Chapter 5.

A note on the property of linear cellular automata

1 Introduction

Cellular automata are discrete dynamical systems with simple construction. We define a cellular automaton as follows.

Put $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ for $n \in \mathbb{N}$. Let p be a prime number, r a natural number and $\mathcal{P}$ the set of all configurations $w : \mathbb{Z} \to \mathbb{Z}_{p^r}$ with compact support. Let a linear transition rule $L : \mathcal{P} \to \mathbb{Z}_{p^r}$ be defined as follows:

$$Lw(x) \equiv \sum_{k \in G} c_k w(x+k) \pmod{p^r} \quad \text{for } w \in \mathcal{P}, \tag{1.1}$$

where the set G is a finite subset of $\mathbb{Z}$ with $\sharp G \geq 2$ and $c_k \in \mathbb{N}$.

Patterns of linear cellular automata were studied by some people. Existence of the limit of a series of space-time patterns is proved [1, 3, 5, 6]. E. Jen showed that a series $\{L^t w(x) \,|\, t \in \mathbb{N}\}$ is aperiodic for some L with $p = 2$ in [2]. In [5], S. Takahashi considered the case where L is p^r-state linear cellular automata with the initial state δ_0 which is 1 at the origin and 0 at others. He examined the limit set with respect to each non-zero state, by using the fact that every state appears in the set $\{L^t\delta_0(-(t-1)r_1 - r_2) \,|\, t = 1, \ldots, p^{r+1}\}$. However, when we consider the limit set as a multi-valued function, the set $\{L^t\delta_0(-(t-1)r_1 - r_2) \,|\, t = 1, \ldots, p^{r+1}\}$ does not work well. Hence we need another set which includes every state and plays a useful role in examing the limit set. So we give a systematic set which has one-to-one, onto correspondence with the set $\{0, 1, 2, \ldots, p^r - 1\}$. This set may play an important role in examing the limit set of space-time patterns as a $\mathbb{Z}_{p^r}$-valued upper semi continuous function [4].

2 The result

We deal with the specified transition rule L, which satisfies some condition. We say that L *satisfies the condition* (A) if there exist $r_1, r_2 \in G$ satisfying

(I) $c_{r_1}/p, c_{r_2}/p \notin \mathbb{N}$,

(II) r_1 is an either maximum or minimum element of the set G,

(III) r_2 is extreme or $r_2 = \sum_{k\in G, r_2\neq k} \beta_k k$ with $0 \leq \beta_k < 1$ such that $\sum_{k\in G, r_2\neq k} \beta_k = 1$ and $p^{r-1}\beta_k \notin \mathbb{N}$,

(IV) if r_1 is maximum [resp. minimum], then for $s \in \{1, 2, \dots, p-1\}$, $l \in \{1, 2, \dots, |r_1 - r_2| - 1\}$ there does not exist a path from $-r_1 s(p^r - p^{r-1}) + l$ [resp. $-r_1 s(p^r - p^{r-1}) - l$] to the origin, that is, we have

$$-\sum_{k\in G} \alpha_k k \notin \{-r_1 s(p^r - p^{r-1}) + l \,|\, l \in \{1, 2, \dots, |r_1 - r_2| - 1\}\}$$

$$[\text{resp. } -\sum_{k\in G} \alpha_k k \notin \{-r_1 s(p^r - p^{r-1}) - l \,|\, l \in \{1, 2, \dots, |r_1 - r_2| - 1\}\}]$$

for the set $\{\alpha_k\}_{k\in G} \subset \mathbb{N} \cup \{0\}$ such that $\sum_{k\in G} \alpha_k = s(p^r - p^{r-1})$ with $s \in \{1, 2, \dots, p-1\}$.

Here, an element $k \in G$ is *extreme* if an element k is not expressed as a convex linear combination of other elements of G. We note that a maximum or minimum element of the set G is extreme.

By using $r_1, r_2 \in G$ which satisfy (I),(II),(III) and (IV), put

$$t(r, j) = j(p^r - p^{r-1}) \tag{2.1}$$

and

$$i(r, j) = -(t(r, j) - p^{r-1})r_1 - p^{r-1} r_2 \tag{2.2}$$

for $j \in \mathbb{N}$. We define $\delta_0 \in \mathcal{P}$ as

$$\delta_0(x) = \begin{cases} 1 & x = 0 \\ 0 & x \neq 0. \end{cases}$$

```
                                                x
 ──────────────────────────────────────────────────▶
│00000000000000000000100000000000000000000
│00000000000000000005030000000000000000000
│00000000000000000010601000000000000000000
│00000000000000000501070300000000000000000
│00000000000000001040604010000000000000000
│00000000000000050702060103000000000000000
│00000000000000102070407020100000000000000
│00000000000005050101070703030000000000000
│00000000000010004000600040001000000000000
│00000000000503040406020404050300000000000
│00000000001060500020402000506010000000000
│00000000050103070202060601050703000000000
│00000000104020407000400070402040100000000
│00000005070602070504040301060201030000000
│00000010203040106030003060104030201000000
│00000505050501010101070707070303030300000
│00001000000004000000060000000400000001000
│00050300000040400000602000004040000050300
│00106010004000400060406000400040001060100
│05010703040404040606020204040404050107030
t ↓10406040500000002000400020000000504060401
```

Figure 1: Space-time pattern of $L_3\delta_0(x) \equiv 3\delta_0(x-1) + 5\delta_0(x+1) \pmod{2^3}$

We shall prove that the set $\{L^{t(r,j)}\delta_0(i(r,j)) | 1 \le j \le p^r\}$ has one-to-one, onto correspondence with the set $\{0, 1, 2, \ldots, p^r - 1\}$. We shall call the set $\{a_n \,|\, n = 1, \ldots, k\}$ a *k-set*, if the set has one-to-one, onto correspondence with the set $\{0, 1, \ldots, k-1\}$.

We need the following lemmas later.

Lemma 2.1. [5] *Suppose* L *is defined as* (1.1). *For* $j, l \in \mathbb{N}$, *we have*

$$L^{p^{l+r-1}j}\delta_0(x) = \begin{cases} L^{jp^{r-1}}\delta_0(y) & \text{if there exists } y \text{ such that } p^l y = x, \\ 0 & \text{otherwise.} \end{cases}$$

Lemma 2.2. *Suppose* $q \in \mathbb{N}$ *with* $q/p \notin \mathbb{N}$, $t = jp^{r-1}$ *with* $j \in \mathbb{N}$ $v = p^l q$ *with* $l \in \{0, 1, \ldots, r-2\}$ *and* $v < t$.

Then there exists $q' \in \mathbb{N}$ *with* $q'/p \notin \mathbb{N}$ *such that* $t - v = p^l q'$.

Proof. We have $t - v = p^l(jp^{r-l-1} - q)$. Put $q' = jp^{r-l-1} - q$. So we obtain $q'/p \notin \mathbb{N}$ by $q/p \notin \mathbb{N}$. □

Lemma 2.3. *Let* L *be defined as* (1.1) *and satisfy the condition* (A). *Suppose* $r \in \mathbb{N}$, $r \ge 2$ *and* $j \in \{1, 2, \ldots, p^r\}$. *Let* $r_1, r_2 \in G$ *satisfy* (I),(II),(III) *and* (IV) *of the condition* (A). *Then the following assertions hold:*

(1) $L^{t(r,1)}\delta_0(i(r,1))/p \notin \mathbb{N}$.

(2) *The set* $\{nL^{t(1,1)}\delta_0(i(1,1)) \bmod p \,|\, 1 \le n \le p\}$ *is a* p*-set.*

(3) *Suppose* $|r_1 - r_2| \ge 2$. *If* $r_1 > r_2$*[resp.* $r_1 < r_2$*], then*

$$\begin{aligned} L^{t(r,j)}\delta_0(-t(r,j)r_1 + l) &= 0 \\ [\text{resp. } L^{t(r,j)}\delta_0(-t(r,j)r_1 - l) &= 0] \end{aligned} \tag{2.3}$$

holds for $l \in \{1, 2, \ldots, |r_1 - r_2| - 1\}$ *and*

$$\begin{aligned} L^{t(r,sp^{r-1})}\delta_0(-t(r,sp^{r-1})r_1 + l) &= 0 \\ [\text{resp. } L^{t(r,sp^{r-1})}\delta_0(-t(r,sp^{r-1})r_1 - l) &= 0] \end{aligned}$$

holds for $l \in \{1, 2, \ldots, p^{r-1}|r_1 - r_2| - 1\}$ *and* $s \in \{1, 2, \ldots, p-1\}$.

Proof. (1) For $a, b \in \mathbb{N}$ put ${}_{a+b}\mathrm{C}_b = (a+b)!/(a!b!)$. We have

$$L^{t(r,1)}\delta_0(i(r,1)) \equiv {}_{p^r - p^{r-1}}\mathrm{C}_{p^{r-1}} c_{r_1}^{p^r - p^{r-1} - p^{r-1}} c_{r_2}^{p^{r-1}} \pmod{p^r}$$

by (II) and (III) of the condition (A). Since

$${}_{p^r - p^{r-1}}\mathrm{C}_{p^{r-1}} = \frac{(p^r - p^{r-1})(p^r - p^{r-1} - 1)\cdots(p^r - p^{r-1} - p^{r-1} + 1)}{p^{r-1}!},$$

p does not divide ${}_{p^r - p^{r-1}}\mathrm{C}_{p^{r-1}}$ by Lemma 2.2. Then p does not divide $L^{t(r,1)}\delta_0(i(r,1))$ by (I) of the condition (A).

(2) We shall show that $nL^{t(1,1)}\delta_0(i(1,1)) \not\equiv 0 \pmod p$ holds for all $n \in \{1, 2, \ldots, p-1\}$. The proof is by contradiction. Assume that there exists $n_0 \in \{1, 2, \ldots, p-1\}$ such that $n_0 L^{t(1,1)}\delta_0(i(1,1)) = s_0 p$ holds with some $s_0 \in \mathbb{N}$. Then we have $L^{t(1,1)}\delta_0(i(1,1)) = s_0 p/n_0$. Since $n_0 \le p-1$, $s_0/n_0 \in \mathbb{N}$ holds. Therefore p divide $L^{t(1,1)}\delta_0(i(1,1))$, which contradicts assumption.

(3) Suppose $r_1 > r_2$. Since $1 \le l \le r_1 - r_2 - 1$, there does not exist any path from the origin to the point $-t(r,j)r_1 + l$ by (IV) of the condition (A). So we have $L^{t(r,j)}\delta_0(-t(r,j)r_1 + l) = 0$.

Since $t(r, sp^{r-1}) = p^{r-1}t(r, s)$, we have

$$\begin{aligned}
L^{t(r,sp^{r-1})}\delta_0(-t(r, sp^{r-1})r_1) &= L^{t(r,s)}\delta_0(-t(r, s)r_1) \\
L^{t(r,sp^{r-1})}\delta_0(-t(r, sp^{r-1})r_1 + p^{r-1}(r_1 - r_2))) &= L^{t(r,s)}\delta_0(-t(r, s)r_1 + (r_1 - r_2)) \\
L^{t(r,sp^{r-1})}\delta_0(-t(r, sp^{r-1})r_1 + l) &= 0
\end{aligned}$$

for $l \in \{1, 2, \dots, p^{r-1}(r_1 - r_2) - 1\}$ and $s \in \{1, 2, \dots, p-1\}$ by Lemma 2.1 and the equation (2.3).

In case $r_1 < r_2$, we can prove it in the same way as above. $\square$

Lemma 2.4. *Suppose $r \geq 2$ and L satisfies the condition (A). Then*

$$L^{t(r,j)}\delta_0(i(r, j)) \equiv L^{t(r,m)}\delta_0(i(r, m)) + sL^{t(r,p^{r-1})}\delta_0(i(r, p^{r-1})) \pmod{p^r}$$

holds for $j = sp^{r-1} + m$ with $s \in \{0, 1, \dots, p-1\}$ and $m \in \{1, 2, \dots, p^{r-1}\}$.

Proof. Let $r_1, r_2 \in G$ satisfy (I),(II),(III) and (IV) of the condition (A). We first consider the case where $r_1 > r_2$. We compute $L^{t(r,j)}\delta_0(i(r, j))$ from the values at time $t(r, j-1)$. We have

$$\begin{aligned}
L^{t(r,j)}\delta_0(i(r, j)) \equiv\ & {}_{p^r - p^{r-1}}\mathrm{C}_{p^{r-1}} c_{r_1}^{p^r - 2p^{r-1}} c_{r_2}^{p^{r-1}} \\
& + \sum_{k=1}^{p^{r-1}(r_1 - r_2) - 1} B(r, k)b(r, j-1, k) \\
& \quad + c_{r_1}^{p^r - p^{r-1}} L^{t(r,j-1)}\delta_0(i(r, j-1)) \pmod{p^r},
\end{aligned}$$

where $b(r, j, k) = L^{t(r,j)}\delta_0(-t(r, j)r_1 + k)$ and $B(r, k) \in \mathbb{N}$ for $k \in \{1, 2, \dots, p^{r-1}(r_1 - r_2) - 1\}$ and $B(r, k)$ does not depend on j.

Put

$$d(j) = \sum_{k=1}^{p^{r-1}(r_1 - r_2) - 1} B(r, k)b(r, j, k)$$

and we rewrite the equation above as follows:

$$\begin{aligned}
L^{t(r,j)}\delta_0(i(r, j)) &\equiv L^{t(r,1)}\delta_0(i(r, 1)) + d(j-1) + L^{t(r,j-1)}\delta_0(i(r, j-1)) \\
&\equiv jL^{t(r,1)}\delta_0(i(r, 1)) + \sum_{l=1}^{j-1} d(l) \pmod{p^r}
\end{aligned}$$

from Euler's theorem ($n^{p^r - p^{r-1}} \equiv 1 \pmod{p^r}$).

We have $b(r, sp^{r-1}, k) = 0$ for all $k \in \{1, 2, \ldots, p^{r-1}(r_1 - r_2) - 1\}$ and all $s \in \{1, 2, \ldots, p-1\}$ by Lemma 2.3(3) and $L^{t(r,sp^{r-1})}\delta_0(-t(r, sp^{r-1})r_1) \equiv 1 \pmod{p^r}$. Since $B(r, k)$ does not depend on j, we have

$$d(m + sp^{r-1}) \equiv d(m) \pmod{p^r} \tag{2.4}$$

for $m \in \{1, 2, \ldots, p^{r-1}\}$ and $s \in \{1, 2, \ldots, p-1\}$ by (II) of the condition (A).

For $j = sp^{r-1} + m$ with $m \in \{1, 2, \ldots, p^{r-1}\}$ and $s \in \{0, 1, \ldots, p-1\}$

$$\begin{aligned} L^{t(r,j)}\delta_0(i(r,j)) &\equiv jL^{t(r,1)}\delta_0(i(r,1)) + \sum_{l=1}^{j-1} d(l) \\ &\equiv sp^{r-1}L^{t(r,1)}\delta_0(i(r,1)) + s\sum_{l=1}^{p^{r-1}-1} d(l) + mL^{t(r,1)}\delta_0(i(r,1)) + \sum_{l=1}^{m-1} d(l) \\ &\equiv L^{t(r,m)}\delta_0(i(r,m)) + sL^{t(r,p^{r-1})}\delta_0(i(r,p^{r-1})) \pmod{p^r} \end{aligned}$$

by (2.4). In case $r_1 < r_2$, putting $b(r,j,k) = L^{t(r,j)}\delta_0(-t(r,j)r_1 - k)$, we can prove in the same way. □

Put

$$a(r,j) = L^{t(r,j)}\delta_0(i(r,j)) \tag{2.5}$$

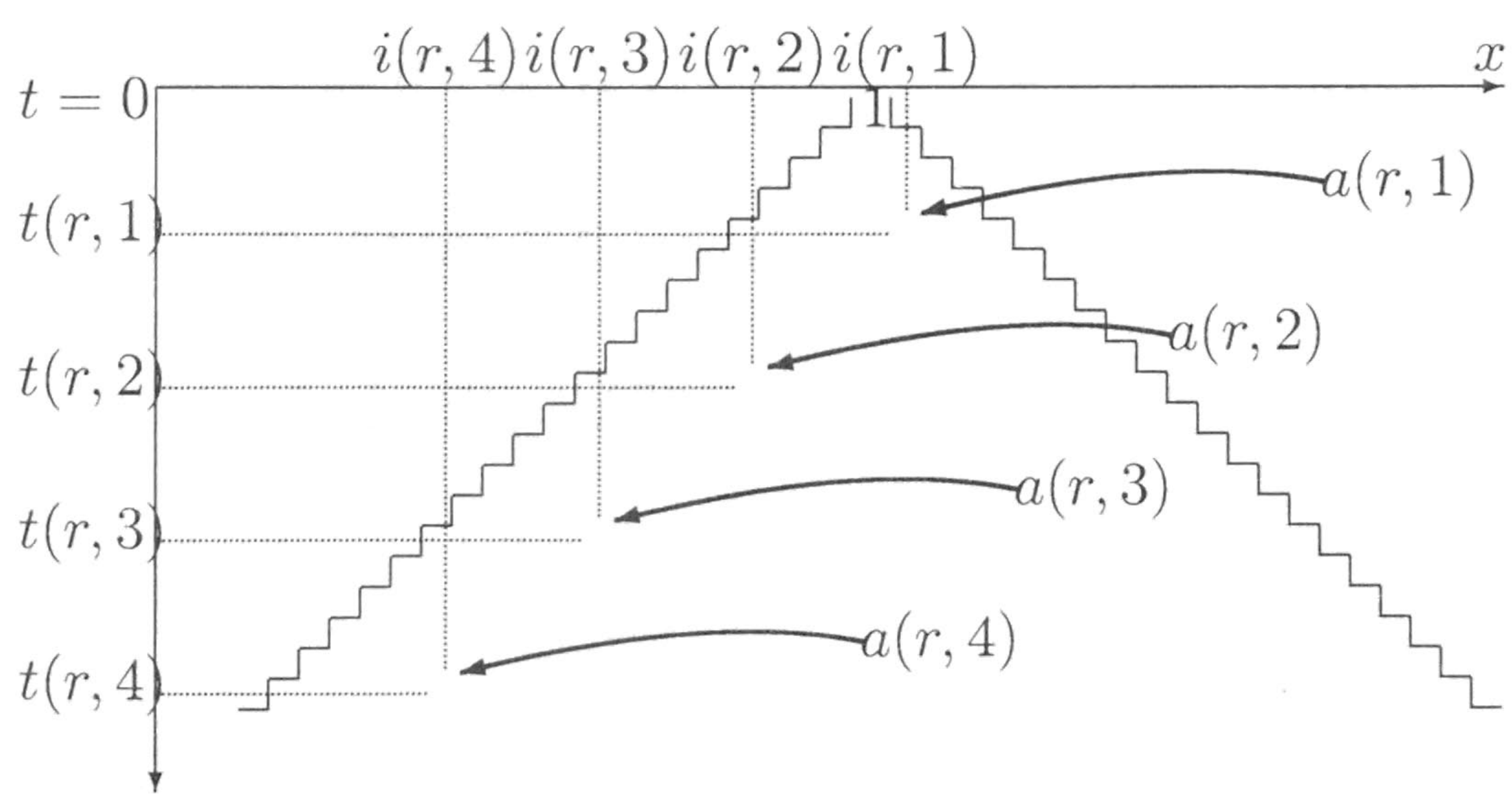

Figure 2 : The relation among $t(r,j), i(r,j)$ and $a(r,j)$.

for convenience. We will prove the set $\{a(r,j)\,|\,1 \le j \le p^r\}$ is a p^r-set. In order to prove the following lemma, we define a map $\mathcal{L} : \mathcal{P} \to \mathbb{N}$ as follows:

$$\mathcal{L}w(x) = \sum_{k \in G} c_k w(x+k), \tag{2.6}$$

where the set G and c_k are as in the definition of L. We note that there exists $k(r,j) \in \mathbb{N}$ such that

$$\mathcal{L}^{t(r,j)} \delta_0(i(r,j)) = k(r,j)p^r + a(r,j). \tag{2.7}$$

Lemma 2.5. *Suppose $a(r,j)$ is defined as (2.5) and the set $\{a(r,j)\,|\,1 \le j \le p^r\}$ is a p^r-set. Then the following assertions hold:*

(1) *$a(r+1,j) \neq a(r+1,l)$ holds for $j,l \in \{1,2,\dots,p^r\}$ with $j \neq l$.*

(2) *There exists $k_0 \in \mathbb{N}(0 \le k_0 \le p-1)$ such that $a(r,p^{r-1}) = p^{r-1}k_0$.*

(3) *$a(r+1,j) \not\equiv a(r+1,l) + ka(r+1,p^r) \pmod{p^{r+1}}$ holds for any $k \in \{1,2,\dots,p-1\}$ and $j,l \in \{1,2,\dots,p^r\}$ with $j \neq l$.*

(4) *$a(r+1,j) + k_1 a(r+1,p^r) \not\equiv a(r+1,j) + k_2 a(r+1,p^r) \pmod{p^{r+1}}$ holds for any $k_1,k_2 \in \{1,2,\dots,p-1\}$ with $k_1 \neq k_2$ and $j \in \{1,2,\dots,p^r\}$.*

Proof. We have

$$a(r,j) \equiv \mathcal{L}^{t(r,j)} \delta_0(i(r,j)) \equiv \mathcal{L}^{t(r+1,j)} \delta_0(i(r+1,j)) \pmod{p^r} \tag{2.8}$$

for $j \in \{1,2,\dots,p^r\}$ by Lemma 2.4, since

$$\mathcal{L}^{pt(r,j)} \delta_0(pi(r,j)) = \mathcal{L}^{t(r+1,j)} \delta_0(i(r+1,j))$$

by Lemma 2.1 and

$$\mathcal{L}^{t(r,j)} \delta_0(i(r,j)) \equiv \mathcal{L}^{pt(r,j)} \delta_0(pi(r,j)) \pmod{p^r}.$$

Therefore by (2.8) there exists $k'(r,j) \in \mathbb{N}$ for $j \in \{1,2,\dots,p^r\}$ such that

$$\mathcal{L}^{t(r+1,j)} \delta_0(i(r+1,j)) = k'(r,j)p^r + a(r,j). \tag{2.9}$$

So we obtain by (2.7) and (2.9)

$$k(r+1,j)p^{r+1} + a(r+1,j) = k'(r,j)p^r + a(r,j) \tag{2.10}$$
$$k(r+1,l)p^{r+1} + a(r+1,l) = k'(r,l)p^r + a(r,l). \tag{2.11}$$

for $j, l \in \{1, 2, \dots, p^r\}$.

(1) Assume $a(r+1,j) = a(r+1,l)$ holds for $j, l \in \{1, 2, \dots, p^r\}$ with $j \neq l$. By (2.10) and (2.11) $a(r,j) - a(r,l) = (k(r+1,j) - k(r+1,l))p^{r+1} - (k'(r,j) - k'(r,l))p^r$, which contradicts the assumption.

(2) We will prove it by induction on r.

   (a) In case $r = 1$, it is clear by definition.

   (b) In case $r > 1$, assume that it is true for $r = r'$. Then we have $a(r', p^{r'}) \equiv pa(r', p^{r'-1}) \equiv pp^{r'-1}k_0 \equiv p^{r'}k_0 \pmod{p^{r'}}$ by Lemma 2.4 and the assumption of induction. So there exists $k_0' \in \mathbb{N}(0 \leq k_0' \leq p-1)$ such that $a(r'+1, p^{r'}) = p^{r'}k_0'$ by (2.10).

(3) The proof is by contradiction. Assume that there exists $k_1 \in \mathbb{N}$ such that $a(r+1,j) \equiv a(r+1,l) + k_1 a(r+1,p^r) \pmod{p^{r+1}}$. Then there exists $s_0 \in \mathbb{N}$ such that $a(r+1,j) - a(r+1,l) - k_1 a(r+1,p^r) = s_0 p^{r+1}$. There exists $k_0 \in \{0, 1, \dots, p-1\}$ such that $a(r+1,p^r) = p^r k_0$ by the assertion (2). By the equations (2.10) and (2.11), we have

$$\begin{aligned}
a(r,j) - a(r,l) &= (k(r+1,j) - k(r+1,l))p^{r+1} - (k'(r,j) - k'(r,l))p^r \\
&\qquad + a(r+1,j) - a(r+1,l) \\
&= (k(r+1,j) - k(r+1,l))p^{r+1} - (k'(r,j) - k'(r,l))p^r \\
&\qquad + s_0 p^{r+1} + k_0 k_1 p^r \\
&= p^r\{(k(r+1,j) - k(r+1,l))p - (k'(r,j) - k'(r,l)) + s_0 p + k_0 k_1\},
\end{aligned}$$

which contradicts $a(r,j) \neq a(r,l)$ by $0 \leq a(r,j) - a(r,l) \leq p^r - 1$.

(4) It is clear by the property of modulus.

□

Proposition 2.6. *Suppose $r \in \mathbb{N}$. If the set $\{a(r,j) \mid 1 \le j \le p^r\}$ is a p^r-set, then the set $\{a(r+1,j) \mid 1 \le j \le p^{r+1}\}$ is a p^{r+1}-set.*

Proof. We obtain the conclusion by Lemma 2.4 and the assertion (1), (3) and (4) of Lemma 2.5. □

Theorem 2.7. *For a prime number p and $r \in \mathbb{N}$, let L be defined as (1.1) and satisfy the condition (A). Put $t(r,j) = j(p^r - p^{r-1})$ and $i(r,j) = -(t(r,j) - p^{r-1})r_1 - p^{r-1}r_2$, where $r_1, r_2 \in G$ satisfy (I),(II),(III) and (IV) of the condition (A).*

Then the set $\{L^{t(r,j)}\delta_0(i(r,j)) \mid 1 \le j \le p^r\}$ is a p^r-set.

Proof. The proof is by induction on r.

(1) In case $r = 1$, from Lemma 2.3(3),

$$\begin{aligned} L^{t(1,j)}\delta_0(i(1,j)) &\equiv {}_{t(1,1)}C_p c_{r_1}^{t(1,1)-1} c_{r_2} + c_{r_1}^{t(1,1)} L^{t(1,j-1)}\delta_0(i(1,j-1)) \\ &\equiv L^{t(1,1)}\delta_0(i(1,1)) + L^{t(1,j-1)}\delta_0(i(1,j-1)) \\ &\equiv jL^{t(1,1)}\delta_0(i(1,1)) \qquad \pmod p \end{aligned}$$

for $1 \le j \le p$ by Euler's theorem ($n^{p^r - p^{r-1}} \equiv 1 \pmod{p^r}$ for any $r \in \mathbb{N}$) and $L^{t(1,1)}\delta_0(i(1,1)) \equiv {}_{t(1,1)}C_p c_{r_1}^{t(1,1)-1} c_{r_2} \pmod p$. So the assertion holds for $r = 1$ from Lemma 2.3(2).

(2) In case $r \ge 2$, we get the conclusion by the proposition above and the assumption of induction.

□

References

[1] F. v. Haeseler, H.-O. Peitgen and G. Skordev, *Linear cellular automata, substitutions, hierarchical iterated function systems and attractors.* Fractal Geometry and Computer Graphics, J. L. Encarnação, H.-O. Peitgen, G. Sakas, and G. Englert, Eds. Springer-Verlag, 1992.

[2] E. Jen, *Aperiodicity in one-dimensional cellular automata.* Physica D **45** (1990), 3–18.

[3] M. Matsuto and F. Takeo, *The limit set of cellular automata.* Natur. Sci. Rep. Ochanomizu Univ. **48** (1997), 9–22.

[4] M. Matsuto, *Convergence to the limit set of linear cellular automata, II.* in preparation.

[5] S. Takahashi, *Self-similarity of linear cellular automata.* J. Comput. System Sci. **44** (1992), 114–140.

[6] S. Willson, *Cellular automata can generate fractals.* Discrete Appl. Math. **8** (1984), 91–99.