97-112

International Journal of Bifurcation and Chaos, Vol. 9, No. 1 (1999) 67–95
© World Scientific Publishing Company

AUTOMATICITY OF COARSE-GRAINING INVARIANT ORBITS OF ONE-DIMENSIONAL LINEAR CELLULAR AUTOMATA

ANDRÉ BARBÉ
Katholieke Universiteit Leuven, Department of Electrical Engineering, Kardinaal Mercierlaan 94, B-3001, Leuven, Belgium

HEINZ-OTTO PEITGEN and GENCHO SKORDEV
Center for Complex Systems and Visualization, University of Bremen, Universitätsallee 29, 28359 Bremen, Germany

Received December 15, 1997; Revised May 14, 1998

We consider one-dimensional linear cellular automata whose states are the integers modulo a prime power p^d and their orbital patterns. We are particulary interested in initial states and their orbital patterns which are invariant under a certain coarse-graining operation. We show that these coarse-graining invariant initial states are p-automatic. The relationship between the solutions of a certain family of coarse-graining invariant problems concerning linear cellular automata over the integers modulo p^n is investigated.

1. Introduction

Coarse-graining is a particular way of rescaling a pattern. It is a standard technique in renormalization, a concept that is used in the analysis of critical phenomena in physics. The p-coarse-graining operation for linear p-state cellular automata was introduced and investigated in [Barbé *et al.*, 1995; Barbé, 1996, 1997] in the case p is a prime number. It was conjectured in the last two of these references that the initial configurations with p-coarse-graining invariant orbits are p-automatic sequences for p prime. This means, among other things, that any element of the sequence can be obtained from a finite automaton whose input is the digit-sequence of the base-p representation of its position (see e.g. [Allouche, 1990; Allouche & Mendès France, 1994; Allouche *et al.*, 1997]). It was shown in [Barbé *et al.*, 1995] that this is true for some cases with $p = 2$, because the generating functions of the corresponding initial configuration were shown to satisfy some functional equation (Mahler equation) and are therefore algebraic w.r.t. the field of rational functions with coefficients modulo 2 [Christol, 1979; Christol *et al.*, 1980].

In this paper, we shall prove this conjecture for p-Fermat linear cellular automata with states in the ring of the integers modulo a power of the prime number p. For this we consider a more general case of m-coarse-graining invariant initial configurations for m-Fermat linear cellular automata with states in a finite commutative ring R with unity (m-Fermat cellular automata were introduced in [von Haeseler *et al.*, 1992, 1993; Allouche *et al.*, 1996], see also Definition 3 in this paper). As in the case $R = \mathbb{F}_p$ (the Galois field wih p elements), considered in [Barbé *et al.*, 1995] and [Barbé, 1996], there are only finitely many m-coarse-graining invariant initial configurations. The left and the right part of these bilateral sequences are solutions of particular m-Mahler equations in the ring R.

The functional equations of Mahler (in the case where R is the field of complex numbers) were introduced and investigated by K. Mahler for holomorphic functions in connection with the problem

of transcendence of values of their solutions, see [Mahler, 1929; Loxton & van der Poorten, 1977; Lipshitz & van der Poorten, 1989; Nishioka, 1996]. Later on it was observed that the generating functions $F(X)$ of p-automatic sequences satisfy a p^d-Mahler equation in $R = \mathbb{F}_m$, $m = p^d$:

$$a(X) + a_0(X)F(X) + a_1(X)F(X^m) + \cdots + a_k(X)F(X^{m^k}) = 0\,. \qquad (1)$$

Here $a(X)$, $a_0(X), \ldots, a_k(X)$ are polynomials with coefficient in the Galois field $\mathbb{F}_m$, and the equation is considered in $\mathbb{F}_m$. Moreover, all solutions of such equations are generating functions of p-automatic sequences ([Christol, 1979; Christol *et al.*, 1980]).

Using the fact that, when $F(X)$ is a power series in $\mathbb{F}_m$, it holds that $F(X^m) = (F(X))^m$, and considering the case $m = p$ (prime), Eq. (1) can be rewritten as

$$a(X) + a_0(X)F(X) + a_1(X)F(X)^p + \cdots + a_k(X)F(X)^{p^k} = 0\,. \qquad (2)$$

In [Christol, 1986; Denef & Lipshitz, 1987; Lipshitz & van der Poorten, 1989] it was proven that Eq. (2), considered as an equation in $R = \mathbb{Z}_p$ — the ring of p-adic numbers (see e.g. [Neukirch, 1991]) — has a solution in the form of a power series $\tilde{F}(X)$ with coefficients in $\mathbb{Z}_p$ (such power series is usually called algebraic w.r.t. the field of rational functions with p-adic coefficients), with $\tilde{F}(X) \equiv F(X) \bmod p$. Moreover, for all algebraic power series $\tilde{F}(X)$ (w.r.t. the rational functions with p-adic coefficients), the sequence of coefficients of $\tilde{F}(X)$ reduced modulo p^d is a p-automatic sequence for all d.

This assertion implies the automaticity of some integer sequences modulo p^d as follows. Suppose that the generating function $F(X)$ of an integer sequence satisfies an equation of the type Eq. (2) for $R = \mathbb{Z}$. Then considering this equation as an equation in p-adic numbers, it still has the solution $F(X)$, i.e. this power series with integer (and therefore p-adic) coefficients is algebraic w.r.t. the field of rational functions with p-adic coefficients. Then the above theorem from [Christol, 1979; Christol *et al.*, 1980] implies that the sequence of coefficients of $F(X)$ modulo p^d is p-automatic for all $d \in \mathbb{N}$.

In general, it is not possible to apply the same reasoning for an integer solution $F(X)$ of Eq. (1), i.e. in the case $R = \mathbb{Z}$. Such a solution is a solution of the same p-Mahler equation (1) in $R = \mathbb{Z}_p$ (the p-adic integers), but in general $F(X)$ is not an algebraic power series w.r.t. the field of rational functions with p-adic coefficients, e.g. the integer solution of the integer p-Mahler equation $F(X) = X + F(X^p)$ is also a p-adic solution of this equation but is not an algebraic element w.r.t. the field of rational functions with p-adic coefficients [Lipshitz & van der Poorten, 1989].

In general the question of the automaticity of the solution of an m-Mahler equation for m not a prime power and for polynomials and power series in a given ring R is open. von Haeseler considered this question and obtained results in some cases. He also presented an example of a solution of a Mahler equation with $m = 2$, and $R = \mathbb{F}_p$, $p \geq 3$, which is not p-automatic [von Haeseler, 1996]. Jürgensen considered the case of arbitrary m and $R = \mathbb{F}_p$ [Jürgensen, 1997].

After a preliminary section concerning cellular automata, automaticity, decimation and coarse-graining operations, we consider the automaticity of solutions of an m-Mahler equation for the case $m = p$, with p a prime number and R the ring of integers modulo p^d. In this case it is not possible to apply the theorem of Christol *et al.* [1980], (see also [Christol, 1979]), or the theorem of Denef and Lipshitz [1987], to obtain the p-automaticity of the solutions of these equations.

In Sec. 3, we consider the case $R = \mathbb{Z}$, i.e. we assume that the coefficients $a(X)$, $a_0(X), \ldots, a_k(X)$ of Eq. (1) are polynomials with integer coefficients and that there exists a solution as a formal Laurent power series $\overline{F}(X)$ with integer coefficients.

In Sec. 4, we prove that the sequence of the coefficients of $\overline{F}(X)$ reduced modulo p^d is p-automatic for all d. The generating functions of p^d-coarse-graining invariant initial configurations for p-Fermat linear cellular automata with p^d states is a solution of an equation of type Eq. (1) modulo p^d satisfying the above assumptions. Therefore we obtain as a corollary that p^d-coarse-graining invariant sequences modulo a prime power p^d are p-automatic. The proof uses some properties about the solutions of homogeneous difference equations with constant integer coefficients, see e.g. [Jungnickel, 1993]. Remind that the solutions of homogeneous difference equations with constant integer coefficients reduced modulo m are generating functions of shift register sequences modulo m [Lidl & Niederreiter, 1983].

Section 5 concerns the two-dimensional automaticity of the orbit of a linear cellular automaton (LCA) that is obtained from a one-dimensional automatic initial configuration.

In Sec. 6, we present some results concerning the relationship between the coarse-graining invariant orbit-patterns of a certain family of LCA over the integers modulo p^n (p prime). These patterns are all solutions of the same underlying coarse-graining invariant problem, but for different n.

2. Preliminaries

2.1. *R-state linear cellular automata*

We shall use the usual notations: $\mathbb{N} = \{0, 1, 2, \ldots\}$; $\mathbb{Z}$ for the integers; $\mathbb{Z}^2$ for the two-dimensional integer lattice; $\mathbb{F}_p$ for the residues modulo a prime number p. We denote also the ring of integers modulo m by $Z_m (\stackrel{\text{def}}{=} \mathbb{Z}/m\mathbb{Z})$ and the ring of p-adic numbers by $\mathbb{Z}_p$. For a given ring R we use the notations: $R[X]$ for the ring of polynomials with coefficients in R, $R[[X]]$ for the ring of formal power series $\sum_{n\in\mathbb{N}} a_n X^n$ with coefficients in R, and we use the notation $R((X))$ in a nonstandard way for indicating a formal Laurent series of the form $\sum_{n\in\mathbb{Z}} a_n X^n$ with coefficients in R.

By Σ_1 we shall denote the set of all maps $\underline{a} : \mathbb{Z} \to R$. We call these maps one-dimensional R-state configurations. By Σ_2 we shall denote the set of all maps $\underline{\omega} : \mathbb{Z} \times \mathbb{N} \to R$. We call these maps two-dimensional R-state configurations.

Definition 1. An R-state *linear cellular automaton* (LCA) with generating Laurent polynomial

$$l(X) = \sum_{i=-d_1}^{d_2} l_i X^i, \quad l_i \in R \tag{3}$$

is a map $A : \Sigma_1 \to \Sigma_1$ defined by

$$A\underline{a}(n) = \sum_{i=-d_2}^{d_1} l_{-i}\underline{a}(n+i), \quad n \in \mathbb{Z},$$

see [Wolfram, 1994; Allouche *et al.*, 1996], i.e. the sequence $A\underline{a}$ is the convolution $\underline{l} * \underline{a}$, where $\underline{l} = (l(n))_{n\in\mathbb{Z}}$ is the sequence of coefficients of the polynomial $l(X)$.

An equivalent definition is:

Definition 2. Let

$$F(X) = \sum_{i=-\infty}^{\infty} \underline{a}(i) X^i$$

be the generating Laurent series of the one-dimensional configuration $\underline{a} = (\underline{a}(i))_{i\in\mathbb{Z}}$, then

$$F(X)l(X) = \sum_{i=-\infty}^{\infty} A\underline{a}(i) X^i,$$

(Cauchy multiplication of power series).

We say that a Laurent polynomial $l(X)$ as given by Eq. (3) has degree (d_1, d_2) if $l_{d_2} l_{-d_1} \neq 0$.

Definition 3. The R-state linear cellular automaton A with generating Laurent polynomial $l(X) \in R((X))$ is called *m-Fermat cellular automaton* if

$$l(X)^m = l(X^m).$$

In this case we say also that the Laurent polynomial is m-Fermat, see [von Haeseler *et al.*, 1992, 1993; Allouche *et al.*, 1996].

Remark 1. The property m-Fermat is equivalent to the small Fermat theorem in the case $m = p$ (prime number) and $R = \mathbb{F}_p$, see [Childs, 1979, p. 176]. For more examples of m-Fermat polynomials, see [Allouche *et al.*, 1996].

2.2. *m-Automata*

An m-automaton $\mathcal{A} = (S, s_0, \varphi, T, \tau)$ consists of five objects:

- *state alphabet*, a finite set S,
- *initial state*, an element $s_0 \in S$,
- *input alphabet* $[m] \stackrel{\text{def}}{=} \{0, \ldots, m-1\}$,
- *input map*, $\varphi : [m] \times S \to S$,
- *output alphabet*, a finite set T,
- *output map*, $\tau : S \to T$.

See [Cobham, 1972; Christol *et al.*, 1980; Allouche, 1990; Allouche & Mendès France, 1994]. The general notions are defined in [Eilenberg, 1985].

Instead of the input map $\varphi : [m] \times S \to S$ we shall consider the maps $i : S \to S$, $i \in [m]$, defined by $i \cdot s = \varphi(i, s)$ for $s \in S$.

For $n \in \mathbb{N}$, the maps $n : S \to S$ are defined recursively. Write $n = mn' + n_0$ with $n_0 \in [m]$ and $n' \neq 0$, then the map $n : S \to S$ is defined as

$$n \cdot s = n' \cdot (n_0 \cdot s) = \varphi(n', n_0 \cdot s).$$

The m-automaton $\mathcal{A}$ produces a sequence

$$(u(n))_{n\in\mathbb{N}} = (\tau(n \cdot s_0))_{n\in\mathbb{N}}$$

in the output set T. The sequence $(u(n))_{n\in\mathbb{N}}$ is called m-automatic.

An equivalent definition of m-automaticity uses the notion of the *m-kernel* $\mathcal{K}_m(\underline{u})$ of a sequence $\underline{u} = (u(n))_{n\in\mathbb{N}}$:

$$\mathcal{K}_m(\underline{j}) = \{(u(m^k n + j))_{n\in\mathbb{N}} | k \geq 0,\ 0 \leq j \leq m^k - 1\}.$$

The sequence $\underline{u}$ is m-automatic if and only if the m-kernel $\mathcal{K}_m(\underline{u})$ is a finite set, see [Allouche, 1990; Allouche & Mendès France, 1994; Cobham, 1972].

2.3. m^s-Decimation operators for m-fermat LCA

Let $m, s \in \mathbb{N}$, $m \geq 2$, $s \geq 1$. Let $d_u : \mathbb{Z} \to \mathbb{Z}$, $d_{u,v} : \mathbb{Z}^2 \to \mathbb{Z}^2$, $u \in \mathbb{Z}$, $v \in \mathbb{N}$ be the maps defined by

$$d_u(n) = m^s n + u\,, \quad n \in \mathbb{Z}\,,$$

$$\begin{aligned} d_{u,v}(k, l) &= d_u \times d_v(k, l) \\ &= (m^s k + u, m^s l + v)\,, \quad (k, l) \in \mathbb{Z}^2\,. \end{aligned}$$

They induce the maps

$$d_u^* : \Sigma_1 \to \Sigma_1\,,$$
$$d_{u,v}^* : \Sigma_2 \to \Sigma_2\,, \quad u \in \mathbb{Z},\ v \in \mathbb{N}$$

as follows

$$d_u^*(\underline{a}) = \underline{a} \circ d_u\,, \quad \underline{a} \in \Sigma_1\,,$$
$$d_{u,v}^*(\underline{\omega}) = \underline{\omega} \circ d_{u,v} = \underline{\omega}(d_u \times d_v)\,, \quad \underline{\omega} \in \Sigma_2\,.$$

We call the maps d_u^* and $d_{u,v}^*$: (m^s, u)- and $(m^s, (u, v))$-*decimation operators*, respectively. The results of applying these operators to $\underline{a}$ or $\underline{\omega}$ are called (m^s, u)-decimation and $(m^s, (u, v))$-decimation. The decimation operators are linear maps (R-module maps) if we consider Σ_1 and Σ_2 as linear spaces (R-modules) over R.

Definition 4. Let $u \in \mathbb{Z}$ and $v \in \mathbb{N}$. A one-dimensional configuration $\underline{a} \in \Sigma_1$ [two-dimensional configuration $\underline{\omega} \in \Sigma_2$] is called (m^s, u)-*decimation invariant* [$(m^s, (u, v))$-decimation invariant] if $d_u^*(\underline{a}) = \underline{a}$ [$d_{u,v}^*(\underline{\omega}) = \underline{\omega}$].

Let $A : \Sigma_1 \to \Sigma_1$ be an R-state LCA and let $O_A(\underline{a})$ be the orbit of the initial configuration $\underline{a} \in \Sigma_1$ w.r.t. A, i.e.

$$O_A(\underline{a}) = \{A^n \underline{a} | n \in \mathbb{N}\}\,.$$

We consider $O_A(\underline{a})$ as a two-dimensional configuration, i.e. $O_A(\underline{a}) \in \Sigma_2$, as follows:

$$O_A(\underline{a}) : \mathbb{Z} \times \mathbb{N} \to R\,,$$
$$O_A(\underline{a})(k, l) = A^l \underline{a}(k)\,, \quad k \in \mathbb{Z},\ l \in \mathbb{N}\,.$$

Lemma 1. *Let A be an R-state m-Fermat linear cellular automaton and let d_u^*, $d_{u,v}^*$ be m^s-decimation operators, $u \in \mathbb{Z}$, $v \in \mathbb{N}$. Then*

1. $d_u^*(A^{m^s}\underline{a}) = \mathrm{A}(d_u^*(\underline{a}))$,
2. $d_{u,v}^*(O_A(\underline{a})) = O_A(d_u^* \mathrm{A}^v(\underline{a}))$

for every $\underline{a} \in \Sigma_1$.

Proof. The proofs of the assertions of Lemma 1 follow the proof of Lemma 1 in [Barbé *et al.*, 1995]. The crucial point is that the Laurent polynomial $l(X) \in R((X))$ has the m-Fermat property: $l(X^m) = l(X)^m$, implying that $l(X^{m^s}) = l(X)^{m^s}$. ∎

Corollary 1. *The $(m^s, (u, 0))$-decimation of the orbit of a one-dimensional configuration $\underline{a}$ w.r.t. an R-state m-Fermat LCA is the orbit of the (m^s, u)-decimation of the configuration $\underline{a}$, and also: the orbit of a (m^s, u)-decimation invariant one-dimensional configuration is $(m^s, (u, 0))$-decimation invariant.*

2.4. m^s-coarse-graining operators for m-Fermat LCA

In this section we introduce m^s-coarse-graining operators and study m^s-coarse-graining invariant orbits of a given R-state m-Fermat LCA.

Definition 5. Let

$$c_u : \Sigma_1 \to \Sigma_1\,,$$
$$c_{u,v} : \Sigma_2 \to \Sigma_2\,, \quad u \in \mathbb{Z},\ v \in \mathbb{N}$$

be the maps defined by

$$c_u = \sum_{j=0}^{m^s-1} d_{u+j}^*\,,$$

$$c_{u,v} = c_u \times c_v\,.$$

They are called m^s-*coarse-graining operators*.

We shall consider also an m^s-coarse-graining operator

$$\bar{c}_u : \Sigma_1 \times [m^s] \to \Sigma_1 ,$$

which produces from an m^s-row configuration $\underline{\alpha} : \mathbb{Z} \times [m^s] \to R$ a one-row configuration as follows:

$$\bar{c}_u(\underline{\alpha})(n) = \sum_{j,k=0}^{m-1} \underline{\alpha}(m^s n + u + j, k)$$

for $u, n \in \mathbb{Z}$.

Let $\underline{a} \in \Sigma_1$. Then we denote by $\underline{\alpha}_a$ the m^s-row configuration:

$$\{\underline{\alpha}_a(n, v) = A^v \underline{a}(n) | n \in \mathbb{Z},\ v \in [m^s]\} .$$

We say that the one-row configuration $\underline{a}$ is m^s-*coarse-graining invariant* (CGI) w.r.t. A, if

$$\bar{c}_u(\underline{\alpha}_a) = \underline{a} , \quad \text{for} \quad u \in [m^s] .$$

A two-dimensional configuration $\underline{\omega} \in \Sigma_2$ is called m^s-coarse-graining invariant (m^s-CGI) w.r.t. A, if

$$c_{u,0}(\underline{\omega}) = \underline{\omega} , \quad \text{for} \quad u \in [m^s] .$$

Lemma 2. *Let $\underline{a} \in \Sigma_1$ be a one-dimensional configuration and let c_u, $c_{u,0}$ be m^s-coarse-graining operators, $u \in \mathbb{Z}$. Then for any R-state m-Fermat LCA $A : \Sigma_1 \to \Sigma_1$ we have*

$$c_{u,0}(O_A(\underline{a})) = O_A(\bar{c}_u(\underline{\alpha}_a)) .$$

Corollary 2. *Let A be an R-state m-Fermat linear cellular automaton. Let $\underline{a}$ be a one-dimensional configuration that is m^s-CGI w.r.t. A. Then its orbit $O_A(\underline{a})$ is an m^s-CGI two-dimensional configuration.*

The proof of Lemma 2 directly follows from the definitions, just as for Lemma 2 in [Barbé *et al.*, 1995].

Lemma 3. *Let A be an R-state m-Fermat linear cellular automaton induced by the Laurent polynomial $l(X)$ of degree (d_1, d_2), $d_1 d_2 > 0$, $d = d_1 + d_2$. Suppose that the coefficients l_{-d_1}, l_{d_2} are invertible in R. Then there exist $|R|^{(m^s-1)(d+1)}$ m^s-coarse-graining invariant one-dimensional configurations.*

Moreover, for every set

$$\{a_i | -(m^s-1)d_2 \le i \le (m^s-1)(d_1+1)-1,\ a_i \in R\} ,$$

there is a unique one-dimensional configuration $\underline{a}$ that is m^s-coarse-graining invariant w.r.t. A, with

$$\underline{a}(i) = a_i , \quad \text{for} \quad -(m^s-1)d_2 \le i \le (m^s-1)(d_1+1) - 1 . \quad (4)$$

Proof. Fix the set $S = \{a_i | a_i \in R,\ -(m^s-1)d_2 \le i \le (m^s-1)(d_1+1)-1\}$. Then m^s-CGI requires that for all $k \in \mathbb{Z}$ and for all $\sigma \in [m^s]$:

$$\begin{aligned} \underline{a}(k) = \sum_{i=0}^{m^s-1} [&\underline{a}(m^s k + i + \sigma) + A\underline{a}(m^s k + i + \sigma) \\ &+ A^2 \underline{a}(m^s k + i + \sigma) \\ &+ \cdots + A^{m^s-1} \underline{a}(m^s k + i + \sigma)] . \end{aligned} \quad (5)$$

Putting $k = 0$, and using Definition 1, the $A^l \underline{a}(m^s k + i + \sigma)$-terms in this equation can be expressed as a function of the $\underline{a}(j)$, yielding, for $\sigma = 0$:

$$\begin{aligned} \underline{a}(0) = w\underline{a}(-(m^s-1)d_2) + &\sum_{i=-(m^s-1)+1}^{(m^s-1)(d_1+1)-1} w_i \underline{a}(i) \\ &+ w' \underline{a}((m^s-1)(d_1+1)) , \end{aligned}$$

where $w_i \in R$, and $w = (l_{-d_2})^{m^s-1}$ and $w' = (l_{d_1})^{m^s-1}$ are invertible in R. From this last equation, $\underline{a}((m^s-1)(d_1+1))$ can be solved. Then let $k = 0$, $\sigma = 1$ in Eq. (5) to obtain

$$\begin{aligned} \underline{a}(0) = w\underline{a}(&-(m^s-1)d_2 + 1) \\ &+ \sum_{i=-(m^s-1)+1}^{(m^s-1)(d_1+1)-1} w_i \underline{a}(i+1) \\ &+ w' \underline{a}((m^s-1)(d_1+1)+1) , \end{aligned}$$

from which $\underline{a}(-(m^s-1)(d_1+1)+1)$ can now be solved. Then consider the CGI-equation Eq. (5) for $k = 0$, $\sigma = 2, 3, \ldots, m^s-1$; $k = 1$, $\sigma = 0, 1, \ldots, m^s-1$, $k = 2$, $\sigma = 0, 1, \ldots, m^s-1$, etc., in order to find that $\underline{a}(l)$ can be solved recursively for increasing l.

In the same way, $\underline{a}(l)$ for $l < -(m^s-1)d_2$ can be constructed recursively from the CGI-equation Eq. (5). For each possible configuration S, we find a different and unique solution of the CGI-equation. ■

Remark 2. The example $l(X) = 1 + X$ shows that the condition $d_1 d_2 > 0$ is necessary for Lemma 3 to hold (though not necessary for the existence of a nontrivial solution of Eq. (5) and its corresponding coarse-graining invariant orbit).

In [Barbé *et al.*, 1995] and [Barbé, 1996], p^s coarse-graining invariance in p-Fermat linear CA for the cases $R = Z_p = \mathbb{F}_p$, p prime were considered. In what follows, we will investigate p^s-CGI of p-Fermat LCA with $R = Z_{p^d}$ (the ring of integers modulo p^d), p prime. This is possible because of the following property [Robinson, 1987; Allouche *et al.*, 1996].

Lemma 4. *Let $r(X) \in Z_{p^d}[X]$, then $l(X) = r(X)^{p^d-1} \bmod p^d$ is a p-Fermat polynomial, i.e. $l(X)^p = l(X^p)$.*

Thus, any LCA with such a generating polynomial $l(X) = r(X)^{p^d-1} \in Z_{p^d}[X]$ is p-Fermat, and it is possible to construct p^s-CGI orbits from initial configurations which are p^s-CGI w.r.t. such $l(X)$. For the study of the automaticity of these initial configurations and orbits, we will next show that these p^s-CGI initial configurations satisfy a Mahler equation. It will be useful to consider first integer p^s-CGI equations and corresponding integer Mahler equations, after which these equations and sequences can be reduced modulo p^d.

3. Integer m-Mahler Equation for Coarse-Graining Invariant Initial Configurations

Here we shall consider the case $R = \mathbb{Z}$ and a Laurent polynomial $l(X)$ with integer coefficients. This polynomial generates a $\mathbb{Z}$-state linear cellular automaton which is m-Fermat only in the case that $l(X)$ is a monomial. Since we need assertions similar to the assertions proved for m-Fermat LCA we shall generalize the notion of m-coarse-graining invariant configurations as follows.

Consider the integer sequences $\underline{a} : \mathbb{Z} \to \mathbb{Z}$, $\underline{a} = (a(k))_{k\in\mathbb{Z}}$. By $a(X)$ we shall denote the generating function of this sequence $a(X) = \sum_{k\in\mathbb{Z}} \underline{a}(k) X^k$. Suppose $l(X)$ is a Laurent polynomial with integer coefficients:

$$l(X) = \sum_{j=-d_1}^{d_2} l_j X^j . \tag{6}$$

With $\underline{a}_v$ we shall denote the sequence with generating function

$$a_v(X) = a(X) l(X)^v = \sum_{k\in\mathbb{Z}} \underline{a}(k, v) X^k . \tag{7}$$

Definition 6. Let z be a natural number, $z \geq 2$. We say that the integer sequence $\underline{a} : \mathbb{Z} \to \mathbb{Z}$ is z-CGI (z-coarse-graining invariant) w.r.t. the Laurent polynomial $l(X)$ if

$$\underline{a}(k) = \sum_{u,v=0}^{z-1} \underline{a}(zk + u + w, v) \tag{8}$$

for every $w \in [z]$, $k \in \mathbb{Z}$.

Remark 3. Compare with the definition of m^s-CGI for m-Fermat cellular automata in Sec. 2.4.

Lemma 5. *When $d_1 d_2 > 0$ in Eq. (6), a z-CGI integer sequence $\underline{a}$ w.r.t. the Laurent polynomial $l(X)$ is uniquely determined by its values $\underline{a}(j)$ for $-(z-1)d_2 \leq j \leq (z-1)(d_1+1) - 1$.*

Proof. As the proof of Lemma 3. ■

Writing the $\underline{a}(zk + u + w, v)$ in Eq. (8) as a function of the sequence elements $\underline{a}(i)$, using $\underline{a}(l, v) = \sum_{i=-d_2}^{d_1} l_{-i} \underline{a}(l + i, v - 1)$, one obtains the CGI-equation

$$\underline{a}(k) = \sum_{i=i_{\min}}^{i_{\max}} w_i \underline{a}(zk + i + w) \quad \text{for all } w \in [z],\ k \in \mathbb{Z} . \tag{9}$$

Important for the sequel is that the coefficients $w_{i_{\min}}$ and $w_{i_{\max}}$ satisfy $w_{i_{\min}} = \pm 1$, $w_{i_{\max}} = \pm 1$ ($d_1 d_2 > 0$ and $l_{-d_1} = \pm 1$, $l_{d_2} = \pm 1$ in Eq. (6) is a sufficient condition).

Lemma 6. *Let $\underline{a}$ be a z-CGI integer sequence satisfying Eq. (9) with $i_{\max} \geq 0$, $w_{i_{\min}} = \pm 1$, $w_{i_{\max}} = \pm 1$. Let $a(X)$ be the generating function of $\underline{a}$. Then there are polynomials with integer coefficients $P(X)$, $Q(X)$ with $Q(0) = 1$ such that*

$$Q(X) a(X) = P(X) a(X^z) , \tag{10}$$

i.e. $a(X)$ satisfies an integer z-Mahler equation.

Proof. Suppose $w_{i_{\max}} = 1$ (the -1-case is similar). The CGI-equation Eq. (9) can then be written as

$$\underline{a}(zk + i_{\max} + w) = \underline{a}(k) - \sum_{i=i_{\min}}^{i_{\max}-1} w_i \underline{a}(zk + i + w) \quad \text{for all } w \in [z],\ k \in \mathbb{Z}. \tag{11}$$

Use this in

$$a(X) = \sum_{w\in[z]} \sum_{k\in\mathbb{Z}} \underline{a}(zk + i_{\max} + w) X^{zk+i_{\max}+w} \tag{12}$$

to obtain

$$a(X)\left[1 + \sum_{i=1}^{i_{\max}-i_{\min}} w_{i_{\max}-i} X^i\right] = \left(\sum_{w\in[z]} X^{i_{\max}+w}\right) a(X^z), \tag{13}$$

which is in the form of Eq. (10); as $i_{\max} \geq 0$, all summations in this expression represent polynomials. ■

Remark 4. In the forthcoming sections where automaticity will be the central issue, we will consider only sequences $(b(k))_{k\in\mathbb{N}}$ that are defined over $\mathbb{N}$ instead of over $\mathbb{Z}$. Corresponding generating functions are then defined as $b(X) = \sum_{k\in\mathbb{N}} b(k)X^k$. We call the sequences over $\mathbb{N}$ unidirectional, and the sequences over $\mathbb{Z}$ bidirectional.

Lemma 7. *Let $\underline{a}$ be a bidirectional z-CGI integer sequence satisfying Eq. (9) with $w_{i_{\min}} = \pm 1$, $w_{i_{\max}} = \pm 1$. Then it is always possible to find an integer n_+ such that for $n \geq n_+$, the unidirectional sequence $(a_n^+(k))_{k\in\mathbb{N}} = (a(k+n))_{k\in\mathbb{N}}$ has a generating function $a_n^+(X)$ that satisfies the integer z-Mahler equation*

$$Q_n^+(X)a_n^+(X) = P_n^+(X)a_n^+(X^z) + R_n^+(X), \tag{14}$$

with $Q_n^+(X)$, $P_n^+(X)$, $R_n^+(X)$ polynomials, $Q_n^+(0) = 1$.

Also, it is possible to find an n_- such that for $n \geq n_-$, $(a_n^-(k))_{k\in\mathbb{N}} = (a(-k+n))_{k\in\mathbb{N}}$ has a generating function $a_n^-(X)$ that satisfies

$$Q_n^-(X)a_n^-(X) = P_n^-(X)a_n^-(X^z) + R_n^-(X), \tag{15}$$

with $Q_n^-(X)$, $P_n^-(X)$, $R_n^-(X)$ polynomials, $Q_n^-(0) = 1$.

Proof. Although a bit more involved because of the emergence of expressions like $\sum_{k\in\mathbb{N}'} a(k+n_+)X^k$, where $\mathbb{N}' = \{b, b+1, b+2, \ldots\}$ for some $b \neq 0$, the proof of this property is similar to the proof of Lemma 6. Actually, the fact that $\mathbb{N}' \neq \mathbb{N}$ causes the appearance of the $R_n^{\pm}$ terms. ■

4. *p*-Automaticity of Solutions of *p*-Mahler Equations Modulo p^d

Let p be an integer $p \geq 2$. Primality of p will be assumed from Sec. 4.5 on. Sections 4.1 to 4.4 are also valid when p is replaced by p^s (which corresponds to underlying p^s-decimations).

4.1. *p-decimation of sequences and their generating functions*

Firstly, we shall introduce some notions and notations for unidirectional sequences and their generating functions. They are similar to the corresponding notions for the bidirectional sequences introduced in Sec. 2.3.

Let R be a commutative ring with unity. We shall consider sequences $\underline{c} = (c(n))_{n\in\mathbb{N}}$ with elements in R, i.e. maps $\underline{c} : \mathbb{N} \to R$, or $\underline{c} \in R^{\mathbb{N}}$. The generating function of the sequence $\underline{c}$ is the formal power series

$$c(X) = \sum_{n\in\mathbb{N}} c(n)X^n$$

with coefficients in R, i.e. $c(X) \in R[[X]]$.

Let $P(X)$, $Q(X)$ be polynomials with coefficients in R, i.e. $P(X)$, $Q(X) \in R[X]$, and let $Q(0)$ be an invertible element in the ring R. We say that the rational function $P(X)/Q(X)$ is the generating function of the sequence $\underline{c}$ if

$$P(X) = Q(X)c(X) \tag{16}$$

as a formal power series.

The p-decimation operators

$$d_u : R^{\mathbb{N}} \to R^{\mathbb{N}},$$
$$\delta_u : R[[X]] \to R[[X]], \quad u \in [p]$$

are defined as follows

$$d_u(\underline{c})(n) = c(pn + u),$$
$$\delta_u(c(X)) = \sum_{n\in\mathbb{N}} c(pn + u)X^n,$$

i.e. $\delta_u(c(X))$ is the generating function of the sequence $d_u(\underline{c})$.

In the case that the rational function $P(X)/Q(X)$ is the generating function of the sequence $\underline{c}$ [in the sense of Eq. (16)] we shall write

$$\delta_u\left(\frac{P(X)}{Q(X)}\right) = \sum_{n\in\mathbb{N}} c(pn+u)X^n\,. \qquad (17)$$

Using these definitions of p-decimations we have: The p-kernel $\mathcal{K}_m(\underline{c})$ of the sequence $\underline{c}$ is the set

$$\mathcal{K}_m(\underline{c}) = \{\underline{c},\, d_{u_n}\ldots d_{u_0}(\underline{c})|u_0,\ldots,\, u_n \in [p],\, n\in\mathbb{N}\}\,.$$

The p-kernel of the formal power series $c(X) \in R[[X]]$ is defined as

$$\mathcal{K}_m(c(X)) = \{c(X),\, \delta_{u_n}\ldots\delta_{u_0}(c(X))|u_0,\ldots, u_n \in [p],\, n\in\mathbb{N}\}\,.$$

The p-automaticity of the sequence $\underline{c}$ means that the p-kernel $\mathcal{K}_m(\underline{c})$ is a finite set, i.e. the p-kernel $\mathcal{K}_m(c(X))$ is a finite set. This is equivalent to the existence of a finite set of sequences $\mathcal{S}$ such that

- the sequence $\underline{c}$ belongs to $\mathcal{S}$,
- the set $\mathcal{S}$ is invariant under the p-decimations d_u, $u \in [p]$.

Clearly, this is equivalent to the existence of a finite set $\mathcal{P}$ of formal power series such that

- the generating function $c(X)$ of the sequence $\underline{c}$ belongs to $\mathcal{P}$,
- the set $\mathcal{P}$ is invariant under the p-decimations δ_u, $u \in [p]$.

Later on we shall use the second formulation.

4.2. *Shift register sequences and their decimation*

Here we shall work with unidirectional integer sequences, i.e. $R = \mathbb{Z}$.

A sequence $\underline{b} = (b(n))_{n\in\mathbb{N}}$ with elements $b(n) \in \mathbb{Z}$, which satisfies

$$b(n+L) + q_1 b(n+L-1) + \cdots + q_{L-1}b(n+1) + b(n) = 0 \qquad (18)$$

for all $n \in \mathbb{N}$ is called a *shift register sequence* (SRS) generated by the *characteristic polynomial*

$$Q_0^*(X) = X^L + q_1 X^{L-1} + \cdots + q_{L-1}X + 1 \qquad (19)$$

(see [Jungnickel, 1993; Lidl & Niederreiter, 1983]). The polynomial

$$Q_0(X) \stackrel{\text{def}}{=} X^L Q_0^*\left(\frac{1}{X}\right) = 1 + q_1 X + q_2 X^2 + \cdots + q_{L-1}X^{L-1} + X^L$$

is called the *reciprocal* characteristic polynomial [Jungnickel, 1993; Lidl & Niederreiter, 1983]. (We shall further use the notation $T(X)$ and $T^*(X)$ for reciprocal pairs of polynomials: If $\deg T(X) = N$, then $T^*(X) = X^N T(1/X)$ and $T(X) = X^N T^*(1/X)$.)

The SRS $\underline{b}$, as given by Eq. (18), is uniquely determined by the initial values $b(0),\ldots, b(L-1)$. The generating function $b(X)$ of the sequence $\underline{b}$ is a rational function $P_0(X)/Q_0(X)$, where $P_0(X)$ is a polynomial with integer coefficients and degree $\deg P_0(X) \le L-1$ (which depends on the initial values), and $Q_0(X)$ is the reciprocal characteristic polynomial defined above [Jungnickel, 1993; Lidl & Niederreiter, 1983]. Moreover, all such rational functions are generating functions of SRS with characteristic polynomial $Q_0^*(X)$, [Jungnickel, 1993, p. 204]. We shall also use the following description of the SRS $\underline{b}$.

Let

$$Q_0^*(X) = \prod_{j=1}^{N}(X-\alpha_j)^{m_j}\,, \qquad (20)$$

where α_j are different (in general complex) numbers. There exist complex numbers $C_{j,k}$, $0 \le k \le m_j - 1$, $1 \le j \le N$ such that

$$b(n) = \sum_{j=1}^{N}\sum_{k=0}^{m_j-1} C_{j,k} n^k \alpha_j^n \qquad (21)$$

for all $n \in \mathbb{N}$.

The numbers $C_{j,k}$ are uniquely determined by the initial values $b(0),\ldots, b(L-1)$ and by $Q_0^*(X)$. For all choices of $C_{j,k}$ such that $b(0),\ldots, b(L-1)$ are integers, the sequence defined by Eq. (21) is a SRS generated by the polynomial $Q_0^*(X)$.

Consider the p-decimation of the rational function $P_0(X)/Q_0(X)$ corresponding to the sequence $\underline{b}$. By definition, see Eq. (17), it is

$$\delta_u\left(\frac{P_0(X)}{Q_0(X)}\right) = \sum_{n=0}^{\infty} b(pn+u)X^n$$

for $0 \le u \le p-1$.

From Eq. (21) we obtain

$$b(pn+u) = \sum_{j=1}^{N} \sum_{k=0}^{m_j-1} C_{j,k}(pn+u)^k \alpha_j^{pn+u}$$

$$= \sum_{j=1}^{N} \sum_{k=0}^{m_j-1} \hat{C}_{j,k} n^k (\alpha_j^p)^n ,$$

where

$$\hat{C}_{j,k} = \alpha_j^u p^k \sum_{s=k}^{m_j-1} C_{j,s} \binom{s}{k} u^{s-k} .$$

Therefore the sequence $d_u(\underline{b}) = (b(pn+u))_{n\in\mathbb{N}}$ is a SRS with characteristic polynomial

$$Q_1^*(X) = \prod_{j=1}^{N} (X - \alpha_j^p)^{m_j} , \tag{22}$$

and has a generating function

$$\delta_u \left(\frac{P_0(X)}{Q_0(X)} \right) = \frac{P_1(X)}{Q_1(X)} , \tag{23}$$

where $P_1(X)$ is a polynomial with integer coefficients and $\deg P_1(X) \leq L-1 = \deg Q_1(X) - 1$, and $Q_1(X)$ is the reciprocal polynomial of $Q_1^*(X)$.

Remark 5. The polynomial $Q_1(X)$ is also a polynomial with integer coefficients. It coincides (up to sign) with the polynomial $\psi_p(Q_0(X))$ that was introduced in [Jürgensen, 1997], p. 29, and which is the determinant of the p-decimation matrix

$$A_p(Q_0(X)) = \begin{vmatrix} \delta_0(Q_0) & X\delta_{p-1}(Q_0) & \cdots & X\delta_1(Q_0) \\ \delta_1(Q_0) & \delta_0(Q_0) & \ddots & \vdots \\ \vdots & \vdots & \ddots & X\delta_{p-1}(Q_0) \\ \delta_{p-1}(Q_0) & \delta_{p-2}(Q_0) & \cdots & \delta_0(Q_0) \end{vmatrix} .$$

In general, for successive decimations, the following property holds.

Lemma 8. *Let $P_0(X)$ and $Q_0^*(X)$ [as defined by Eq. (20) and with reciprocal $Q_0(X)$], be polynomials with integer coefficients and*

$$Q_1^*(X) = \prod_{j=1}^{N} (X - \alpha_j^p)^{m_j} , \quad \alpha_j \neq \alpha_k, j \neq k$$

and $\deg P_0(X) \leq \deg Q_0(X) - 1$. *Let* $\delta_{u_n u_{n-1} \ldots u_0} = \delta_{u_n} \delta_{u_{n-1}} \ldots \delta_{u_0}$, $u_j \in [p]$, $0 \leq j \leq n$ *represent a succession of* $(n+1)$ *decimations.*

Then

$$\delta_{u_n u_{n-1} \ldots u_0} \left(\frac{P_0(X)}{Q_0(X)} \right) = \frac{P_{n+1}(X)}{Q_{n+1}(X)} ,$$

where $P_{n+1}(X)$, $Q_{n+1}(X)$ are polynomials with integer coefficients,

$$\deg P_{n+1}(X) \leq \deg Q_{n+1}(X) - 1 ,$$

and $Q_{n+1}(X)$ is the reciprocal polynomial of

$$Q_{n+1}^*(X) = \prod_{j=1}^{N} (X - \alpha_j^{p^{n+1}})^{m_j} . \tag{24}$$

Remark 6. Since α_j are zeros of the polynomial $Q_0^*(X)$ of degree L, it holds that

$$\alpha_j^k = A_0 + A_1\alpha_j + \cdots + A_{L-1}\alpha_j^{L-1} , \tag{25}$$

where $A_0, \ldots, A_{L-1}$ are integers (depending on k but not on j).

4.3. *Shift register sequences modulo m*

Suppose $\underline{b}$ is a SRS with characteristic polynomial $Q_0^*(X)$ as before. Here we shall consider the sequence $\underline{b}_m = (b(n) \bmod m)_{n\geq 0}$ for $m \in \mathbb{N}$, $m \geq 2$.

The sequences $\underline{b}_m$ are SRS with values in $Z_m = \mathbb{Z}/m\mathbb{Z}$ and characteristic polynomial $Q_0^*(X) \bmod m$. Equations (21)–(23) and Lemma 8 hold for the sequence $\underline{b}_m$ and its generating function. These formulas hold since calculations are made with rational functions with coefficients in the extension ring $Z_m(\alpha_1, \ldots, \alpha_n)$ of the ring Z_m.

Reducing Eq. (25) modulo m we obtain that the sequences $(\alpha_j^k \bmod m)_{k\in\mathbb{N}}$ are ultimately periodic with the same period and preperiod, since the coefficients $A_0, \ldots, A_{L-1}$ modulo m have only finitely many values and do not depend on j. Therefore, it holds for the sequences $(\alpha_j^{p^l} \bmod m)_{l\in\mathbb{N}}$ that there exist natural numbers n_0, l_0, $0 \leq l_0 \leq n_0$ such that

$$\alpha_j^{p^{n_0}} \equiv \alpha_j^{p^{l_0}} \bmod m , \quad j = 1, \ldots, N . \tag{26}$$

Combining this with Lemma 8, this means that the set

$$\left\{ \frac{P_n(X)}{Q_n(X)} \bmod m \,|\, n \in \mathbb{N} \right\}$$

is finite, implying the well-known fact that the p-kernel of the sequence $\underline{b}_m$ is finite, which means that it is p-automatic (this follows also from the ultimate periodicity of this sequence).

4.4. *p-decimation of integer sequences with generating functions satisfying p-Mahler equations*

Let $\underline{c} = (c(n))_{n\in\mathbb{N}}$ be a unidirectional integer sequence and $c(X) = \sum_{k\in\mathbb{N}} c(k)X^k$ its generating function, a formal power series with integer coefficients. We say that $c(X)$ is a solution of a p-Mahler equation if there are integer polynomials $Q_0(X)$, $P_0(X), \ldots, P_k(X)$ such that

$$Q_0(X)c(X) = P_0(X)c(X^{p^k}) + \cdots + P_{k-1}(X)c(X^p) + P_k(X), \tag{27}$$

with $Q_0(0) = 1$.

Let $\deg P_j(X) = d_j$, $d = \max_j\{d_j - L, 0\}$, $L = \deg Q_0(X)$, and

$$Q_n^*(X) = \prod_{j=1}^{N}(X - \alpha_j^{p^n})^{m_j}, \quad n = 0, 1, 2, \ldots,$$

with reciprocals $Q_n(X)$.

Lemma 9. *The decimations of the generating function $c(X)$ which satisfies the p-Mahler equation (27) are given by*

$$\delta_{u_n\ldots u_0}(c(X)) = \frac{\tilde{P}_{0,u_n\ldots u_0}(X)}{Q_{n+1}(X)\ldots Q_1(X)}c(X^{p^{k-1}}) + \cdots + \frac{\tilde{P}_{k-1,u_n\ldots u_0}(X)}{Q_{n+1}(X)\ldots Q_1(X)}c(X) + \frac{\tilde{P}_{k,u_n\ldots u_0}(X)}{Q_{n+1}(X)\ldots Q_1(X)},$$

where $\tilde{P}_{j,u_n\ldots u_0}(X)$ are polynomials with integer coefficients and

$$\deg \tilde{P}_{j,u_n\ldots u_0}(X) \le (n+1)L + \frac{d}{p}\left(1 + \frac{1}{p} + \cdots + \frac{1}{p^n}\right).$$

Proof. Induction w.r.t. the integer n using Lemma 8, the formula

$$\delta_u(G(X)F(X^p)) = \delta_u(G(X))F(X) \tag{28}$$

for $G(X)$, $F(X) \in \mathbb{Z}[[X]]$, and

$$\delta_{u_n\ldots u_0}(c(X)) = \frac{P_{0,u_n\ldots u_0}(X)}{Q_{n+1}(X)\ldots Q_1(X)Q_0}c(X^{p^{k-1}}) + \cdots + \frac{P_{k-1,u_n\ldots u_0}(X)}{Q_{n+1}(X)\ldots Q_1(X)Q_0(X)}c(X^p) + \frac{P_{k,u_n\ldots u_0}(X)}{Q_{n+1}(X)\ldots Q_1(X)Q_0(X)},$$

where $P_{j,u_n\ldots u_0}(X)$ are polynomials with integer coefficients and

$$\deg P_{j,u_n\ldots u_0}(X) \le (n+2)L + \frac{d}{p}\left(1 + \frac{1}{p} + \cdots + \frac{1}{p^{n+1}}\right).$$

This formula for $\delta_{u_n\ldots u_0}(c(X))$ is obtained by replacing $c(X)$ by its expression from the p-Mahler equation (27) and applying Lemma 8. Then decimating the final expression and using Eq. (28) we obtain the assertion for $n+1$.

4.5. *Sequences modulo p^d with generating functions satisfying p-Mahler equations*

Let p be a prime number from here on. We shall prove the following assertion.

Proposition 1. *Let p be a prime number and $d \in \mathbb{N}$, $d \ge 1$. Suppose that the generating function $c(X)$ of the integer sequence $\underline{c} = (c(n))_{n\in\mathbb{N}}$ satisfies the p-Mahler equation*

$$Q_0(X)c(X) = P_0(X)c(X^{p^k}) + \cdots + P_{k-1}(X)c(X^p) + P_k(X),$$

where $Q_0(X)$, $P_0(X), \ldots, P_k(X)$ are integer polynomials and $Q_0(0) = 1$. Then the sequence $\underline{c}_{p^d} = (c(n) \bmod p^d)_{n\in\mathbb{N}}$ is p-automatic.

Proof. We have to prove that the p-kernel of the sequence $\underline{c}_{p^d}$ (or the p-kernel of its generating function $c_{p^d}(X)$) is finite. We shall do so by constructing a finite set of formal power series with coefficients in

Z_{p^d} which contains $c_{p^d}(X)$ and which is invariant w.r.t. the decimations δ_u, $u \in [p]$.

Let $\mathcal{P}$ be the set of all power series defined by

$$A(X) \equiv \sum_{j=0}^{k-1} \frac{A_j(X)}{Q(X)} c(X^{p^{k-j}}) + \frac{A_k(X)}{Q(X)} \bmod p^d , \tag{29}$$

where $A_j(X)$ are polynomials with integer coefficients, $j = 0, \ldots, k$, and

$$\deg A_j(X) \le (a+2)L + d\left(1 + \frac{1}{p} + \cdots + \frac{1}{p^{a+1}}\right) ,$$
$$a = p^d(n_0 - l_0) - 2 ,$$
$$d = \max_j \deg P_j(X) .$$

The natural numbers n_0 and l_0 are defined by Eq. (26), and

$$Q(X) = [Q_{n_0-1}(X) \ldots Q_{l_0}(X)]^{p^d} Q_{l_0-1}(X) \ldots Q_0(X),$$

where the polynomials $Q_j(X)$ are the reciprocals of the polynomials defined in Eq. (24).

The set $\mathcal{P}$ is finite and contains the generating function $c_{p^d}(X) = c(X) \bmod p^d$. We shall show that it is invariant w.r.t. the decimations δ_u, $u \in [p]$.

Let $A(X) \in \mathcal{P}$ as given by Eq. (29). Then

$$\delta_u(A(X)) = \sum_{j=0}^{k-1} \delta_u \left[\frac{A_j(X) c(X^{p^{k-j}})}{R_1(X) R_2(X^p)^{p^{d-1}}} \right] + \delta_u \left[\frac{A_k(X)}{R_1(X) R_2(X^p)^{p^{d-1}}} \right] ,$$

where

$$R_1(X) = Q_{l_0-1}(X) \ldots Q_0(X) ,$$
$$R_2(X) = Q_{n_0-1}(X) \ldots Q_{l_0}(X) .$$

Here we have used the p-Fermat property of polynomials in $Z_{p^d}[X]$ which are p^{d-1} powers (see Lemma 4), i.e.

$$R_2(X)^{p^d} = R_2(X^p)^{p^{d-1}} \bmod p^d .$$

Then using Eq. (28), Lemma 9, and writing all expressions with denominator $[Q_{n_0-1}(X) \cdots Q_{l_0}(X)]^d Q_{l_0-1}(X) \cdots Q_0(X)$, we obtain the assertion. ■

5. *p*-Automaticity of the Orbits of a *p*-State Linear Cellular Automaton with a *p*-Automatic Initial Configuration

Let p be a prime number. The notion of p-automatic sequences $f : \mathbb{N} \to V$ with values in a finite set V was introduced in [Cobham, 1969], see [Allouche, 1990; Allouche & Mendès France, 1994]. The notion of p-automaticity was extended for sequences $f : \mathbb{N}^l \to V$, [Salon, 1986, 1987; Allouche, 1990; Allouche & Mendès France, 1994] and for $f : \mathbb{Z}^k \times \mathbb{N}^l \to V$ or even more general for maps $f : R \to V$, where R is a (D, b)-semi-ring [Allouche *et al.*, 1997]. For convenience we shall review this generalization. A semi-ring is a set with two commutative and associative operations: addition (with a zero) and multiplication (with a unity, and distributive over the addition [Eilenberg, 1985], pp. 122–123). All commutative rings are semi-rings. The simplest example of a semi-ring is the set of natural numbers $\mathbb{N}$ with addition and multiplication, or more generally $\mathbb{Z}^k \times \mathbb{N}^l$ where the operations addition and multiplications are componentwise.

A semi-ring is called a (D, b)-semi-ring if there is "radix representation" of its elements with base b and digits D, i.e. $b \in R$ and D is a finite subset containing the zero of R such that for every $r \in R$, $r \neq 0$ there is a unique representation

$$r = r_s b^s + \cdots + r_1 b + r_0 , \quad r_j \in D , \quad r_s \neq 0 . \tag{30}$$

Examples of (D, b)-semi-rings are given in [Allouche *et al.*, 1997].

For the ring $\mathbb{Z}$ we shall use the digit set $\hat{D}_p = \{-1, 0, \ldots, p-2\}$ and base $b = p$; for $\mathbb{N}$: $D_p = \{0, \ldots, p-1\}$, $b = p$; for $\mathbb{Z} \times \mathbb{N}$: $D = \hat{D}_p \times D_p$ and $b = (p, p)$ ($p > 0$, and p not necessarily prime).

A map $f : R \to V$ of a (D, b)-semi-ring in a finite set V is called (D, b)-automatic, if there is a finite automaton with input D and output V, such that reading the word $r_s \ldots r_1 r_0$ (from right to left), corresponding to the element $r \in R$ as given by (30), the automaton produces the value $f(r)$, [Allouche *et al.*, 1997]. For our case $R = \mathbb{Z} \times \mathbb{N}$ and $D = \hat{D}_p \times D_p$, $b = (p, p)$ the notion of (D, b)-automaticity does not depend on the digit set D (see [Allouche *et al.*, 1997], Theorem 6, p. 299, Lemma 4, p. 320). For this reason we shall call $(D, (p, p))$-automatic sequences (maps) p-automatic. The same remark also holds for sequences $g : \mathbb{Z} \to V$.

Remark 7. Suppose that the sequence $f : \mathbb{Z} \times \mathbb{N} \to V$ satisfies

$$f(m, n) = 0\,, \quad m \leq C(n)$$

for all $m \in \mathbb{Z}$ and $n \in \mathbb{N}$, and for some $C(n)$ depending on n but not on m. Then $\underline{f}$ is p-automatic iff its generating function

$$f(X, Y) = \sum_{n=0}^{\infty} \sum_{m=-\infty}^{\infty} f(m, n) X^m Y^n \qquad (31)$$

is an algebraic element of the field of Laurent series $\mathbb{F}_p((X, Y))$ over the field of rational functions $\mathbb{F}_p(X, Y)$. Here the elements of $\mathbb{F}_p((X, Y))$ are formal Laurent series $\sum_{n\in\mathbb{Z}} \sum_{m\in\mathbb{Z}} b(m, n) X^m Y^n$, such that for every m, n there are $C_1(n)$, $C_2(m)$ with $b(m, n) = 0$ for $m \leq C_1(n)$ or $n \leq C_2(m)$. [Here $\mathbb{F}_p((X, Y))$ is the quotient field of the ring of formal power series, i.e. its elements are formal Laurent series with only finitely many negative powers of X.] The assertion follows from the proof of Theorem 5.1 in ([Salon, 1986, 1987], p. 4, p. 06).

Proposition 2. *Let $\underline{a} : \mathbb{Z} \to \mathbb{F}_p$ be a p-automatic sequence with generating function $a(X)$ and $l(X)$ be a Laurent polynomial with coefficients in $\mathbb{F}_p$. The double sequence $(a(m, n))_{m,\in\mathbb{Z},n\in\mathbb{N}}$ with generating function*

$$\frac{a(X)}{1 - Yl(X)} = \sum_{n=0}^{\infty} a(X) l(X)^n Y^n$$

is p-automatic.

Proof. The sequence $\underline{a} : \mathbb{Z} \to \mathbb{F}_p$ is p-automatic iff the sequences $\underline{a}_+, \underline{a}_- : \mathbb{N} \to V$ defined by

$$\underline{a}_+ = (a_+(n))_{n\in\mathbb{N}}\,, \quad a_+(n) = a(n)\,, \quad n \geq 0\,,$$
$$\underline{a}_- = (a_-(n))_{n\in\mathbb{N}}\,, \quad a_-(n) = a(-n)\,,$$
$$n \geq 1\,, \quad \text{and} \quad \underline{a}_-(0) = 0$$

are p-automatic (see [Allouche *et al.*, 1997], Theorem 15).

Then by the theorem of Christol *et al.* [1980], the generating functions $a_-(X)$, $a_+(X)$ of the sequences $\underline{a}_-, \underline{a}_+$ are algebraic elements of $\mathbb{F}_p((X))$ over $\mathbb{F}_p(X)$. Here $\mathbb{F}_p((X))$ is the field of formal Laurent series with coefficients in $\mathbb{F}_p$ which are finite to the left. Therefore the formal power series $a_-(X)$, $a_+(X)$ are algebraic elements of $\mathbb{F}_p((X, Y))$ over $\mathbb{F}_p(X, Y)$.

Then

$$\frac{a_+(X)}{1 - Yl(X)} \quad \text{and} \quad \frac{a_-(X)}{1 - Yl(X^{-1})}$$

are also algebraic elements of $\mathbb{F}_p((X, Y))$ over $\mathbb{F}_p(X, Y)$ as a quotient of algebraic elements, since $1 - Yl(X)$, $1 - Yl(X^{-1})$ are rational functions; see ([van der Waerden, 1991], Corollary p. 120). From the Salon Theorem (see Remark 7), it follows that the double sequences $\underline{A}_- = (A_-(m, n))_{m\in\mathbb{Z},n\in\mathbb{N}}$ and $\underline{A}_+ = (A_+(m, n))_{m\in\mathbb{Z},n\in\mathbb{N}}$, defined by

$$\frac{a_+(X)}{1 - Yl(X)} = \sum_{n=0}^{\infty} \sum_{-\infty}^{\infty} A_+(m, n) X^m Y^n\,,$$

$$\frac{a_-(X)}{1 - Yl(X^{-1})} = \sum_{n=0}^{\infty} \sum_{-\infty}^{\infty} A_-(m, n) X^m Y^n\,,$$

are p-automatic sequences as sequences $\underline{A}_-, \underline{A}_+ : \mathbb{Z} \times \mathbb{N} \to \mathbb{F}_p$.

Then the sequence $\hat{\underline{A}}_- = (A_-(-m, n))_{m\in\mathbb{Z},n\in\mathbb{N}}$ is also automatic, [Salon, 1986, 1987]. This implies that the sequence $\underline{B} : \mathbb{Z} \times \mathbb{N} \to \mathbb{F}_p$, which is the sum modulo p of the sequences $\underline{A}_+$ and $\hat{\underline{A}}_-$, is a p-automatic sequence. This gives the assertion of the proposition since the generating function of the sequence $\underline{B}$ is $a(X)/(1 - Yl(X))$. ■

6. Coarse-Graining Orbits of Z_{p^n}-LCA: Extensions and Examples

In analogy with [Barbé, 1996], we will now consider some generalizations of the z-CGI problem by introducing more general tile-shapes and/or a nonuniform weighting of the states of tile-cells, and/or by allowing the coarse-grained orbit to be a shifted version of the original orbit. This leads in the present context to z-CGI-equations which are extensions of the ones given in Eq. (5), (where $z = m^s$):

$$\forall k \in \mathbb{Z},\ \sigma \in [z]:$$
$$\underline{a}(k + \alpha_\sigma) = \sum_{i,j\in[z]} w(i, j) \underline{a}(zk + \beta_j + \gamma_{i,j} z + i + \sigma, j)\,,$$

where $\underline{a}(c, r)$ denotes the state of the orbit-cell at column (address) c and row (time) r; $w(i, j)$ are the weights; β_j and $\gamma_{i,j}$ are integers defining the shape of the coarse-graining tile; α_σ are integers defining

the shifts (see [Barbé, 1996]). Following the last mentioned reference, the associated CGI-problem will be denoted as the $[\mathcal{T}_{z,\Xi}, W, \alpha, r(X)]$-CGI problem, where $\mathcal{T}_{z,\Xi}$ refers to the coarse-graining tile whose size and shape are determined by z and Ξ, where Ξ is the matrix with elements $\xi_{i,j} = \gamma_{i,j} + \beta_j$; W is the matrix with elements $w(i, j)$; α is the shift-vector $(\alpha_0, \alpha_1, \ldots, \alpha_{z-1})$; and $r(X)$ is the polynomial form of the cellular automaton rule (CA-rule). Writing the $\underline{a}(c, r)$ as function of the $\underline{a}(j)$ of the initial configuration (using the LCA's local rule and recalling that all arithmetic is done in the ring R) leads to CGI-equations which are similar to Eq. (9):

$$\underline{a}(k + \alpha_\sigma) = \sum_{i=i_{\min}}^{i_{\max}} w_i \underline{a}(zk + i + \sigma), \qquad (32)$$

where $i_{\min}$, $i_{\max}$, w_i depend on the α_σ, β_j, $\gamma_{i,j}$, $w(i, j)$ and on the particular CA-rule. These CGI-equations over R can be solved recursively, by invoking the techniques introduced in [Barbé, 1996], under the condition that $w_{i_{\min}}$ and $w_{i_{\max}}$ are invertible elements of R. When this condition is satisfied, we qualify the CGI-problem and CGI-equations as *regular*.

The recursion starts from some *seed* $S = \{\underline{a}(j) | j = \kappa+1, \kappa+2, \ldots, \lambda-2, \lambda-1\}$, $(\lambda-\kappa \geq 2)$, using the so-called standard right-propagating form for generating $\underline{a}(\lambda)$, $\underline{a}(\lambda+1)$, $\underline{a}(\lambda+2), \ldots$ and the standard left-propagating form for generating $\underline{a}(\kappa)$, $\underline{a}(\kappa-1)$, $\underline{a}(\kappa-2), \ldots$.

This standard right-propagating CGI-equation corresponding to Eq. (32) is

$$\underline{a}(k) = w_{i_{\max}}^{-1} \left[\underline{a}\left(\frac{k - i_{\max} - \sigma}{z} + \alpha_\sigma \right) - \sum_{i=1}^{i_{\max}-i_{\min}} w_{i_{\max}-i} \underline{a}(k-i) \right], \quad [k \in \mathbb{Z},\ \sigma = (k - i_{\max}) \bmod z]. \qquad (33)$$

The standard left-propagating equation is

$$\underline{a}(k) = w_{i_{\min}}^{-1} \left[\underline{a}\left(\frac{k - i_{\min} - \sigma}{z} + \alpha_\sigma \right) - \sum_{i=1}^{i_{\max}-i_{\min}} w_{i_{\min}+i} \underline{a}(k+i) \right], \quad [k \in \mathbb{Z},\ \sigma = (k - i_{\min}) \bmod z]. \qquad (34)$$

We remind the fact that a seed S itself depends on

- the *core(-interval)* $[\kappa+1, \kappa+2, \ldots, \lambda-2, \lambda-1]$, with minimal length, in which κ and λ are determined by the extremal values of the *addresses* that appear on the right-hand side of the above mentioned standard left- and right-propagating CGI-equations. These extremal values are to be found among $([(k-i_{\max}-\sigma)/z]+\alpha_\sigma)$, $([(k-i_{\min}-\sigma)/z]+\alpha_\sigma)$, $(k - i_{\max} + i_{\min})$, $(k + i_{\max} - i_{\min})$. Cores are not necessarily unique, but a specific one should be selected, thereby fixing the position of the elements (cells) in the seed.
- the solution of the *seed-internal* equations, i.e. all equations of the type Eq. (32), whose elements all belong to the seed. This determines which seed-cells can be freely chosen (these being the so-called *freecells*) and which are dependent on the freecells (the so-called *depcells*, see [Barbé, 1996]). When there are no seed-internal equations, all seed-cells are freecells that can be given arbitrary values in R in an independent way. With N_f the number of freecells, the number of different seeds and of different CGI-orbits is $|R|^{N_f}$.

In what follows, we will exclusively concentrate on Z_{p^n}-LCA generated by $\bmod p^n$ reductions of the polynomial

$$l(X) = r(X)^{p^{d-1}}, \qquad (35)$$

where $r(X)$ is an integer Laurent-polynomial, and $p \geq 2$ is a prime number, d is a natural number ≥ 2. According to Lemma 4, $l_{p^n}(X) \stackrel{\text{def}}{=} l(X) \bmod p^n$ is p-Fermat for all integers n, $1 \leq n \leq d$, and so it is possible to consider the p^s-CGI-orbits of linear cellular automata over Z_{p^n} generated by $l_{p^n}(X)$ for these n (the tile-shape parameters Ξ and the shifts α_σ remaining the same as such, while the weights in W also remain the same, but get reduced $\bmod p^n$). We say that we are considering $[\mathcal{T}_{p^s,\Xi}, W, \alpha, l(X)]_{\bmod p^n}$-CGI problems (or the $\bmod p^n$-versions of the $[\mathcal{T}_{p^s,\Xi}, W, \alpha, l(X)]$-CGI problem). Due to the linearity of the cellular automata considered, and because of the (natural) homomorphism $H_{m,n} : Z_{p^m} \to Z_{p^n}$ $(m > n)$ such that $a \mapsto H_{m,n}(a) = a \bmod p^n$, this homomorphism also exists between the CGI-equations, the resulting CGI-initial configuration solutions and the associated CGI-orbits when reducing the $\bmod p^m$-version of a CGI-problem to the $\bmod p^n$-version $(1 \leq n < m \leq d)$. This means that a CGI-orbit in Z_{p^m} generated by the CA-rule $l_{p^m}(X)$, when reduced $\bmod p^n$, $(1 \leq n < m \leq d)$, is a CGI-orbit generated by $l_{p^n}(X)$ in Z_{p^n}. We say that

$[\mathcal{T}_{p^s,\Xi}, W, \alpha, l(X)]_{\mathrm{mod}\, p^n}$-CGI problems (equations, solutions, orbits...) form a *homomorphic chain* (for decreasing n, $n \leq d$).

Lemma 10. *Let $l(X)$ be of type Eq. (35), then the homomorphic chain of regular $[\mathcal{T}_{p^s,\Xi}, W, \alpha, l(X)]_{\mathrm{mod}\, p^n}$-CGI equations have the same core(s).*

Proof. This is a consequence of the fact that the extremal values of the addresses in the left- and right-propagating equations, (33) and (34), remain the same under reduction $\mathrm{mod}\, p^n$, because the $\underline{a}$-elements with these extremal addresses are associated with the invertible (and therefore nonzero) coefficients $w_{i_{\max}}^{-1}$, $w_{i_{\max}}^{-1} w_{i_{\min}}$, $w_{i_{\min}}^{-1}$, $w_{i_{\min}}^{-1} w_{i_{\max}}$ (elements which are invertible in Z_{p^d}, are also invertible and nonzero when reduced $\mathrm{mod}\, p^n$, $n < d$). ■

Because the selection of a particular core determines the seed-internal CGI-equations, and because CGI-equations form a homomorphic chain, we obtain:

Corollary 3. *For each particular selection of the core, the seed-internal equations associated with the homomorphic chain of CGI-equations also form a homomorphic chain, while the number of seed-internal equations remains constant (w.r.t. n). Also, the set of possible seed-configurations associated with the p^n-version of a CGI-problem forms a homomorphic chain.*

Proposition 3. *Let $l(X)$ be of type Eq. (35). If a regular $[\mathcal{T}_{p^s,\Xi}, W, \alpha, l(X)]_{\mathrm{mod}\, p^m}$-CGI problem ($m \leq d$) has a seed with only freecells, N_f being their number, it has $(p^m)^{N_f}$ different seed-configurations, and as many solutions. Then any $[\mathcal{T}_{p^s,\Xi}, W, \alpha, l(X)]_{\mathrm{mod}\, p^n}$-CGI problem for $1 \leq n \leq d$ has the same seed. This seed consists only of freecells, which may all take values in Z_{p^n} independently, and so it has $(p^n)^{N_f}$ solutions.*

Proof. Consider the $[\mathcal{T}_{p^s,\Xi}, W, \alpha, l(X)]_{\mathrm{mod}\, p^m}$-CGI equations, and suppose they produce a seed with only freecells. Corollary 3 says that the $[\mathcal{T}_{p^s,\Xi}, W, \alpha, l(X)]_{\mathrm{mod}\, p^n}$-CGI equations have the same set of seed-internal equations (but $\mathrm{mod}\, p^n$) for all $1 \leq n \leq d$.

That the $\mathrm{mod}\, p^m$-version of the CGI-equations has only freecells means that either

(a) there are no seed-internal equations among any of these $\mathrm{mod}\, p^m$-related CGI equations, or

(b) all seed-internal equations ($\mathrm{mod}\, p^m$) are identities.

We first show, by contradiction, that (b) is not possible. Suppose that (b) holds, then this means that all coefficients for the different $\underline{a}(j)$ that appear in the $\mathrm{mod}\, p^m$-related seed-internal equations must be 0. As these coefficients can be obtained by reduction $\mathrm{mod}\, p^m$ of the corresponding $\mathrm{mod}\, p^d$-related seed-internal equations, this implies that all coefficients in these $\mathrm{mod}\, p^d$ seed-internal equations should be noninvertible (because invertible elements in Z_{p^d} cannot become 0 under reduction $\mathrm{mod}\, p^m$). But the assumed regularity of the CGI-problem implies that there are invertible coefficients, and so there is a contradicition.

This leaves (a) as the only possibility, and because the seed-internal equations remain the same for all $\mathrm{mod}\, p^n$-versions of the CGI-problem ($1 \leq n \leq d$), there are no seed-internal equations for any of these $\mathrm{mod}\, p^n$-versions, implying that all seed-cells are freecells for all these n. As the number of seed-cells is invariant over these n (Corollary 3), the proposition follows. ■

Corollary 4. *Let $r(X) = \sum_{i=-c_1}^{c_2} r_i X^i$ be an integer Laurent polynomial with $c_1 c_2 > 0$, and $l(X) = r(X)^{p^{d-1}}$. Then the $[\mathcal{T}_{p^s,\Xi\equiv 0}, W \equiv 1, \alpha \equiv 0, l(X)]_{\mathrm{mod}\, p^n}$-CGI problem, $n \leq d$, has $(p^n)^{N_f}$ solutions, with*

$$N_f = (p^s - 1)[(c_1 + c_2)p^{d-1} + 1]\,.$$

Proof. The condition on $r(X)$, and $\Xi \equiv 0$ (implying a square coarse-graining tile), and $\alpha \equiv 0$ are sufficient for Lemma 3 to hold (with $m = p$, and $d_i = c_i p^{d-1}$, $i = 1, 2$). This implies that the seed associated with this CGI-problem has only freecells, so that Proposition 3 applies. ■

When a $[\mathcal{T}_{p^s,\Xi}, W, \alpha, l(X)]_{\mathrm{mod}\, p^d}$-CGI problem leads to seed-internal equations (implying the existence of dependent seed-cells), the relationship between its number of solutions and the number of solutions of the corresponding p^n-reduced CGI problem ($n < d$) is generally more complex. This will be illustrated in the forthcoming Example 3.

Proposition 4. *Consider the $[\mathcal{T}_{p^s,\Xi}, W, \alpha, l(X)]_{\mathrm{mod}\, p^n}$-CGI problems for $l(X)$ satisfying Eq. (35), with $n \leq d$, and define*

$$\mathcal{M}_{p^n} = \{0, p^{n-1}, 2p^{n-1}, \ldots, (p-1)p^{n-1}\} \in Z_{p^n}\,.$$

Then

(a) *For the Z_{p^n}-version of the problem: If all seed-cells have their values restricted to $\mathcal{M}_{p^n}$, then the whole CGI-orbit has its values restricted to $\mathcal{M}_{p^n}$.*

(b) *Define the mapping $\mathcal{H}_{m,n} : \mathcal{M}_{p^m} \to \mathcal{M}_{p^n}$, such that $kp^{m-1} \mapsto kp^{n-1}$. Let $\mathcal{O}_{\mathcal{M}_{p^m}}$ be a CGI-orbit of the Z_{p^m}-version of the problem ($m \leq d$) with all its values in $\mathcal{M}_{p^m}$. Then the elementwise application of $\mathcal{H}_{m,n}$ ($m, n \leq d$) to $\mathcal{O}_{\mathcal{M}_{p^m}}$ produces $\mathcal{O}_{\mathcal{M}_{p^n}} = \mathcal{H}_{m,n}(\mathcal{O}_{\mathcal{M}_{p^m}})$, which is a CGI-orbit of the Z_{p^n}-version of the CGI-problem.*

Proof

(a) Observe that when $u \in Z_{p^n}$ and $v \in \mathcal{M}_{p^n}$, then $uv \in \mathcal{M}_{p^n}$ when multiplication is considered in Z_{p^n} (i.e. $\bmod p^n$). Also observe that $\mathcal{M}_{p^n}$ is closed under addition $\bmod p^n$. This means that any linear combination $\sum_i u(i)v(i)$ $(\bmod p^n)$ with $u(i) \in Z_{p^n}$, $v(i) \in \mathcal{M}_{p^n}$ has its value in $\mathcal{M}_{p^n}$. As any element of the CGI-orbit can ultimately be written as such a linear combination of the seed-cells, the proposition follows when the seed-cells have their values in $\mathcal{M}_{p^n}$.

(b) This is a consequence of the following observations

1. When $u \in Z_{p^d}$ and $v \in \mathcal{M}_{p^d}$, then for $n \leq d$:

$$[u\mathcal{H}_{d,n}(v)] \bmod p^n = \mathcal{H}_{d,n}(uv) \tag{36}$$

and

$$\left[\sum_i u(i)\mathcal{H}_{d,n}(v(i))\right] \bmod p^n$$

$$= \mathcal{H}_{d,n}\left[\sum_i u(i)v(i)\right]. \tag{37}$$

2. Let $\underline{a}_d(j, k)$, with $j \in \mathbb{Z}$, $k \in \mathbb{N}$ be the (j, k)th element of an orbit $\mathcal{O}_{\mathcal{M}_{p^d}}$ in the Z_{p^d}-version, then

$$\underline{a}_d(j, k) = \left[\sum_{i \in C} u_{j,k}(i)\underline{a}_d(i)\right] \bmod p^n, \tag{38}$$

with $u_{j,k}(i) \in Z_{p^d}$ and $\underline{a}_d(i) \in \mathcal{M}_{p^d}$, and implying according to (a) that $\underline{a}_d(j, k) \in \mathcal{M}_{p^d}$. C is a core for the CGI-equations. As the corresponding orbit $\mathcal{O}_{\mathcal{M}_{p^n}}$ in the Z_{p^n}-version ($n < d$), i.e. the orbit generated by the seed $\{\underline{a}_n(i) = \mathcal{H}_{d,n}(\underline{a}_d(i)) | i \in C\}$ satisfies the same CGI-equations (but reduced $\bmod p^n$), the element $\underline{a}_n(j, k)$ of this orbit is given by

$$\begin{aligned}\underline{a}_n(j, k) &= \left[\sum u_{j,k}(i)\underline{a}_n(i)\right] \bmod p^n \\ &= \left[\sum u_{j,k}(i)\mathcal{H}_{d,n}(\underline{a}_d(i))\right] \bmod p^n \\ &\overset{(37),(38)}{=} \mathcal{H}_{d,n}[\underline{a}_d(j, k)]. \end{aligned} \tag{39}$$

This proves the proposition for $m = d$. For arbitrary $m < n < d$, observe that $\mathcal{H}_{n,m}[\underline{a}_n(j,k)] = \mathcal{H}_{n,m}\mathcal{H}_{d,n}[\underline{a}_d(j, k)] = \mathcal{H}_{d,m}[\underline{a}_d(j, k)] \overset{(38)}{=} \underline{a}_m(j, k)$. ■

Remark 8. This Proposition 4 means that *all* solutions of the Z_p-version of a CGI-problem also appear as solutions of all Z_{p^n}-versions ($n \leq d$) through the mapping $\mathcal{H}_{1,n} : k(\in Z_p) \mapsto kp^{n-1}(\in Z_{p^n})$. (The generalization of this fact in the sense that *all* solutions of the Z_{p^m}-versions ($m < n \leq d$) appear as solutions of the Z_{p^n}-versions under the mapping $\mathcal{H}_{m,n}$ is not true: It only holds when Z_{p^m} is an orbit with values in $\mathcal{M}_{p^m}$.)

Example 1. Let $p = 2$, $d = 2$, $r(X) = (X^{-1} + 1 + X)$, and $l(X) = r(X)^2$, then according to Lemma 4, $l_4(X) = l(X) \bmod 4 = X^{-2} + 2X^{-1} + 3 + 2X + X^2$ $(\bmod 4)$ is 2-Fermat. We consider the $[\mathcal{T}_{2^1,\Xi\equiv 0}, W \equiv 1, \alpha \equiv 0, l(X)]_{\bmod 4}$-CGI problem (regular 2×2 square tiling, with uniform weights equal to 1).

The CGI-equations are: For all $k \in \mathbb{Z}$, $\sigma = 0, 1$:

$$\begin{aligned}\underline{a}(k) = &\underline{a}(2k - 2 + \sigma) + 3\underline{a}(2k - 1 + \sigma) \\ &+ 2\underline{a}(2k + \sigma) + 2\underline{a}(2k + 1 + \sigma) \\ &+ 3\underline{a}(2k + 2 + \sigma) + \underline{a}(2k + 3 + \sigma). \end{aligned} \tag{40}$$

Using the procedure for solving these CGI-equations introduced in [Barbé, 1996] and recapitulated above, it is found that these equations can be solved recursively, using the right-propagating

equations

$$\begin{aligned} &k \text{ even}: \\ &\underline{a}(k) = \underline{a}(k-1) + 2\underline{a}(k-2) \\ &\qquad + 2\underline{a}(k-3) + \underline{a}(k-4) \\ &\qquad + 3\underline{a}(k-5) + \underline{a}\left(\frac{k-4}{2}\right) \\ &k \text{ odd}: \\ &\underline{a}(k) = \underline{a}(k-1) + 2\underline{a}(k-2) \\ &\qquad + 2\underline{a}(k-3) + \underline{a}(k-4) \\ &\qquad + 3\underline{a}(k-5) + \underline{a}\left(\frac{k-3}{2}\right), \end{aligned} \tag{41}$$

and the left-propagating equations

$$\begin{aligned} &k \text{ even}: \\ &\underline{a}(k) = \underline{a}(k+1) + 2\underline{a}(k+2) \\ &\qquad + 2\underline{a}(k+3) + \underline{a}(k+4) \\ &\qquad + 3\underline{a}(k+5) + \underline{a}\left(\frac{k+2}{2}\right) \\ &k \text{ odd}: \\ &\underline{a}(k) = \underline{a}(k+1) + 2\underline{a}(k+2) \\ &\qquad + 2\underline{a}(k+3) + \underline{a}(k+4) \\ &\qquad + 3\underline{a}(k+5) + \underline{a}\left(\frac{k+1}{2}\right). \end{aligned} \tag{42}$$

Possible seeds for starting the recursions are given by the sets $S_\mu = \{\underline{a}(\mu), \underline{a}(\mu+1), \ldots, \underline{a}(\mu+4)\}$, with $\mu = -7, -6, \ldots, -1$. Taking $\mu = 2$ produces the seed $S = \{\underline{a}(-2), \underline{a}(-1), \underline{a}(0), \underline{a}(1), \underline{a}(2)\}$, which corresponds to the one appearing in Lemma 3. All seed-cells are freecells, each of which can be attributed a value from Z_4 in an independent way, and so there are $4^5 = 1024$ possible seed configurations, and as many solutions to the CGI-equation and CGI-orbits. Apart from the trivial solution, there seems to be one visually self-similar solution, while all other solutions are quasiperiodic (see [Barbé *et al.*, 1995; Barbé, 1996]).

Figure 1 shows a few solutions to this Z_4-problem (of course only a finite part is displayed), and so do the colored parts of the patterns in Fig. 2. Figures 2(a)–2(g) are solutions with values in $\mathcal{M}_4 = \{0, 2\}$, and so the complete orbit is restricted to these values [see Proposition 4(a)]. Figure 2(a) is the unique visually self-similar solution. All other solutions with values in $\mathcal{M}_4$ are similar to one of the solutions displayed in Figs. 2(b)–2(g). The black and white parts in some of the figures are particular *shift-identity correlation patterns* (SIPs, see [Barbé *et al.*, 1995]). Recall that a (h, v)-SIP of a pattern $\underline{a}(c, r)$, $(c, r) \in \mathbb{Z} \times \mathbb{N}$, indicates where this pattern has the same value as its shifted version $\underline{a}(c+h, r+v)$. A white pixel in the SIP corresponds to identical values in both the original pattern and its (h, v)-shifted version; otherwise the pixel is black. SIPs uncover hidden long-range correlations in the solutions. Figures 3–5 show the $(h, v) = (128, 0)$-, $(0, 64)$-, $(127, 0)$-, $(0, 63)$-SIPs of the solutions shown in Figs. 1(a), 1(b) and 2(b). These structures will be related to each other at the end of Example 2.

The generating function $a(X) = \sum_{k\in\mathbb{Z}} \underline{a}(k)X^k$ of the CGI-initial configuration generated by the CGI-equations (40) satisfies the 2-Mahler equation

$$Q(X)a(X) = P(X)a(X^2) \pmod 4$$

with

$$\begin{aligned} Q(X) &= 1 + 3X + 2X^2 + 2X^3 + 3X^4 + X^5, \\ P(X) &= X^3(1+X). \end{aligned}$$

(See Lemma 6.)

For $n \geq n_0 = -3$ (cf. Lemma 7), the generating function of $a_n^+(X) = \sum_{k\in\mathbb{N}} \underline{a}(k+n)X^k$ satisfies the 2-Mahler equation

$$\begin{aligned} Q_n^+(X)a_n^+(X) = P_n^+(X)\underline{a}_n^+(X^2) \\ + R_n^+(X) \pmod 4, \end{aligned} \tag{43}$$

with

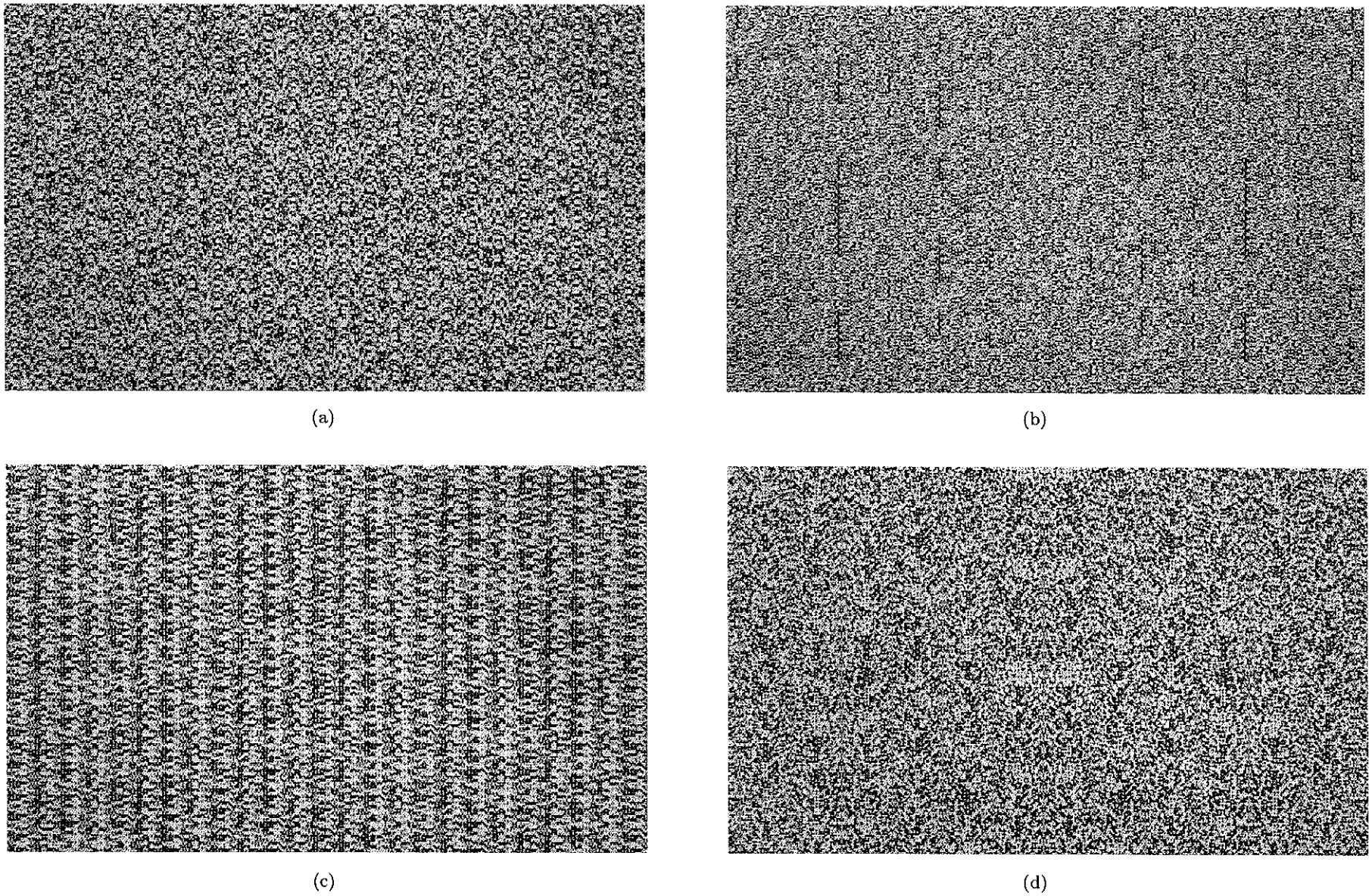
$$\begin{aligned} Q_n^+(X) &= Q(X) \\ &= 1 + 3X + 2X^2 + 2X^3 + 3X^4 + X^5, \\ P_n^+(X) &= X^{n+3}(1+X), \end{aligned}$$

and

$$R_n^+(X) = T_n^+(X) - \sum_{j=0}^{4} \left[\sum_{i=1}^{5-j} w_{3-j-i}\underline{a}(n-i)\right] X^j,$$

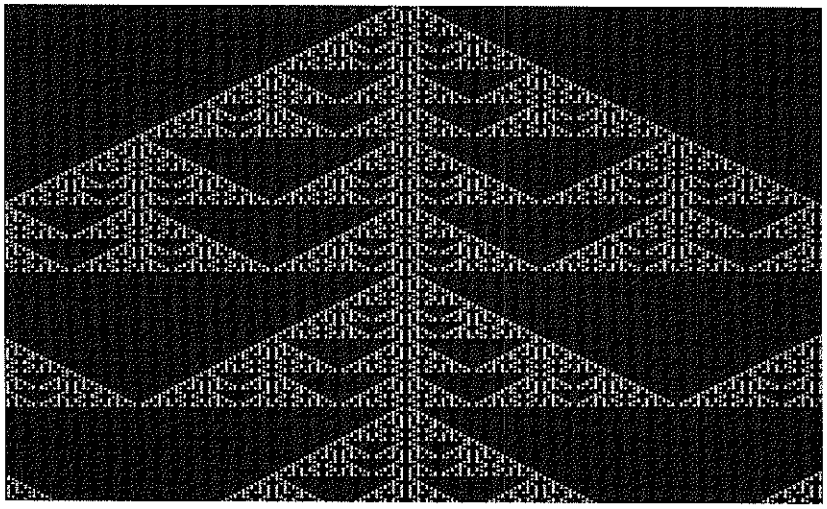
with $w_{-2} = 1$, $w_0 = w_1 = 2$, $w_{-1} = w_2 = 3$, and

$$\begin{aligned} T_n^+(X) &= X^{n+2}(1+X)\sum_{j=1}^{\frac{n+2}{2}} \underline{a}(n-j)X^{-2j+2} \\ &\quad + \underline{a}\left(\frac{n}{2} - 2\right) \quad \text{when } n \text{ is even}, \\ &= X^{n+1}(1+X)\sum_{j=1}^{\frac{n+3}{2}} \underline{a}(n-j)X^{-2j+2} \\ &\quad \text{when } n \text{ is odd}. \end{aligned}$$

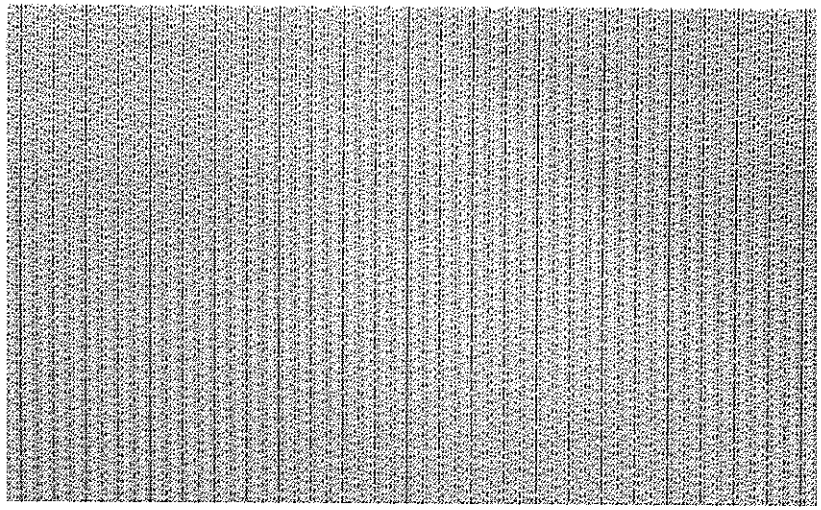


(a) (b) (c) (d)

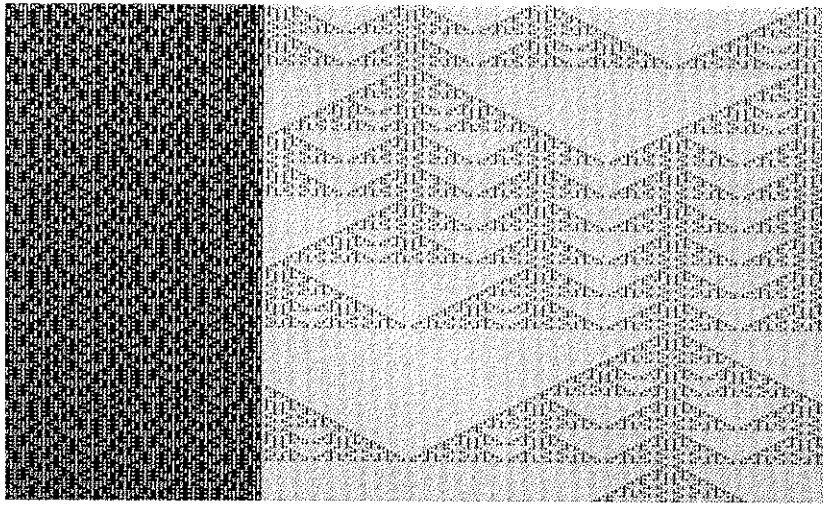
Fig. 1. A few of the 1024 possible solutions of the Z_4-CGI problem in Example 1. (a) seed $[a(-2), \ldots, a(2)] = [30323]$; (b) seed [12303]; (c) seed [21232]; (d) seed [01013]. (Color code: dark blue = 0, light blue = 1, yellow = 2, red = 3. Display size of the $a(c, r)$-pattern: $-200 \leq c \leq 200$, $0 \leq r \leq 244$.)



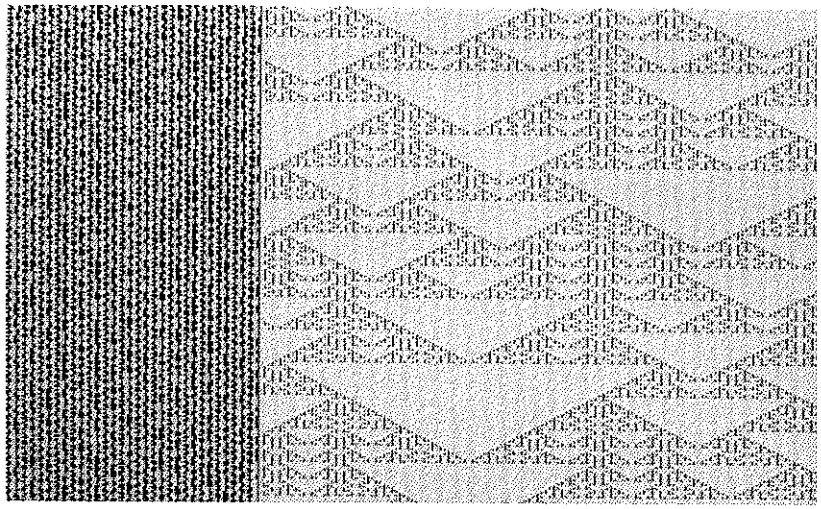
(a)



(b)

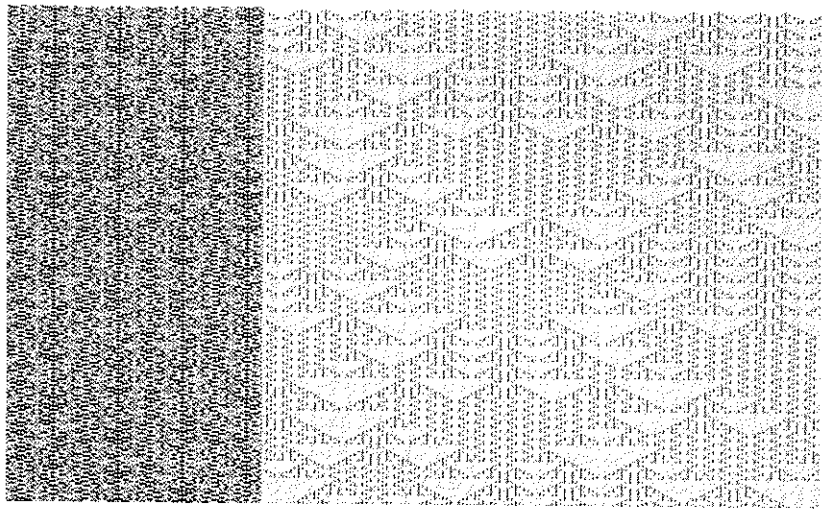


(c)

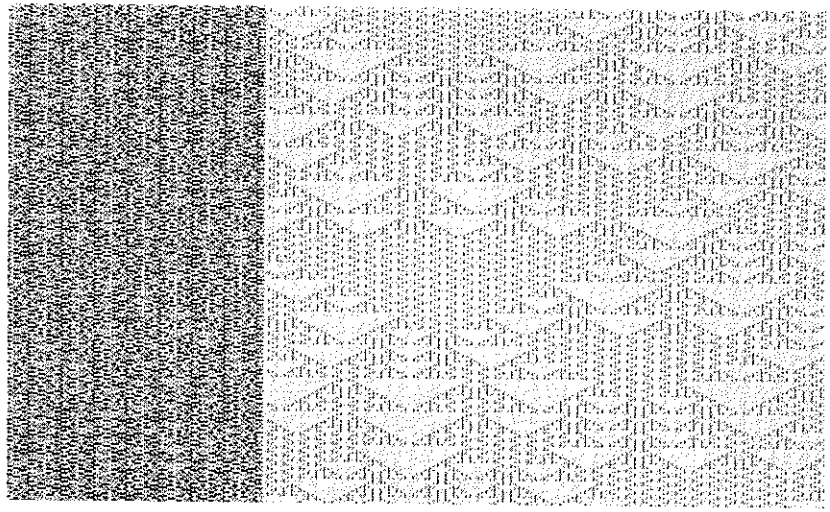


(d)

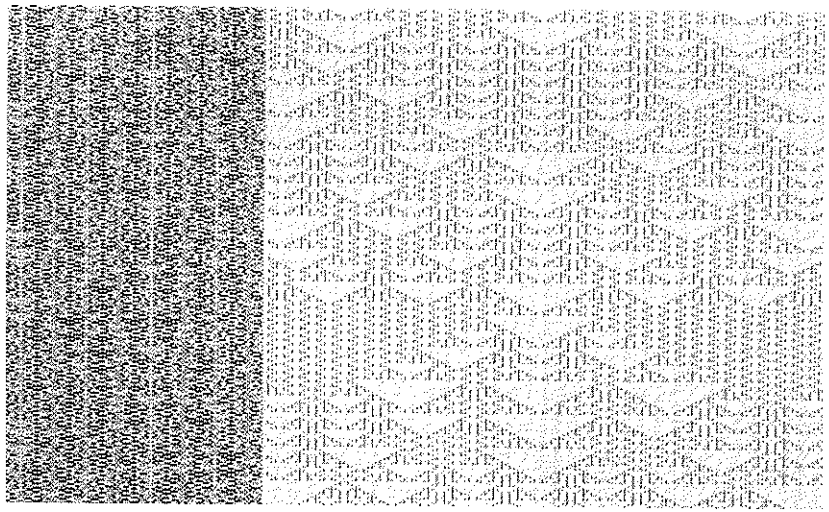
Fig. 2. (a)–(g): The colored parts are typical solutions of the Z_4-CGI problem in Example 1, with values in $\mathcal{M}_4 = \{0, 2\}(= \{\text{blue, yellow}\})$. (a) seed [00020]; (b) seed [20202]; (c) seed [02000]; (d) seed [02220]; (e) seed [00022]; (f) seed [00222]; (g) seed [02002]. The black and white parts are the SIPs (shift-identity patterns) for the horizontal shift $h = 128$. The solution patterns (colored parts) are also solutions for the Z_2-version of the same CGI-problem (Example 2), but the yellow pixels then correspond to the value 1. Figure 2(b) [interpreted in Z_2] is the mod 2-reduction of both Figs. 1(a) and 1(b). (h) is a Z_4-solution of Example 1 (seed [00010] in Z_4) whose reduction mod 2 produces pattern 2(a) [interpreted in Z_2].



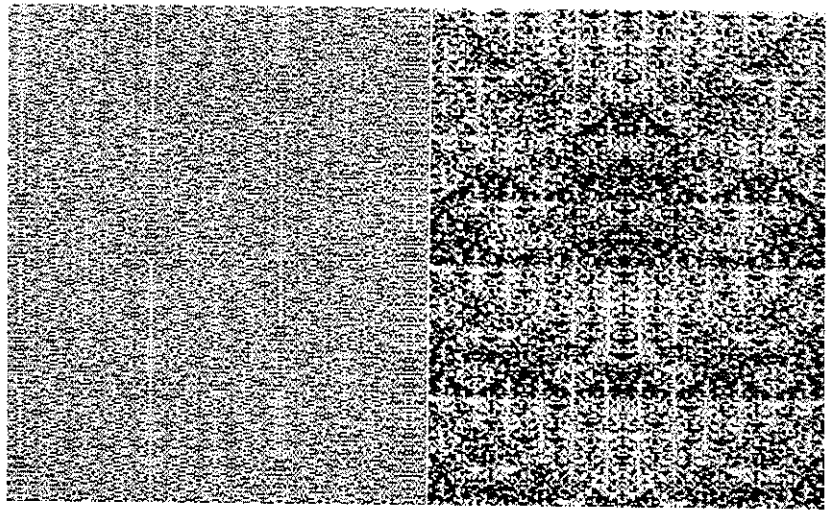
(e)



(f)



(g)



(h)

Fig. 2. (*Continued*)

The simplest form of Eq. (43) exists for $n = n_0 = -3$, for which it becomes

$$(1+3X+2X^2+2X^3+3X^4+X^5)\underline{a}^+_{-3}(X) = (1+X)\underline{a}^+_{-3}(X^2) - \sum_{j=0}^{4}\left[\sum_{i=1}^{5-j} w_{3-j-i}\underline{a}(-3-i)\right]X^j .$$

Since the generating function of $a^+_n(X)$ satisfies a 2-Mahler equation, it follows that the sequence $(\underline{a}^+_n(k))_{k\in\mathbb{N}}$ is 2-automatic.

Example 2. Let us now consider the mod 2-version of the problem from Example 1. The LCA-polynomial belongs now to $Z_2[X]$ and is $l_2(X) = (X^{-1}+1+X)^2 (\mathrm{mod}\,2) = X^{-2}+1+X^2 (\mathrm{mod}\,2)$. Straightforward application of the solution procedure for the CGI-problem produces the CGI-equations (in Z_2): for all $k \in \mathbb{Z}$ and $\sigma = 0, 1$:

$$\underline{a}(k) = \underline{a}(2k-2+\sigma) + \underline{a}(2k-1+\sigma) + \underline{a}(2k+2+\sigma) + \underline{a}(2k+3+\sigma) . \quad (44)$$

The right-propagating CGI-equations are

$$\begin{aligned} k \text{ even} &: \underline{a}(k) = \underline{a}(k-1) + \underline{a}(k-4) + \underline{a}(k-5) + \underline{a}\left(\frac{k-4}{2}\right) \\ k \text{ odd} &: \underline{a}(k) = \underline{a}(k-1) + \underline{a}(k-4) + \underline{a}(k-5) + \underline{a}\left(\frac{k-3}{2}\right) , \end{aligned} \quad (45)$$

and the left-propagating equations

$$\begin{aligned} k \text{ even} &: \underline{a}(k) = \underline{a}(k+1) + \underline{a}(k+4) + \underline{a}(k+5) + \underline{a}\left(\frac{k+2}{2}\right) \\ k \text{ odd} &: \underline{a}(k) = \underline{a}(k+1) + \underline{a}(k+4) + \underline{a}(k+5) + \underline{a}\left(\frac{k+1}{2}\right) . \end{aligned} \quad (46)$$

Observe that these equations are the mod 2-reductions of the corresponding equations of Example 1, and that the extremal addresses $(k+1)$, $(k+5)$, $(k-1)$, $(k-5)$, $(k-4)/2$, $(k-3)/2$, $(k+2)/2$, $(k+1)/2$ that determine the location and size of the seed, also remain the same as in Example 1 (recall that this fact was used in proving Lemma 10, which in its turn led to Corollary 3 and Proposition 3). As a consequence, the possible seeds are located at the same core-positions as in Example 1. We select again the seed $\{\underline{a}(-2), \underline{a}(-1), \underline{a}(0), \underline{a}(1), \underline{a}(2)\}$. The possible seed-configurations are the same as those in Example 1, but now reduced to mod 2. As also here all five seed-cells are freecells, there are $2^5 = 32$ solutions (compare to the $4^5 = 1024$ solutions in the Z_4-case of Example 1). It means that under the $H_{2,4}$-homomorphism that maps the Z_4-CGI problem into the Z_2-CGI problem, there are 32 solutions in the Z_4-case that map into each Z_2 solution.

Typical solutions for this Z_2-version of the Z_4-CGI problem that was introduced in Example 1 are displayed in Figs. 2(a)–2(g). They correspond to the $\mathcal{M}_4$-solutions of the Z_4-version, but the yellow pixels should now be interpreted as 1's instead of as 2's (dark blue remains 0) [see Proposition 4(b)]. All solutions in the Z_4-version become solutions of the Z_2-version under reduction mod 2. Figures 1(a) and 1(b), with seed-configurations $[a(-2), \ldots, a(2)] = [30323]$ and $[12303]$, respectively, map into the same Z_2-solution with seed-configuration $[10101]$, and the pattern corresponding to this solution can be found in Fig. 2(b) [interpreted as a Z_2-solution]. The mod 2-reduction of Fig. 2(b), interpreted as a Z_4-solution, is the trivial solution ($\equiv 0$) in the Z_2-case [all $\mathcal{M}_4$-solutions in Z_4 map into the 0-solution of the Z_2-case under reduction mod 2; this is the case for all patterns 2(a)–2(g)].

The solution displayed in Fig. 2(h) (seed [00010] in Z_4), maps into the pattern of Fig. 2(a) under reduction mod 2 (this now being interpreted in Z_2, with seed [00010]).

Figures 3–5 show the $(h, v) = (128, 0)$-, $(0, 64)$-, $(127, 0)$-, $(0, 63)$-SIPs of the Z_4-solutions that are shown in Figs. 1(a), 1(b) and 2(b), respectively. Observe that corresponding SIPs of these three solutions have a similar "super"-structure. This is particularly clear when comparing the structure consisting of the larger triangles in Figs. 3(a), 3(b) and 5(a) [and in 3(c), 3(d) and 5(b)]. This structure is the same in the three corresponding cases. These triangles are empty in Fig. 5(a) [5(b)], but contain some finer structure in Figs. 3(a) and 3(b) [3(c) and 3(d)]. The nature of this finer structure is reminiscent of the one displayed in Fig. 2(a), and the black pixels in it indicate the presence of different pixels in the original solutions and their shifted versions. These triangle-internal black pixels in Figs. 3(a) and 3(b) vanish under reduction mod 2, as can be seen in Figs. 5(a) and 5(b) [interpreted in Z_2]. This means that these

triangle-internal structures in the SIPs of Figs. 3(a) and 3(b) correspond to coincidences of the type $(0,2)$, $(2,0)$, $(1,3)$ or $(3,1)$ in the original patterns and their (v, h)-shifted versions (the first number in these pairs corresponds to a value in the original pattern, the second to a value in the shifted version). Indeed, these are the only coincidences that become $(0,0)$ or $(1,1)$ under reduction mod 2, and these produce a white pixel in the Z_2-case. Invoking the same argument, it is also clear that the black-pixel set in the (h, v)-SIP of a mod 2-reduced Z_4-solution (which is a Z_2-solution) is a subset of the black-pixel set of the (h, v)-SIP of that Z_4-solution. So the black-pixel set of the SIP in Fig. 5(c) is a subset of the black-pixel sets of the SIPs in Figs. 3(a) and 3(b) [and the black-pixel set of the SIP in 5(d) is a subset of the black-pixel set of the SIPs in 3(c) and 3(d)]. For the white-pixel set in the SIPs, this subset relationship is reversed.

Example 3. This example compares the Z_4 and Z_2-version of a CGI-problem for which seed-internal equations do appear, and for which the numbers of freecells is not invariant, although the seed-location and seed-size are invariant. It concerns the mod 2 and mod 4 versions of the $[\mathcal{T}_{2^1,\Xi\equiv 0},\ W = \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}$, $(\alpha_0 = 0,\ \alpha_1 = 6);\ l(X)]$-CGI problem, with $l(X) = (X^{-1}+1+X)^2$, the same rule as used in the Examples 1 and 2. The only difference with the previous examples lies in the fact that the shift-parameter $\alpha_1 \neq 0$ and that $W \not\equiv 1$.

We first consider the Z_2**-case.** The CGI-equations are: for all $k \in \mathbb{Z}$ and $\sigma = 0,\ 1$:

$$\begin{aligned} \underline{a}(k+\alpha_\sigma) = {} & \underline{a}(2k-2+\sigma) + \underline{a}(2k-1+\sigma) \\ & + \underline{a}(2k+\sigma) + \underline{a}(2k+1+\sigma) \\ & + \underline{a}(2k+2+\sigma) + \underline{a}(2k+3+\sigma)\,. \end{aligned} \tag{47}$$

The right-propagating form is

k even :

$$\begin{aligned} \underline{a}(k) = {} & \underline{a}(k-1) + \underline{a}(k-2) \\ & + \underline{a}(k-3) + \underline{a}(k-4) \\ & + \underline{a}(k-5) + \underline{a}\left(\frac{k+8}{2}\right) \end{aligned} \tag{48}$$

k odd :

$$\begin{aligned} \underline{a}(k) = {} & \underline{a}(k-1) + \underline{a}(k-2) \\ & + \underline{a}(k-3) + \underline{a}(k-4) \\ & + \underline{a}(k-5) + \underline{a}\left(\frac{k-3}{2}\right), \end{aligned}$$

and the left-propagating form

k even :

$$\begin{aligned} \underline{a}(k) = {} & \underline{a}(k+1) + \underline{a}(k+2) \\ & + \underline{a}(k+3) + \underline{a}(k+4) \\ & + \underline{a}(k+5) + \underline{a}\left(\frac{k+2}{2}\right) \end{aligned} \tag{49}$$

k odd :

$$\begin{aligned} \underline{a}(k) = {} & \underline{a}(k+1) + \underline{a}(k+2) \\ & + \underline{a}(k+3) + \underline{a}(k+4) \\ & + \underline{a}(k+5) + \underline{a}\left(\frac{k+13}{2}\right). \end{aligned}$$

There is a unique core, yielding the seed

$$\{\underline{a}(2),\ \underline{a}(3),\ \underline{a}(4),\ \underline{a}(5),\ \underline{a}(6),\ \underline{a}(7),\ \underline{a}(8)\}\,.$$

There are two seed-internal equations:

$$\begin{aligned} \underline{a}(8) = {} & \underline{a}(8) + \underline{a}(7) + \underline{a}(6) \\ & + \underline{a}(5) + \underline{a}(4) + \underline{a}(3) \end{aligned} \tag{50a}$$

$$\begin{aligned} \underline{a}(7) = {} & \underline{a}(2) + \underline{a}(6) + \underline{a}(5) \\ & + \underline{a}(4) + \underline{a}(3) + \underline{a}(2)\,. \end{aligned} \tag{50b}$$

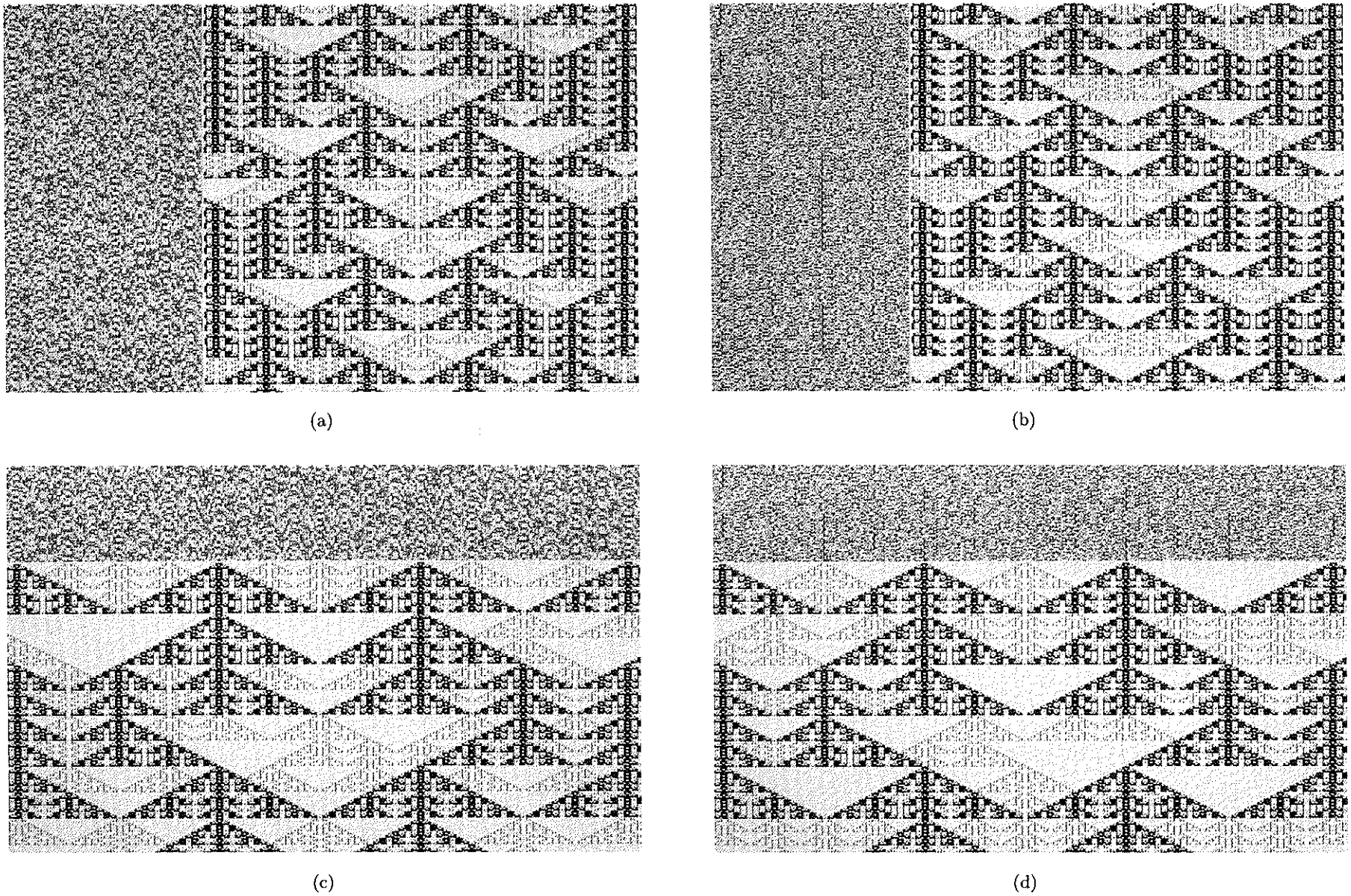
(right-propagating form). Observe that both equations are identical (in Z_2). Selecting $\underline{a}(3)$ as depcell gives the solution

$$\underline{a}(3) = \underline{a}(4) + \underline{a}(5) + \underline{a}(6) + \underline{a}(7)\,. \tag{51}$$

This means that $\underline{a}(2)$, $\underline{a}(4)$, $\underline{a}(5)$, $\underline{a}(6)$, $\underline{a}(7)$, $\underline{a}(8)$ can be taken as freecells which may be given the values 0 or 1 arbitrarily and independently, while $\underline{a}(3)$ depends on the freecells as given by Eq. (51). So there are $2^6 = 64$ solutions to this Z_2-CGI problem.

Let us now turn towards the corresponding Z_4**-case.** The CGI-equations are: for all $k \in \mathbb{Z}$ and $\sigma = 0,\ 1$:

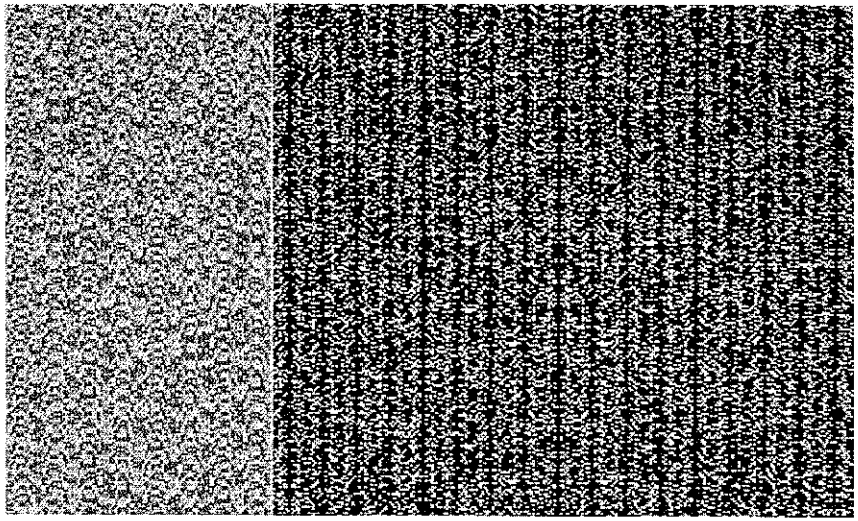
$$\begin{aligned} \underline{a}(k+\alpha_\sigma) = {} & \underline{a}(2k-2+\sigma) + 3\underline{a}(2k-1+\sigma) \\ & + \underline{a}(2k+\sigma) + \underline{a}(2k+1+\sigma) \\ & + 3\underline{a}(2k+2+\sigma) + \underline{a}(2k+3+\sigma)\,. \end{aligned} \tag{52}$$



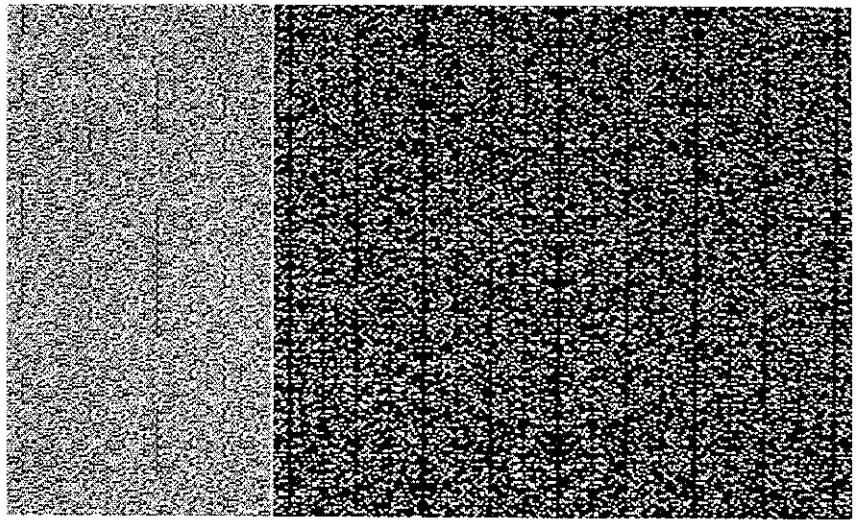
(a) (b)

(c) (d)

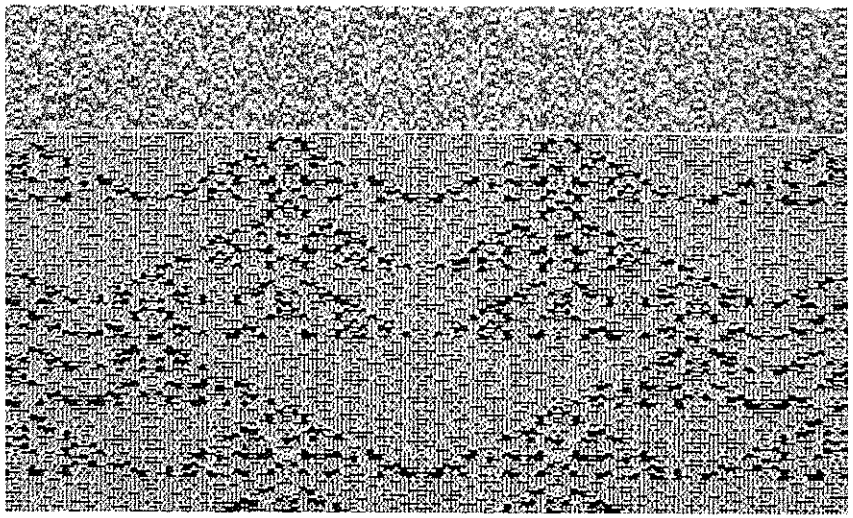
Fig. 3. SIPs for the patterns of Figs. 1(a) and 1(b). (a) $(128, 0)$-SIP of the pattern in Fig. 1(a); (b) $(128, 0)$-SIP of the pattern in Fig. 1(b); (c) $(0, 64)$-SIP of the pattern in Fig. 1(a); (d) $(0, 64)$-SIP of the pattern in Fig. 1(b). Observe the common structure formed by the large-scale triangles for the figures on the left-hand side and right-hand side.



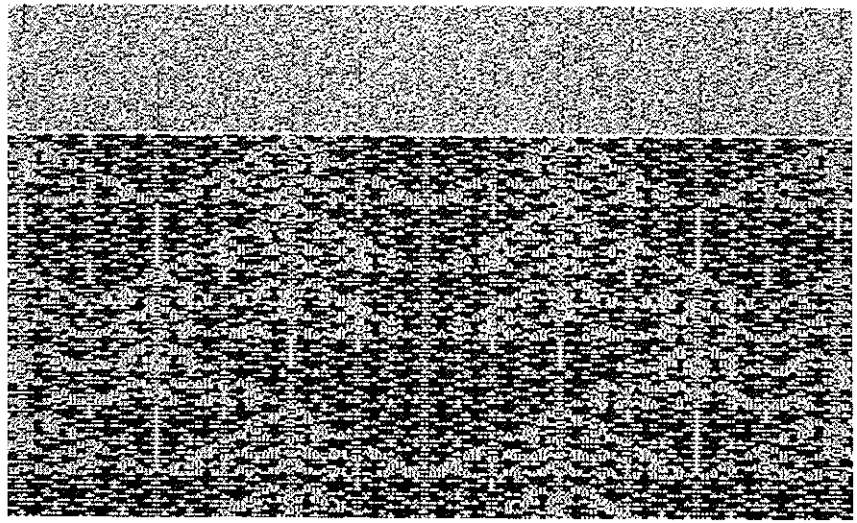
(a)



(b)



(c)



(d)

Fig. 4. SIPs of the patterns in Figs. 1(a) and 1(b) [continued from Fig. 3]. (a) $(127, 0)$-SIP of the pattern in Fig. 1(a); (b) $(127, 0)$-SIP of the pattern in Fig. 1(b); (c) $(0, 63)$-SIP of the pattern in Fig. 1(a); (d) $(0, 63)$-SIP of the pattern in Fig. 1(b).

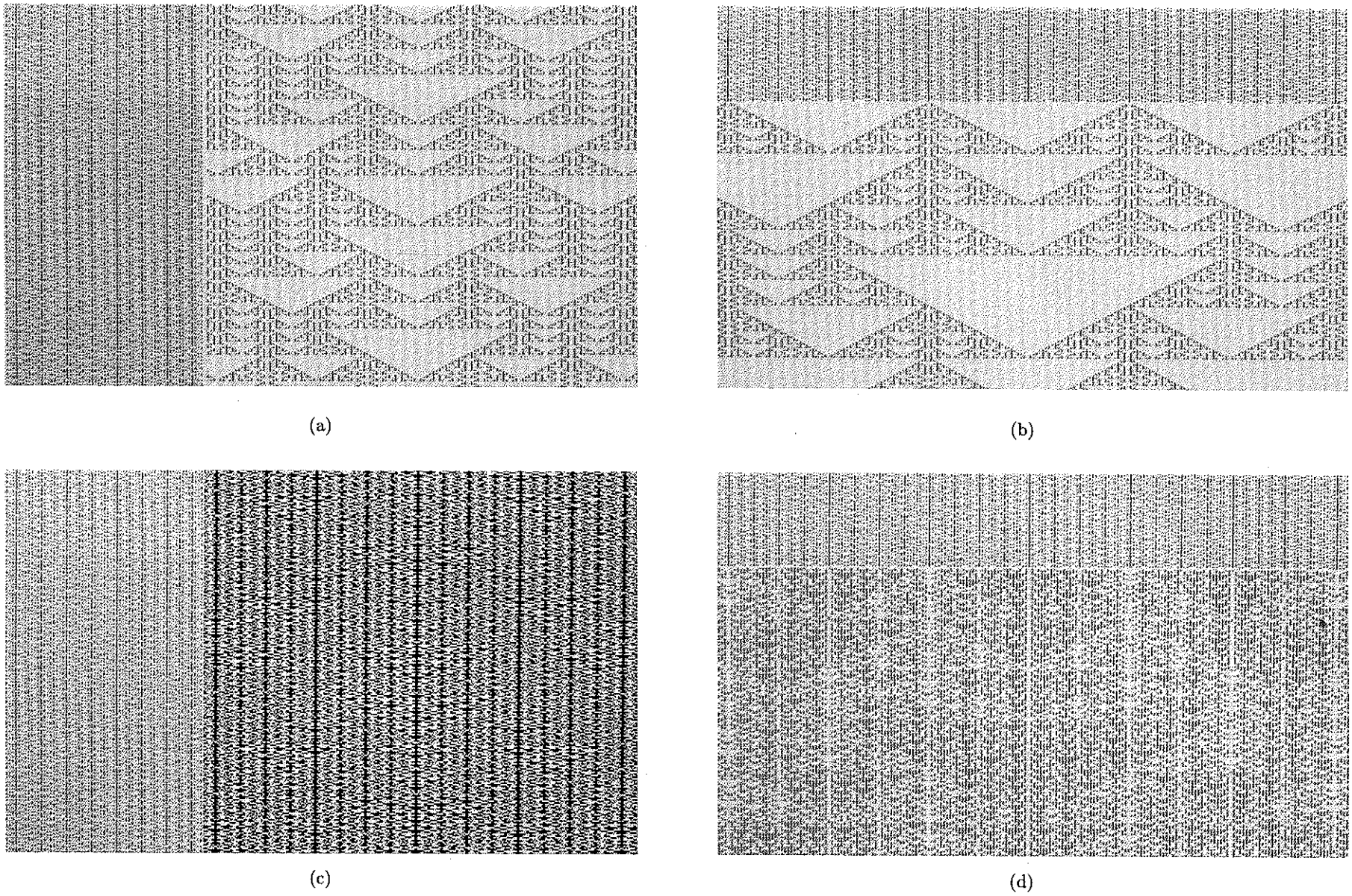


Fig. 5. SIPs of the pattern in Fig. 2(b), i.e. SIPs of the mod 2-reductions of the patterns in Figs. 1(a) and 1(b). (a) $(128, 0)$-SIP; (b) $(0, 64)$-SIP; (c) $(127, 0)$-SIP; (d) $(0, 63)$-SIP. Compare with the corresponding SIPs in Figs. 3 and 4.

The right-propagating form is

$$\begin{aligned} &k \text{ even}: \\ &\underline{a}(k) = \underline{a}(k-1) + 3\underline{a}(k-2) \\ &\qquad + 3\underline{a}(k-3) + \underline{a}(k-4) \\ &\qquad + 3\underline{a}(k-5) + \underline{a}\left(\frac{k+8}{2}\right) \\ &k \text{ odd}: \\ &\underline{a}(k) = \underline{a}(k-1) + 3\underline{a}(k-2) \\ &\qquad + 3\underline{a}(k-3) + \underline{a}(k-4) \\ &\qquad + 3\underline{a}(k-5) + \underline{a}\left(\frac{k-3}{2}\right), \end{aligned} \tag{53}$$

and the left-propagating form

$$\begin{aligned} &k \text{ even}: \\ &\underline{a}(k) = \underline{a}(k+1) + 3\underline{a}(k+2) \\ &\qquad + 3\underline{a}(k+3) + \underline{a}(k+4) \\ &\qquad + 3\underline{a}(k+5) + \underline{a}\left(\frac{k+2}{2}\right) \\ &k \text{ odd}: \\ &\underline{a}(k) = \underline{a}(k+1) + 3\underline{a}(k+2) \\ &\qquad + 3\underline{a}(k+3) + \underline{a}(k+4) \\ &\qquad + 3\underline{a}(k+5) + \underline{a}\left(\frac{k+13}{2}\right). \end{aligned} \tag{54}$$

There is again a unique core, yielding the seed

$$\{\underline{a}(2), \underline{a}(3), \underline{a}(4), \underline{a}(5), \underline{a}(6), \underline{a}(7), \underline{a}(8)\},$$

which is actually the same as for the Z_2-version of the problem (see Lemma 10 and Corollary 3). There are two seed-internal equations:

$$\begin{aligned} \underline{a}(8) &= \underline{a}(8) + \underline{a}(7) + 3\underline{a}(6) \\ &\quad + 3\underline{a}(5) + \underline{a}(4) + 3\underline{a}(3) \qquad (55a) \\ \underline{a}(7) &= \underline{a}(2) + \underline{a}(6) + 3\underline{a}(5) \\ &\quad + 3\underline{a}(4) + \underline{a}(3) + 3\underline{a}(2). \qquad (55b) \end{aligned}$$

Observe that all equations in the Z_2-case are the images of the corresponding Z_4-equations under reduction mod 2 [compare Eqs. (47)–(50b) to Eqs. (52)–(55b)].

Adding these two equations (mod 4) produces $2\underline{a}(5) = 0$. This means that there are two solutions for $\underline{a}(5)$:

$$\underline{a}(5) = 0 \qquad (56a)$$

$$\underline{a}(5) = 2. \qquad (56b)$$

We denote this by

$$a(5) = 0 + [[2]], \tag{57}$$

where $[[2]]$ indicates that we are free to add 2 or not. Inserting this condition in Eq. (55a), as well as in Eq. (55b) gives the unique condition

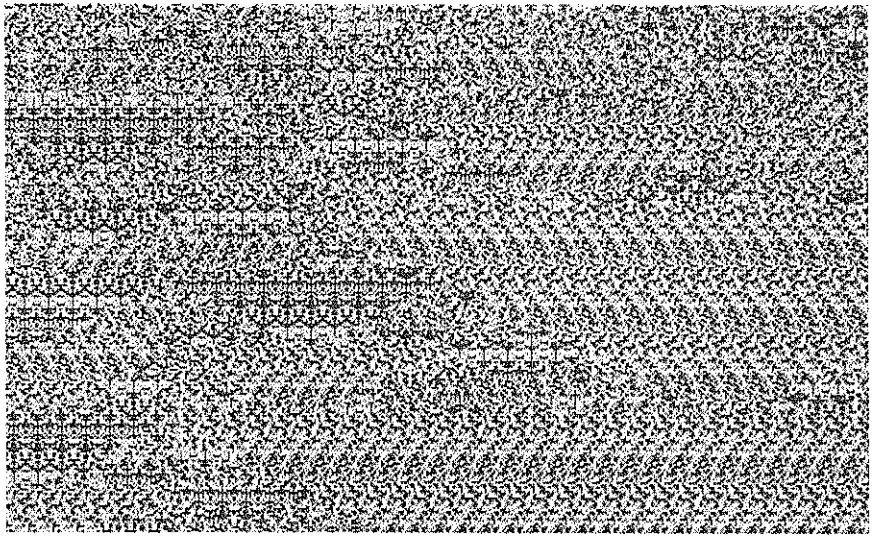
$$\underline{a}(3) = \underline{a}(7) + 3\underline{a}(6) + \underline{a}(4) + [[2]], \tag{58}$$

where the additional term $[[2]]$ is either selected or not in *both* Eqs. (57) and (58). It is easily checked by substitution that both possibilities that are present in the Eqs. (57) and (58) satisfy the original seed-internal Eqs. (55a) and (55b).

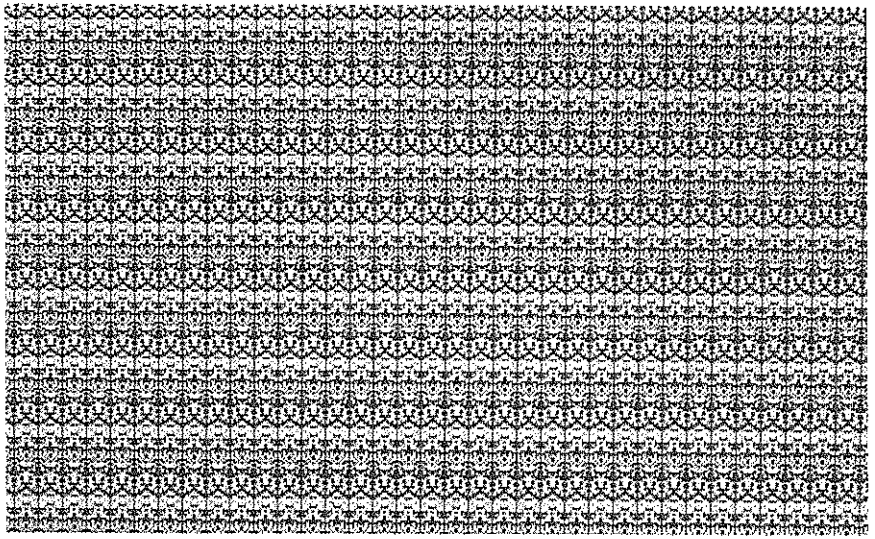
We conclude that the five seed-cells $\underline{a}(2)$, $\underline{a}(4)$, $\underline{a}(6)$, $\underline{a}(7)$, $\underline{a}(8)$ are freecells which may be attributed the values 0, 1, 2, 3 arbitrarily and independently. Seed-cells $\underline{a}(3)$ and $\underline{a}(5)$ are cells of *hybrid type*: They are neither completely free, nor completely dependent, but they share a reduced degree of freedom as they may take one of both values given by Eqs. (57) and (58). So there are $4^5 \times 2 = 2048$ solutions for this Z_4-version of the CGI-problem. Or: Each Z_2-solution has 32 different preimages in Z_4.

Figure 6 shows a few solutions of the CGI-problem for this example. The Figs. 6(a)–6(c) and 6(h) are solutions in $\mathcal{M}_4 = \{0, 2\} \subset Z_4$ for the Z_4-version of the problem. They can also be interpreted as solutions of the corresponding Z_2-problem [yellow pixels should then be associated with the value 1]. Figure 6(a) corresponds to the seed-configuration $[a(2), \ldots, a(8)] = [\underline{0}2\underline{0}2\underline{000}]$ (the underlined digits correspond to the freecells in the seed). It corresponds to the case where the additional term 2 is selected in both the Eqs. (57) and (58), while all freecells are put to 0. The alternative choice would produce the trivial solution ($\equiv 0$). If we consider the solutions obtained from the selection of 0 in these equations (they form half of all solutions), then adding the solution displayed in Fig. 6(a) to them generates the other half of the solutions (pixelwise addition mod 4).

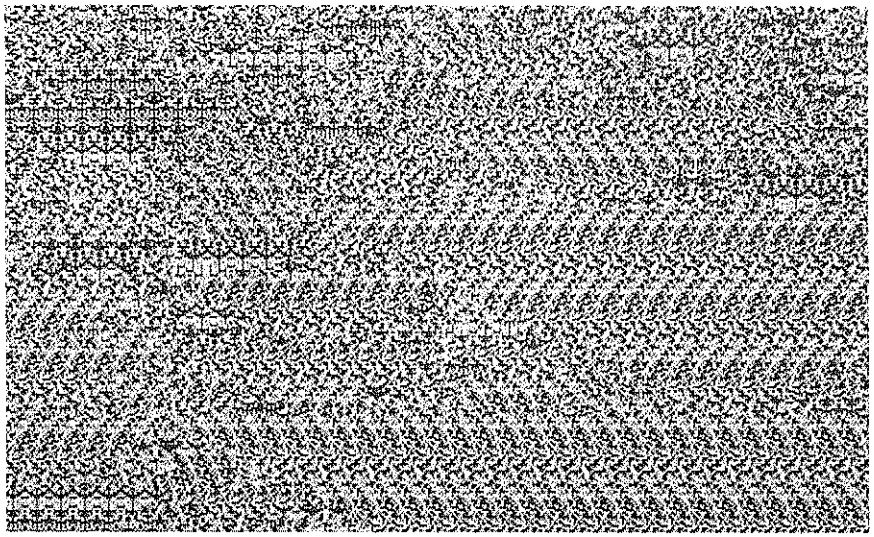
Figure 6(b) is the unique periodic solution under the $\mathcal{M}_4$- (or Z_2-)solutions (seed $[\underline{2}000\underline{002}]$). Figure 6(c) is the sum of 6(a) and 6(b) (seed $[\underline{2}2\underline{02}002]$). Figure 6(d) is a full-Z_4 periodic solution (seed $[\underline{3}000\underline{001}]$). Its reduction mod 2 produces Fig. 6(b) [interpreted as a solution in Z_2]. The same is true for the two solutions shown in Figs. 6(e) and 6(f) (colored parts; seeds $[\underline{3}2\underline{00}203]$ and $[\underline{3}00\underline{2}203]$). These patterns are not at all periodic (rather quasirandom, see [Barbé, 1996]), but they collapse into



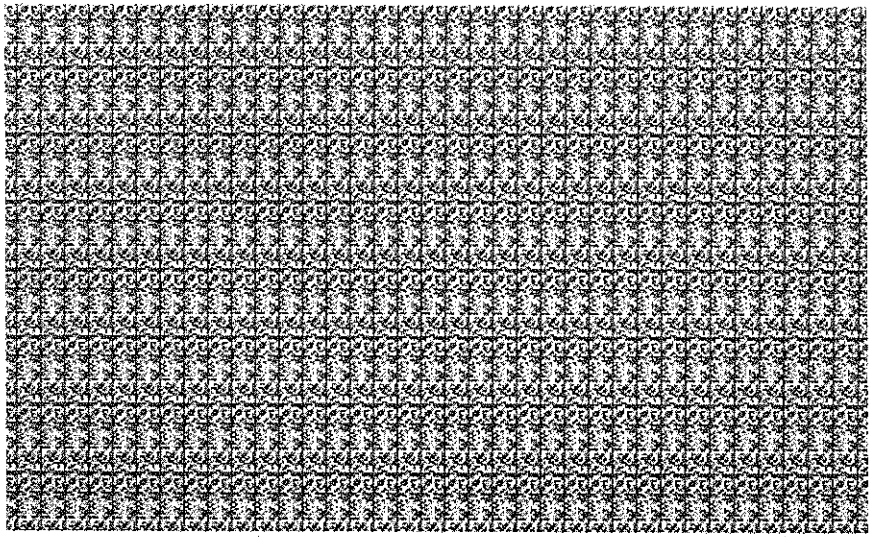
(a)



(b)

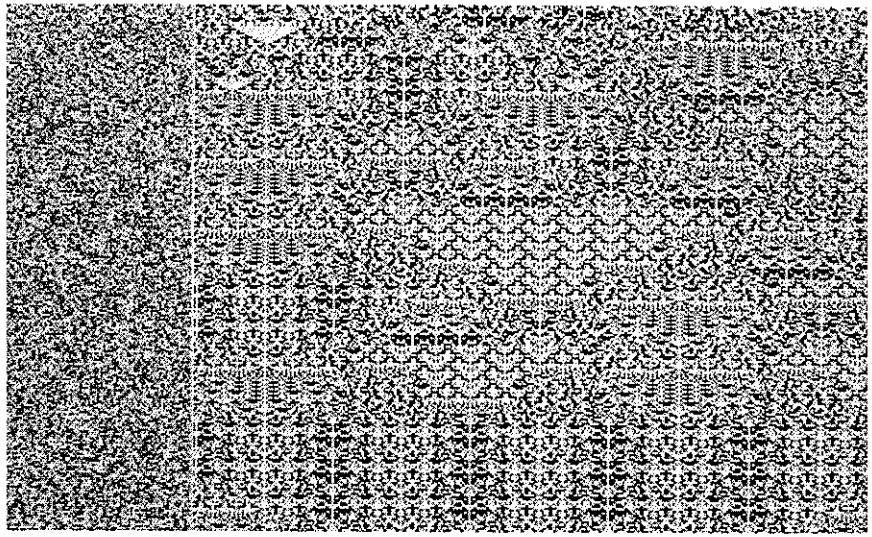


(c)

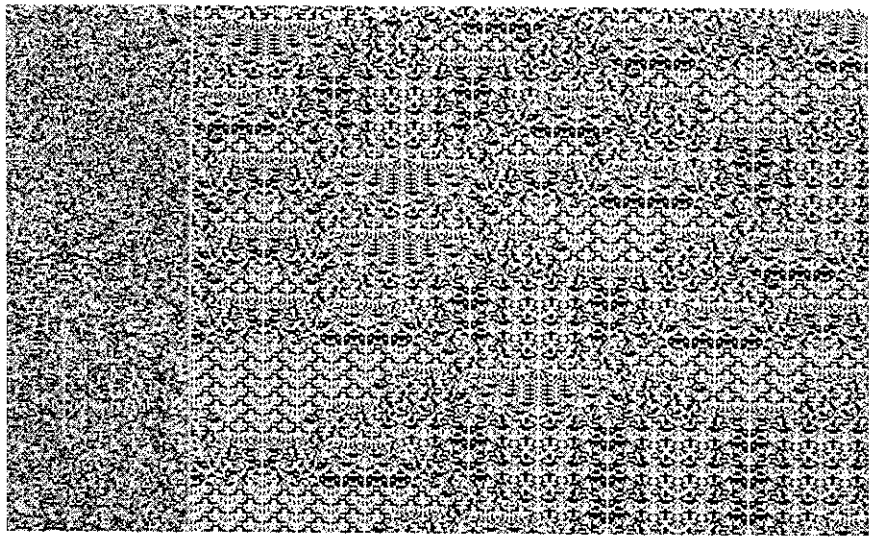


(d)

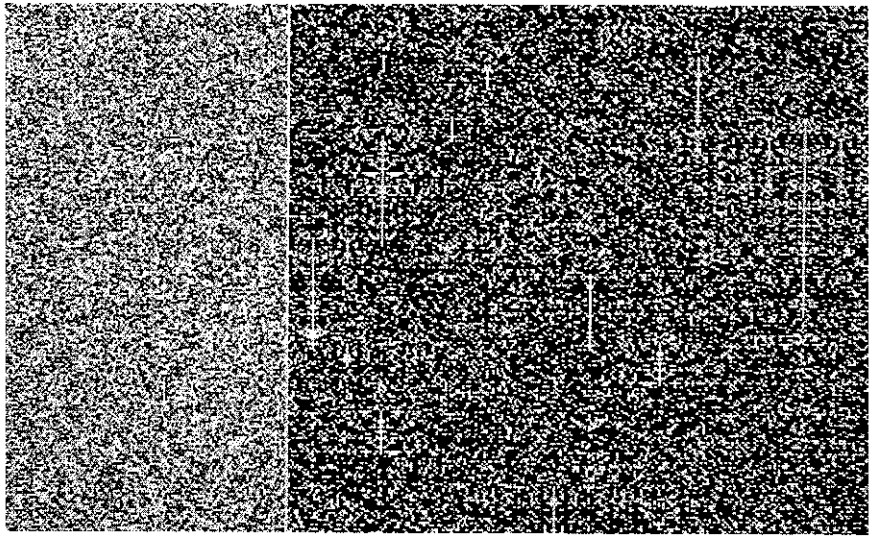
Fig. 6. Some solutions for the Z_4-CGI problem in Example 3. (a) seed $[a(2)\ldots a(8)] = [\underline{0}2\underline{0}2\underline{0}\underline{0}\underline{0}]$ (underlined digits correspond to freecells); (b) seed $[\underline{2}\underline{0}\underline{0}\underline{0}\underline{0}\underline{0}\underline{2}]$; (c) seed $[\underline{2}\underline{2}\underline{0}\underline{2}\underline{0}\underline{0}\underline{2}]$; (d) seed $[\underline{3}\underline{0}\underline{0}\underline{0}\underline{0}\underline{0}\underline{1}]$; (e) seed $[\underline{3}\underline{2}\underline{0}\underline{0}\underline{2}\underline{0}\underline{3}]$, $(88,0)$-SIP; (f) seed $[\underline{3}\underline{0}\underline{0}\underline{2}\underline{2}\underline{0}\underline{3}]$, $(88,0)$-SIP; (g) seed $[\underline{0}\underline{2}\underline{1}\underline{0}\underline{2}\underline{3}\underline{0}]$, $(132,0)$-SIP; (h) seed $[\underline{0}\underline{0}\underline{2}\underline{0}\underline{0}\underline{2}\underline{0}]$, $(132,0)$-SIP. The solution-patterns (colored parts) in (e) and (f) both produce the pattern (b) under reduction mod 2 [(b) to be interpreted in Z_2]. The solution-pattern in (g) maps into (h) under mod 2-reduction. The black-pixel set in the SIP-part in (h) is a subset of the black-pixel set in (g).



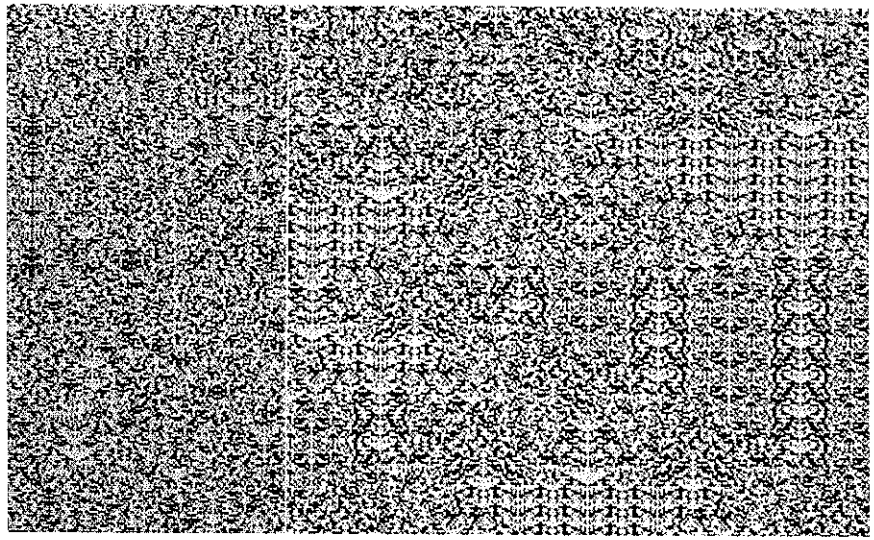
(e)



(f)



(g)



(h)

Fig. 6. (*Continued*)

the periodic solution of Fig. 6(b) under reduction mod 2. Moreover, Fig. 6(f) is the sum (in Z_4) of 6(a) and 6(e). Compare the SIPs for these solutions.

Figure 6(g) shows another solution. Its reduction mod 2 produces 6(h) [interpreted as a solution in Z_2]. The black-pixel set in the SIP of 6(h) is a subset of the black-pixel set in the SIP of 6(g).

Observe that the (local) periodic structures that appear in the solutions have period 11. This equals $p^s(\alpha_1 - \alpha_0) - 1 = 2.6 - 1$ (this formula was derived in [Barbé, 1996] and seems to hold also for p^s-CGI problems in Z_{p^n}). Interesting SIP-structures occur for horizontal shifts which are multiples of this period [like 88 and 132 that are used in Figs. 6(e)–6(h)].

The last example suggests the next proposition. It is based on the property that a given set of equations in Z_{p^d} (for example the seed-internal equations), when reduced mod p^n ($n < d$), can only increase the degree of freedom in its solutions.

Proposition 5. *Let N_{p^n} be the number of solutions of a regular $[\mathcal{T}_{p^s,\Xi}, W, \alpha, l(X)]_{\bmod p^n}$-CGI problem, with $l(X)$ satisfying Eq. (35) and $n \leq d$. Then it holds for $m < n \leq d$ that*

$$N_{p^n} \leq (N_{p^m})^{p^{n-m}} .$$

Acknowledgment

The authors thank Jean-Paul Allouche, Fritz von Haeseler and Wibke Jürgensen for interesting and stimulating discussions. A. Barbé gratefully acknowledges the University of Bremen and the DFG for their support.

This research was also partially supported by the Concerted Action Project GOA-MIPS of the Flemish Community, and by the Belgian Program on Interuniversity Attraction Poles of the Belgian Prime Minister's Office for Science, Technology and Culture (IUAP P4-02).

References

Allouche, J.-P. [1990] "Finite automata in 1-dimensional and 2-dimensional physics," in *Number Theory and Physics*, eds. Luck, J. *et al.*, *Proc. Physics* **47** (Springer, Berlin), pp. 177–184.

Allouche, J.-P. & Mendès France, M. [1994] "Automata and automatic sequences," in *Beyond Quasicristals*, eds. Axel, F. & Gratias, D. (Les Editions de Physique & Springer, Berlin), pp. 293–367.

Allouche, J.-P., von Haeseler, F., Peitgen, H.-O. & Skordev, G. [1996] "Linear cellular automata, finite automata and Pascal's triangle," *Discrete Appl. Math.* **66**, 1–22.

Allouche, J.-P., Cateland, E., Gilbert, W., Peitgen, H.-O., Shallit, J. & Skordev, G. [1997] "Automatic maps in exotic numeration systems," *Theor. Comput. Syst.* **30**, 285–331.

Barbé, A., von Haeseler, F., Peitgen, H.-O. & Skordev, G. [1995] "Coarse-graining invariant orbits of one-dimensional two-state linear cellular automata," *Int. J. Bifurcation and Chaos* **5**(6), 1611–1631.

Barbé, A. [1996] "Coarse-graining invariant orbits of one-dimensional $\mathbb{Z}_p$-linear cellular automata," *Int. J. Bifurcation and Chaos* **6**(12A), 2237–2297.

Barbé, A. [1997] "Complex order from disorder and from simple order in coarse-graining invariant orbits of certain two-dimensional linear cellular automata," *Int. J. Bifurcation and Chaos* **7**(7), 1451-1496.

Childs, L. [1979] *A Concrete Introduction to Higher Algebra* (Springer, NY).

Cobham, A. [1972] "Uniform tag sequences," *Math. Syst. Theor.* **6**, 164–192.

Christol, G. [1979] "Ensembles presque périodiques k-reconnaissables," *Theoret. Comput. Sci.* **9**, 141–145.

Christol, G., Kamae, T., Mendès France, M. & Rauzy, G. [1980] "Suites algébriques, automates et substitutions," *Bull. Soc. Math. France* **108**, 401–419.

Christol G. [1986] "Fonctions et éléments algébriques," *Pacific J. Math.* **125**, 1–37.

Denef, J. & Lipshitz, L. [1987] "Algebraic power series and diagonals," *J. Number Theor.* **26**, 46–67.

Eilenberg, S. [1985] *Automata, Languages and Machines, Vol. A* (Academic Press, NY).

Jungnickel, D. [1993] *Finite Fields* (BI-Wissenschaftsverlag, Mannheim).

Jürgensen, W. [1997] "Über die Lösungen von Mahlergleichungen," Diplomarbeit, Fachbereich Mathematik, Univ. Bremen.

Lidl, R. & Niederreiter, H. [1983] *Finite Fields* (Addison-Wesley, Reading, MA).

Lipshitz, L. & van der Poorten, A. [1989] "Rational functions, diagonals, automata and arithmetic," in *Number Theory, Proc. First. Conf. Canadian Number Theory Association*, ed. Mollin, R. (W. De Gruyter, Berlin), pp. 339–358.

Loxton, J. & van der Poorten, A. [1977] "Transcendence and algebraic independence by a method of Mahler," in *Transcendence Theory — Advances and Applications*, eds. Baker, A. & Masser, D. (Academic Press, NY), pp. 211–226.

Mahler, K. [1929] "Arithmetische Eigenschaften der Lösungen einer Klasse von Funktionalgleichungen," *Math. Ann.* **101**, 342–366.

Neukirch, J. [1991] "The p-adic numbers," in *Numbers*, eds. Ebbinghaus, H.-D. *et al.* (Springer, NY), pp. 155–178.

Nishioka, K. [1996] *Mahler Functions and Transcendence*, Lecture Notes in Mathematics **1631** (Springer, NY).

Robinson, A. [1987] "Fast computation of additive cellular automata," *Compl. Syst.* **1**, 211–216.

Salon, O. [1986] "Propriétés arithmétiques des automates multidimensionnels," *Séminaire de Théorie des Nombres de Bordeaux* **4** (1986–87), p. 4.06.

Salon, O. [1987] "Suites automatiques à multi-indices et algébricité," *C. R. Acad. Sci. Paris Série I* **305**, 501–504.

van der Waerden, B. L. [1991] *Algebra I* (Springer, NY).

von Haeseler, F., Peitgen, H.-O. & Skordev, G. [1992] "On the fractal structure of rescaled evolution set of a class of cellular automata," Report **278**, Institut für Dynamische Systeme, Univ. Bremen.

von Haeseler, F., Peitgen, H.-O. & Skordev, G. [1993] "Cellular automata, matrix substitutions, and fractals," *Ann. Math. Art. Intell.* **8**, 345–362.

von Haeseler, F. [1996] "On algebraic properties of sequences generated by substitutions over a group," Habilitationsschrift, Fachbereich Mathematik, Univ. Bremen.

Wolfram, S. [1994] *Cellular Automata and Complexity* (World Scientific, Singapore).