the graph Cartesian product,[3] this matrix of σ as well as its characteristic polynomial, have nice descriptions. In fact, in this case the matrix of σ is related to what we will refer to as a Chebyshev matrix:

$$\mathrm{Cb}_m(A) := \begin{pmatrix} A & I & 0 & 0 & \cdots & 0 & 0 & 0 \\ I & A & I & 0 & \cdots & 0 & 0 & 0 \\ 0 & I & A & I & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & I & A & I \\ 0 & 0 & 0 & 0 & \cdots & 0 & I & A \end{pmatrix},$$

an $m \times m$ block matrix, where I denotes the $n \times n$ identity matrix while A is an arbitrary $n \times n$ matrix. Using these, one can describe the matrices of the maps σ for the d-dimensional parallelotopes by induction on d.

If $G = P_n$ then

$$\sigma_{P_n} = \mathrm{Cb}_n(1) = \begin{pmatrix} 1 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 & 1 \end{pmatrix},$$

[3] The graph Cartesian product $G = G_1 \square G_2$ of graphs G_1 and G_2 with disjoint vertex sets V_1 and V_2 and edge sets X_1 and X_2 is the graph with vertex set $V_1 \times V_2$ and (u_1,u_2) adjacent with (v_1,v_2) whenever $[u_1 = v_1$ and u_2 is adjacent with $v_2]$ or $[u_2 = v_2$ and u_1 is adjacent with $v_1]$.

each column describing precisely the action of the corresponding vertex on itself and on its two adjacent neighbors.

Let us now consider the case when $G = H \square P_n$, where H is an arbitrary graph. With $P_n = \{v_1, \ldots, v_n\}$, put $X_i := H \square \{v_i\}$ $(i = 1, \ldots, n)$, the "layers" of G. Two layers, X_i, X_j are said to be adjacent when $|i - j| = 1$. Note that the action of a layer on itself is given by the matrix of σ_H, while the action of a layer on an adjacent layer (and only on these is there any action) is given by identity matrices, since each vertex of any given layer only acts on the vertex located exactly on the same position on an adjacent layer. Therefore, the matrix of σ_G is $\mathrm{Cb}_n(\sigma_H)$, an $n \times n$ block matrix.

It is now clear, by a simple induction, that for parallelotopes one has

Proposition 3.2. *The map σ for the graph $G = P_{m_1} \square \cdots \square P_{m_d}$ has the matrix*:

$$\sigma_{P_{m_1} \square \ldots \square P_{m_d}} = \mathrm{Cb}_{m_d}(\cdots \mathrm{Cb}_{m_2}(\mathrm{Cb}_{m_1}(1)))$$

with respect to the standard basis of $\mathscr{C}_G$.

From now on, the matrix $\mathrm{Cb}_{m_d}(\cdots \mathrm{Cb}_{m_2}(\mathrm{Cb}_{m_1}(1)))$ corresponding to the map $\sigma_{P_{m_1} \square \ldots \square P_{m_d}}$ will be denoted simply by $\mathrm{Cb}_{m_1, \ldots, m_d}$.

In regard to the characteristic polynomial, note that $\mathrm{Cb}(A) - xI = \mathrm{Cb}(A - xI)$, for any matrix A. Using well-known facts on determinants of block matrices (see [6,17] for simple and elementary proofs; or see Theorem 4.10, Section 4 of Chapter XV in [9,10]), one gets:

$$\det(\mathrm{Cb}_n(A) - xI) = \det(f_{n+1}(A - xI)) = \prod_{\alpha \in \{\text{roots of } f_{n+1}(x)\}} \det(A - (x + \alpha)I).$$

If one denotes, as usual, the characteristic polynomial of A by $\chi_A(x)$, then one can write

$$\det(\mathrm{Cb}(A) - xI) = \pm \prod_{\alpha \in \{\text{roots of } f_{n+1}(x)\}} \chi_A(x + \alpha).$$

But the product on the right-hand side is just the resultant

$$\mathrm{Res}_y(\chi_A(x + y), f_{n+1}(y))$$

(see [10, Section 10 Chapter V], and note that both $\chi_A(x)$ and $f_{n+1}(x)$ are monic). All this shows:

Proposition 3.3. *For any graph G, let $\chi_G(x)$ denote the characteristic polynomial of σ_G. Then*:

(a) *For all $n \in \mathbb{N}$,*

$$\chi_{P_n}(x) = \pm f_{n+1}(1 - x).$$

(b) *For an arbitrary graph H and for all $n \in \mathbb{N}$,*

$$\chi_{H \square P_n}(x) = \pm \mathrm{Res}_y(\chi_H(x + y), f_{n+1}(y)).$$

From this result, by a simple induction, one obtains the characteristic polynomial for any parallelotope. These were obtained, in a different way, for hypercubes and only modulo 2, in [16, Theorem 5.9, Corollary 5.2, p. 131]. Note that above result is true over $\mathbb{Z}$, and therefore modulo ℓ for all primes ℓ. It is very easy to determine the signs above, which depend on n and the number of elements in H, but they are irrelevant for all our considerations, and therefore we do not bother to make them explicit.

An important particular case is the two-dimensional rectangles case, for which we get:

Corollary 3.4. *For positive integers m and n*

$$\det(\sigma_{P_m \square P_n}) = \pm \mathrm{Res}_x(f_{m+1}(1-x), f_{n+1}(x)).$$

In particular, $\sigma_{P_m \square P_n}$ is reversible if and only if $\gcd(f_{m+1}(1-x), f_{n+1}(x)) = 1$.

Corollary 3.5. *If $m+1 | n+1$, then $\chi_{H \square P_m}(x) | \chi_{H \square P_n}(x)$.*

Proof. This follows at once from the bi-multiplicativity of the resultant. □

Definition 3.6. We define the set $\mathscr{S}_\ell$ by

$$\mathscr{S}_\ell := \{n \in \mathbb{N} : \gcd(f_n(x), f_n(1-x)) \neq 1 \text{ over } \mathbb{F}_\ell\}.$$

By the above we have that $\sigma_{P_n \square P_n}$ is irreversible over $\mathbb{F}_\ell$ if and only if the number $n+1$ belongs to $\mathscr{S}_\ell$. It immediately follows from Corollary 3.5 that:

Corollary 3.7. *The set $\mathscr{S}_\ell$ is a semigroup under multiplication.*

Definition 3.8. We define the subset of primitive elements in $\mathscr{S}_\ell$ as follows:

$$\mathscr{P}_\ell := \{n \in \mathscr{S}_\ell : \text{ if } m | n \text{ and } m \in \mathscr{S}_\ell \text{ then } m = n\}.$$

In other words, primitive elements are generators of the semigroup $\mathscr{S}_\ell$. For any element $n \in \mathscr{P}_\ell$, the automaton $\sigma_{P_{n-1} \square P_{n-1}}$ is irreversible. Furthermore, for such n any nontrivial configuration from the all-off state to the all-off state on the grid $P_{n-1} \square P_{n-1}$ (i.e. an element in the kernel of the corresponding map σ) cannot be constructed from those on $P_{d-1} \square P_{d-1}$, where d is a divisor of n. We call such an irreversible additive cellular automaton *primitive*. We will extensively study the elements in $\mathscr{P}_\ell$ later.

Remark. Some interesting results are also known about the kernel of $\sigma_{P_m \square P_n}$. In [20] Sutner shows that the dimension of this kernel is precisely the degree of the polynomial $\gcd(f_{m+1}(x), f_{n+1}(1-x))$ when $\ell = 2$. This result can be shown to hold for all primes ℓ. Using this fact together with Proposition 2.7, one can easily prove some otherwise mysterious relations between the numbers $d_n := \dim(\mathrm{Ker}(\sigma_{P_{n-1} \square P_{n-1}}))$. For example, the numbers $d_{\ell^k m}$ and d_m are related (the relation, which depends on whether $\ell \neq 3, 5$ or not, generalizes the one conjectured by Sutner [18]), and so are $d_{(\ell^k-1)/2}$ and $d_{(\ell^k+1)/2}$, for all k.

4. Irreversibility and roots of unity

Throughout this section, the primitive mth root of unity $e^{2\pi i/m}$ is denoted by ζ_m. The aim of this section is to study elements in $\mathscr{S}_\ell$, using number theory over cyclotomic field extensions of $\mathbb{Q}$. In particular, we will find all the elements in the intersection of all $\mathscr{S}_\ell$.

The Chebyshev polynomial $U_{n-1}(x)$ of the second kind is known to be factorized as

$$U_{n-1}(x) = \prod_{k=1}^{n-1} \left(2x - 2\cos\frac{k\pi}{n}\right) = \prod_{k=1}^{n-1} (2x - \zeta_{2n}^{k} - \zeta_{2n}^{-k}).$$

This identity will show a connection between Chebyshev polynomials and cyclotomic field extensions.

Proposition 4.1. *The automaton $\sigma_{P_{m_1}\square\ldots\square P_{m_d}}$ is irreversible if and only if*

$$\prod_{k_1=1}^{m_1} \cdots \prod_{k_d=1}^{m_d} (1 - \eta_1^{k_1} - \cdots - \eta_d^{k_d}) \equiv 0 \bmod \ell,$$

where $\eta_i^{k_i} = \zeta_{2(m_i+1)}^{k_i} + \zeta_{2(m_i+1)}^{-k_i}$.

Proof. Here, we consider all the matrices as ones defined over $\mathbb{Z}$, not over $\mathbb{F}_\ell$. Note that the matrix $\mathrm{Cb}_{m_1,\ldots,m_d}$ can be defined over $\mathbb{Z}$ in the same way as that for $\mathbb{F}_\ell$. It is clear $\sigma_{P_{m_1}\square\ldots\square P_{m_d}}$ is irreversible if and only if the determinant of the matrix $\mathrm{Cb}_{m_1,\ldots,m_d}$ is zero modulo ℓ.

It is easy to check that the determinant of $\mathrm{Cb}_{m_1,\ldots,m_d}$ is

$$\begin{aligned}
\det(\mathrm{Cb}_{m_1\ldots,m_d}) &= \prod_{k_1=1}^{m_1} \det(\mathrm{Cb}_{m_2,\ldots,m_d} - \eta_1^{k_1} I_{r_1}) \\
&= \prod_{k_1=1}^{m_1} \prod_{k_2=1}^{m_2} \det(\mathrm{Cb}_{m_3,\ldots,m_d} - (\eta_1^{k_1} + \eta_2^{k_2}) I_{r_2}) \\
&\vdots \\
&= \prod_{k_1=1}^{m_1} \cdots \prod_{k_{d-1}=1}^{m_{d-1}} \det(\mathrm{Cb}_{m_d} - (\eta_1^{k_1} + \cdots + \eta_{d-1}^{k_{d-1}}) I_{r_{d-1}}) \\
&= \prod_{k_1=1}^{m_1} \cdots \prod_{k_d=1}^{m_d} \{1 - (\eta_1^{k_1} + \cdots + \eta_d^{k_d})\},
\end{aligned}$$

where I_{r_j} is the $(\prod_{i=j+1}^{d} m_i) \times (\prod_{i=j+1}^{d} m_i)$ identity matrix. This completes the proof. □

For any integer $n>1$, $\sigma_{P_n\square P_n}$ can be irreversible over some $\mathbb{F}_\ell$. Needless to say, irreversibility depends on the prime number ℓ. Unless the determinant of the matrix $\mathrm{Cb}_{n,n}$ defined over $\mathbb{Z}$ is zero, $\sigma_{P_n\square P_n}$ can be irreversible over only finitely many number of fields $\mathbb{F}_\ell$. The numbers n for which $\sigma_{P_n\square P_n}$ is irreversible over any field $\mathbb{F}_\ell$ deserve our attention. It is clear that these can be found by searching for the integers n such that the determinants of the matrices $\mathrm{Cb}_{n,n}$ defined over $\mathbb{Z}$ are zero. It turns out that a trigonometric diophantine equation enable us to find all such numbers.

Lemma 4.2. *Let n be a positive integer. There is an integral solution (x, y) to the equation*

$$\cos\frac{\pi x}{n}+\cos\frac{\pi y}{n}=\tfrac{1}{2}$$

if and only if the integer n is a multiple of 5 or 6.

Proof. See [3]. □

Theorem 4.3 (Global irreversibility). *The automaton $\sigma_{P_n\square P_n}$ is irreversible for any prime ℓ if and only if the integer $n+1$ is a multiple of 5 or 6*

Proof. This is an immediate result from Lemma 4.2. □

The proposition above tells us that for any number n such that $n+1$ is a multiple of 5 or 6 and for any prime number ℓ we can find a nontrivial configuration to an $n\times n$ Lights Out game from the all-off state to the all-off state. For the cases $n=4$ and 5 the following are nontrivial configurations:

0	1	$\ell-1$	0
$\ell-1$	0	0	1
1	0	0	$\ell-1$
0	$\ell-1$	1	0

1	$\ell-1$	0	1	$\ell-1$
0	0	0	0	0
$\ell-1$	1	0	$\ell-1$	1
0	0	0	0	0
1	$\ell-1$	0	1	$\ell-1$

Also from these one can construct nontrivial configurations for all numbers of the form $5k-1$ and $6k-1$, by stacking the above configurations leaving a row or a column in between any two.

Meanwhile, it is also interesting to ask for global reversibility, i.e. for what n the automaton $\sigma_{P_n\square P_n}$ is reversible over any finite prime field $\mathbb{F}_\ell$. Even though our intuition supports the claim that any number n except 1 has a prime number ℓ such that $\sigma_{P_n\square P_n}$ is irreversible over $\mathbb{F}_\ell$ and it looks easy to show, we could not find an elementary proof. Instead we prove our claim using p-adic techniques.

Theorem 4.4 (Global reversibility). *Only for $n=1$ is the automaton $\sigma_{P_n\square P_n}$ reversible for any prime ℓ.*

Proof. Suppose that the automaton $\sigma_{P_n\square P_n}$ is reversible for any prime ℓ. Then the determinant of the matrix $\mathrm{Cb}_{n,n}$ defined over $\mathbb{Z}$ must be ± 1. Therefore, we have

$$\det(\mathrm{Cb}_{n,n}) = \prod_{k=1}^{n}\prod_{l=1}^{n}(1-\zeta^k-\zeta^{-k}-\zeta^l-\zeta^{-l}) = \pm 1,$$

where $\zeta=\zeta_{2(n+1)}$. For now, we consider

$$a_{n+1} := \prod_{k=1}^{n}(1-2(\zeta^k+\zeta^{-k}))$$

which is an integer. Since a_{n+1} is a divisor of $\det(\mathrm{Cb}_{n,n})$, we must have $a_{n+1}=\pm 1$.

On the other hand, we see that

$$a_{n+1} = \prod_{k=1}^{n}\left(1-4\cos\frac{k\pi}{n+1}\right) = 2^n\prod_{k=1}^{n}\left(1/2-2\cos\frac{k\pi}{n+1}\right) = 2^nF_{n+1}(1/2).$$

From the recurrence $F_{n+2}(x)=xF_{n+1}(x)-F_n(x)$ with $F_0(x)=0$ and $F_1(x)=1$, we obtain

$$a_{n+2} = a_{n+1} - 4a_n, \quad a_0 = 0, a_1 = 1.$$

The following lemma completes the proof. □

Lemma 4.5. *Let $\{b_n\}$ be the sequence of integers defined by*

$$b_{n+2} = b_{n+1} - 4b_n, \quad b_0 = 1, b_1 = 1.$$

Then, there is no $n>2$ for which $b_n=\pm 1$.

Proof. This can be proved by the exactly same method for Lemma 6.1 [2, pp. 67–70]. For the proof, we use local field $\mathbb{Q}_{17}$ instead of $\mathbb{Q}_{11}$. □

To close this section we prove two statements about the properties of additive cellular automata on square grids from the point of view of cyclotomic field extension theory (all we use here is covered in Chapters 12 and 13 of [7]).

Proposition 4.6. *The following are equivalent*:
1. $\sigma_{P_n \square P_n}$ *is irreversible*.
2. *The prime* ℓ *divides the integer*

$$\prod_{k=1}^{n}\prod_{l=1}^{n}(1-\zeta^k-\zeta^{-k}-\zeta^l-\zeta^{-l}),$$

where $\zeta=\zeta_{2(n+1)}$.
3. *There are elements* x *and* y *in* $\mathbb{F}_{\ell^m}-\{1,-1\}$ *such that*

$$x+\frac{1}{x}+y+\frac{1}{y}=x^{2(n+1)}=y^{2(n+1)}=1,$$

where m *is the order of* l *in* $(\mathbb{Z}/n\mathbb{Z})^*$.

Proof. (1) $\Leftrightarrow$ (2): This is an immediate consequence from Proposition 4.1.

(2) $\Rightarrow$ (3): Let $q=\prod_{k=1}^{n}\prod_{l=1}^{n}(1-\zeta^k-\zeta^{-k}-\zeta^l-\zeta^{-l})$. Suppose that ℓ is factored into $p_1p_2\cdots p_t$ over $\mathbb{Z}[\zeta]$, where each p_i is a prime in $\mathbb{Z}[\zeta]$. Since $\ell|q$ and the field $\mathbb{F}_{\ell^m}\cong\mathbb{Z}[\zeta]/(p_1)$ (in fact, you can use any p_i), q is zero in $\mathbb{F}_{\ell^m}$. Therefore, there are integers $1\leqslant i,j\leqslant n$ such that $1-(\zeta^i+\zeta^{-i}+\zeta^j+\zeta^{-j})=0$ in $\mathbb{F}_{\ell^m}$.

(3) $\Leftarrow$ (2): Let x and y be elements in $\mathbb{F}_{\ell^m}-\{1,-1\}$ satisfying the given equations. Then, there are integers $1\leqslant i,j\leqslant n$ such that $x=\zeta^i+(p_1)$ and $y=\zeta^j+(p_1)$, where p_1 is a prime factor of ℓ over $\mathbb{Z}[\zeta]$. The condition $x+\frac{1}{x}+y+\frac{1}{y}=1$ implies $\zeta^i+\zeta^{-i}+\zeta^j+\zeta^{-j}\in 1+(p_1)$. Therefore,

$$p_1|(1-\zeta^i-\zeta^{-i}-\zeta^j-\zeta^{-j})$$

over $\mathbb{Z}[\zeta]$. This implies

$$\mathrm{Nr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(p_1)|\mathrm{Nr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(1-\zeta^i-\zeta^{-i}-\zeta^j-\zeta^{-j}),$$

where $\mathrm{Nr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}$ is the norm map of the field extension $\mathbb{Q}(\zeta)/\mathbb{Q}$. It is clear that the norm $\mathrm{Nr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(1-\zeta^i-\zeta^{-i}-\zeta^j-\zeta^{-j})$ divides the integer q^4. Therefore, the norm $\mathrm{Nr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(p_1)$ divides q^4. Since $\mathrm{Nr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(p_1)=\ell^m$ and ℓ is a prime, ℓ divides q. □

Proposition 4.7. *Let* p *be a prime number greater than* 5. *If* ℓ *is a primitive root modulo prime number* p, *then* $\sigma_{P_{p-1}\square P_{p-1}}$ *is reversible.*

Proof. Assume that this was not so. Then one would have

$$\ell\left|\prod_{k,l=1}^{p-1}(1-\zeta_{2p}^k-\zeta_{2p}^{-k}-\zeta_{2p}^l-\zeta_{2p}^{-l})\right..$$

The fact that ℓ is a primitive root modulo p implies that it remains prime in $\mathbb{Z}[\zeta_p]=\mathbb{Z}[\zeta_{2p}]$. Therefore one must have, for some $k,l\in\{1,\ldots,p-1\}$,

$$\ell|(1-\zeta_{2p}^k-\zeta_{2p}^{-k}-\zeta_{2p}^l-\zeta_{2p}^{-l}).$$

If one chooses $a, b \in \mathbb{Z}$ so that $1 = (p+2)a + 2pb$, from $\zeta_{2p}^{p+2} = -\zeta_p$ one gets $\zeta_{2p} = (-\zeta_p)^a$. Hence

$$\ell \mid (1 \pm \zeta_p^{ak} \pm \zeta_p^{-ak} \pm \zeta_p^{al} \pm \zeta_p^{-al}).$$

Using the Galois automorphism $\zeta_p \mapsto \zeta_p^{ak}$, this reduces to:

$$\ell \mid (1 - \zeta_p - \zeta_p^{-1} - \zeta_p^{j} - \zeta_p^{-j}),$$

for some $j \in \{1, \ldots, p-1\}$, which is clearly false when $p > 5$. □

This result shows that $p \notin \mathscr{S}_\ell$, when ℓ is a primitive root modulo the prime $p > 5$. It would then follow from a proof of Artin's conjecture on primitive roots (see [11]) that there are infinitely many primes outside $\mathscr{S}_\ell$. By a result of Heath-Brown (see [11] again) one gets that this is true for at least one of the sets $\mathscr{S}_2$, $\mathscr{S}_3$, $\mathscr{S}_5$.

5. Infinitude of primitive irreversible σ-automata

This section is devoted to study $\mathscr{P}_\ell$. The main task here is to show the set $\mathscr{P}_\ell$ is infinite for $\ell = 2$ and 3. For convenience we say the polynomial $f_n(x) \in \mathbb{F}_\ell[x]$ is singular if $\sigma_{P_{n-1}\square P_{n-1}}$ is irreversible, or equivalently $\gcd(f_n(x), f_n(1-x)) \neq 1$, i.e. $n \in \mathscr{S}_\ell$.

Lemma 5.1. *If $\ell = 2$ or 3, then the polynomial $f_{(\ell^p-1)/(\ell-1)}(x)$ is singular, for all primes $p > 3$ (for $\ell = 3$ this holds for $p > 2$).*

Proof. In general, if p does not divide $\ell - 1$, then $\gcd((\ell^p-1)/(\ell-1), \ell^2-1) = 1$, and therefore $\gcd(f_{(\ell^p-1)/(\ell-1)}(x), f_{\ell-1}(x) f_{\ell+1}(x)) = 1$, which implies (see Proposition 2.7) that all the roots of $f_{(\ell^p-1)/(\ell-1)}(x)$ are in $\mathbb{F}_{\ell^p} \setminus \mathbb{F}_\ell$. But then the same is true for the roots of $f_{(\ell^p-1)/(\ell-1)}(a-x)$, for any $a \in \mathbb{F}_\ell$.

When $\ell = 3$, each of these ℓ polynomials has $(\ell^p - \ell)/(\ell - 1)$ roots (they are square-free), and therefore at least two must have a common root. Using an automorphism of $\mathbb{F}_\ell[x]$ together with the fact that $f_{(\ell^p-1)/(\ell-1)}(-x) = \pm f_{(\ell^p-1)/(\ell-1)}(x)$, one concludes that for some $a \in \mathbb{F}_\ell^*$, $\gcd(f_{(\ell^p-1)/(\ell-1)}(x), f_{(\ell^p-1)/(\ell-1)}(a-x)) \neq 1$. This means that either $\gcd(f_{(\ell^p-1)/(\ell-1)}(x), f_{(\ell^p-1)/(\ell-1)}(1-x)) \neq 1$, or $\gcd(f_{(\ell^p-1)/(\ell-1)}(x), f_{(\ell^p-1)/(\ell-1)}(2-x)) \neq 1$. In the first case we are done; on the second just use the automorphism of $\mathbb{F}_\ell[x]$ determined by $x \mapsto x - 1$.

The case $\ell = 2$ was proved in [5]. Here is an alternative (shorter) proof: in this case the polynomial $f_{(\ell^p-1)/(\ell-1)}(x)$ is no longer square-free, but is the square of a square-free polynomial (Proposition 2.11) and has therefore $(\ell^p - \ell)/2$ roots in $\mathbb{F}_{\ell^p} \setminus \mathbb{F}_\ell$. If it were not singular, then it would follow from Proposition 2.7 that $f_{2^p+1}(x) = (1-x)^2 f_{2^p-1}(1-x)$. Using the recurrence relation and (c) of Lemma 2.6, we get

$$x^{2^p} = f_{2^p-1}(x) + (1-x)^2 f_{2^p-1}(1-x).$$

Now, if a is a root of $f_{2^p-1}(x)$, then substituting x by a and $1-a$ in the equality just obtained (and recalling that $a \in \mathbb{F}_{2^p}$, so that $a^{2^p} = a$), one gets that $a = (1-a)^3$. Hence $f_{2^p-1}(x) \mid ((x-1)^3 + x)^2$, which is impossible if $p > 3$. □

Remark. This lemma shows that a Mersenne prime is in $\mathscr{P}_2$. In [5] it is shown that the polynomial $f_{2^k+1} \in \mathbb{F}_2[x]$ is also singular. This implies that a Fermat prime is also in $\mathscr{P}_2$.

The infinitude of the set $\mathscr{P}_\ell$ for $\ell = 2$ and 3 easily follows from this lemma.

Theorem 5.2. *For $\ell = 2$ and 3 the set $\mathscr{P}_\ell$ is infinite.*

Proof. Suppose not. Then we can choose a prime number p greater than all the elements in $\mathscr{P}_\ell$. Since all prime divisors of $(\ell^p - 1)/(\ell - 1)$ are congruent to 1 modulo p, all its divisors except 1 are greater than the biggest element in $\mathscr{P}_\ell$. However, one of the divisors of $(\ell^p - 1)/(\ell - 1)$ must be in the set $\mathscr{P}_\ell$. This is a contradiction. □

As we see, the infinitude of $\mathscr{P}_\ell$ for any prime ℓ can be obtained by proving the following conjecture:

Conjecture 5.3. *For any prime $\ell > 3$ and any odd prime p the polynomial $f_{(\ell^p-1)/(\ell-1)}(x)$ is singular.*

We do not expect that the conjecture has a simple proof. In the sense of arithmetical progressions, what we can do as the second best thing might be to consider whether $f_{(\ell^p-1)/2}(x)$ is singular or not. This question is answered affirmatively by the following:

Proposition 5.4. *For all primes $\ell \geqslant 23$, the polynomials $f_{(\ell-1)/2}(x)$ and $f_{(\ell+1)/2}(x)$ are singular.*

Proof. It follows from Lemma 2.5 that

$$f_{(\ell-1)/2}(x) f_{(\ell+1)/2}(x) = \prod_{a \in \mathbb{F}_\ell \setminus \{\pm 2\}} (x - a).$$

In particular, both these polynomials split over $\mathbb{F}_\ell$.

Now, for each $a \in \mathbb{F}_\ell \setminus \{\pm 2\}$, let $b \in \mathbb{F}_{\ell^2} \setminus \{0, \pm 1\}$ be a solution of the quadratic equation $a = b + b^{-1}$. Then, using the identity right below Proposition 2.3 we get

$$\begin{aligned} f_{(\ell-1)/2}(a) = 0 &\Leftrightarrow b^{(\ell-1)/2} - b^{-(\ell-1)/2} = 0 \quad \Leftrightarrow \quad b^{\ell-1} = 1 \\ &\Leftrightarrow b \in \mathbb{F}_\ell \quad \Leftrightarrow \quad \left(\frac{a^2-4}{\ell}\right) = 1, \end{aligned}$$

where $\left(\frac{\cdot}{\ell}\right)$ is the Legendre symbol, i.e. the quadratic character of $\mathbb{F}_\ell$.

Note that it follows from the two previous paragraphs that

$$f_{(\ell+1)/2}(a) = 0 \quad \Leftrightarrow \quad \left(\frac{a^2-4}{\ell}\right) = -1.$$

The idea is to show that, for each of the two polynomials under consideration, there is an element $a \in \mathbb{F}_\ell \setminus \{\pm 2\}$ such that both a and $1-a$ are among its roots. We start by noting that, for $\ell \geqslant 7$,

$$\mathbb{F}_\ell \setminus \{\pm 2\} = \left\{\frac{1}{2}\right\} \cup \{-1, 3\} \cup \bigcup_{a \in S} \{a, 1-a\},$$

where $S = \{0, 4, 5, \ldots, (\ell-1)/2\}$.

Now, if $f_{(\ell-1)/2}(x)$ is non-singular then $\frac{1}{2}$ is not among its roots. This implies that $\left(\frac{(\frac{1}{2})^2-4}{\ell}\right) = (-15/\ell) = -1$, which means $(-3/\ell) = -(5/\ell)$. Therefore -1 and 3 cannot both be roots of $f_{(\ell-1)/2}(x)$. Since this polynomial has degree $(\ell-3)/2$ and the number of elements in S is equal to $(\ell-5)/2$, it follows that if $f_{(\ell-1)/2}(x)$ is non-singular then for every $b \in S$ either b or $1-b$, but not both, is among its roots. Therefore:

$$\left(\frac{b^2-4}{\ell}\right) = -\left(\frac{(1-b)^2-4}{\ell}\right), \quad \text{for every } b \in S. \qquad (*)$$

Similarly, if $f_{(\ell+1)/2}(x)$ is non-singular, then $\frac{1}{2}$ is not one of its roots, and again by considering its degree it also follows that $(*)$ must be satisfied. Hence if $f_{(\ell-1)/2}(x)$ and $f_{(\ell+1)/2}(x)$ are not both singular then $(*)$ holds.

If $\ell \geqslant 23$ it is easy to see that $7, 9, 10 \in S$, and one gets from $(*)$ that:

$$b = 9 \Rightarrow \left(\frac{7 \cdot 11}{\ell}\right) = -\left(\frac{3 \cdot 5}{\ell}\right),$$

$$b = 10 \Rightarrow \left(\frac{2 \cdot 3}{\ell}\right) = -\left(\frac{7 \cdot 11}{\ell}\right),$$

which together imply that $(5/\ell) = (2/\ell)$. Taking now $b = 7$ in $(*)$ gives the desired contradiction. □

References

[1] R. Barua, S. Ramakrishnan, σ-game, σ^+-game and two-dimensional additive cellular automata, Theoret. Comput. Sci. 154 (1996) 349–366.
[2] J.W.S. Cassels, Local Fields, Cambridge University Press, Cambridge, 1986.
[3] J.H. Conway, A.J. Jones, Trigonometric diophantine equations (On vanishing sums of roots of unity), Acta Arith. 30 (1976) 229–240.
[4] Y. Dodis, P. Winkler, Universal configurations in light-flipping games, Proc. of 12th ACM/SIAM Symp. on Discrete Algorithms, 2001, pp. 926–927.
[5] J. Goldwasser, W. Klostermeyer, H. Ware, Fibonacci polynomials and parity domination in grid graphs, Graphs Combin. 18 (2002) 271–283.
[6] M.H. Ingraham, A note on determinants, Bull. Amer. Math. Soc. 43 (1937) 579–580.
[7] K. Ireland, M. Rosen, A Classical Introduction to Modern Number Theory, 2nd Ed., Springer, Berlin, 1990.
[8] D.E. Knuth, The Art of Computer Programming, 2nd Ed., Addison-Wesley, Reading, MA, 1997.
[9] D. Laksov, L. Svensson, A. Thorup, The spectral mapping theorem, norms on rings, and resultants, Enseign. Math. 46 (2000) 349–358.

[10] S. Lang, Algebra, 2nd Ed., Addison-Wesley, Reading, MA, 1984.
[11] M.R. Murty, Artin's conjecture for primitive roots, Math. Intelligencer 10 (1988) 59–67.
[12] D. Pelletier, Merlin's magic square, Amer. Math. Monthly 94 (1987) 143–150.
[13] T.J. Rivlin, Chebyshev polynomials. From Approximation Theory to Algebra and Number Theory, 2nd Ed., Addison-Wesley, Reading, MA, 1990.
[14] M. Rosen, Number Theory in Function Fields, Springer, Berlin, 2002.
[15] P. Sarkar, σ^+-automata on square grids, Complex Systems 10 (1996) 121–141.
[16] P. Sarkar, R. Barua, Multidimensional σ-automata, π-polynomials and generalised S-matrices, Theoret. Comput. Sci. 197 (1998) 111–138.
[17] J.R. Silvester, Determinants of block matrices, Maths Gazette 84 (2000) 460–467.
[18] K. Sutner, Linear cellular automata and the Garden-of-Eden, Math. Intelligencer 11 (1989) 49–53.
[19] K. Sutner, The σ-game and cellular automata, Amer. Math. Monthly 94 (1990) 24–34.
[20] K. Sutner, σ-Automata and Chebyshev-polynomials, Theoret. Comput. Sci. 230 (2000) 49–73.