Period lengths of cellular automata on square lattices with Rule 90

Kawahara, Yasuo
Research Institute of Fundamental Information Science, Kyushu University

Kumamoto, Satoru
Faculty of Economics and Business Administration, Kitakyushu University

Mizoguchi, Yoshihiro
Department of Control Engineering and Science, Kyushu Institute of Technology

Nomi, Masaya
Department of Artificial Intelligence, Kyushu Institute of Technology

他

Period lengths of cellular automata on square lattices with Rule 90

Yasuo Kawahara
Research Institute of Fundamental Information Science, Kyushu University 33, Fukuoka 812, Japan

Satoru Kumamoto
Faculty of Economics and Business Administration, Kitakyushu University, Kitakyushu 802, Japan

Yoshihiro Mizoguchi
Department of Control Engineering and Science, Kyushu Institute of Technology, Iizuka 820, Japan

Masaya Nohmi
Department of Artificial Intelligence, Kyushu Institute of Technology, Iizuka 820, Japan

Hiroshi Ohtsuka
Department of Mathematics, Kyushu University 33, Fukuoka 812, Japan

Takayoshi Shoudai
Computer Science Laboratory, Kyushu University 01, Ropponmatsu, Fukuoka 810, Japan

This paper studies two-dimensional cellular automatma $ca{-}90(m,n)$ having states 0 and 1 and working on a square lattice of size $(m-1)\times(n-1)$. All their dynamics, driven by the local transition rule 90, can be simply formulated by representing their configurations with Laurent polynomials over a finite field $F_2 = \{0,1\}$. The initial configuration takes the next configuration to a particular configuration whose cells all have the state 1. This paper answers the question of whether the initial configuration lies on a limit cycle or not, and, if that is the case, some properties on period lengths of such limit cycles are studied.

I. INTRODUCTION

Dynaimical behaviors of finite additive cellular automata were investigated by many authors.[1–3] In their pioneer work[1] Martin, Oldlyzko, and Wolfram studied many fundamental properties of additive cellular automata with cells arranged around a circle, by using Laurent polynomials which algebraically represent configurations of these automata. Guan and He[3] showed formulas for the length of limit cycles of additive cellular automata of such types using primitive roots of unity 1. Recently dynamical behaviors of cellular automata on square lattices, namely two-dimensional cellular automata, have been extensively investigated by many authors. For example, Manna and Stauffer[4] analyzed phase transitions of all nearest neighbor cellular automata on square lattices without memory, and da Silva[5] studied critical behavior at the transition to chaos of several binary mixtures of cellular automata and fractal dimensions associated with the damage spreading and the propagation time of damage. Among elementary cellular automata in which the cells can take the values 0 or 1 and only nearest neighbors interact, there are eight additive local transition rules, namely, the rules $R = 0, 60, 90, 102, 150, 170, 204, 240$ by Wolfram's rule labeling scheme. It is well known that elementary additive cellular automata with rules 90 and 150 are the simplest nontrivial ones. Based on an extensive numerical study of basin and attractor sizes of the 88 distinct elementary cellular automata, Binder[6] proposed a topological classification of cellular automata, complementary to that of Wolfram derived from the attractor globality. Kawahara[7] studied one-dimensional cellular automata $ca-90(m)$ $(m > 1)$ having states 0 and 1 and working on a linear array of size $m - 1$ with the local transition rule 90.

Local Transition Rule 90

111	110	101	100	011	010	001	000
0	1	0	1	1	0	1	0

The global transition function of $ca-90(m)$ computes simultaneously the next state of a cell by adding the present states of its neighboring cells to the left and right and taking the result modulo 2 under the null boundary condition. Trivially a cellular automaton $ca-90(m)$ has 2^{m-1} possible configurations. Figure 1 illustrates a configuration of $ca-90(7)$.

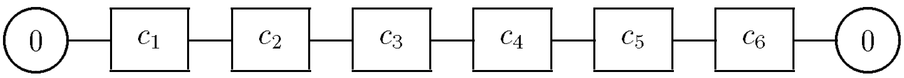

FIG. 1. A configuration of $ca-90(7)$.

Formally a configuration of $ca-90(m)$ is an $(m-1)$-dimensional vector

$$c = (c_1, c_2, \cdots, c_{m-2}, c_{m-1})$$

with all entries 0 or 1, and its global transition function τ_m is given by

$$\tau_m(c) = (c_0 + c_2, c_1 + c_3, \cdots, c_{m-3} + c_{m-1}, c_{m-2} + c_m) \mod 2,$$

where $c_0 = c_m = 0$ (the null boundary condition). In a similar fashion the global transition function δ_m of $ca-150(m)$ is given by $\delta_m(c) = \tau_m(c) + c \mod 2$, which is a reason why $ca-90(m)$ can be considered as more elementary cellular automata. On the analogy with Ref. 2 all configurations of $ca-90(m)$ can be represented by Laurent polynomials and its global transition function τ_m is given by multiplying each configuration by a simple Laurent polynomial $x + x^{-1}$. The notion of Laurent polynomials discussed here is a modification of those in Ref. 1. Polynomial representation of configurations of finite additive cellular automata was systematically investigated by Nohmi.[8] Usage of Laurent polynomials enables us to effectively compute and analyze iterative transitions of cellular automata $ca-90(m)$. For example, it is easy to see that the initial configuration a_m of $ca-90(m)$ whose all cells have the constant state 1 is on a limit cycle if and only if m is odd. Also Ref.7 dealt with the period length of a limit cycle on which the next configuration $\tau_m(a_m)$ to a_m lies, and gave some formulas concerned with the period length, which is called the characteristic number associated with $ca-90(m)$.

This paper is a continuation of Ref. 7 and we study *two-dimensional* cellular automata $ca-90(m,n)$ having states 0 and 1 and working on a square lattice of size $(m-1)\times(n-1)$. All their dynamics, driven by the local transition rule 90, can be simply formulated by representing their conifgurations with Laurent polynomials. Exactly speaking this transition rule computes the next state of a cell by adding the present states of its neighboring cells to the north, east, south, west and taking the result modulo 2 under the null boundary condition. Trivially a cellular automaton $ca-90(m,n)$ has $2^{(m-1)(n-1)}$ possible configurations. Figure 2 illustrates a configuration of $ca-90(5,6)$.

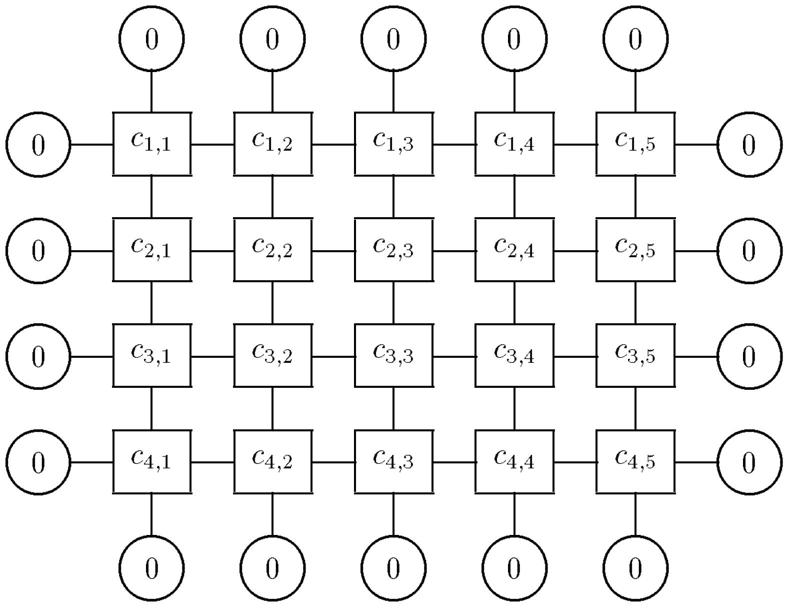

FIG. 2. A configuration of $ca-90(5,6)$.

This paper is especially concerned with the problem of whether a given initial configuration of ca–$90(m,n)$ is on a limit cycle or not, and, if it is the case, certain possible multiples of the period lengths of such limit cycles will be given.

Now we formally introduce two-dimensional cellular automaton $ca-90(m,n)$ for integers $m,n>1$. A *configuration* of $ca-90(m,n)$ is a two-dimensional array, namely, an $(m-1)\times(n-1)$ matrix,

$$c=\begin{pmatrix} c_{1,1} & c_{1,2} & \cdots & c_{1,n-2} & c_{1,n-1} \\ c_{2,1} & c_{2,2} & \cdots & c_{2,n-2} & c_{2,n-1} \\ \vdots & \vdots & & \vdots & \vdots \\ c_{m-2,1} & c_{m-2,2} & \cdots & c_{m-2,n-2} & c_{m-2,n-1} \\ c_{m-1,1} & c_{m-1,2} & \cdots & c_{m-1,n-2} & c_{m-1,n-1} \end{pmatrix},$$

where $c_{i,j}=0$ or 1 for all i and j. The *global transition function* $\tau_{m,n}$ of ca–$90(m,n)$ is defined by

$$\tau_{m,n}(c)_{i,j}=c_{i-1,j}+c_{i,j-1}+c_{i,j+1}+c_{i+1,j} \bmod 2$$

for all integers i,j with $1\leqslant i\leqslant m-1, 1\leqslant j\leqslant n-1$, where $c_{i,0}=c_{i,n}=c_{0,j}=c_{m,j}=0$ (the null boundary condition). ¿From the above definition two-dimensional automaton $ca-90(m,2)$ [or $ca-90(2,m)$] is identical to one-dimensional cellular automaton $ca-90(m)$, and $ca-90(m,n)$ is isomorphic to $ca-90(n,m)$.

Now let $\alpha_{m,n}$ be the next configuration to a particular configuration of $ca-90(m,n)$ whose cells all have the state 1. For example

$$\alpha_{5,6} = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

Consider another global transition function $\hat{\tau}_{m,n}$ of $ca-90(m,n)$ transforming each configuration of ca–$90(m,n)$ into the next configuration to its reversed configuration by $\tau_{m,n}$, that is, $\hat{\tau}_{m,n}(c) = \tau_{m,n}(c) + \alpha_{m,n}$. Our original problem is as follows.

Problem A: Find a necessary and sufficient condition that there is a positive integer h such that $\hat{\tau}^h_{m,n}(c) = \tau^h_{m,n}(c)$ for all configurations c of $ca-90(m,n)$.

It is easy to see that $\hat{\tau}^h_{m,n}(c) = \tau^h_{m,n}(c)$ for all configurations c if and only if $\sum_{j=0}^{h-1} \tau^j_{m,n}(\alpha_{m,n}) = 0$. Hence the above problem is equivalent to the following problem, which is the subject of this paper.

Problem B: Find a necessary and sufficient condition that the configuration α of $ca-90(m,n)$ lies on a limit cycle. (What is the period length of the limit cycle when that is the case?)

As ca–$90(m,n)$ is a finite automaton, the configuration $\alpha_{m,n}$ of ca–$90(m,n)$ lies on a limit cycle if and only if there is a positive integer k such that $\tau^k_{m,n}(\alpha_{m,n}) = \alpha_{m,n}$. If such k exists, the least positive integer $k = K(m,n)$ with $\tau^k_{m,n}(\alpha_{m,n}) = \alpha_{m,n}$ is the period length of a limit cycle on which $\alpha_{m,n}$ lies. Hence we say that the period length $K(m,n)$ of $ca-90(m,n)$ *exists* if $\alpha_{m,n}$ lies on a limit cycle. And the period length $K(m,n)$ of $ca-90(m,n)$ *does not exist* if $\alpha_{m,n}$ does not lie on a limit cycle. With these terminologies the main result of the paper can be stated as follows.

Main Theorem: The period length $K(m,n)$ of ca–$90(m,n)$ exists if and only if there exists no integer $D > 1$ such that $2D|m$ and $D|n$, or $D|m$ and $2D|n$. Supposed that m and n are odd integers > 1 and k is a positive integer, then

(a) $K(m,n) \mid 2^w - 1$,

(b) $K(m,2^k) \mid 2^{k-1}(2^u - 1)$,

(c) $K(m,2^k n) \mid 2^k(2^w - 1)$ if m and n are mutually disjoint,

(d) $K(2m,2) \mid 2(2^u - 1)$,

(e) $K(2m,2n) \mid 2(2^w - 1)$ if m and n are mutually disjoint,

where u is the multiplicative suborder of 2 modulo m, v is the multiplicative suborder of 2 modulo n, and w is the least common multiple of u and v. (The multiplicative suborder of 2 modulo m is the least positive integer u satisfying $2^u = \pm 1 \mod m$.) □

In Sec. II we recall some fundamentals on one-dimensional cellular automata $ca-90(m)$ for the later study of two-dimensional cellular automata $ca-90(m,n)$. In Sec. III we provide an algebraic reformulation of $ca-90(m,n)$ using Laurent polynomials and some results on $ca-90(m)$ needed in the later sections. In Sec.

IV we prove the existence theorems of period lengths $K(m, n)$ by explicitly giving some multiples of the period lengths. In Sec. V nonexistence theorems of the period lengths are shown. The appendix at the end of the paper is a table of the period lengths $K(m, n)$ $(1 < m < 20,\ 1 < n < 20)$ calculated by computers.

II. ONE-DIMENSIONAL CELLULAR AUTOMATA ca$-$90(m)

In this section we recall some fundamentals on one-dimensional cellular automata $ca-90(m)$ for the later study of two-dimensional cellular automata $ca-90(m, n)$.

In what follows we assume that m is an integer > 1. Let $F_2 = \{0, 1\}(= \mathbf{Z}/2\mathbf{Z})$ be the prime field of characteristic 2, $F_2[x]$ be the polynomial ring over F_2 with an indeterminate x, and $F_2[x]/(x^{2m} - 1)$ be the quotient ring of $F_2[x]$ by the ideal $(x^{2m} - 1)$ generated by a polynomial $x^{2m} - 1$. For non-negative integers i, k, r with $i = 2mk + r$ and $0 \leqslant r < 2m$ it easily follows that $x^i = (x^{2m})^k x^r = x^r$. Further, $x^{2m-r}x^i = x^{2m(k+1)} = 1$ and so $x^{-i} = x^{2m-r}$. Thus any monomial x^i is equal to one of $1, x, x^2, \cdots, x^{2m-1}$. A polynomial in the quotient ring $F_2[x]/(x^{2m} - 1)$ is sometimes called a *Laurent* polynomial (cf. Ref. 1). Define Laurent polynomials $t_m(i) = x^i + x^{-i}$ in $F_2[x]/(x^{2m} - 1)$ for all integers i. In particular, we set $t_m = t_m(1)(= x + x^{-1})$. The following proposition gives elementary formulas on Laurent polynomials $t_m(i)$.

Proposition 2.1: In the quotient ring $F_2[x]/(x^{2m} - 1)$ the following holds for integers i, j and a non-negative integer k:

(a) $t_m(0) = t_m(m) = 0$,

(b) $t_m(-i) = t_m(i)$,

(c) $t_m^{2^k} = t_m(2^k)$, $[t_m(i)]^{2^k} = t_m(2^k i)$,

(d) $t_m(i)t_m(j) = t_m(i - j) + t_m(i + j)$,

(e) $t_m(2m + i) = t_m(i)$,

(f) $t_m(m + i) = t_m(m - i)$. □

The next lemma indicates a fundamental relationship between cellular automata $ca-90(m)$ and the quotient ring $F_2[x]/(x^{2m} - 1)$.

Lemma 2.2: Let f be a function assigning a Laurent polynomial

$$f(c) = \sum_{i=1}^{m-1} c_i t_m(i)$$

in $F_2[x]/(x^{2m} - 1)$ to each configuration $c = (c_1, c_2, \cdots, c_{m-2}, c_{m-1})$ of $ca-90(m)$. Then f is an additive and injective function such that $f(\tau_m(c)) = t_m f(c)$ for all configurations c.

Proof: First note that the addition on configurations of $ca-90(m)$ is trivially defined by component-wise (modulo 2). It is easy to see that f is additive, that is, $f(c + c') = f(c) + f(c')$. For the injectivity of f it suffices to show that $c = 0$ if $f(c) = 0$. Assume that $f(c) = 0$ in the quotient ring $F_2[x]/(x^{2m} - 1)$. Since $t_m(i) = x^i + x^{2m-i}$ for an integer i with $1 \leqslant i \leqslant m - 1$ an identity

$$\sum_{i=1}^{m-1} c_i(x^i + x^{2m-i}) = p(x)(x^{2m} - 1)$$

holds in the polynomial ring $F_2[x]$ for some polynomial $p(x)$. Comparing with the degrees of x on both sides of the identity, it turns out that it is impossible unless $p(x) = 0$. Hence we have $c_1 = c_2 = \cdots = c_{m-2} = c_{m-1} = 0$. [The injectivity of f means the linear independence of the family $\{t_m(1), t_m(2), \cdots, t_m(m-1)\}$ of Laurent polynomials.] An easy computation using Proposition 2.1 shows the following equation:

$$t_m \sum_{i=1}^{m-1} c_i t_m(i) = \sum_{i=1}^{m-1} (c_{i-1} + c_{i+1}) t_m(i) \quad (c_0 = c_m = 0),$$

which claims $t_m f(c) = f(\tau_m(c))$. □

The last lemma ensures that the following reformulation of cellular automata $ca-90(m)$ with Laurent polynomials $t_m(i)$ is the same as the combinatorial one stated in the Introduction.

Definition 2.3: A configuration c of a cellular automaton $ca-90(m)$ is a Laurent polynomial

$$c = \sum_{i=1}^{m-1} c_i t_m(i)$$

in the quotient ring $F_2[x]/(x^{2m} - 1)$, where $c_i = 0$ or 1 for all integers i with $1 \leqslant i \leqslant m-1$. The global transition function τ_m of $ca-90(m)$ is defined by $\tau_m(c) = t_m c$ for every configuration c. A configuration a_m of $ca-90(m)$ is a particular configuration whose cells all have the state 1, that is, $a_m = \sum_{i=1}^{m-1} t_m(i)$. □

The following is the basic properties of cellular automata $ca-90(m)$ useful for the later discussion.

Lemma 2.4: The following statements hold in a cellular automaton $ca-90(m)$:

(a) $t_m a_m = t_m(m-1) a_m = t_m(1) + t_m(m-1)$. In general, $t_m(i) a_m = t_m(i) + t_m(m-i)$ for each integer i.

(b) If $m = 2^k$ for a positive integer k, then $t_m^{2^{k-1}} a_m = 0$. In general, $t_m(m/2) a_m = 0$ if m is even.

(c) If $2D|m$ for a positive integer D, then $t_m(D) \sum_{i=1}^{m/2D-1} t_m(2iD) = t_m(D) a_m$.

(d) If m is odd, then $t_m c = 0$ is equivalent to $c = 0$ for a configuration c of $ca-90(m)$. [That is, if m is odd, then the global transition function τ_m of $ca-90(m)$ is a bijection and so all configurations are on limit cycles.]

(e) If m is odd and $2^u = \pm 1 \bmod m$ for a positive integer u, then $t_m^{2^u - 1} a_m = a_m$.

Proof: (a) Using the formulas 2.1 we have

$$\begin{aligned} t_m a_m &= \sum_{i=1}^{m-1} t_m(i-1) + \sum_{i=1}^{m-1} t_m(i+1) \\ &= t_m(1) + \sum_{i=2}^{m-2} t_m(i) + \sum_{i=2}^{m-2} t_m(i) + t_m(m-1) \\ &= t_m(1) + t_m(m-1), \end{aligned}$$

and

$$\begin{aligned}
t_m(m-1)a_m &= \sum_{i=1}^{m-1} t_m(i-m+1) + \sum_{i=1}^{m-1} t_m(i+m-1) \\
&= \sum_{i=2-m}^{-2} t_m(i) + t_m(-1) + t_m(m+1) + \sum_{i=m+2}^{2m-2} t_m(i) \\
&= t_m(1) + t_m(m-1),
\end{aligned}$$

because of

$$\sum_{i=2-m}^{-2} t_m(i) = \sum_{i=m+2}^{2m-2} t_m(i) \text{ by 2.1(e).}$$

(b) It follows directly from (a) that $t_m(m/2)a_m = t_m(m/2) + t_m(m - m/2) = 0$.

(c) Using the formulas 2.1 we have

$$\begin{aligned}
t_m(D) \sum_{i=1}^{m/2D-1} t_m(2iD) &= \sum_{i=1}^{m/2D-1} t_m(2iD-D) + \sum_{i=1}^{m/2D-1} t_m(2iD+D) \\
&= t_m(D) + t_m(m-D) \\
&= t_m(D)a_m.
\end{aligned}$$

(d) Assume that $t_m c = 0$ for $c = \sum_{i=1}^{m-1} c_i t_m(i)$. Then we have $c_{i-1} = c_{i+1}$ for $i = 1, 2, \cdots, m-1$ (where $c_0 = c_m = 0$). Hence, noticing that m is odd, $c_0 = c_2 = c_4 = \cdots = c_{m-1}$ and $c_m = c_{m-2} = c_{m-4} = \cdots = c_3 = c_1$. This shows that $c = 0$.

(e) As $2^u = \pm 1 \bmod m$ there is an integer r such that $2^u = m(2r+1) \pm 1$. Hence by Proposition 2.1 $t_m^{2^u} = t_m(2mr + m \pm 1) = t_m(m \pm 1) = t_m(m-1)$ and so $t_m^{2^u} a_m = t_m(m-1)a_m = t_m(1) + t_m(m-1) = t_m a_m$ by (a), which proves $t_m t_m^{2^u-1} a_m = t_m a_m$. Therefore the desired equation follows from (d). $\square$

Denote a configuration c of $ca{-}90(m)$ (with the combinatorial definition in the introduction) by a column vector

$$c = \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_{m-2} \\ c_{m-1} \end{pmatrix}$$

and define an $(m-1) \times (m-1)$ matrix

$$T_m = \begin{pmatrix} 0 & 1 & & & & \\ 1 & 0 & 1 & & & \\ & 1 & 0 & 1 & & \\ & & \ddots & \ddots & \ddots & \\ & & & 1 & 0 & 1 \\ & & & & 1 & 0 \end{pmatrix}.$$

Then the global transition function τ_m of $ca-90(m)$ is represented by

$$\tau_m(c) = \begin{pmatrix} 0 & 1 & & & & \\ 1 & 0 & 1 & & & \\ & 1 & 0 & 1 & & \\ & & \ddots & \ddots & \ddots & \\ & & & 1 & 0 & 1 \\ & & & & 1 & 0 \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ \vdots \\ c_{m-2} \\ c_{m-1} \end{pmatrix},$$

or simply by $\tau_m(c) = T_m c$. Now let $\varphi_m(z)$ be the characteristic polynomial (in $F_2[z]$) of T_m, that is,

$$\varphi_m(z) = |T_m - zE_{m-1}| = \begin{vmatrix} z & 1 & & & & \\ 1 & z & 1 & & & \\ & 1 & z & 1 & & \\ & & \ddots & \ddots & \ddots & \\ & & & 1 & z & 1 \\ & & & & 1 & z \end{vmatrix},$$

where E_{m-1} is the $(m-1)$-dimensional unit matrix.

The following lemma states the important properties of the characteristic polynomial $\varphi_m(z)$ of T_m.

Lemma 2.5: (a) $\varphi_{k+2}(z) = z\varphi_{k+1}(z) + \varphi_k(z)$ for all non-negative integers k.

(b) $\varphi_m(t_m)c = 0$ for all configurations c of $ca-90(m)$.

Proof: (a) Expanding the determinant $|T_{k+2} - zE_{k+1}|$ twice by Laplace's expansion theorem it follows that $\varphi_{k+2}(z) = z\varphi_{k+1}(z) + \varphi_k(z)$. A direct computation shows that $\varphi_2(z) = z$ and $\varphi_3(z) = z^2 + 1$. [Define $\varphi_0(z) = 0$ and $\varphi_1(z) = 1$. Then all $\varphi_k(z)$ are computed by the recursion formula $\varphi_{k+2}(z) = z\varphi_{k+1}(z) + \varphi_k(z)$.]

(b) From a well-known theorem of Cayley–Hamilton it follows that $\varphi_m(T_m) = 0$(zero matrix). Recall that the function f defined in Lemma 2.2 satisfies an equation $f(T_m c) = t_m f(c)$ for all configurations c of $ca-90(m)$. Generalizing this equation one can see that $f(\psi(T_m)c) = \psi(t_m)f(c)$ for any polynomial $\psi(z)$ in $F_2[z]$. {Note that $\psi(T_m) = b_0E_{m-1} + b_1T_m + b_2T_m^2 + \cdots + b_kT_m^k$ for a polynomial $\psi(z) = b_0 + b_1z + b_2z^2 + \cdots + b_kz^k$ in $F_2[x]$.} Hence $\varphi_m(t_m)c = 0$ for all configurations c in $ca-90(m)$, because $\varphi_m(t_m)f(c) = f(\varphi_m(T_m)c) = f(0) = 0$ and $f(c)$ can be identified with c. □

The lemma below is a crux for analyzing the kernel of global transition functions of two-dimensional cellular automata $ca-90(m,n)$.

Lemma 2.6: Let c be a configuration of $ca-90(m)$.

(a) If $\varphi_k(t_m)c = 0$ for a positive integer k, then $\varphi_{k+i}(t_m)c = \varphi_{k-i}(t_m)c$ for each integer i with $1 \leqslant i \leqslant k$.

(b) Assume that $\varphi_k(t_m)c = 0$ and r is an integer with $0 \leqslant r < k$. If q is odd, then $\varphi_{qk+r}(t_m)c = \varphi_{k-r}(t_m)c$, and if q is even, then $\varphi_{qk+r}(t_m)c = \varphi_r(t_m)c$.

(c) Let D be the least positive integer such that $\varphi_D(t_m)c = 0$ in $ca-90(m)$. Then $\varphi_k(t_m)c = 0$ if and only if $D|k$. In particular, $D|m$.

Proof: (a) Assume that $\varphi_k(t_m)c = 0$. Then by the recursion formula Lemma 2.5(a) we have

$$\varphi_{k+1}(t_m)c = t_m\varphi_k(t_m)c + \varphi_{k-1}(t_m)c = \varphi_{k-1}(t_m)c.$$

Assume that $\varphi_{k+i-2}(t_m)c = \varphi_{k-i+2}(t_m)c$ and $\varphi_{k+i-1}(t_m)c = \varphi_{k-i+1}(t_m)c$ for an integer i with $2 \leqslant i \leqslant k$. Then it follows that

$$\varphi_{k+i}(t_m)c = t_m\varphi_{k+i-1}(t_m)c+\varphi_{k+i-2}(t_m)c = t_m\varphi_{k-i+1}(t_m)c+\varphi_{k-i+2}(t_m)c = \varphi_{k-i}(t_m)c.$$

(b) As $\varphi_k(t_m)c = 0$ it follows from (a) that $\varphi_{2k}(t_m)c = \varphi_0(t_m)c = 0$, $\varphi_{3k}(t_m)c = \varphi_k(t_m)c = 0$, and so on. Hence $\varphi_{qk}(t_m)c = 0$ for all positive integers q. If $q = 2q'+1$ ($q' \geqslant 0$), then

$$\varphi_{qk+r}(t_m)c = \varphi_{(q'+1)k+q'k+r}(t_m)c = \varphi_{(q'+1)k-q'k-r}(t_m)c = \varphi_{k-r}(t_m)c,$$

since $\varphi_{(q'+1)k}(t_m)c = 0$. If $q = 2q'$ ($q' \geqslant 1$), then

$$\begin{aligned}\varphi_{qk+r}(t_m)c &= \varphi_{(q'+1)k+(q'-1)k+r}(t_m)c = \varphi_{(q'+1)k-(q'-1)k-r}(t_m)c = \varphi_{k+(k-r)}(t_m)c \\ &= \varphi_{k-(k-r)}(t_m)c = \varphi_r(t_m)c,\end{aligned}$$

since $\varphi_{(q'+1)k}(t_m)c = 0$ and $\varphi_k(t_m)c = 0$.

(c) It has been showed in the proof of (b) that $\varphi_k(t_m)c = 0$ if $D|k$. Next assume that $\varphi_k(t_m)c = 0$ and $k = qD + r(0 \leqslant r < D)$. If q is even, then $\varphi_k(t_m)c = \varphi_r(t_m)c$ by (b) and so $r = 0$ by the minimality of D. If q is odd, then $\varphi_k(t_m)c = \varphi_{D-r}(t_m)c$ by (b) and so $r = 0$ by the minimality of D. □

Let D be a positive integer. The substitution operator

$$\sigma_D : F_2[x]/(x^{2m} - 1) \to F_2[x]/(x^{2mD} - 1)$$

is a function defined by $\sigma_D(p(x)) = p(x^D)$ for all Laurent polynomial $p(x)$ in $F_2[x]/(x^{2m} - 1)$. Assume that $p(x) = q(x)$ in $F_2[x]/(x^{2m} - 1)$. Then $p(x) - q(x) = u(x)(x^{2m} - 1)$ for some polynomial $u(x)$ and so $p(x^D) - q(x^D) = u(x^D)(x^{2mD} - 1)$ (by substituting x^D into x), which shows that $p(x^D) = q(x^D)$ in $F_2[x]/(x^{2mD} - 1)$. Hence σ_D is well defined. It is easy to see that σ_D is a ring homomorphism, namely, $\sigma_D(p(x) + q(x)) = \sigma_D(p(x)) + \sigma_D(q(x))$ and $\sigma_D(p(x)q(x)) = \sigma_D(p(x))\sigma_D(q(x))$ for all $p(x), q(x)$ in $F_2[x]/(x^{2m} - 1)$.

The reduction operator

$$\rho_D : F_2[x]/(x^{2mD} - 1) \to F_2[x]/(x^{2m} - 1)$$

is a function defined by $\rho_D(p(x)) = p(x)$ for all Laurent polynomial $p(x)$ in $F_2[x]/(x^{2mD} - 1)$. Assume that $p(x) = q(x)$ in $F_2[x]/(x^{2mD}-1)$. Then $p(x)-q(x) = u(x)(x^{2mD}-1)$ for some polynomial $u(x)$ and so

$$p(x) - q(x) = u(x)(x^{2m} - 1)(x^{2m(D-1)} + x^{2m(D-2)} + \cdots + x^{2m} + 1),$$

which shows that $p(x) = q(x)$ in $F_2[x]/(x^{2m} - 1)$. Hence ρ_D is well defined. It is also easy to see that ρ_D is a ring homomorphism, namely, $\rho_D(p(x) + q(x)) = \rho_D(p(x)) + \rho_D(q(x))$ and $\rho_D(p(x)q(x)) = \rho_D(p(x))\rho_D(q(x))$ for all $p(x), q(x)$ in $F_2[x]/(x^{2mD} - 1)$. The following is the basic properties of the substitution and reduction operators.

Proposition 2.7:

(a) $\sigma_D(t_m(i)) = t_{mD}(iD)$ for $i = 1, 2, \cdots, m-1$. In particular, $\sigma_D(t_m) = t_{mD}(D)$.

(b) $\sigma_D(a_m) = \sum_{i=1}^{m-1} t_{mD}(iD)$.

(c) If $t_m^k a_m = a_m$ in $ca-90(m)$, then $\{t_{mD}(D)\}^k \sigma_D(a_m) = \sigma_D(a_m)$ in $ca-90(mD)$.

(d) $\rho_D(t_{mD}(i)) = t_m(i)$ for $i = 1, 2, \cdots, mD-1$.

(e) If D is even, then $\rho_D(a_{mD}) = 0$, and if D is odd, then $\rho_D(a_{mD}) = a_m$.

Proof: The proposition follows from the following simple computations.
(a) $\sigma_D(t_m(i)) = \sigma_D(x^i + x^{2m-i}) = x^{Di} + x^{2mD-iD} = t_{mD}(iD)$.
(b) $\sigma_D(a_m) = \sum_{i=1}^{m-1} \sigma_D(t_m(i)) = \sum_{i=1}^{m-1} t_{mD}(iD)$.
(c) $\sigma_D(a_m) = \sigma_D(t_m^k a_m) = \{\sigma_D(t_m)\}^k \sigma_D(a_m) = \{t_{mD}(D)\}^k \sigma_D(a_m)$.
(d) $\rho_D(t_{mD}(i)) = \rho_D(x^i + x^{2mD-i}) = x^i + x^{2mD-i} = x^i + x^{2m(D-1)} x^{2m-i} = x^i + x^{2m-i} = t_m(i)$.
(e) $\rho_D(a_{mD}) = \sum_{i=1}^{mD-1} \rho_D(t_{mD}(i)) = \sum_{i=1}^{mD-1} t_m(i) = Da_m$. □

In Ref. 7 the inner product has been found to be a useful tool for not only vector analysis but also theory of cellular automata. Here we recall some basic facts on inner product of configurations of $ca-90(m)$. Let $c = \sum_{i=1}^{m-1} c_i t_m(i)$ and $c' = \sum_{i=1}^{m-1} c'_i t_m(i)$ be two configurations of $ca-90(m)$. The inner product $\langle c, c' \rangle$ of c and c' is defined by

$$\langle c, c' \rangle = \sum_{i=1}^{m-1} c_i c'_i \mod 2.$$

Proposition 2.8: The following statements hold for configurations c, c' and c'' of $ca-90(m)$:

(a) $\langle c, c' \rangle = \langle c', c \rangle$.

(b) $\langle c, c' + c'' \rangle = \langle c, c' \rangle + \langle c, c'' \rangle$.

(c) $\langle c, t_m(i) \rangle = c_i$ for all $i = 1, 2, \cdots, m-1$.

(d) If $\langle c, t_m(i) \rangle = \langle c', t_m(i) \rangle$ for $i = 1, 2, \cdots, m-1$, then $c = c'$.

(e) $\langle c^{2^k}, a_m \rangle = \langle c, a_m \rangle$ for a non-negative integer k.

(f) $\langle t_m c, c' \rangle = \langle c, t_m c' \rangle$.

(g) If $\langle c, t_m(i) \rangle = \langle c, t_m(m-i) \rangle$ for all $i = 1, 2, \cdots, m-1$, then $\langle t_m c, t_m(i) \rangle = \langle t_m c, t_m(m-i) \rangle$ for all integers i.

(h) $\langle t_m^k a_m, t_m(i) \rangle = \langle t_m^k a_m, t_m(m-i) \rangle$ for all integers i and a non-negative integer k.

Proof: (a)–(d) are clear. (e) If $c = \sum_{i=1}^{m-1} c_i t(i)$, then

$$\langle c^2, a_m \rangle = \left\langle \sum_{i=1}^{m-1} {c_i}^2 \{t(i)\}^2, a_m \right\rangle = \left\langle \sum_{i=1}^{m-1} c_i t(2i), a_m \right\rangle = \sum_{i=1}^{m-1} c_i = \langle c, a_m \rangle.$$

(f) $\langle t_m c, c' \rangle = \sum_{i=1}^{m-1} (c_{i-1} + c_{i+1}) c'_i = \sum_{i=1}^{m-1} c_i (c'_{i-1} + c'_{i+1}) = \langle c, t_m c' \rangle$.
(g) For an integer i with $0 \leqslant i < m$ we have

$$\langle t_m c, t_m(i) \rangle = c_{i-1} + c_{i+1} = c_{m-i+1} + c_{m-i-1} = \langle t_m c, t_m(m-i) \rangle.$$

Otherwise let $i = 2mk + r$ $(0 \leqslant r < 2m)$. Then if $0 \leqslant r < m$, then $t_m(i) = t_m(r)$ and $t_m(m-i) = t_m(m-r)$ and so $\langle t_m c, t_m(i)\rangle = \langle t_m c, t_m(r)\rangle = \langle t_m c, t_m(m-r)\rangle = \langle t_m c, t_m(m-i)\rangle$. If $m \leqslant r < 2m$, then $t_m(i) = t_m(2m-r)$ and $t_m(m-i) = t_m(r-m)$ and so $\langle t_m c, t_m(i)\rangle = \langle t_m c, t_m(2m-r)\rangle = \langle t_m c, t_m(r-m)\rangle = \langle t_m c, t_m(m-i)\rangle$.

(h) It is simply a corollary of (g). □

III. TWO-DIMWNSIONAL CELLULAR AUTOMATA $\mathbf{ca-90(m,n)}$

In this section we provide an algebraic reformulation of two-dimensional cellular automata $ca-90(m,n)$ using Laurent polynomials and some results on $ca-90(m)$ needed in the later sections.

In what follows we assume that m and n are inetegers > 1. Let $F_2 = \{0,1\}(= \mathbf{Z}/2\mathbf{Z})$ be a prime field of characteristic 2, $F_2[x,y]$ be the polynomial ring over F_2 with two indeterminates x and y, and $F_2[x,y]/(x^{2m}-1, y^{2n}-1)$ be the quotient ring of $F_2[x,y]$ by the ideal $(x^{2m}-1, y^{2n}-1)$ generated by two polynomials $x^{2m}-1$ and $y^{2n}-1$. A polynomial in the quotient ring $F_2[x,y]/(x^{2m}-1, y^{2n}-1)$ is sometimes called a *Laurent* polynomial. Define Laurent polynomials $t_m(i) = x^i + x^{-i}$ and $s_n(j) = y^j + y^{-j}$ for all inetgers i and j. In particular, we set $t_m = t_m(1)(= x + x^{-1})$ and $s_n = s_n(1)(= y + y^{-1})$. Further we set $a_m = \sum_{i=1}^{m-1} t_m(i)$ and $b_n = \sum_{j=1}^{n-1} s_n(j)$. The following proposition gives elementary formulae on Laurent polynomials $t_m(i)$ and $s_n(j)$. [We will omit suffixes m and n in $t_m(i)$, t_m, $s_n(j)$, s_n, a_m, and b_n unless confusion occurs.]

Proposition 3.1: In the quotient ring $F_2[x,y]/(x^{2m}-1, y^{2n}-1)$ the following holds for integers i, j and a non-negative integer k:

(a) $t(0) = t(m) = 0$, $s(0) = s(n) = 0$;

(b) $t(-i) = t(i)$, $s(-j) = s(j)$;

(c) $t^{2^k} = t(2^k)$, $t(i)^{2^k} = t(2^k i)$, $s^{2^k} = s(2^k)$, $s(j)^{2^k} = s(2^k j)$;

(d) $t(i)t(j) = t(i-j) + t(i+j)$, $s(i)s(j) = s(i-j) + s(i+j)$;

(e) $t(2m+i) = t(i)$, $s(2n+j) = s(j)$;

(f) $t(m+i) = t(m-i)$, $s(n+j) = s(n-j)$. □

The following lemma indicates a fundamental relationship between cellular automata $ca-90(m,n)$ and the quotient ring $F_2[x,y]/(x^{2m}-1, y^{2n}-1)$.

Lemma 3.2: Let f be a function asigning a Laurent polynomial

$$f(c) = \sum_{i=1,j=1}^{m-1,n-1} c_{i,j} t(i) s(j)$$

in $F_2[x,y]/(x^{2m}-1, y^{2n}-1)$ to each configuration $c = (c_{i,j})_{1 \leqslant i \leqslant m-1, 1 \leqslant j \leqslant n-1}$ of $ca-90(m,n)$. Then f is an additive and injective function such that $f(\tau(c)) = (t+s)f(c)$ for all configurations c.

Proof: First note that the addition on configurations of $ca-90(m,n)$ is trivially defined by component-wise (mod2). It is easy to see that f is additve, that is, $f(c+c') = f(c) + f(c')$. For the injectivity of f it suffices to show that $c = 0$ if

$f(c) = 0$. Assume that $f(c) = 0$ in the quotient ring $F_2[x,y]/(x^{2m}-1, y^{2n}-1)$. Since $t(i) = x^i + x^{2m-i}$ and $s(j) = y^j + y^{2n-j}$ an identity

$$\sum_{i=1,j=1}^{m-1,n-1} c_{i,j}(x^i + x^{2m-i})(y^j + y^{2n-j}) = p(x,y)(x^{2m}-1) + q(x,y)(y^{2n}-1)$$

holds in the polynomial ring $F_2[x,y]$ for some polynomials $p(x,y)$ and $q(x,y)$. However, comparing with the degree of both sides of the last identity with respect to x and y it turns out that it is impossible unless $p(x,y) = q(x,y) = 0$. Hence we have $c_{i,j} = 0$ for all i,j. [The injectivity of f is equivalent to the linear independence of the family $\{t(i)s(j) : 1 \leqslant i \leqslant m-1, 1 \leqslant j \leqslant n-1\}$ of Laurent polynomials.] An easy computation using Proposition 3.1(d) shows the following equation:

$$(t+s)\sum_{i=1,j=1}^{m-1,n-1} c_{i,j}t(i)s(j) = \sum_{i=1,j=1}^{m-1,n-1}(c_{i-1,j} + c_{i,j-1} + c_{i,j+1} + c_{i+1,j})t(i)s(j),$$

where $c_{i,0} = c_{i,n} = c_{0,j} = c_{m,j} = 0$, and hence this claims $f(\tau(c)) = (t+s)f(c)$. $\square$

Lemma 3.2 ensures that the following reformulation of cellular automata $ca-90(m,n)$ with Laurent polynomials $t(i)$ and $s(j)$ is the same as the combinatorial one stated in the Introduction.

Definition 3.3: A configuration c of a cellular automaton $ca-90(m,n)$ is a Laurent polynomial

$$c = \sum_{i=1,j=1}^{m-1,n-1} c_{i,j}t(i)s(j)$$

in the quotient ring $F_2[x,y]/(x^{2m}-1, y^{2n}-1)$, where $c_{i,j} \in F_2$ for all i and j with $1 \leqslant i \leqslant m-1$ and $1 \leqslant j \leqslant n-1$. The global transition function $\tau(=\tau_{m,n})$ of $ca{-}90(m,n)$ is defined by $\tau(c) = (t+s)c$ for every configuration c. A configuration ab of $ca{-}90(m,n)$ is a particular configuration whose all cells have the state 1, that is,

$$ab = \sum_{i=1,j=1}^{m-1,n-1} t(i)s(j).$$

The next configuration to ab is denoted by $\alpha(=\alpha_{m,n})$, that is, $\alpha = (t+s)ab$. $\square$

Lemma 3.2 points out that the configuration space $ca-90(m,n)$ consisting of all configurations is an $(m-1)(n-1)$-dimensional vector space over F_2 with a basis $\{t(i)s(j) : 1 \leqslant i \leqslant m-1, 1 \leqslant j \leqslant n-1\}$. With the above reformulations our original problem[7] is as follows.

Problem A: Find a necessary and sufficient condition that there is a positive integer h such that $\hat{\tau}^h(c) = \tau^h(c)$ for all configurations c of $ca-90(m,n)$.

It is easy to see that

$$\hat{\tau}^h(c) = \tau^h(c) + \sum_{j=0}^{h-1}\tau^j(\alpha),$$

and so $\hat{\tau}^h(c) = \tau^h(c)$ for all c (or, equivalently for some c) if and only if $\sum_{j=0}^{h-1}\tau^j(\alpha) = 0$. Assume that $\sum_{j=0}^{h-1}\tau^j(\alpha) = 0$. Then

$$\tau^h(\alpha) + \alpha = \tau\left(\sum_{j=0}^{h-1}\tau^j(\alpha)\right) + \sum_{j=0}^{h-1}\tau^j(\alpha) = 0,$$

which claims that $\tau^h(\alpha) = \alpha$. Conversely if $\tau^h(\alpha) = \alpha$, then

$$\sum_{j=0}^{2h-1} \tau^j(\alpha) = \sum_{j=0}^{h-1} \tau^j(\alpha) + \sum_{j=0}^{h-1} \tau^j \tau^h(\alpha) = 0.$$

Hence Problem A is equivalent to the following problem, which is the subject of this paper.

Problem B: Find a necessary and sufficient condition that the initial configuration α of $ca{-}90(m,n)$ lies on a limit cycle. (What is the period length of the limit cycle when that is the case?)

As $ca-90(m,n)$ is finite, the initial configuration α lies on a limit cycle if and only if there is a positive integer k such that $\tau^k(\alpha) = \alpha$. If such k exists, the least positive integer $k = K(m,n)$ with $\tau^k(\alpha) = \alpha$ is the period length of a limit cycle on which α lies. Hence we say that the period length $K(m,n)$ of $ca{-}90(m,n)$ *exists* if α lies on a limit cycle. And the period length $K(m,n)$ of $ca{-}90(m,n)$ *does not exist* if α does not lie on a limit cycle. It is immediate that $K(m,2) = K(2,m) = K(m)$, where $K(m)$ is the period length of one-dimensional cellular automata $ca-90(m)$ studied in Ref. 7. [Recall that the period length $K(m)$ of one-dimensional cellular automaton $ca-90(m)$ is the least positive integer k such that $t_m^k t_m a_m = t_m a_m$ in $ca-90(m)$.]

Let D and E be positive integers. The substitution operator

$$\sigma_{D,E} : F_2[x,y]/(x^{2m}-1, y^{2n}-1) \to F_2[x,y]/(x^{2mD}-1, y^{2nD}-1)$$

is a function which assigns a Laurent polynomial $p(x^D, y^E)$ in $F_2[x,y]/(x^{2mD} - 1, y^{2nE} - 1)$ to each Laurent polynomial $p(x,y)$ in $F_2[x,y]/(x^{2m}-1, y^{2n}-1)$, that is, $\sigma_{D,E}(p(x,y)) = p(x^D, y^E)$. Trivially $\sigma_{D,E}$ is well defined and a ring homomorphism such that $\sigma_{D,E}(p(x)) = \sigma_D(p(x))$ and $\sigma_{D,E}(q(y)) = \sigma_E(q(y))$.

The reduction operator

$$\rho_{D,E} : F_2[x,y]/(x^{2mD}-1, y^{2nE}-1) \to F_2[x,y]/(x^{2m}-1, y^{2n}-1)$$

is a function which assigns a Laurent polynomial $p(x,y)$ in $F_2[x,y]/(x^{2m} - 1, y^{2n} - 1)$ to each Laurent polynomial $p(x,y)$ in $F_2[x,y]/(x^{2mD} - 1, y^{2nE} - 1)$, that is, $\rho_{D,E}(p(x,y)) = p(x,y)$. Similarly $\rho_{D,E}$ is well defined and a ring homomorphism such that $\rho_{D,E}(p(x)) = \rho_D(p(x))$ and $\rho_{D,E}(q(y)) = \rho_E(q(y))$.

At the end of the section we define inner products of configurations of cellular automata $ca - 90(m,n)$. The inner product $\langle c, c' \rangle$ of two configurations $c = \sum_{i=1,j=1}^{m-1,n-1} c_{i,j} t(i) s(j)$ and $c' = \sum_{i=1,j=1}^{m-1,n-1} c'_{i,j} t(i) s(j)$ of $ca-90(m,n)$ is defined by

$$\langle c, c' \rangle = \sum_{i=1,j=1}^{m-1,n-1} c_{i,j} c'_{i,j} \mod 2.$$

Proposition 3.4: The following statements hold for configurations c, c', and c'' of $ca-90(m,n)$:

(a) $\langle c, c' \rangle = \langle c', c \rangle$.

(b) $\langle c, c' + c'' \rangle = \langle c, c' \rangle + \langle c, c'' \rangle$.

(c) $\langle c, t_m(i) s_n(j) \rangle = c_{i,j}$ for all $i = 1, 2, \cdots, m-1$ and all $j = 1, 2, \cdots, n-1$.

(d) If $\langle c, t_m(i)s_n(j)\rangle = \langle c', t_m(i)s_n(j)\rangle$ for all $i = 1, 2, \cdots, m-1$ and all $j = 1, 2, \cdots, n-1$, then $c = c'$. $\square$

Remark that for a configuration c of ca–$90(m)$ and a configuration d of ca–$90(n)$ the multiplication cd gives a configuration of $ca-90(m,n)$.

Lemma 3.5: If c, c' are configurations of $ca-90(m)$ and d, d' are configurations of $ca-90(n)$, then $\langle cd, c'd'\rangle = \langle c, c'\rangle\langle d, d'\rangle$.

Proof: Let $c = \sum_{i=1}^{m-1} c_i t_m(i)$, $c' = \sum_{i=1}^{m-1} c'_i t_m(i)$, $d = \sum_{j=1}^{n-1} c_j s_n(j)$, and $d' = \sum_{j=1}^{n-1} d'_j s_n(j)$. Then

$$\begin{aligned}\langle cd, c'd'\rangle &= \left\langle \sum_{i=1,j=1}^{m-1,n-1} c_i d_j t_m(i)s_n(j), \sum_{i=1,j=1}^{m-1,n-1} c'_i d'_j t_m(i)s_n(j)\right\rangle \\ &= \sum_{i=1,j=1}^{m-1,n-1} c_i d_j c'_i d'_j = \left(\sum_{i=1}^{m-1} c_i c'_i\right)\left(\sum_{j=1}^{n-1} d_j d'_j\right) = \langle c, c'\rangle\langle d, d'\rangle.\end{aligned}$$

$\square$

IV. EXISTENCE OF PERIOD LENGTHS K(m, n)

In this section we disscuss existence theorems on the period lengths $K(m,n)$ of two-dimensional cellular automata $ca-90(m,n)$. The least positive integer u satisfying $2^u = \pm 1 \mod m$ is called the *multiplicative suborder of* 2 *modulo* m and denoted by sord(2;m). It easily follows from the Euler−Fermat theorem that the multiplicative suborder of 2 modulo m exists if and only if m is odd.

Theorem 4.1: If m and n are odd integers, then $K(m,n)|2^w - 1$, where w denotes the least common multiple of u =sord(2;m) and v =sord(2;n).

Proof: It follows from Lemma 2.4(e) that $t^{2^u-1}a = a$ in ca–$90(m)$ and $s^{2^v-1}b = b$ in ca–$90(n)$. As $2^u - 1|2^w - 1$ and $2^v - 1|2^w - 1$ we have $t^{2^w-1}a = a$ and $s^{2^w-1}b = b$. Hence

$$(t+s)^{2^w-1}\alpha = (t+s)^{2^w}ab = t^{2^w}ab + as^{2^w}b = tab + asb = \alpha$$

in $ca-90(m,n)$. $\square$

Theorem 4.2: Let m be odd and k a positive integer. If $t_m^H a_m = a_m$ in $ca-90(m)$ for a positive integer H, then $K(m, 2^k)|2^{k-1}H$. In particular, $K(m, 2^k)|2^{k-1}(2^u - 1)$ for u =sord(2;m).

Proof: Since $t^H a = a$ by the hypothesis and $s^{2^{k-1}}b = 0$ from Lemma 2.4(b) we have

$$(t+s)^{2^{k-1}H}ab = (t^{2^{k-1}} + s^{2^{k-1}})^H ab = t^{2^{k-1}H}ab = ab$$

in $ca-90(m, 2^k)$. Hence $(t+s)^{2^{k-1}H}\alpha = \alpha$. Finally remark that u =sord(2;m) satisfies $t^{2^u-1}a = a$ by Lemma 2.4(e). $\square$

Lemma 4.3: Let D be the greatest common divisor of m and n. If a configuration

$$c = \sum_{i=1,j=1}^{m-1,n-1} c_{i,j}t(i)s(j)$$

of $ca-90(m,n)$ satisfies $(t+s)c = 0$, then

$$c_{i,j} = \begin{cases} 0 & \text{if } i' = 0 \text{ or } j' = 0 \\ c_{i',j'} & \text{if } 0 < i',\ 0 < j',\ k: \text{even and } l: \text{even} \\ c_{i',D-j'} & \text{if } 0 < i',\ 0 < j',\ k: \text{even and } l: \text{odd} \\ c_{D-i',j'} & \text{if } 0 < i',\ 0 < j',\ k: \text{odd and } l: \text{even} \\ c_{D-i',D-j'} & \text{if } 0 < i',\ 0 < j',\ k: \text{odd and } l: \text{odd} \end{cases}$$

where $i = kD + i', j = lD + j'$ $(0 \leqslant i' < D, 0 \leqslant j' < D)$.

Proof: Define a sequence $c_0, c_1, \cdots, c_n$ of configurations of $ca-90(m)$ by $c_j = \sum_{i=1}^{m-1} c_{i,j} t(i)$ for $j = 1, 2, \cdots, n-1$ and $c_0 = c_n = 0$. Then a computation

$$(t+s)c = (t+s)\sum_{j=1}^{n-1} c_j s(j) = \sum_{j=1}^{n-1}\{tc_j s(j) + c_j s(j-1) + c_j s(j+1)\} = \sum_{j=1}^{n-1}(tc_j + c_{j+1} + c_{j-1})s(j)$$

shows that $c_{j+1} = tc_j + c_{j-1}(j = 1, 2, \cdots, n-1)$ because of $(t+s)c = 0$. Hence $c_j = \varphi_j(t)c_1$ for all $j = 0, 1, \cdots, n$. Let E be the least positive integer such that $c_E = \varphi_E(t)c_1 = 0$. Then by Lemma 2.6(c) $E|m$ and $E|n$ since $\varphi_n(t)c_1 = c_n = 0$ (the null boundary condition). Hence $E|D$ and so $c_D = c_{2D} = \cdots = 0$ by Lemma 2.6(c). Therefore $c_{i,j} = 0$ if $j' = 0$. Moreover, if l is odd, then $c_{lD+j'} = c_{D-j'}$ by Lemma 2.6(b), and, if l is even, then $c_{lD+j'} = c_{j'}$. Similarly set $\hat{c}_i = \sum_{j=1}^{n-1} c_{i,j} s(j)$ for $i = 1, 2, \cdots, m-1$ and $\hat{c}_0 = \hat{c}_m = 0$. Then we have $c_{i,j} = 0$ if $i' = 0$, $\hat{c}_{kD+i'} = \hat{c}_{D-i'}$ if k is odd, and $\hat{c}_{kD+i'} = \hat{c}_{i'}$ if k is even. Therefore the proof is completed. $\square$

The following corollary is an important result from the last lemma.

Corollary 4.4: If m and n are mutually disjoint, then an equality $(t+s)c = 0$ implies $c = 0$ for a configuration c of $ca-90(m,n)$, that is, the global transition function τ of $ca-90(m,n)$ is a bijection. $\square$

Theorem4.5: If m and n are mutually disjoint odd integers and k is a positive integer, then $K(2^k m, n) | 2^k(2^w - 1)$, where w denotes the least common multiple of u =sord(2;m) and v =sord(2;n).

Proof: We write t, a, s, b and α for $t_{2^k m}$, $a_{2^k m}$, s_n, b_n and $\alpha_{2^k m,n}$, respectively. Applying the substitution operator σ_{2^k} to the equality ${t_m}^{2^u-1} a_m = a_m$ in ca–$90(m)$ which comes from Lemma 2.4(e) we have $t^{2^k(2^u-1)}\sigma_{2^k}(a_m) = \sigma_{2^k}(a_m)$ in ca–$90(2^k m)$ by Propsition 2.1(c) and 2.7(c). However, by Lemma 2.4(c) and Propsition 2.7(b) $t^{2^{k-1}}\sigma_{2^k}(a_m) = t^{2^{k-1}}a$ in $ca-90(2^k m)$ and so $t^{2^k(2^u-1)}t^{2^k}a = t^{2^k}a$ in $ca-90(2^k m)$ from

$$\begin{aligned} t^{2^k(2^u-1)}t^{2^k}a &= t^{2^{k-1}}t^{2^k(2^u-1)}t^{2^{k-1}}a = t^{2^{k-1}}t^{2^k(2^u-1)}t^{2^{k-1}}\sigma_{2^k}(a_m) = t^{2^{k-1}}t^{2^{k-1}}\sigma_{2^k}(a_m) \\ &= t^{2^{k-1}}t^{2^{k-1}}a. \end{aligned}$$

Also $s^{2^v-1}b = b$ follows from Lemma 2.4(e). Therefore

$$\begin{aligned} (t+s)^{2^k-1}(t+s)^{2^k(2^w-1)}\alpha &= (t+s)^{2^{k+w}}ab = (t^{2^{k+w}} + s^{2^{k+w}})ab = t^{2^k(2^w-1)}t^{2^k}ab + as^{2^k}s^{2^k(2^w-1)}b \\ &= t^{2^k}ab + as^{2^k}b = (t+s)^{2^k-1}\alpha \end{aligned}$$

in $ca-90(2^k m)$ because of $2^u - 1 | 2^w - 1$ and $2^v - 1 | 2^w - 1$. As $2^k m$ and n are mutually disjoint, the global transition function τ of $ca-90(2^k m, n)$ is a bijection by Corollary 4.4. Hence $(t+s)^{2^k(2^w-1)}\alpha = \alpha$. $\square$

Lemma 4.6: If m and n are odd, then an equation

$$(t+s)^{2(2^w-1)}ab = \sigma_2(a_m)b + a\sigma_2(b_n) + (t+s)^{2(2^w-1)}\sigma_2(a_m)\sigma_2(b_n)$$

holds in $ca-90(2m, 2n)$, where $t = t_{2m}$, $s = s_{2n}$, $a = a_{2m}$, $b = b_{2n}$, and w denotes the least common multiple of u =sord(2;m) and v =sord(2;n).

Proof: First note from Lemma 2.4(c), (e) and Propsition 2.7(b), (c) that $t\sigma_2(a_m) = ta$, $t^{2(2^w-1)}\sigma_2(a_m) = \sigma_2(a_m)$ in ca–$90(2m)$ and $s\sigma_2(b_n) = sb$, $s^{2(2^w-1)}\sigma_2(b_n) =$

$\sigma_2(b_n)$ in $ca-90(2n)$. Set $H = 2(2^w - 1)$. Then we have

$$\begin{aligned}(t+s)^H ab + (t+s)^H \sigma_2(a_m)\sigma_2(b_n) &= t^H ab + as^H b + \sum_{j=1}^{H-1}\binom{H}{j} t^{H-j}s^j ab + t^H\sigma_2(a_m)\sigma_2(b_n) \\ &\quad +\sigma_2(a_m)s^H\sigma_2(b_n) + \sum_{j=1}^{H-1}\binom{H}{j} t^{H-j}s^j \sigma_2(a_m)\sigma_2(b_n) \\ &= t^H\sigma_2(a_m)b + as^H\sigma_2(b_n) + \sum_{j=1}^{H-1}\binom{H}{j} t^{H-j}s^j ab \\ &\quad +\sigma_2(a_m)\sigma_2(b_n) + \sigma_2(a_m)\sigma_2(b_n) + \sum_{j=1}^{H-1}\binom{H}{j} t^{H-j}s^j ab \\ &= \sigma_2(a_m)b + a\sigma_2(b_n)\end{aligned}$$

in $ca-90(2m, 2n)$. □

Theorem 4.7: If m and n are mutually disjoint odd integers, then $K(2m, 2n)|2(2^w - 1)$, where w denotes the least common multiple of u =sord(2;m) and v =sord(2;n).

Proof: We write t, s, a, b and α for t_{2m}, s_{2n}, a_{2m}, b_{2n}, and $\alpha_{2m,2n}$, respectively. First note from Lemma 2.4(c) and Proposition 2.7(b) that $t\sigma_2(a_m) = ta$ in $ca-90(2m)$ and $s\sigma_2(b_n) = sb$ in $ca-90(2n)$. As m and n are mutually disjoint, the equality $(t_m + s_n)^{2^w-1}a_m b_n = a_m b_n$ in $ca-90(m, n)$ follows from Theorem 4.1 and Corollary 4.4. Applying the substitution operator $\sigma_{2,2}$ to this equality we have

$$(t+s)^{2(2^w-1)}\sigma_2(a_m)\sigma_2(b_n) = \sigma_2(a_m)\sigma_2(b_n)$$

in $ca-90(2m, 2n)$ and so by Lemma 4.6

$$\begin{aligned}(t+s)^{2(2^w-1)}\alpha &= (t+s)(t+s)^{2(2^w-1)}ab \\ &= (t+s)\{\sigma_2(a_m)b + a\sigma_2(b_n) + (t+s)^{2(2^w-1)}\sigma_2(a_m)\sigma_2(b_n)\} \\ &= (t+s)\{\sigma_2(a_m)b + a\sigma_2(b_n) + \sigma_2(a_m)\sigma_2(b_n)\} \\ &= tab + ta\sigma_2(b_n) + ta\sigma_2(b_n) + \sigma_2(a_m)sb + asb + \sigma_2(a_m)sb \\ &= (t+s)ab \\ &= \alpha\end{aligned}$$

in $ca-90(2m, 2n)$. □

V. NONEXISTENCE OF PERIOD LENGTHS K(m, n)

In this section we will disscuss nonexistence theorems on the period lengths $K(m, n)$ of two-dimensional cellular automata $ca-90(m, n)$.

Theorem 5.1: If m and n are even and at least one of m and n is a multiple of 4, then the period length $K(m, n)$ does not exist.

Proof: Assume that n is a a multiple of 4. The $m/2$th row of a configuration $(t+s)^k\alpha$ $(k \geqslant 0)$ in ca–$90(m, n)$ is identical with the configuration $s^k sb$ in ca–$90(n)$, because of the symmetry. Hence, if $(t+s)^k\alpha = \alpha$ in $ca-90(m, n)$ for some positive integer k, then $s^k sb = sb$ in ca–$90(n)$, which contradicts the fact (Ref. 7, Theorem 2.8) that the period length $K(n)$ of $ca-90(n)$ does not exist if $4|n$. □

Lemma 5.2: If m is odd and a configuration

$$c = \sum_{i=1,j=1}^{m-1,n-1} c_{i,j}t(i)s(j)$$

in $ca-90(m,m)$ satisfies $(t+s)c=0$, $c_{1,1}=c_{2,2}=\cdots=c_{m-1,m-1}$ and $c_{1,m-1}=c_{2,m-2}=\cdots=c_{m-1,1}$, then $c_{i,j}=0$ for every pair (i,j) with $j\neq i$ and $j\neq m-i$.

Proof: The assumption $(t+s)c=0$ means that

$$c_{i-1,j}+c_{i,j-1}+c_{i,j+1}+c_{i+1,j}=0$$

for every site (i,j) with $0<i<m$ and $0<j<n$. By the induction the followng (i)–(iv) can be proved:

$$\text{(i)}c_{i,i+2j}=0,\ \text{(ii)}c_{i+2j,i}=0,\ \text{(iii)}c_{m-i,i+2j}=0,\ \text{and (iv)}\ c_{i,m-i-2j}=0$$

for $0<j<m$ and $0<i<m-2j$. Here we prove only (i). From the assumption $(t+s)c=0$ at a site $(i,i+2j-1)$ we have

$$c_{i-1,i-1+2j}+c_{i,i+2(j-1)}+c_{i,i+2j}+c_{i+1,i+1+2(j-1)}=0.$$

First set $j=1$. Then $c_{i-1,i+1}=c_{i,i+2}$ (by $c_{i,i}=c_{i+1,i+1}$) and so $0=c_{0,2}=c_{1,3}=\cdots=c_{m-3,m-1}$. Hence $c_{i,i+2j}=0$ for $j=1$ and $0<i<m-2j$. Assume that $c_{i,i+2(j-1)}=0$ for $0<i<m-2(j-1)$. Then $c_{i-1,i-1+2j}=c_{i,i+2j}$ for $0<i<m-2j$ [if $0<i<m-2j$, then $i+1<m-2(j-1)$ and $c_{i,i+2(j-1)}=c_{i+1,i+1+2(j-1)}=0$ by the induction hypothesis] and so $0=c_{0,2j}=c_{1,1+2j}=\cdots=c_{m-2j-1,m-1}$. This proves (i). Similarly (ii) follows from

$$c_{i+2(j-1),i}+c_{i-1+2j,i-1}+c_{i+1+2(j-1),i+1}+c_{i+2j,i}=0$$

at $(i+2j-1,i)$, (iii) follows from

$$c_{m-(i+1),i+1+2(j-1)}+c_{m-i,i+2(j-1)}+c_{m-i,i+2j}+c_{m-(i-1),i-1+2j}=0$$

at $(m-i,i+2j-1)$, and (iv) follows from

$$c_{i-1,m-(i-1)-2j}+c_{i,m-i-2j}+c_{i,m-i-2(j-1)}+c_{i+1,i+1-2(j-1)}=0$$

at $(i,m-i-2j+1)$. Now let (i,j) be a pair of positive integers such that $0<i<m, 0<j<m$, $j\neq i$ and $j\neq m-i$. We have to prove $c_{i,j}=0$. If $i+j$ is even and $i<j$, then $c_{i,j}=c_{i,i+2j'}=0$ by (i), where $2j'=j-i$. If $i+j$ is even and $i>j$, then $c_{i,j}=c_{i'+2j',i'}=0$ by (ii), where $i'=j, 2j'=i-j$. If $i+j$ is odd and $i+j>m$, then $c_{i,j}=c_{m-i',i'+2j'}=0$ by (iii), where $i'=m-i$ and $2j'=i+j-m$. If $i+j$ is odd and $i+j<m$, then $c_{i,j}=c_{i,m-i-2j'}=0$ by (iv), where $2j'=m-i-j$. This completes the proof. $\square$

Corollary 5.3: If m is odd, k is a nonnegative integer and u =sord(2;m), then

$$ab+(t+s^{2^k})^{2^u-1}ab=\sum_{i=1}^{m-1}t(i)\{s(2^ki)+s(m-2^ki)\}$$

in $ca-90(m,m)$.

Proof: Set $N=2^u-1$ for short. First assume that $k=0$. Two configurations t^ja and s^jb of ca–$90(m)$ are essentially the same. Hence, if $t(i)$ and $s(i)$ [or $s(m-i)$] simultaneously appear in terms $t^{N-j}a$ and s^jb of

$$(t+s)^Nab=\sum_{j=0}^{N}\binom{N}{j}t^{N-j}s^jab \tag{1}$$

respectively, then they also simultaneously appear in $t^j a$ and $s^{N-j}b$, respectively, and their sum vanishes in (1) since $\binom{N}{j} = \binom{N}{N-j}$. Thus all the diagonal components of $ab + (t+s)^N ab$ are equal to 1. On the other hand, Theorem 4.1 indicates $(t+s)\{ab+(t+s)^N ab\} = 0$. Therefore the proof in the case of $k=0$ is completed by Lemma 5.2. Making use of inner products the result in the case of $k=0$ can be restated as for $0 < i, j < m$:

$$\langle ab + (t+s)^N ab, t(i)s(j)\rangle = \begin{cases} 1 & \text{if } j = i \text{ or } j = m-i, \\ 0 & \text{otherwise,} \end{cases}$$

in $ca-90(m,m)$. For the desired equality in the case of $k > 0$ it is enough to see that for $0 < i, j < m$,

$$\langle ab + (t+s^{2^k})^N ab, t(i)s(j)\rangle = \begin{cases} 1 & \text{if } s(j) = s(2^k i) \text{ or } s(j) = s(m-2^k i) \\ 0 & \text{otherwise,} \end{cases}$$

in $ca-90(m,m)$. When $s(j) = s(2^k j')$ $(0 < j' < m)$, making use of Proposition 2.8 we have

$$\begin{aligned} L &= \langle ab + (t+s^{2^k})^N ab, t(i)s(j)\rangle = 1 + \sum_{r=0}^{N}\binom{N}{r}\langle t^{N-r}s^{2^k r}ab, t(i)s(j)\rangle \\ &= 1 + \sum_{r=0}^{N}\binom{N}{r}\langle t^{N-r}a, t(i)\rangle\langle s^{2^k r}b, s(j)\rangle \\ &= 1 + \sum_{r=0}^{N}\binom{N}{r}\langle t^{N-r}a, t(i)\rangle\langle s^{2^k r}b, s(2^k j')\rangle \\ &= 1 + \sum_{r=0}^{N}\binom{N}{r}\langle t^{N-r}a, t(i)\rangle\langle b, s^{2^k r}s(2^k j')\rangle \\ &= 1 + \sum_{r=0}^{N}\binom{N}{r}\langle t^{N-r}a, t(i)\rangle\langle b, (s^r s(j'))^{2^k}\rangle \\ &= 1 + \sum_{r=0}^{N}\binom{N}{r}\langle t^{N-r}a, t(i)\rangle\langle b, s^r s(j')\rangle \\ &= 1 + \sum_{r=0}^{N}\binom{N}{r}\langle t^{N-r}s^r ab, t(i)s(j')\rangle \\ &= \langle ab + (t+s)^N ab, t(i)s(j')\rangle \\ &= \begin{cases} 1 & \text{if } j' = i \text{ or } j' = m-i \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$

Hence $L = 1$ if $s(j) = s(2^k i)$. If $s(j) = s(m-2^k i)$, then

$$\langle s^{2^k r}b, s(j)\rangle = \langle s^{2^k r}b, s(m-2^k i)\rangle = \langle s^{2^k r}b, s(2^k i)\rangle$$

by the symmetry of $s^{2^k r}b$ [Proposition 2.8(h)] and so $L = 1$ in the same way. Now remark that if j is even there is a unique integer j' with $s(j) = s(2^k j')$ and $0 < j' < m$. [Since 2^{k-1} and m are mutually disjoint there are integers P, Q such that $2^{k-1}P + mQ = 1$. As $jP/2$ is an integer there are integers h, j' such that $jP/2 = hm + j'$ and $0 \leqslant j' < m$. Hence $s(2^k j') = s(2^k(Pj/2 - hm)) = s(j - jmQ - 2^k hm) = s(j)$ since j and 2^k are even.] Assume that $s(j) \neq s(2^k i)$ and $s(j) \neq s(m-2^k i)$ for $0 < i, j < m$. If j is even, we can take an integer j' such that $s(j) = s(2^k j')$ and $0 < j' < m$, and obviously $j' \neq i$ [if $j' = i$ then $s(j) = s(2^k j') = s(2^k i)$] and $j' \neq m-i$ [if $j' = m-i$ then $s(j) = s(2^k j') = s(2^k(m-i)) = s(2^k i)$], and hence $L = 0$. If j is odd, we can take an integer j' such that $s(m-j) = s(2^k j')$ and $0 < j' < m$, and $j' \neq i$ [if $j' = i$ then $s(j) = s(m - 2^k j') = s(m - 2^k i)$] and $m - j' \neq i$ [if $j' = m - i$ then $s(j) = s(m - 2^k j') = s(m - 2^k(m-i)) = s(m - 2^k i)$], and hence $L = 0$. {Note that $t_m(i) = t_m(i')$ implies $t_m(m-i) = t_m(m-i')$ because $t_m(m-i) = t_m(i)a_m + t_m(i)$ [by Lemma 2.4(a)] $= t_m(i')a_m + t_m(i') = t_m(m-i')$.} The proof is completed. □

Theorem 5.4: For an odd integer m the period length $K(2m, 2m)$ does not exist.

Proof: Applying the substitution operator $\sigma_{2,2}$ to the equation ($k = 0$) obtained in Corollary 5.3 we have the equality

$$\sigma_2(a_m)\sigma_2(b_m) + (t+s)^{2(2^u-1)}\sigma_2(a_m)\sigma_2(b_m) = \sum_{i=1}^{m-1} t(2i)\{s(2i) + s(2m-2i)\} \quad (2)$$

in $ca-90(2m, 2m)$. Also it follows from Lemma 4.6 that

$$(t+s)^{2(2^u-1)}ab = \sigma_2(a_m)b + a\sigma_2(b_m) + (t+s)^{2(2^u-1)}\sigma_2(a_m)\sigma_2(b_m)$$

in $ca-90(2m, 2m)$. Hence we have the following equality in $ca-90(2m, 2m)$:

$$\begin{aligned}
(t+s)^{2^{u+1}-1}ab &= (t+s)(t+s)^{2(2^u-1)}ab \\
&= (t+s)\{\sigma_2(a_m)b + a\sigma_2(b_m) + (t+s)^{2(2^u-1)}\sigma_2(a_m)\sigma_2(b_m)\} \\
&= (t+s)\{\sigma_2(a_m)b + a\sigma_2(b_m) + \sigma_2(a_m)\sigma_2(b_m) + R\} \\
&= tab + ta\sigma_2(b_m) + ta\sigma_2(b_m) + \sigma_2(a_m)sb + asb + \sigma_2(a_m)sb + (t+s)R \\
&= (t+s)ab + (t+s)R \\
&= \alpha + (t+s)R,
\end{aligned}$$

where R denotes the right-hand side of (2). As $R_{1,j} = 0$ for $j = 1, 2, \cdots, 2m-1$ and $R_{2,2} = 1$ it is easy to see that $\tau(R) = (t+s)R \neq 0$, for example,

$$R = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

when $m = 3$. Hence $(t+s)^{2^{u+1}-1}ab \neq \alpha$. On the other hand $(t+s)^{2^{u+1}}ab = (t+s)^2 ab$ holds in $ca-90(2m, 2m)$ from Theorem 4.1. We now assume that there exists a positive integer k such that $(t+s)^k\alpha = \alpha$. Then

$$\begin{aligned}
(t+s)^{2^{u+1}-1}ab &= (t+s)^{2^{u+1}-2}\alpha = (t+s)^{2^{u+1}-2}(t+s)^k\alpha = (t+s)^{k-1}(t+s)^{2^{u+1}}ab \\
&= (t+s)^{k-1}(t+s)^2 ab = (t+s)^k\alpha = \alpha,
\end{aligned}$$

which is in contradiction to $(t+s)^{2^{u+1}-1}ab \neq \alpha$. □

corollary 5.5: If m, n are odd integers with the greatest common divisor > 1, then the period length $K(2m, 2n)$ does not exist.

Proof: Let m, D, E be odd integers such that $m > 1, D > 0, E > 0$ and D, E are mutually disjoint. We prove that the period length $K(2mD, 2mE)$ does not exist. Assume that $(t_{2mD} + s_{2mE})^k \alpha_{2mD,2nE} = \alpha_{2mD,2nE}$ in $ca-90(2mD, 2mE)$ for some positive integer k. Then by applying the reduction operator $\rho_{D,E}$ to this equation we have $(t_{2m} + s_{2m})^k \alpha_{2m,2m} = \alpha_{2m,2m}$ in $ca-90(2m, 2m)$ making use of Proposition 2.7(d) and (e), since D, E are odd. This contradicts the result of Theorem 5.4. □

Theorem 5.6: If m is odd and k is a positive integer, then the period length $K(2^k m, m)$ does not exist.

Proof: We write t, s, a, b and α for $t_{2^k m}, s_m, a_{2^k m}, b_m$ and $\alpha_{2^k m,m}$. Set $u = sord(2; m)$ and $N = 2^u - 1$. As has been seen at the proof of Theorem 4.5 an equation

$$(t+s)^{2^k N}(t+s)^{2^k-1}\alpha = (t+s)^{2^k-1}\alpha$$

holds in $ca-90(2^k m, m)$. Now assume that $(t+s)^h\alpha = \alpha$ in $ca-90(2^k m, m)$ for a positive integer h. Choose a positive integer M with $hM > 2^k - 1$. Then we have $(t+s)^{2^k N}\alpha = \alpha$ in $ca-90(2^k m, m)$ because

$$\begin{aligned}(t+s)^{2^k N}\alpha &= (t+s)^{2^k N}(t+s)^{hM}\alpha = (t+s)^{hM-(2^k-1)}(t+s)^{2^k N}(t+s)^{2^k-1}\alpha \\ &= (t+s)^{hM-(2^k-1)}(t+s)^{2^k-1}\alpha = (t+s)^{hM}\alpha = \alpha.\end{aligned}$$

On the other hand, an equality

$$a_m b + (t_m + s^{2^k})^N a_m b = \sum_{i=1}^{m-1} t_m(i)\{s(2^k i) + s(m - 2^k i)\}$$

in $ca-90(m, m)$ is valid by Corollary 5.3. Applying the substitution operator $\sigma_{2^k,1}$ to this equality we have

$$\sigma_{2^k}(a_m)b + (t^{2^k} + s^{2^k})^N \sigma_{2^k}(a_m)b = \sum_{i=1}^{m-1} t(2^k i)\{s(2^k i) + s(m - 2^k i)\} \tag{3}$$

in ca–$90(2^k m, m)$. In the proof of Theorem 4.5 it has been seen that $t^{2^k N}\sigma_{2^k}(a_m) = \sigma_{2^k}(a_m)$ and $t^{2^k-1}\sigma_{2^k}(a_m) = t^{2^k-1}a$ in $ca-90(2^k m)$ and $s^N b = b$ in $ca-90(m)$. Therefore we have

$$\begin{aligned}(t+s)^{2^k(2^u-1)}\alpha &= (t+s)(t^{2^k} + s^{2^k})^N ab = (t+s)\left\{as^{2^k N}b + \sum_{j=0}^{N-1} t^{2^k(N-j)}s^{2^k j}ab\right\} \\ &= (t+s)\left\{ab + \sum_{j=0}^{N-1} t^{2^k(N-j)}s^{2^k j}\sigma_{2^k}(a_m)b\right\} \\ &= (t+s)\{ab + t^{2^k N}\sigma_{2^k}(a_m)b + (t^{2^k} + s^{2^k})^N\sigma_{2^k}(a_m)b\} \\ &= (t+s)\{ab + \sigma_{2^k}(a_m)b + (t^{2^k} + s^{2^k})^N\sigma_{2^k}(a_m)b\} \\ &= (t+s)(ab + S) \\ &= \alpha + (t+s)S,\end{aligned}$$

where S denotes the right-hand side of (3). As $S_{2^k-1,j} = 0$ for $0 < j < 2^k m$ and $S_{2^k,j_0} = 1$ for a unique (even) integer j_0 such that $0 < j_0 < m$ and $s(j_0) = s(2^k)$, it is clear that $(t+s)S \neq 0$. This contradicts $(t+s)^{2^k N}\alpha = \alpha$. □

Corollary 5.7: If m, n are odd integers with the greatest common divisor > 1 and k is a positive integer, then the period length $K(2^k m, n)$ does not exist.

Proof: Let m, D, E be odd integers such that $m > 1, D > 0, E > 0$ and D, E are mutually disjoint and k a positive integer. We prove that the period length $K(2^k mD, mE)$ does not exist. By Proposition 2.7(e) the reduction operator $\rho_{D,E}$ satisfies $\rho_{D,E}(a_{2^k mD}b_{mE}) = a_{2^k m}b_m$ since D, E are odd. Assume that $(t+s)^k\alpha = \alpha$ in ca–$90(2^k mD, mE)$ for some positive integer k. Then by applying the reduction operator $\rho_{D,E}$ it follows that $(t+s)^k\alpha = \alpha$ in $ca-90(2^k m, m)$, which contradicts the result of Theorem 5.6. □

The following is a summary of our results obtained above.

Theorem 5.8: The period length $K(m,n)$ of $ca-90(m,n)$ exists if and only if there exists no integer $D>1$ such that $2D|m$ and $D|n$, or $D|m$ and $2D|n$. Supposed that m and n are odd integers >1 and k is a positive integer, then

(a) $K(m,n)|2^w-1$,

(b) $K(m,2^k)|2^{k-1}(2^u-1)$,

(c) $K(m,2^kn)|2^k(2^w-1)$ if m and n are mutually disjoint,

(d) $K(2m,2)|2(2^u-1)$,

(e) $K(2m,2n)|2(2^w-1)$ if m and n are mutually disjoint,

where w is the least common multiple of $u=$sord(2;m) and $v=$sord(2;n).

Proof: It suffices to show that if there exists an integer $D>1$ such that

$$(*)\quad 2D|m \text{ and } D|n, \text{ or } D|m \text{ and } 2D|n,$$

then the period length $K(m,n)$ does not exist, and if there exists no integer $D>1$ satisfying the condition $(*)$, then the period length $K(m,n)$ exists. Let $m=2^hm'$ and $n=2^kn'$, where h,k are non-negative integers and m',n' are odd integers. Logically there are the following six cases : (i) $h=k=0$, (ii) $h=k=1$, (iii) $h=0$ and $k>0$, (iii') $h>0$ and $k=0$, (iv) $h\geqslant 2$ and $k\geqslant 1$, (iv') $h\geqslant 1$ and $k\geqslant 2$. (i) In this case both of m and n are odd and there exists no $D>1$ satisfying the condition $(*)$. Thus the period length $K(m,n)$ exists by Theorem 4.1, which proves (a). (ii) An integer $D>0$ satisfies $(*)$ if and only if it is a common divisor of m' and n'. If m' and n' are mutually disjoint, then there exists no $D>1$ with $(*)$ and the period length $K(m,n)$ exists by Theorem 4.7 and (Ref. 7, Corollary 3.3 and Theorem 3.6), which proves (e) and (d), respectively. On the other hand if m' and n' have a common divisor $D>1$, then D satisfies $(*)$ and the period length $K(m,n)$ does not exist by Corollary 5.5. (iii) An integer $D>0$ satisfies $(*)$ if and only if it is a common divisor of m and n'. If m and n' are mutually disjoint, then there exists no $D>1$ such that $(*)$ and the period length $K(m,n)$ exists by Theorems 4.2 and 4.5, which proves (b) and (c), respectively. On the other hand, if m and n' have a common divisor $D>1$, then D satisfies $(*)$ and the period length $K(m,n)$ does not exist by Corollary 5.7. (iv) In this case $4|m$ and $2|n$, in which case the period length $K(m,n)$ does not exist by Theorem 5.1. This cpmpletes the proof. □

Appendix

A. Table of the period lengths $K(m,n)$ $(1 < m < 20, 1 < n \leqslant 10)$

m \ n	2	3	4	5	6	7	8	9	10
2	1	1	$*$	3	2	7	$*$	7	6
3	1	1	2	3	$*$	7	4	7	6
4	$*$	2	$*$	6	$*$	14	$*$	14	$*$
5	3	3	6	1	6	63	12	63	$*$
6	2	$*$	$*$	6	$*$	14	$*$	$*$	6
7	7	7	14	63	14	7	28	7	126
8	$*$	4	$*$	12	$*$	28	$*$	28	$*$
9	7	7	14	63	$*$	7	28	7	126
10	6	6	$*$	$*$	6	126	$*$	126	$*$
11	31	31	62	341	62	32767	124	32767	682
12	$*$	$*$	$*$	12	$*$	28	$*$	$*$	$*$
13	63	21	126	63	126	63	252	63	126
14	14	14	$*$	126	14	$*$	$*$	14	126
15	15	15	30	15	$*$	4095	60	4095	$*$
16	$*$	8	$*$	24	$*$	56	$*$	56	$*$
17	15	15	30	15	30	4095	60	4095	30
18	14	$*$	$*$	126	$*$	14	$*$	$*$	126
19	511	511	1022	87381	1022	511	2044	511	174762

B. Table of the period lengths $K(m,n)$ ($1 < m < 20, 11 \leqslant n < 20$

m \ n	11	12	13	14	15	16	17	18	19
2	31	$*$	63	14	15	$*$	15	14	511
3	31	$*$	21	14	15	8	15	$*$	511
4	62	$*$	126	$*$	30	$*$	30	$*$	1022
5	341	12	63	126	15	24	15	126	87381
6	62	$*$	126	14	$*$	$*$	30	$*$	1022
7	32767	28	63	$*$	4095	56	4095	14	511
8	124	$*$	252	$*$	60	$*$	60	$*$	2044
9	32767	$*$	63	14	4095	56	4095	$*$	511
10	682	$*$	126	126	$*$	$*$	30	126	174762
11	31	124	$2^{30}-1$	65534	349525	248	1048575	65534	$(2^{45}-1)/7$
12	124	$*$	252	$*$	$*$	$*$	60	$*$	2044
13	$2^{30}-1$	252	63	126	4095	504	4095	126	262143
14	65534	$*$	126	$*$	8190	$*$	8190	14	1022
15	349525	$*$	4095	8190	15	120	15	$*$	$(2^{36}-1)/3$
16	248	$*$	504	$*$	120	$*$	120	$*$	4088
17	1048575	60	4095	8190	15	120	15	8190	$2^{36}-1$
18	65534	$*$	126	14	$*$	$*$	8190	$*$	1022
19	$(2^{45}-1)/7$	2044	262143	1022	$(2^{36}-1)/3$	4088	$2^{36}-1$	1022	511

(The symbol $*$ denotes the nonexistence of the period lengths.)

[1]O. Martin, A.M. Oldlyzko and S. Wolfram, "Algebraic properties of cellular automata," Commun. Math. Phys. **93,** 219–258 (1984).
[2]S. Wolfram, *Theory and applications of cellular automata* (World Scientific, Singapore, 1986).
[3]P. Guan and Y. He, "Exact results for deterministic cellular automata with additive rules," J. Stat. Phys. **43,** 463–478 (1986).
[4]S.S. Manna and D. Stauffer, "Systematics of transitions of square-lattice cellular automata," Phys. A **162,** 176–186 (1990).
[5]L.R. da Silva, "Fractal dimension at the phase transition of inhomogenous cellular automata," J. Stat. Phys. **53,** 985–990 (1988).
[6]P.M. Binder, "Topological classification of cellular automata," J. Phys. A **24,** L31–L34 (1991).
[7]Y. Kawahara, "Existence of the characteristic numbers associated with cellular automata with lacal transition rule 90," Bull. Inform. Cybernet. **24**(3-4), 121–136 (1991).
[8]M. Nohmi, "On a polynomial representation of finite linear cellular automata," Bull. Inform. Cybernet. **24**(3-4), 137–145 (1991).