Complex Systems **10** (1996) 121–141

σ^+-Automata on Square Grids

Palash Sarkar[*]
Computer Science Unit,
Indian Statistical Institute,
203, B.T. Road,
Calcutta 700035, India

Abstract. In this paper σ^+-automata on square grids are studied using a special sequence of polynomials called the π-polynomials. It is shown that for $m \neq 4$, $\pi_{m+1}(n) \neq \pi^+_{m+1}(n)$, which rules out totally irreversible $m \times m$ grids for $m \neq 4$. Results are presented on the roots of π-polynomials which have direct relevance to the reversibility question for σ^+-automata on square grids.

1. Introduction

The study of σ-automata rises from two sources: the study of the σ-game and the study of additive (linear) cellular automata (CA). The σ-game is a combinatorial game based upon the battery operated toy *Merlin* [4]. The connection of the σ-game to two-dimensional CA was first investigated in [7] and later in [1]. A phenomenological study of CA was undertaken in [12] that led to an extensive body of work on both theory and applications of CA as in [11]. Algebraic properties of additive one-dimensional CA were first studied in [3]. From [8,10], *σ-automata* is defined as a class of binary CA on a graph, where each node of the graph can assume the states 0 or 1. The state of a node in a particular time step is given by the local rule, which is equal to the sum (modulo two) of the states of all its neighbors in the previous time step. If the underlying graph is a finite D-dimensional grid, then the corresponding σ-automata becomes equivalent to a finite D-dimensional additive CA with orthogonal neighborhood. The *σ^+-automata* is defined similarly, except that each node itself is considered to be one of its neighbors.

A *configuration* of a $\sigma(\sigma^+)$-automata is an assignment of values 0 or 1 to the vertices of the underlying graph. The automata evolves synchronously in discrete time steps according to the local rule applied individually to each cell. The global dynamics of such a system are captured by a directed graph called the *state transition graph* or the *state transition diagram* (STD). The

[*] Electronic mail address: `palash@isical.ernet.in`.

vertices of the STD are the configurations of the automata and an edge exists from vertex i to vertex j if and only if configuration i leads to configuration j in one time step. Each component of the STD consists of a single cycle with trees of height ≥ 0 rooted on each cycle vertex (e.g., [3]). A large number of results on the structure of STD for additive CA are also available in [3].

The transition rule of an n-cell one-dimensional σ-automata is given by the following matrix [1], with entries from $GF(2)$:

$$S_n = \begin{bmatrix} 0 & 1 & . & . & . & . & 0 \\ 1 & 0 & 1 & . & . & . & 0 \\ . & & & . & . & . & . \\ . & & & . & . & . & . \\ 0 & & & . & 1 & 0 & 1 \\ 0 & & & . & . & 1 & 0 \end{bmatrix}.$$

Note that S_n is a tridiagonal matrix with the upper and lower subdiagonals having all ones. The characteristic and minimal polynomial of S_n coincides [6,10] and is given by $\pi_{n+1}(x)$ (over $GF(2)$) defined below (see also [1,8,10]):

$$\begin{aligned} \pi_0 &= 0 \\ \pi_1 &= 1 \\ \pi_{n+1}(x) &= x\pi_n(x) + \pi_{n-1}(x) \qquad \text{for } n \geq 1. \end{aligned}$$

Alternatively, $\pi_n(x)$ can be written as [10]

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

These polynomials have interesting divisibility properties which have been studied in [1,10]. It turns out that the π-polynomials also satisfy the following recurrence ([10], see also [1]):

$$\pi_{p+q}(x) = \pi_{q+1}(x)\pi_p(x) + \pi_q(x)\pi_{p-1}(x).$$

As a consequence, the following properties can be derived.

1. $m|n$ iff $\pi_m(x)|\pi_n(x)$.
2. $\gcd(\pi_m(x), \pi_n(x)) = \pi_{\gcd(m,n)}(x)$.
3. $\pi_{2^d n}(x) = x^{2^d-1}\pi_n^{2^d}(x)$.
4. $\pi_{2n+1}(x) = \pi_{n+1}^2(x) + \pi_n^2(x) = (\pi_{n+1}(x) + \pi_n(x))^2$.

The factorization of the π-polynomials are worked out in [10]. Let $\tau(x)$ be an irreducible polynomial over $GF(2)$. Then the depth of $\tau(x)$ is the least positive integer $n = dp(\tau)$ such that $\tau(x)$ divides $\pi_n(x)$. It is shown in [10] that $dp(\tau)$ exists for all irreducible polynomials $\tau(x)$ and $\deg(\tau)$ is the suborder ($\text{sord}_n(2)$) of 2 in the multiplicative group $Z^*_{dp(\tau)}$ (recall that for odd n, $\mathrm{sord}_n(2)$ is the least integer j such that $2^j \equiv \pm 1 \bmod n$). So it immediately follows that $dp(\tau)$ divides either $2^{\deg(\tau)}+1$ or $2^{\deg(\tau)}-1$. Let

$$\rho_n(x) = \prod_{dp(\tau)=n} \tau^2(x).$$

Then $\rho_n(x)$ is called the *critical term* of $\pi_n(x)$ (e.g., [10]). The number of distinct irreducible factors of $\rho_n(x)$ is equal to $\frac{\phi(n)}{2\mathrm{sord}_n(2)}$ (here $\phi(n)$ is the Euler function with a value that is the number of positive integers less than n and coprime to n). It is possible to obtain a factorization of $\pi_n(x)$ in terms of $\rho_n(x)$ (e.g., [10]). Let $n = 2^k p$, where p is odd. Then,

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

and degree $\rho_d = \phi(d)$ for $d \neq 1$. So if n is prime and $\phi(n) = 2\mathrm{sord}_n(2)$, then $\pi_n(x) = \tau^2(x)$ where $\tau(x)$ is irreducible. We use this later to derive a sufficient condition for reversibility of σ^+-automata.

For one-dimensional σ^+-automata, the transition matrix is given by $S_m^+ = S_m + I_m$, and the characteristic and minimal polynomial of S_m^+ is given by $\pi_{m+1}^+(x) = \pi_{m+1}(1+x)$. Similar divisibility properties hold for the π^+-polynomials. Any irreducible polynomial $\tau(x)$ divides $\pi_m^+(x)$ for some m [10].

A $\sigma(\sigma^+)$-automata is said to be reversible if and only if the corresponding linear transformation is invertible. Reversibility is an important phenomena for this class of automata (see also [8]). It means that the state transition graph consists entirely of cycles, and as a result it is possible to start from one configuration and return to it after a finite number of steps. The σ-automata on an $m \times n$ grid are reversible if and only if $\pi_{m+1}(x)$ and $\pi_{n+1}(x)$ are relatively prime if and only if $m+1$ and $n+1$ are relatively prime. This result has been derived using different methods [1,7,8,10]. The coprimeness of $m+1$ and $n+1$ present a nice characterization of reversibility. Unfortunately, for the σ^+-automata obtaining such a simple characterization seems to be difficult, though it is known [1,10] that σ^+-automata on an $m \times n$ grid are reversible if and only if $\pi_{m+1}^+(x)$ and $\pi_{n+1}(x)$ are coprime. The problem has, however, been solved for certain special cases [1,10]. Reversibility of higher dimensional $\sigma(\sigma^+)$-automata have also been studied [5].

In this paper we study σ^+-automata on square $m \times m$ grids. Our work is motivated by two open problems posed in [10]. Before we state them we need to introduce the concept of total irreversibility. In what follows we denote the polynomial obtained from $p(x)$ by the map $x \to 1+x$ over $GF(2)$ with $p^+(x)$.

The concept of total irreversibility is introduced in [10] for σ^+-automata on product graphs $G = H \times P_n$, where H is an arbitrary graph and P_n is the path graph on n vertices. We, however, describe the concept only for graphs of the form $P_m \times P_n$, that is, $m \times n$ grids. The corank (dimension of kernel) of the σ^+-automata on an $m \times n$ grid is given by $\mathrm{cork}(\pi_{m+1}^+(S_n)) =$

cork$(\pi^+_{n+1}(S_m))$ (e.g., [1,10]). If the corank is zero then the automata is reversible and if the corank is positive then it is irreversible. Thus the maximum value of the corank in some sense captures the notion of maximum irreversibility and leads to the following definition of total irreversibility. The σ^+-automata on an $m \times n$ grid is totally irreversible if it has the maximum corank, that is, if cork$(\pi^+_{n+1}(S_m)) = n$ if and only if $\pi^+_{n+1}(S_m) = 0$. But $\pi_{m+1}(x)$ is the minimal polynomial for S_m and hence divides $\pi^+_{n+1}(x)$. The least value of n for which this occurs is defined to be the weak period of P_m, the path graph on m vertices. For some interesting results on weak periods see [10]. For the case of square grids, $m = n$ and $\pi_{m+1}(x) \mid \pi^+_{n+1}(x)$ implies $\pi_{m+1}(x) = \pi^+_{m+1}(x)$. So a square grid is totally irreversible under σ^+-automata if and only if $\pi_{m+1}(x) = \pi^+_{m+1}(x)$. Now we can state the two open problems from [10] that are studied.

1. "For the $m \times m$ grid to be reversible under rule σ^+ we must have $6 \not| m + 1$ and for all odd $e > 3$ such that $e | m + 1$ and $\tau | \rho_e$ irreducible: $dp(\tau^+) \not| m+1$. Is there a simple algorithm to test the second property?"
2. "Are there any totally irreversible squares other than 4×4? Equivalently, is there any $m > 4$ such that $\pi_{m+1}(x) = \pi^+_{m+1}(x)$?"

It is conjectured in [10] that the answer to the second question is no and here we prove that indeed it is no. Doing this also proves that the corank of the σ^+-automata on a square $m \times m$ grid is strictly less than m for $m \neq 4$.

As for the first question we derive an alternative equivalent condition for reversibility and use it to obtain several sufficient conditions for both reversibility and irreversibility. The analysis leads us to obtain a complete characterization of irreducible polynomials $\tau(x)$ over $GF(2)$ with $\tau(x) = \tau^+(x)$. It turns out that characterizing the depths of such polynomials is essential for obtaining a simple characterization of reversibility. Our results indicate that this in general is difficult.

2. Total irreversibility

In this section we prove that totally irreversible grids do not exist for $m \neq 4$. We essentially prove that $\pi_{m+1}(x) \neq \pi^+_{m+1}(x)$ for $m \neq 4$. Then the result follows from what has been discussed in the introduction. We start by proving some preliminary results.

The following can easily be proved by induction.

Lemma 2.1. *If m is even, then we have the following.*

1. *$\pi_{m+1}(x)$ contains only even powers of x, that is, for odd r the coefficient of x^r in $\pi_{m+1}(x)$ is 0.*
2. *The coefficient of x^{m-2} in $\pi_{m+1}(x)$ is 1.*

Lemma 2.2. *If $\pi^+_{m+1}(x) = \pi_{m+1}(x)$, then $m \equiv 4 \bmod 16$.*

Proof: We prove this in four steps.

Step 1: If $\pi^+_{m+1}(x) = \pi_{m+1}(x)$, then m must be even.

If $\alpha_1, \dots, \alpha_m$ are the roots of $\pi_{m+1}(x)$ then $1 + \alpha_1, \dots, 1 + \alpha_m$ are the roots of $\pi^+_{m+1}(x)$.

The coeficient of x^{m-1} in $\pi_{m+1}(x)$ is $\sum_{i=1}^m \alpha_i$ and the coefficient of x^{m-1} in $\pi^+_{m+1}(x)$ is $\sum_{i=1}^m (1 + \alpha_i)$.

So if $\pi^+_{m+1}(x) = \pi_{m+1}(x)$, then

$$\sum_{i=1}^m \alpha_i = \sum_{i=1}^m (1 + \alpha_i)$$

which gives that m mod $2 = 0$. Hence m must be even.

Step 2: If $\pi^+_{m+1}(x) = \pi_{m+1}(x)$ then $m \equiv 0$ mod 4.

By Step 1, we have that m is even, say equal to $2r$. Hence $\pi_{m+1}(x)$ contains only even powers of x (by Lemma 2.1(1)). Let $\alpha_1, \dots, \alpha_m$ be the roots of $\pi_{m+1}(x)$. Then $\sum_{i=1}^m \alpha_i = 0$.

So if $\pi^+_{m+1}(x) = \pi_{m+1}(x)$, equating the coefficient of x^{m-2}, we get,

$$\begin{aligned}
\sum_{i=1}^m \sum_{j=i+1}^m \alpha_i \alpha_j &= \sum_{i=1}^m \sum_{j=i+1}^m (1 + \alpha_i)(1 + \alpha_j) \\
&= \binom{m}{2} \bmod 2 + (m-1) \sum_{i=1}^m \alpha_i \\
&\quad + \sum_{i=1}^m \sum_{j=i+1}^m \alpha_i \alpha_j \\
&= \binom{m}{2} \bmod 2 + \sum_{i=1}^m \sum_{j=i+1}^m \alpha_i \alpha_j
\end{aligned}$$

$$\begin{aligned}
&\Rightarrow \binom{m}{2} \bmod 2 = 0 \\
&\Rightarrow \frac{2r(2r-1)}{2} \bmod 2 = 0 \\
&\Rightarrow r \text{ must be even} \\
&\Rightarrow m \equiv 0 \bmod 4.
\end{aligned}$$

Step 3: If $\pi_{m+1}(x) = \pi^+_{m+1}(x)$, then $m \equiv 4$ mod 8.

By Step 2, we have $m = 4k$. Since by assumption $\pi^+_{m+1}(x) = \pi_{m+1}(x)$ equating the coefficient of x^{m-4} on both sides we get,

$$\sum_{i_1, i_2, i_3, i_4} \alpha_{i_1} \alpha_{i_2} \alpha_{i_3} \alpha_{i_4} = \sum_{i_1, i_2, i_3, i_4} (1 + \alpha_{i1})(1 + \alpha_{i_2})(1 + \alpha_{i_3})(1 + \alpha_{i_4}).$$

Again using the fact that m is even, we know that $\pi_{m+1}(x)$ contains only the even powers of x, hence

$$\sum_i \alpha_i = \sum_{i_1, i_2, i_3} \alpha_{i_1} \alpha_{i_2} \alpha_{i_3} = 0.$$

Therefore,

$$\begin{aligned}\sum_{i_1,i_2,i_3,i_4} \alpha_{i_1}\alpha_{i_2}\alpha_{i_3}\alpha_{i_4} &= \binom{m}{4} \bmod 2 + \binom{m-2}{2} \bmod 2 \sum_{i_1,i_2} \alpha_{i_1}\alpha_{i_2} \\ &\quad + \sum_{i_1,i_2,i_3,i_4} \alpha_{i_1}\alpha_{i_2}\alpha_{i_3}\alpha_{i_4}.\end{aligned}$$

Now,

$$\begin{aligned}\binom{m-2}{2} \bmod 2 &= \binom{4k-2}{2} \bmod 2 \\ &= \frac{(4k-2)(4k-3)}{2} \bmod 2 \\ &= 1\end{aligned}$$

and by Lemma 2.1(2), $\sum_{i_1,i_2} \alpha_{i_1}\alpha_{i_2} = 1$.

So we get

$$\begin{aligned}\binom{m}{4} \bmod 2 &= 1 \\ \Rightarrow \frac{4k(4k-1)(4k-2)(4k-3)}{1 \times 2 \times 3 \times 4} &\bmod 2 = 1 \\ \Rightarrow \frac{k(4k-1)(2k-1)(4k-3)}{3} &\bmod 2 = 1 \\ \Rightarrow k &\text{ must be odd} \\ \Rightarrow m &\equiv 4 \bmod 8.\end{aligned}$$

Step 4: If $\pi^+_{m+1}(x) = \pi_{m+1}(x)$, then $m \equiv 4 \bmod 16$.

By Step 3, we have that $m = 8k + 4$.

So assuming $\pi^+_{m+1}(x) = \pi_{m+1}(x)$, we equate the coefficient of x^{m-8} on both sides to get,

$$\begin{aligned}\sum_{i_1,\ldots,i_8} \alpha_{i_1}\ldots\alpha_{i_8} &= \sum_{i_1,\ldots,i_8} (1+\alpha_{i_1})\ldots(1+\alpha_{i_8}) \\ &= \binom{m}{8} \bmod 2 + \binom{m-2}{6} \bmod 2 \sum_{i_1,i_2} \alpha_{i_1}\alpha_{i_2} \\ &\quad + \binom{m-4}{4} \bmod 2 \sum_{i_1,\ldots,i_4} \alpha_{i_1}\ldots\alpha_{i_4} \\ &\quad + \binom{m-6}{2} \bmod 2 \sum_{i_1,\ldots,i_6} \alpha_{i_1}\ldots\alpha_{i_6} \\ &\quad + \sum_{i_1,\ldots,i_8} \alpha_{i_1}\ldots\alpha_{i_8}.\end{aligned}$$

Now for $m = 8k + 4$ we have

$$\binom{m}{8} = \binom{8k+4}{8} \equiv k \bmod 2$$

$$\begin{aligned} \binom{m-2}{6} &= \binom{8k+2}{6} \equiv 0 \bmod 2 \\ \binom{m-4}{4} &= \binom{8k}{4} \equiv 0 \bmod 2 \\ \binom{m-6}{2} &= \binom{8k-2}{2} \equiv 1 \bmod 2. \end{aligned}$$

So we get

$$k \bmod 2 + \sum_{i_1,\ldots,i_6} \alpha_{i_1} \ldots \alpha_{i_6} = 0.$$

But $c = \sum_{i_1,\ldots,i_6} \alpha_{i_1} \ldots \alpha_{i_6}$ is the coefficient of x^{m-6} in $\pi_{m+1}(x)$ and is determined as follows (using equation (1)),

$$\begin{aligned} c &= \binom{m+1+m-6}{2(m-6)+1} = \binom{2m-5}{2m-11} = \binom{2m-5}{6} \\ &= \binom{16k+8-5}{6} = \binom{16k+3}{6} \equiv 0 \bmod 2. \end{aligned}$$

Hence it follows that k must be even and so $m \equiv 4 \bmod 16$. ■

Let $c(m,i)$ be the coefficient of x^i in $\pi_m(x)$. Then using equation (1) we can prove the following.

Lemma 2.3. *For* $m \equiv 4 \bmod 16$*:*

1. $c(m+1, m) \equiv 1 \bmod 2$
2. $c(m+1, m-2) \equiv 1 \bmod 2$
3. $c(m+1, m-4) \equiv 1 \bmod 2$
4. $c(m+1, m-6) \equiv 0 \bmod 2$
5. $c(m+1, m-8) \equiv 0 \bmod 2$
6. $c(m+1, m-10) \equiv 1 \bmod 2$
7. $c(m+1, m-12) \equiv 1 \bmod 2$

Proof. As the proofs of 1 through 7 are similar, we only prove 7.

Since $m \equiv 4 \bmod 16$ we can write $m = 16k+4$. So from equation (1) we get

$$\begin{aligned} c(m+1, m-12) &= \binom{m+1+m-12}{2(m-12)+1} \bmod 2 \\ &= \binom{2m-11}{2m-23} \bmod 2 \\ &= \binom{2m-11}{12} \bmod 2 \end{aligned}$$

$$\begin{aligned}
&= \binom{32k-3}{12} \bmod 2 \\
&\equiv \frac{32k-4}{4}\frac{32k-6}{6}\frac{32k-8}{8}\frac{32k-10}{10}\frac{32k-12}{12}\frac{32k-14}{2}Y \bmod 2 \\
&\equiv 1 \bmod 2
\end{aligned}$$

where $Y = \frac{32k-3}{3}\frac{32k-5}{5}\frac{32k-7}{7}\frac{32k-9}{9}\frac{32k-11}{11}\frac{32k-13}{13}$. ■

Lemma 2.4. *For $m \equiv 4 \bmod 16$ the coefficient of x^{m-12} in $\pi^+_{m+1}(x)$ is 0.*

Proof. From equation (1) we have

$$\begin{aligned}
\pi_{m+1}(x) &= \sum_i \binom{m+1+i}{2i+1} x^i \bmod 2 \\
\Rightarrow \pi^+_{m+1}(x) &= \sum_i \binom{m+1+i}{2i+1} (1+x)^i \bmod 2.
\end{aligned}$$

If C is the coefficient of x^{m-12} in $\pi^+_{m+1}(x)$ then

$$C = \sum_{i=0}^{12} \binom{m+1+m-12+i}{2(m-12+i)+1}\binom{m-12+i}{m-12}.$$

Using Lemma 2.3 and the fact that $\pi_{m+1}(x)$ contains only even powers of x we can conclude that the first term is nonzero only for $i = 0, 2, 4, 10, 12$. Hence,

$$C \equiv \binom{m-12}{m-12} + \binom{m-10}{m-12} + \binom{m-4}{m-12} + \binom{m-2}{m-12} + \binom{m}{m-12}$$

$$\Rightarrow C \equiv 1 + \binom{m-10}{2} + \binom{m-4}{8} + \binom{m-2}{10} + \binom{m}{12}$$

Since $m \equiv 4 \bmod 16$ we can write $m = 16k + 4$ and so

$$\begin{aligned}
\binom{m-10}{2} &= \binom{16k-6}{2} \equiv 1 \bmod 2 \\
\binom{m-4}{8} &\equiv \binom{m-2}{10} \equiv \binom{m}{12} \equiv 0 \bmod 2.
\end{aligned}$$

Hence, $C = 1 + 1 \equiv 0 \bmod 2$. ■

Theorem 2.1. *$\pi_{m+1}(x) = \pi^+_{m+1}(x)$ if and only if $m = 4$.*

Proof. For $m = 1, 2$, or 3 it is easy to verify that $\pi_{m+1}(x) \neq \pi^+_{m+1}(x)$ and for $m = 4$ it is also easy to verify that $\pi_{m+1}(x) = \pi^+_{m+1}(x)$.

If $m > 4$ then assume that $\pi^+_{m+1}(x) = \pi_{m+1}(x)$. Then by Lemma 2.2 it follows that $m \equiv 4 \bmod 16$. But by Lemma 2.4 it then follows that the coefficient of x^{m-12} in $\pi^+_{m+1}(x)$ is 0 and by Lemma 2.3 the coefficient of x^{m-12} in $\pi_{m+1}(x)$ is 1. So this means that $\pi^+_{m+1}(x) \neq \pi_{m+1}(x)$, which is a contradiction to our assumption. Hence the result follows. ■

So this proves that totally irreversible grids do not exist for $m \neq 4$.

3. Reversibility

In this section we address the problem of characterizing reversible σ^+-automata on square $m \times m$ grids. A necessary and sufficient condition for reversibility from [1,10] is that $\pi_{m+1}(x)$ and $\pi^+_{m+1}(x)$ are relatively prime. For the case of σ-automata on an $m \times n$ grid, the analogous condition for reversibility is that $\pi_{m+1}(x)$ and $\pi_{n+1}(x)$ are relatively prime [1,10]. Thus on a square $m \times m$ grid, σ-automata are always irreversible. For the σ^+-automata on a square grid an equivalent condition for reversibility is stated in [10]:

> "$6 \not| m+1$ and for all odd $e > 3$, such that $e | m+1$ and $\tau | \rho_e$ irreducible: $dp(\tau^+) \not| m+1$."

The author asked for a simple algorithm to test for the second property.

Here we view the problem from a different angle. We translate the condition for reversibilty into a condition on the roots of $\pi_{m+1}(x)$. From this we are able to derive certain simple sufficient conditions for both reversibility and irreversibility. We also indicate why a simple characterization of reversibility is difficult. Note that reversibility may be determined in $O(N^3)$ steps (where N is the number of cells) by forming the adjacency matrix and reducing it to its Hermite canonical form (HCF). The HCF will also provide the corank (dimension of the kernel) of the σ^+ operator.

The following characterizes reversibility of σ^+-automata on a square $m \times m$ grid.

Lemma 3.1. *The σ^+-automata on an $m \times m$ grid is irreversible if and only if there exist roots α and β of $\pi_{m+1}(x)$, such that $\alpha + \beta = 1$.*

Proof. First note that the roots of $\pi^+_{m+1}(x)$ are $1 + \gamma_i$ where the γ_is are roots of $\pi_{m+1}(x)$. Then the result follows simply from the fact that σ^+-automata are irreversible if and only if $\pi_{m+1}(x)$ and $\pi^+_{m+1}(x)$ are not relatively prime if and only if $\pi_{m+1}(x)$ and $\pi^+_{m+1}(x)$ share a common root. ■

For a more general result on multidimensional automata see [5]. From the above result we can see that irreversibility can occur in the following two ways.

1. There exists an irreducible factor $\tau(x)$ of $\pi_{m+1}(x)$, such that $\tau(x)$ has two roots α and β with $\alpha + \beta = 1$. Later we show that for such $\tau(x)$ it holds that $\tau(x) = \tau^+(x)$.
2. There exists two distinct irreducible factors $\tau_1(x)$ and $\tau_2(x)$ of $\pi_{m+1}(x)$ having roots α and β respectively with $\alpha + \beta = 1$. We will prove that under this condition $\tau_2(x) = \tau_1(1 + x)$.

Now it is easy to see why the condition in [10] holds. It essentially says that for any irreducible polynomial $\tau(x)$, both $\tau(x)$ and $\tau^+(x)$ should not divide $\pi_{m+1}(x)$, that is, the depths of both $\tau(x)$ and $\tau^+(x)$ should not divide

$m+1$. (Note that $6|m+1$ means that $\pi_2(x)|\pi_{m+1}(x)$ and $\pi_3(x)|\pi_{m+1}(x)$, and $\pi_2(x) = x$ and $\pi_3(x) = (1+x)^2$.)

One can generate $\pi_{m+1}(x)$ and $\pi^+_{m+1}(x)$ and run the gcd algorithm on them to check if they are relatively prime. This procedure will in general be more time efficient than determining the HCF and will require less storage space. An interesting related problem is to compute $p^+(x)$ where $p(x)$ is an arbitrary polynomial over $GF(2)$.

Let $c(m,i)$ and $c^+(m,i)$ denote the coefficient of x^i in $p(x)$ and $p^+(x)$ respectively. Then,

$$\begin{aligned} c^+(m, m-r) &= \sum_{1 \le i_1 < i_2 < \ldots < i_r \le m} (1+\alpha_{i_1})(1+\alpha_{i_2})\ldots(1+\alpha_{i_r}) \\ &= \binom{m}{r} + \binom{m-1}{r-1} \bmod 2c(m, m-1) \\ &\quad + \binom{m-2}{r-2} \bmod 2c(m, m-2) + \ldots \\ &\quad + \binom{m-r}{r-r} \bmod 2c(m, m-r) \\ &= \sum_{i=0}^{r} D(m-i, r-i)c(m, m-i) \end{aligned}$$

where $D(m-i, r-i) = \binom{m-i}{r-i} \bmod 2$.

So,

$$\begin{aligned} p^+(x) &= \sum_{r=0}^{m} c^+(m, m-r)x^{m-r} \\ &= \sum_{r=0}^{m} \left(\sum_{i=0}^{r} D(m-i, r-i)c(m, m-i) \right) x^{m-r}. \end{aligned}$$

Therefore, if Pascal's triangle (modulo 2) is available up to integer m, it is easy to compute $p^+(x)$.

Proposition 3.1. *If any one of the following conditions hold then σ^+-automata on an $m \times m$ grid are irreversible.*

1. $6|m+1$
2. $5|m+1$
3. $17|m+1$

Proof.

1. $6|m+1 \;\Leftrightarrow\; 2|m+1$ and $3|m+1 \;\Leftrightarrow\; \pi_2(x)|\pi_{m+1}(x)$ and $\pi_3(x)|\pi_{m+1}(x)$ $\Leftrightarrow x|\pi_{m+1}(x)$ and $(1+x)|\pi_{m+1}(x) \;\Leftrightarrow\; x(1+x)|\gcd(\pi_{m+1}(x), \pi^+_{m+1}(x))$.

2. $\pi_5(x) = x^4 + x^2 + 1 = (x^2 + x + 1)^2$. Let α and β be the roots of $x^2 + x + 1$. Then $\alpha + \beta = 1$ and so if $\pi_5(x)|\pi_{m+1}(x)$ then α and β are also roots of $\pi_{m+1}(x)$ and so irreversibility occurs. But $\pi_5(x)|\pi_{m+1}(x)$ if and only if $5|m + 1$.

3. Consider $\tau(x) = x^4 + x + 1$. Then τ is an irreducible (in fact primitive) polynomial over $GF(2)$ with roots $\alpha, \alpha^2, \alpha^{2^2}$, and α^{2^3}. But $\alpha^4 + \alpha = 1$ since α is a root of τ. So if for some m, $\tau(x)|\pi_{m+1}(x)$, then σ^+-automata on an $m \times m$ grid are irreversible. Since the depth of τ is 17 this can happen if and only if $17|m + 1$. ■

To extend the ideas of 2 and 3 in the previous proof one should be able to do the following.

- Characterize all irreducible polynomials $\tau(x)$ having two roots α and β with $\alpha + \beta = 1$.

- Compute the depths of all such $\tau(x)$.

Next we obtain a complete characterization of all irreducible polynomials $\tau(x)$ having two roots α and β with $\alpha + \beta = 1$. It turns out that these are the irreducible polynomials which are fixed under the map $x \to 1 + x$, that is, $\tau(x) = \tau^+(x)$. In what follows we use some standard results on irreducible polynomials over finite fields which are all available in [2].

Lemma 3.2. *Let $\tau_1(x)$ and $\tau_2(x)$ be two irreducible polynomials over $GF(2)$. Let α be a root of $\tau_1(x)$ and β be a root of $\tau_2(x)$, with $\beta = 1 + \alpha$. Then $\tau_2(x) = \tau_1(1 + x)$.*

Proof. The roots of $\tau_1(x)$ are $\alpha, \alpha^2, \alpha^{2^2}, \ldots, \alpha^{2^{r_1-1}}$ where r_1 is the degree of $\tau_1(x)$. Similarly the roots of $\tau_2(x)$ are $\beta, \beta^2, \beta^{2^2}, \ldots, \beta^{2^{r_2-1}}$ where r_2 is the degree of $\tau_2(x)$. Now,

$$\beta^{2^i} = (1 + \alpha)^{2^i} = 1 + \alpha^{2^i}$$

since we are working over a field of characteristic two.

Also $(1 + \alpha^{2^i})$ $(0 \leq i \leq r_1 - 1)$ are the roots of $\tau_1(1 + x)$ (which is also irreducible) and $(1 + \alpha^{2^i})$ $(0 \leq i \leq r_1 - 1)$ are all distinct. So $r_2 \geq r_1$. Now if $r_2 > r_1$, then $\tau_1(1 + x)$ properly divides $\tau_2(x)$ which is a contradiction since $\tau_2(x)$ is irreducible. So $r_2 = r_1$ and all the roots of $\tau_1(1 + x)$ are the roots of $\tau_2(x)$. Hence $\tau_2(x) = \tau_1(1 + x)$. ■

Lemma 3.3. *Let $\tau(x)$ be an irreducible polynomial such that it has two roots α and β, with $\alpha + \beta = 1$. Then the degree of τ must be even.*

Proof. $\beta = \alpha^{2^i}$ for some $i \in \{0, \ldots, r-1\}$ where r is the degree of τ. So $\alpha + \beta = 1$ means

$$\begin{aligned} \alpha + \alpha^{2^i} &= 1 \\ &\Rightarrow (\alpha + \alpha^{2^i})^{2^j} = 1 \qquad 0 \le j \le r-1 \end{aligned}$$

This gives r equations,

$$\begin{aligned} \alpha + \alpha^{2^i} &= 1 \\ \alpha^2 + \alpha^{2^{i+1}} &= 1 \\ &\vdots \\ \alpha^{2^{r-1}} + \alpha^{2^{i+r-1}} &= 1. \end{aligned}$$

Summing up the left- and right-hand sides we get,

$$\sum_{j=0}^{r-1} \alpha^{2^j} + \sum_{j=0}^{r-1} \alpha^{2^{i+j}} = r \bmod 2.$$

But

$$\begin{aligned} \sum_{j=0}^{r-1} \alpha^{2^j} &= \sum_{j=0}^{r-1} \alpha^{2^{i+j}} \\ &\Rightarrow r \bmod 2 = 0 \end{aligned}$$

and so r is even. ■

Lemma 3.4. *Let $\tau(x)$ be an irreducible polynomial over $GF(2)$. Then $\tau(x) = \tau^+(x)$ if and only if $\tau(x)$ has two roots α and β, such that $\alpha + \beta = 1$.*

Proof. If $\tau(x) = \tau^+(x)$ the result is easy, so we only prove the other direction. Since $\alpha + \beta = 1$, $\tau(x)$ has two roots α and $\alpha + 1$. But then $\tau^+(x)$ also has the roots α and $\alpha + 1$. This means that $\gcd(\tau(x), \tau^+(x))$ is nontrivial. But then it must be whole of both $\tau(x)$ and $\tau^+(x)$. ■

From the preceding two lemmas we can see that the irreducible polynomials which are fixed under the map $x \to 1 + x$ must have even degree. From the proof of Step 1 of Lemma 2.2, it follows that for any polynomial $p(x)$, if $p(x) = p^+(x)$, then the degree of $p(x)$ must be even. Combined with Lemma 3.4, this provides an alternative proof of Lemma 3.3. Next we have the following important result.

Theorem 3.1. *Let $\tau(x)$ be an irreducible polynomial over $GF(2)$. Then $\tau(x) = \tau^+(x)$ if and only if $\tau(x) | (x^{2^i} + x + 1)$ for some i.*

Proof. If $\tau(x) = \tau^+(x)$ and if α is a root of $\tau(x)$, then $\alpha+1$ is a root of $\tau^+(x)$, which must also be a root of $\tau(x)$. But the roots of $\tau(x)$ are of the form α^{2^i} for some i. Thus it follows that $\alpha^{2^i} + \alpha + 1 = 0$ for some i. Since $\tau(x)$ is the minimal polynomial for α, it follows that $\tau(x)|(x^{2^i} + x + 1)$.

Again, if $\tau(x)|(x^{2^i} + x + 1)$, then $\alpha^{2^i} + \alpha + 1 = 0$ for any root α of $\tau(x)$. Then $1 + \alpha = \alpha^{2^i}$ and hence both α and $\alpha + 1$ are roots of $\tau(x)$. Therefore by Lemma 3.4 it follows that $\tau(x) = \tau^+(x)$. ■

Lemma 3.5. *Let $\tau(x)$ be an irreducible polynomial of degree $2d$, such that $\tau(x) = \tau^+(x)$. Then $\tau(x)|x^{2^d} + x + 1$ and $\tau(x) \not| x^{2^i} + x + 1$ for $i < d$.*

Proof. Let α be a root of $\tau(x)$. Since $\tau(x) = \tau^+(x)$, we must have $1+\alpha = \alpha^{2^k}$ for some $0 < k < 2d$:

$$\begin{aligned}&\Rightarrow 1 + \alpha^{2^k} = \alpha^{2^{2k}}\\ &\Rightarrow \alpha^{2^{2k}} = \alpha\\ &\Rightarrow 2k \equiv 0 \bmod 2d.\end{aligned}$$

This, along with $0 < k < 2d$, implies $k = d$ and hence α satisfies $x^{2^d}+x+1$. So $\tau(x)$, being the minimal polynomial for α, divides $x^{2^d} + x + 1$.

If possible let $\tau(x)|x^{2^i} + x + 1$ for some $i < d$. Then

$$\begin{aligned}1 + \alpha &= \alpha^{2^i}\\ &\Rightarrow 1 + \alpha^{2^i} = \alpha^{2^{2i}}\\ &\Rightarrow \alpha^{2^{2i}} = \alpha\\ &\Rightarrow 2i \equiv 0 \bmod 2d\\ &\Rightarrow d|i,\end{aligned}$$

which is a contradiction. ■

Corollary 3.1.

1. *The highest degree of all irreducible factors of $x^{2^n} + x + 1$ is $2n$.*
2. *If $\tau(x)$ of degree k is an irreducible factor of $x^{2^n} + x + 1$, then $k|2n$.*

The second point of Corollary 3.1 is also in [2, page 146].

Theorem 3.2. *Let $\tau(x)$ be an irreducible polynomial of degree $2d$, such that $\tau(x) = \tau^+(x)$. Then $\tau(x)|x^{2^n} + x + 1$ if and only if $n \equiv d$* mod $2d$.

Proof. Since the degree of $\tau(x)$ is $2d$, $\tau(x)|x^{2^d}+x+1$, so any root α of $\tau(x)$ satisfies $x^{2^d}+x+1$, that is,

$$\alpha^{2^d}+\alpha+1=0.$$

If $n \equiv d \bmod 2d$ then $n=2dk+d$. So,

$$\begin{aligned} \alpha^{2^n}+\alpha+1 &= \alpha^{2^{2dk+d}}+\alpha+1 \\ &= \alpha^{2^d}+\alpha+1=0. \end{aligned}$$

Hence $\tau(x)|x^{2^n}+x+1$.

If $\tau(x)|x^{2^n}+x+1$ then $\alpha^{2^n}+\alpha+1=0$. Also $\alpha^{2^d}+\alpha+1=0$. Hence $\alpha^{2^n}=\alpha^{2^d}$ which implies $n \equiv d \bmod 2d$. ■

Definition 3.1.

1. E_{2d} is the product of all irreducible polynomials $\tau(x)$ of degree $2d$, such that $\tau(x)=\tau^+(x)$.
2. C_{2d} is the number of all irreducible polynomials $\tau(x)$ of degree $2d$, with $\tau(x)=\tau^+(x)$.

Thus we can obtain the factorization of $x^{2^n}+x+1$ as in Lemma 3.6.

Lemma 3.6. $$x^{2^n}+x+1=\prod_{n\equiv d \bmod 2d} E_{2d}.$$

In fact, we can state the result in a more convenient form.

Theorem 3.3. $$x^{2^n}+x+1=\prod_{d|n,2d\not| n} E_{2d}.$$

The proof of Theorem 3.3 follows from Result 3.1.

Result 3.1. *For some $d>0$, $n \equiv d \bmod 2d$ if and only if $d|n$ and $2d\not| n$.*

Proof. $d|n$ and $2d\not| n$ implies $n=kd$ with k odd. Then, $n=(k-1)d+d=\frac{k-1}{2}2d+d$. Hence, $n\equiv d \bmod 2d$.

If $n\equiv d \bmod 2d$ then $n=c2d+d=(2c+1)d$. So $d|n$ and $2d\not| n$. ■

Having obtained this we can now determine when a trinomial of the form $x^{2^m}+x+1$ will divide another trinomial of the same form.

Theorem 3.4. $x^{2^m}+x+1|x^{2^n}+x+1$ *if and only if*

1. $D_2(m)=D_2(n)$ *and*
2. $m|n$

where $D_2(m)$ is the greatest integer of the form 2^j that divides m.

Proof. Note that the conditions 1 and 2 are satisfied if and only if for each d such that $d|m$ and $2d\not|m$, it follows that $d|n$ and $2d\not|n$. Hence by Theorem 3.3 it follows that conditions 1 and 2 are satisfied if and only if $x^{2^m}+x+1|x^{2^n}+x+1$. ■

Next we count the number of irreducible poynomials $\tau(x)$ of degree $2n$ that satisfy $\tau(x)=\tau^+(x)$.

Theorem 3.5. *Let $n=2^km$ with m odd and $m\geq 1$ and $k\geq 0$. Then,*

$$C_{2n}=\frac{1}{m}\sum_{e|m}\mu(e)2^{\frac{n}{e}-1-k}$$

where $\mu(n)$ is the Mobius function.

Proof. Using Theorem 3.3 we have

$$\begin{aligned} 2^n &= \sum_{d|n,2d\not|n} 2dC_{2d} \\ \Rightarrow 2^{n-1} &= \sum_{d|n,2d\not|n} dC_{2d} \end{aligned}$$

Now the ds which satisfy $d|n$ and $2d\not|n$ are of the form $d=2^ke$ where $e|m$. Therefore,

$$2^{2^km-1-k}=\sum_{e|m}eC_{2(2^ke)}.$$

Using Mobius inversion we get,

$$\begin{aligned} mC_{2(2^km)} &= \sum_{e|m}\mu(e)2^{2^k(\frac{m}{e})-1-k} \\ \Rightarrow C_{2(2^km)} &= \frac{1}{m}\sum_{e|m}\mu(e)2^{2^k(\frac{m}{e})-1-k} \\ \Rightarrow C_{2n} &= \frac{1}{m}\sum_{e|m}\mu(e)2^{\frac{n}{e}-1-k}. \blacksquare \end{aligned}$$

This completes the characterization of the irreducible polynomials over $GF(2)$ which are fixed under the map $x\rightarrow 1+x$. The computation of the depths of irreducible polynomials is in general difficult (e.g., [10]). In the Appendix we present a complete factorization of the first ten trinomials of the form $x^{2^i}+x+1$. From what has been discussed so far, it follows that this in effect lists all irreducible polynomials $\tau(x)$ of degree less than or equal to twenty such that $\tau(x)=\tau^+(x)$. The numbers in the first column give the depth of the corresponding polynomial. So for any m, if any one of these numbers divide $m+1$, then σ^+-automata on an $m\times m$ grid are irreversible. There does not seem to be any simple formula for the depth function even for this special class of irreducible polynomials. However, it is interesting to note from the results in the Appendix that if either $2^{2i}-1$ or $2^{2i}+1$ $(4 \leq i \leq 10)$ divides $m+1$, then irreversibility occurs.

The coefficient of x^i for this class of irreducible polynomials show certain interesting regularities. In fact some of these can also be proved.

Proposition 3.2. *For any irreducible polynomial $\tau(x)$ over $GF(2)$, with $\tau(x) = \tau^+(x)$, the following holds where $\deg(\tau) = 2n$ and c_i is the coefficient of x^i in $\tau(x)$.*

1. $c_{2n-1} = n \bmod 2$
2. $c_{2n-2} = 1 + \binom{n}{2} \pmod 2$
3. $c_{2n-3} = \binom{n}{3} + (n-1) \pmod 2$

Proof. Since $\tau(x) = \tau^+(x)$, the roots of $\tau(x)$ can be written as $\alpha_i, \alpha_i + 1 (0 \leq i \leq n-1)$ accounting for $2n$ roots. Then the following holds.

1. $c_{2n-1} = \sum_{i=0}^{n-1} \alpha_i + \sum_{i=0}^{n-1}(1+\alpha_i) = n \bmod 2.$
2. Since $\deg(\tau) = 2n$, $\tau(x)|x^{2^n} + x + 1$. So for any root α of $\tau(x)$, $\alpha^{2^n} + \alpha + 1 = 0$ which implies $\alpha^{2^n} = \alpha + 1$.

   Then it follows that $\alpha^{2^i}, 1+\alpha^{2^i}$ $(0 \leq i \leq n-1)$ are all the distinct roots of $\tau(x)$. Let $\alpha_i = \alpha^{2^i}$ for $0 \leq i \leq n-1$. Then $\sum_{i=0}^{n-1} \alpha_i^2 = 1 + \sum_{i=0}^{n-1} \alpha_i$. Now,

   $$C_{2n-2} = \sum_{1 \leq i < j \leq 2n} \beta_i \beta_j$$

   where the β_is are the $2n$ distinct roots of $\tau(x)$. Therefore,

   $$\begin{aligned} c_{2n-2} &= \sum_{0 \leq i < j \leq n-1} \alpha_i \alpha_j + \sum_{0 \leq i < j \leq n-1} (\alpha_i + 1)(\alpha_j + 1) \\ &\quad + \sum_{0 \leq i \leq n-1} \sum_{0 \leq j \leq n-1} \alpha_i (1 + \alpha_j) \\ &= \binom{n}{2} \bmod 2 + \sum_{i=0}^{n-1} (\alpha_i + \alpha_i^2) \\ &= 1 + \binom{n}{2} \pmod 2. \end{aligned}$$

3. The coefficient c_{2n-3} can be written as

   $$c_{2n-3} = \sum_{1 \leq i < j < k \leq 2n} \beta_i \beta_j \beta_k$$

   where the β_is are the $2n$ distinct roots of $\tau(x)$. Then the result follows using a similar, though a bit more tedious, argument as in 2. ■

Note that irreversibility can also occur in another way, that is, if $\tau(x)$ and $\tau^+(x)$ both divide $\pi_{m+1}(x)$, with $\tau(x) \neq \tau^+(x)$. But this means that the depths of both $\tau(x)$ and $\tau^+(x)$ divide $m+1$. It is also difficult to determine this.

Now we provide sufficient conditions for reversibility. A very easy condition is the following.

Proposition 3.3. *If $m+1 = 2^k$ for some k, then σ^+-automata on an $m \times m$ grid are reversible.*

Proof. In this case $\pi_{m+1}(x) = x^m$ (see [1,10]) and $\pi^+_{m+1}(x) = (1+x)^m$. Therefore the two are relatively prime. ∎

Lemma 3.7. *If the following conditions hold then the σ^+-automata on an $m \times m$ grid are reversible.*

1. *$m+1$ is a prime with $\phi(m+1) = 2\text{sord}_{m+1}(2)$.*
2. *$m+1 \equiv 3 \bmod 4$.*

Proof. Condition 1 implies that $\pi_{m+1}(x) = \tau^2(x)$ with τ irreducible (see [5]) and condition 2 implies that the degree of τ is odd. Therefore τ; and as a result, $\pi_{m+1}(x)$, cannot have roots α and β with $\alpha + \beta = 1$ (by Lemma 3.3). Hence the result follows by Lemma 3.1. ∎

The first ten primes that satisfy the conditions of Lemma 3.7, and the corresponding π-polynomials, are given in Table 1.

Thus we see that reversibility of σ^+-automata on a square $m \times m$ grid show an extremely rich behavior. It would indeed be very interesting to obtain a full characterization of reversibility in terms of number theoretic properties of m.

Table 1: The first ten primes that satisfy Lemma 3.7.

$m+1$	$\pi_{m+1}(x)$
3	$1+x^2$
7	$1+x^4+x^6$
11	$1+x^2+x^4+x^8+x^{10}$
19	$1+x^2+x^8+x^{10}+x^{12}+x^{16}+x^{18}$
23	$1+x^4+x^6+x^8+x^{16}+x^{20}+x^{22}$
47	$1+x^8+x^{12}+x^{14}+x^{16}+x^{32}+x^{40}+x^{44}+x^{46}$
59	$1+x^2+x^4+x^{32}+x^{34}+x^{36}+x^{48}+x^{50}+x^{52}+x^{56}+x^{58}$
67	$1+x^2+x^{32}+x^{34}+x^{48}+x^{50}+x^{56}+x^{58}+x^{60}+x^{64}+x^{66}$
71	$1+x^4+x^6+x^{32}+x^{36}+x^{38}+x^{48}+x^{52}+x^{54}+x^{56}+x^{64}+x^{68}+x^{70}$
79	$1+x^8+x^{12}+x^{14}+x^{32}+x^{40}+x^{44}+x^{46}+x^{48}+x^{64}+x^{72}+x^{76}+x^{78}$

Acknowledgement

The author is indebted to Dr. Rana Barua for several stimulating discussions during the course of this work.

References

[1] Barua, R. and Ramakrishna, S., "σ-game, σ^+-game, and Two Dimensional Cellular Automata," *Theoretical Computer Science*, **154** (1996) 349–366.

[2] Lidl, R. and Niederreiter, H., *Encyclopedia of Mathematics, Finite Fields*, (Cambridge University Press, Cambridge, 1986).

[3] Martin, O., Odlyzko, A. M., and Wolfram, S., "Algebraic Properties of Cellular Automata," *Communications in Mathematical Physics*, **93** (1984) 219–258.

[4] Pelletier, D. H., "Merlin's Magic Square," *American Mathematical Monthly*, **94** (1987) 143–150.

[5] Sarkar, P. and Barua, R., "Multidimensional σ-automata, π-polynomials, and Generalised S-matrices," *Theoretical Computer Science*, to appear.

[6] Serra, M., *et. al*, "The Analysis of One-dimensional Cellular Automata and their Aliasing Properties," *IEEE Transactions on Computer Aided Design of Circuits and Systems*, **9** (1990) 767–778.

[7] Sutner, K., "The σ-game and Cellular Automata," *American Mathematical Monthly*, **97** (1990) 24–34.

[8] Sutner, K., "On σ-automata," *Complex Systems*, **2** (1988) 1–28.

[9] Sutner, K., "Linear Cellular Automata and the Garden-of-Eden," *Mathematical Intelligencer*, **11** (1989) 49–53.

[10] Sutner, K., "σ-automata and π-polynomials," (Technical Report CS-9408, Stevens Institute of Technology, December 6, 1994).

[11] Wolfram, S., *Theory and Applications of Cellular Automata: Including Selected Papers 1983–1986* (World Scientific, 1986).

[12] Wolfram, S., "Statistical Mechanics of Cellular Automata," *Reviews of Modern Phyics*, **55** (1983) 601–644.

Appendix

Here we present complete factorizations of the first ten trinomials of the form $T_i(x) = x^{2^i} + x + 1$. Note that such trinomials are square free. The value in the first column is the depth of the corresponding irreducible factor $\tau(x)$ in the second column.

$i = 1$, $T_i(x) = x^2 + x + 1$

Depth	$\tau(x)$
5	$1 + x + x^2$

$i = 2$, $T_i(x) = x^4 + x + 1$

Depth	$\tau(x)$
17	$1 + x + x^4$

$i = 3$, $T_i(x) = x^8 + x + 1$

Depth	$\tau(x)$
5	$1 + x + x^2$
63	$1 + x^2 + x^3 + x^5 + x^6$

$i = 4$, $T_i(x) = x^{16} + x + 1$

Depth	$\tau(x)$
255	$1 + x^3 + x^5 + x^6 + x^8$
257	$1 + x + x^3 + x^4 + x^5 + x^6 + x^8$

$i = 5$, $T_i(x) = x^{32} + x + 1$

Depth	$\tau(x)$
5	$1 + x + x^2$
205	$1 + x + x^2 + x^3 + x^8 + x^9 + x^{10}$
1023	$1 + x^2 + x^3 + x^4 + x^8 + x^9 + x^{10}$
1025	$1 + x + x^5 + x^6 + x^8 + x^9 + x^{10}$

$i = 6$, $T_i(x) = x^{64} + x + 1$, $2^{12} = 4096$

Depth	$\tau(x)$
17	$1 + x + x^4$
1365	$1 + x^2 + x^3 + x^6 + x^8 + x^9 + x^{12}$
4095	$1 + x^2 + x^5 + x^9 + x^{12}$
4095	$1 + x^5 + x^8 + x^9 + x^{12}$
4097	$1 + x + x^4 + x^5 + x^8 + x^9 + x^{12}$
4097	$1 + x + x^2 + x^4 + x^5 + x^9 + x^{12}$

$i = 7$, $T_i(x) = x^{128} + x + 1$, $2^{14} = 16384$

Depth	$\tau(x)$
5	$1 + x + x^2$
5461	$1 + x^4 + x^5 + x^7 + x^8 + x^{10} + x^{11} + x^{13} + x^{14}$
5461	$1 + x^2 + x^4 + x^5 + x^7 + x^{10} + x^{11} + x^{13} + x^{14}$
16383	$1 + x^6 + x^7 + x^9 + x^{11} + x^{13} + x^{14}$
16383	$1 + x^2 + x^6 + x^7 + x^8 + x^9 + x^{11} + x^{13} + x^{14}$
16383	$1 + x^2 + x^3 + x^4 + x^6 + x^7 + x^8 + x^{10} + x^{11} + x^{13} + x^{14}$
16385	$1 + x + x^5 + x^7 + x^8 + x^{10} + x^{11} + x^{13} + x^{14}$
16385	$1 + x + x^3 + x^6 + x^7 + x^{10} + x^{11} + x^{13} + x^{14}$
16385	$1 + x + x^2 + x^3 + x^4 + x^5 + x^7 + x^9 + x^{11} + x^{13} + x^{14}$
16385	$1 + x + x^2 + x^4 + x^6 + x^7 + x^8 + x^9 + x^{11} + x^{13} + x^{14}$

$i = 8$, $T_i(x) = x^{256} + x + 1$, $2^{16} = 65536$

Depth	$\tau(x)$
13107	$1 + x^3 + x^6 + x^7 + x^{10} + x^{11} + x^{13} + x^{14} + x^{16}$
21845	$1 + x^4 + x^5 + x^6 + x^7 + x^8 + x^{11} + x^{12} + x^{13} + x^{14} + x^{16}$
21845	$1 + x^2 + x^3 + x^4 + x^7 + x^8 + x^{11} + x^{12} + x^{13} + x^{14} + x^{16}$
21845	$1 + x^3 + x^4 + x^7 + x^{11} + x^{12} + x^{13} + x^{14} + x^{16}$
65535	$1 + x^2 + x^5 + x^7 + x^{10} + x^{11} + x^{13} + x^{14} + x^{16}$
65535	$1 + x^2 + x^3 + x^5 + x^6 + x^7 + x^9 + x^{10} + x^{11} + x^{12} + x^{13} + x^{14} + x^{16}$
65535	$1 + x^2 + x^3 + x^4 + x^5 + x^7 + x^9 + x^{11} + x^{13} + x^{14} + x^{16}$
65537	$1 + x + x^4 + x^5 + x^7 + x^8 + x^{10} + x^{11} + x^{13} + x^{14} + x^{16}$
65537	$1 + x + x^6 + x^7 + x^9 + x^{11} + x^{13} + x^{14} + x^{16}$
65537	$1 + x + x^2 + x^6 + x^7 + x^8 + x^9 + x^{11} + x^{13} + x^{14} + x^{16}$
65537	$1 + x + x^4 + x^7 + x^9 + x^{10} + x^{11} + x^{12} + x^{13} + x^{14} + x^{16}$
65537	$1 + x + x^2 + x^3 + x^4 + x^5 + x^6 + x^7 + x^9 + x^{10} + x^{11} + x^{12} + x^{13} + x^{14} + x^{16}$
65537	$1 + x + x^3 + x^5 + x^7 + x^8 + x^9 + x^{11} + x^{13} + x^{14} + x^{16}$
65537	$1 + x + x^3 + x^4 + x^5 + x^6 + x^7 + x^8 + x^9 + x^{10} + x^{11} + x^{12} + x^{13} + x^{14} + x^{16}$
65537	$1 + x + x^2 + x^5 + x^6 + x^7 + x^{11} + x^{12} + x^{13} + x^{14} + x^{16}$
65537	$1 + x + x^2 + x^4 + x^5 + x^7 + x^{10} + x^{11} + x^{13} + x^{14} + x^{16}$

$i = 9$, $T_i(x) = x^{512} + x + 1$, $2^{18} = 262144$

Depth	$\tau(x)$
5	$1 + x + x^2$
63	$1 + x^2 + x^3 + x^5 + x^6$
7085	$1 + x + x^2 + x^3 + x^4 + x^5 + x^7 + x^8 + x^{10} + x^{11} + x^{13} + x^{14} + x^{16} + x^{17} + x^{18}$
12483	$1 + x^2 + x^3 + x^5 + x^7 + x^8 + x^{10} + x^{11} + x^{13} + x^{14} + x^{16} + x^{17} + x^{18}$
13797	$1 + x^2 + x^3 + x^6 + x^{10} + x^{12} + x^{16} + x^{17} + x^{18}$
20165	$1 + x + x^3 + x^5 + x^6 + x^7 + x^{11} + x^{12} + x^{13} + x^{14} + x^{16} + x^{17} + x^{18}$
20165	$1 + x + x^3 + x^5 + x^9 + x^{12} + x^{16} + x^{17} + x^{18}$
29127	$1 + x^2 + x^9 + x^{10} + x^{16} + x^{17} + x^{18}$
37449	$1 + x^3 + x^7 + x^8 + x^9 + x^{10} + x^{11} + x^{12} + x^{13} + x^{14} + x^{16} + x^{17} + x^{18}$
37449	$1 + x^4 + x^5 + x^6 + x^{16} + x^{17} + x^{18}$
52429	$1 + x + x^2 + x^5 + x^6 + x^8 + x^{16} + x^{17} + x^{18}$
52429	$1 + x + x^2 + x^5 + x^7 + x^8 + x^9 + x^{11} + x^{13} + x^{14} + x^{16} + x^{17} + x^{18}$
87381	$1 + x^8 + x^9 + x^{10} + x^{16} + x^{17} + x^{18}$
87381	$1 + x^3 + x^4 + x^5 + x^9 + x^{12} + x^{16} + x^{17} + x^{18}$
87381	$1 + x^2 + x^4 + x^7 + x^{11} + x^{12} + x^{13} + x^{14} + x^{16} + x^{17} + x^{18}$
262143	$1 + x^3 + x^4 + x^6 + x^7 + x^8 + x^9 + x^{11} + x^{13} + x^{14} + x^{16} + x^{17} + x^{18}$
262143	$1 + x^2 + x^6 + x^7 + x^{10} + x^{11} + x^{13} + x^{14} + x^{16} + x^{17} + x^{18}$
262143	$1 + x^2 + x^5 + x^6 + x^7 + x^8 + x^9 + x^{10} + x^{11} + x^{12} + x^{13} + x^{14} + x^{16} + x^{17} + x^{18}$
262143	$1 + x^3 + x^5 + x^7 + x^{10} + x^{11} + x^{13} + x^{14} + x^{16} + x^{17} + x^{18}$
262143	$1 + x^5 + x^6 + x^7 + x^9 + x^{10} + x^{11} + x^{12} + x^{13} + x^{14} + x^{16} + x^{17} + x^{18}$
262143	$1 + x^5 + x^{10} + x^{12} + x^{16} + x^{17} + x^{18}$
262145	$1 + x + x^4 + x^6 + x^7 + x^8 + x^{10} + x^{11} + x^{13} + x^{14} + x^{16} + x^{17} + x^{18}$
262145	$1 + x + x^2 + x^3 + x^6 + x^7 + x^9 + x^{11} + x^{13} + x^{14} + x^{16} + x^{17} + x^{18}$
262145	$1 + x + x^2 + x^3 + x^{16} + x^{17} + x^{18}$
262145	$1 + x + x^2 + x^4 + x^9 + x^{10} + x^{16} + x^{17} + x^{18}$
262145	$1 + x + x^3 + x^4 + x^6 + x^8 + x^{10} + x^{12} + x^{16} + x^{17} + x^{18}$
262145	$1 + x + x^2 + x^3 + x^5 + x^8 + x^9 + x^{12} + x^{16} + x^{17} + x^{18}$
262145	$1 + x + x^3 + x^4 + x^5 + x^6 + x^9 + x^{10} + x^{16} + x^{17} + x^{18}$
262145	$1 + x + x^2 + x^4 + x^5 + x^8 + x^{10} + x^{12} + x^{16} + x^{17} + x^{18}$
262145	$1 + x + x^2 + x^3 + x^4 + x^6 + x^{10} + x^{12} + x^{16} + x^{17} + x^{18}$

$i = 10$, $T_i(x) = x^{1024} + x + 1$, $2^{20} = 1048576$

Depth	$\tau(x)$
17	$1 + x + x^4$
13981	$1 + x^2 + x^3 + x^4 + x^6 + x^8 + x^{16} + x^{17} + x^{20}$
25575	$1 + x^2 + x^5 + x^6 + x^{10} + x^{12} + x^{16} + x^{17} + x^{20}$
61681	$1 + x + x^3 + x^5 + x^6 + x^8 + x^9 + x^{12} + x^{16} + x^{17} + x^{20}$
61681	$1 + x + x^2 + x^5 + x^{16} + x^{17} + x^{20}$
69905	$1 + x^2 + x^3 + x^4 + x^6 + x^7 + x^8 + x^9 + x^{10} + x^{11} + x^{12} + x^{13} + x^{14} + x^{17} + x^{20}$
95325	$1 + x^2 + x^3 + x^5 + x^7 + x^{11} + x^{12} + x^{13} + x^{14} + x^{17} + x^{20}$
209715	$1 + x^2 + x^3 + x^4 + x^5 + x^6 + x^9 + x^{12} + x^{16} + x^{17} + x^{20}$
209715	$1 + x^3 + x^5 + x^8 + x^9 + x^{10} + x^{16} + x^{17} + x^{20}$
209715	$1 + x^6 + x^7 + x^{11} + x^{12} + x^{13} + x^{14} + x^{17} + x^{20}$
209715	$1 + x^2 + x^4 + x^5 + x^6 + x^{10} + x^{12} + x^{17} + x^{20}$
349525	$1 + x^3 + x^6 + x^7 + x^9 + x^{10} + x^{11} + x^{12} + x^{13} + x^{14} + x^{16} + x^{17} + x^{20}$
349525	$1 + x^2 + x^3 + x^5 + x^9 + x^{10} + x^{16} + x^{17} + x^{20}$
349525	$1 + x^2 + x^5 + x^6 + x^7 + x^9 + x^{11} + x^{13} + x^{14} + x^{17} + x^{20}$
349525	$1 + x^2 + x^4 + x^7 + x^8 + x^{10} + x^{11} + x^{13} + x^{14} + x^{17} + x^{20}$
349525	$1 + x^2 + x^8 + x^9 + x^{12} + x^{17} + x^{20}$
349525	$1 + x^4 + x^5 + x^6 + x^8 + x^{10} + x^{12} + x^{17} + x^{20}$
349525	$1 + x^4 + x^6 + x^9 + x^{10} + x^{17} + x^{20}$
1048575	$1 + x^2 + x^6 + x^8 + x^9 + x^{10} + x^{16} + x^{17} + x^{20}$
1048575	$1 + x^4 + x^9 + x^{12} + x^{16} + x^{17} + x^{20}$
1048575	$1 + x^4 + x^5 + x^6 + x^7 + x^8 + x^9 + x^{11} + x^{13} + x^{14} + x^{16} + x^{17} + x^{20}$
1048575	$1 + x^2 + x^3 + x^5 + x^6 + x^7 + x^{10} + x^{11} + x^{13} + x^{14} + x^{16} + x^{17} + x^{20}$
1048575	$1 + x^3 + x^{10} + x^{12} + x^{16} + x^{17} + x^{20}$
1048575	$1 + x^5 + x^6 + x^8 + x^{10} + x^{12} + x^{16} + x^{17} + x^{20}$
1048575	$1 + x^2 + x^4 + x^6 + x^7 + x^8 + x^{11} + x^{12} + x^{13} + x^{14} + x^{16} + x^{17} + x^{20}$
1048575	$1 + x^3 + x^6 + x^{17} + x^{20}$
1048575	$1 + x^7 + x^{10} + x^{11} + x^{13} + x^{14} + x^{16} + x^{17} + x^{20}$
1048575	$1 + x^3 + x^4 + x^7 + x^9 + x^{11} + x^{13} + x^{14} + x^{16} + x^{17} + x^{20}$
1048575	$1 + x^2 + x^3 + x^7 + x^8 + x^9 + x^{11} + x^{13} + x^{14} + x^{17} + x^{20}$
1048575	$1 + x^3 + x^4 + x^5 + x^6 + x^7 + x^8 + x^{10} + x^{11} + x^{13} + x^{14} + x^{17} + x^{20}$
1048577	$1 + x + x^2 + x^3 + x^5 + x^7 + x^{11} + x^{12} + x^{13} + x^{14} + x^{16} + x^{17} + x^{20}$
1048577	$1 + x + x^2 + x^4 + x^8 + x^9 + x^{12} + x^{17} + x^{20}$
1048577	$1 + x + x^2 + x^3 + x^5 + x^9 + x^{10} + x^{17} + x^{20}$
1048577	$1 + x + x^3 + x^4 + x^6 + x^{17} + x^{20}$
1048577	$1 + x + x^4 + x^7 + x^{10} + x^{11} + x^{13} + x^{14} + x^{16} + x^{17} + x^{20}$
1048577	$1 + x + x^2 + x^3 + x^4 + x^8 + x^{10} + x^{12} + x^{16} + x^{17} + x^{20}$
1048577	$1 + x + x^2 + x^3 + x^6 + x^8 + x^{16} + x^{17} + x^{20}$
1048577	$1 + x + x^3 + x^5 + x^8 + x^9 + x^{10} + x^{17} + x^{20}$
1048577	$1 + x + x^2 + x^5 + x^6 + x^{10} + x^{12} + x^{17} + x^{20}$
1048577	$1 + x + x^9 + x^{12} + x^{16} + x^{17} + x^{20}$
1048577	$1 + x + x^2 + x^4 + x^5 + x^7 + x^9 + x^{10} + x^{11} + x^{12} + x^{13} + x^{14} + x^{16} + x^{17} + x^{20}$
1048577	$1 + x + x^3 + x^4 + x^5 + x^7 + x^8 + x^{11} + x^{12} + x^{13} + x^{14} + x^{17} + x^{20}$
1048577	$1 + x + x^2 + x^3 + x^4 + x^6 + x^7 + x^8 + x^9 + x^{10} + x^{11} + x^{12} + x^{13} + x^{14} + x^{16} + x^{17} + x^{20}$
1048577	$1 + x + x^3 + x^4 + x^6 + x^7 + x^9 + x^{10} + x^{11} + x^{12} + x^{13} + x^{14} + x^{16} + x^{17} + x^{20}$
1048577	$1 + x + x^4 + x^6 + x^9 + x^{10} + x^{16} + x^{17} + x^{20}$
1048577	$1 + x + x^5 + x^6 + x^8 + x^{10} + x^{12} + x^{17} + x^{20}$
1048577	$1 + x + x^2 + x^4 + x^7 + x^8 + x^{10} + x^{11} + x^{13} + x^{14} + x^{16} + x^{17} + x^{20}$
1048577	$1 + x + x^3 + x^4 + x^7 + x^9 + x^{11} + x^{13} + x^{14} + x^{17} + x^{20}$
1048577	$1 + x + x^4 + x^5 + x^6 + x^7 + x^8 + x^9 + x^{11} + x^{13} + x^{14} + x^{17} + x^{20}$
1048577	$1 + x + x^2 + x^4 + x^6 + x^7 + x^8 + x^{11} + x^{12} + x^{13} + x^{14} + x^{17} + x^{20}$
1048577	$1 + x + x^5 + x^7 + x^8 + x^9 + x^{10} + x^{11} + x^{12} + x^{13} + x^{14} + x^{17} + x^{20}$
1048577	$1 + x + x^2 + x^6 + x^8 + x^9 + x^{10} + x^{17} + x^{20}$