Self-similar carpets over finite fields

Mihai Prunescu *

Abstract

In [6] an informal algorithm 'to display interesting numeric patterns' is described without any proof. We generalize this algorithm over arbitrary finite fields $\mathbb{F}_q$ of characteristic p and we prove that it always generates some self-similar sets. For the prime fields $\mathbb{F}_p$ the generalized algorithm produces $p-1$ different self-similar sets. These sets are classified according to their arithmetic and their groups of symmetry.
A.M.S.-Classification: 11A07, 28A80.

1 Introduction

In [6] is described an informal algorithm 'to produce interesting numerical patterns', as follows: Let $n > 2$ be a fixed natural number. One takes a rectangular matrix, completes the first row and the first column with ones, and recursively computes the other elements as $(N + NW + W)$ mod n, where N, NW and W are the neighbours in the corresponding directions. Finally, one can produce an image following a fixed correspondence of the rests modulo n with a list of colours. The authors observe and state that for primes $n = p$ the patterns are self-similar, but don't prove this. For the notion of self-similarity they citate Mandelbrot's monograph [5]. In [5], Chapter 14, there is a hint to a similar construction for Sierpinski's Carpet atributed to Rose (see [10]). In [7] the authors introduced the more general rule $(N + m \cdot NW + W) \mod n$ for a fixed $m \in \mathbb{N}$ and made remarks around the associated generalized Fibonacci sequences but they didn't interpret the matrix graphically. Respecting the analogy with Sierpinski's Carpet we will constantly use the term carpet, which shall be also rigorously defined below.

One goal of this paper is to prove the conjecture concerning self-similarity suggested in [6]. The problem shall be studied over a finite field $\mathbb{F}_q$ applying the rule $N + m \cdot NW + W$ with a fixed $m \in \mathbb{F}_q$. We prove that such carpets are self-similar provided that they contain at least one zero.

Definition 1.1 Let K be a field and $A = (a(i,j)) \in \mathcal{M}_{n\times n}(K)$ be a matrix. The set $\mathcal{A} \subset \mathbb{R}^2$ associated with the matrix A is defined as follows: one divides the square $[0,1] \times [0,1]$ in $n \times n$ many equal squares $S_{i,j}$. The interior of $S_{i,j}$ shall be excluded from $[0,1] \times [0,1]$ if and only if $a(i,j) = 0$.

Let $\mathbb{F}_q$ be the finite field with q elements of characteristic p, $q = p^k$ for some k. We fix an element $m \in \mathbb{F}_q$. The matrices occurring in this article are always indexed starting with 0.

Definition 1.2 The infinite matrix $G(q,m) = (a(i,j))_{i,j\geq 0}$ is the image of the function $a : \mathbb{N} \times \mathbb{N} \to \mathbb{F}_q$ recurrently defined by $a(i,0) = a(0,j) = 1$ and $a(i,j) = a(i-1,j) + m \cdot a(i-1,j-1) + a(i,j-1) \in \mathbb{F}_q$. For $d \geq 1$ let $G(d,q,m)$ be the $p^d \times p^d$ left-upper minor of $G(q,m)$. The $p \times p$ matrix $F(q,m) = G(1,q,m)$ shall be called the fundamental block.

*Brain Products, Freiburg, Germany, and Institute of Mathematics of the Romanian Academy, Bucharest, Romania. mihai.prunescu@math.uni-freiburg.de.

Definition 1.3 Let $\mathcal{G}(d,q,m) \subset \mathbb{R}^2$ be the set associated with the matrix $G(d,q,m)$. The carpet $\mathcal{G}(q,m)$ is defined to be

$$\mathcal{G}(q,m) = \lim_{d\to\infty} \mathcal{G}(d,q,m)$$

in the Hausdorff metric space of the compact subsets of $\mathbb{R}^2$.

At this moment it is not at all clear that the limit $\mathcal{G}(q,m)$ does really exist. The existence shall be proved in Section 4 together with the self-similarity.

Coming back to the case $q = p$ we prove following things: $\mathcal{G}(p,0)$ is always Pascal's Triangle modulo p, so we have a new proof for its self-similarity. $\mathcal{G}(p,-1)$ is only the full square, the uninteresting case. $\mathcal{G}(p,1)$ are the self-similar sets of [6]. We prove that they always contain a cross of zeros and that they have as group of symmetries the full dihedral group D_8. For the other values of $m \in \mathbb{F}_p$ one gets new self-similar patterns with group of symmetries isomorphic with Klein's group K_4. We will also study the special case of the so called diagonal carpets got for $m \in \{-2, -1/2\}$.

Now just some words about related things. This pattern generation by recurrent double sequences is connatural with the generation of self-similar sets by cellular automata; see [13] for the pattern generation by cellular automata or the rich survey [3] for cellular automata and related problems. The sets generated by cellular automata are also limits of repeated (rescalings and) projections onto a fixed compact. As a difference, they are not limits of sequences of repeated projections of the space $\mathbb{Z}^k$ of the cellular automaton, but limits of such sequences applied to its graph laying in $\mathbb{Z}^{k+1}$, where the discrete time is added as supplementary axis of coordinates. For example, the Pascal Triangle modulo 2 is produced as a limit of projections applied to the graph of a linear cellular automaton. One can remark however that if $m \neq 0$ the pattern generation by recurrent double sequences seems to be different from the pattern generation by cellular automata.

Likely in cellular automata, the recurrent double sequences are strong enough as a model of computation to lead to undecidable problems. In [8] the author studied recurrent double sequences defined as follows: given a finite set A with two distinguished elements called 0 and 1 and a fixed function $f : A \times A \to A$, the double sequence $a : \mathbb{N} \times \mathbb{N} \to A$ satisfies $a(i,0) = a(0,j) = 1$ and $a(i,j) = f(a(i,j-1), a(i-1,j))$ for $i,j \geq 1$. The problem considered in [8] is if arbitrary recurrent double sequences are ultimately zero. It is proven that this problem is undecidable, even if it is restricted to commutative functions f only.

2 The recurrent function

Definition: Let K be a field and let $m \in K$ be a fixed element. We consider the function $f : \mathbb{N} \times \mathbb{N} \to K$ recursively defined by the conditions $f(n,0) = f(0,k) = 1$ and:

$$f(n,k) = f(n,k-1) + m \cdot f(n-1,k-1) + f(n-1,k)$$

for $n,k \geq 1$.

Lemma 2.1 *The function f is symmetric and satisfies:*

$$f(n,k) = \sum_{a=0}^{\min(n,k)} \binom{n}{a}\binom{n+k-a}{k-a} m^a.$$

Proof: The symmetry follows from the symmetry of the recurrence and of the initial conditions. To compute f, use the method of generating functions described in [12]. Define the formal series (generating function) $A_n(x) = \sum_{k\geq 0} f(n,k)\ x^k$. It follows:

$$A_{n+1}(x) = \sum_{k\geq 0} f(n+1,k)\ x^k = 1 + \sum_{k\geq 1} \Big(f(n,k) + f(n+1,k-1) + m \cdot f(n,k-1) \Big)\ x^k =$$

$$= \Big(1+\sum_{k\geq 1} f(n,k)\ x^k\Big) + x\sum_{k\geq 0} f(n+1,k)\ x^k + mx\sum_{k\geq 0} f(n,k)\ x^k = A_n(x) + xA_{n+1}(x) + mxA_n(x).$$

This recurrence have the solution:

$$A_n(x) = \Big(\frac{1}{1-x}\Big)^{n+1}(1+mx)^n.$$

Using that $(1+mx)^n = \sum_{k\geq 0}\binom{n}{k}m^k x^k$ and that $\Big(\frac{1}{1-x}\Big)^{n+1} = \sum_{k\geq 0}\binom{n+k}{k}\ x^k$, one gets the Lemma. □

Remarks:

(1) The terms

$$t(a,k,n) := \binom{n}{a}\binom{n+k-a}{k-a}\ m^a = \frac{(n+k-a)!}{a!(k-a)!(n-a)!}\ m^a.$$

are itself symmetric in n and k.

(2) Replace $m \in K$ with an undeterminate X transcendental over K; the Lemma 2.1 is also true as a statement about a family of polynomials $F : \mathbb{N}\times\mathbb{N} \to K[X]$.

3 Tensor powers and self-similarity

Definition 3.1 Let R be some commutative ring and $A = (a_{i,j}) \in \mathcal{M}_{s\times t}(R)$, $B \in \mathcal{M}_{u\times v}(R)$ two matrices. Then the tensor product in the sense of Kronecker $A \otimes B$ is a matrix in $\mathcal{M}_{su\times tv}(R)$ having the block-wise representation $(a_{i,j}B)$. If A_1, A_2, ..., A_n are arbitrary matrices, we denote the Kronecker tensor term:

$$((\dots((A_1\otimes A_2)\otimes A_3)\dots)\otimes A_{n-1})\otimes A_n \quad \text{by}: \quad A_1\otimes A_2\otimes\cdots\otimes A_{n-1}\otimes A_n.$$

For all $n \geq 1$ we define the Kronecker tensor power $A^{\otimes n}$ of A inductively by: $A^{\otimes 1} = A$ and $A^{\otimes(n+1)} = A^{\otimes n}\otimes A$.

For the history of the name "Kronecker" product, see the commentary in the last section. In the rest of this paper we will speak only about tensor products and tensor powers.

Definition 3.2 A compact topological space X is self-similar if there exists a finite set S indexing a set of non-surjective homeomorphisms $\{f_s\}_{s\in S}$ for which

$$X = \bigcup_{s\in S} f_s(X).$$

The following remark expresses the *principle of substitution* used for constructing self-similar sets.

Remark 3.3 *For some $n \geq 2$ consider a matrix $A = (a(i,j)) \in \mathcal{M}_{n\times n}(\{0,1\})$ containing at least one zero and at least two ones. Let $\mathcal{A}^d$ be the set associated with $A^{\otimes d}$. Then $\mathcal{A} = \lim \mathcal{A}^d$ exists and is a self-similar set.*

One has an infinite sequence $\mathcal{A}^d$ of non-empty compact subsets of $\mathbb{R}^2$ with $\mathcal{A}^{d+1} \subset \mathcal{A}^d$ for all $d \in \mathbb{N}$. It is known that $\lim_{d\to\infty} \mathcal{A}^d$ exists, is always non-empty, and is equal $\cap\mathcal{A}^d$. In order to verify the definition of self-similarity, consider the following family of non-surjective homeomorphisms: for all $i,j \in \{0,\dots,n-1\}$ such that $a(i,j) = 1$ take f to be the linear application carrying the unit square onto $S_{i,j}$.

4 Carpets are self-similar

For the fundamental block $F(q,m) \in \mathcal{M}_{p\times p}(\mathbb{F}_q)$ recall the notation $F(q,m) = (a(i,j))$ with i and $j = 0,\dots,p-1$. It follows already from Lemma 2.1 that $F(q,m)$ is a symmetric matrix. The same is true for all other matrices $G(d,q,m)$ with $d \geq 2$.

Lemma 4.1 *The last column and the last row of $F(q,m)$ are exactly:*

$$1,\ -m,\ (-m)^2,\ \dots,\ (-m)^{p-1}.$$

Proof: Take $k \leq n = p-1$ and compute the term $t(a,n,k)$ in the field $\mathbb{F}_q$. For $a < k$ one gets:

$$t(a,p-1,k) = \binom{p-1}{a}\binom{p-1+k-a}{k-a}\, m^a = \binom{p-1}{a}\cdot p\cdot\dots\times m^a = 0,$$

so all these terms do not contribute to the sum. For the last term one gets:

$$t(k,k,p-1) = \frac{(p-1)\dots(p-k)}{k!}\, m^k = (-1)^k\frac{k!}{k!}\, m^k = (-m)^k.$$

□

Definition 4.2 The automorphism of Frobenius $\varphi : \mathbb{F}_q \to \mathbb{F}_q$ is defined by $\varphi(x) = x^p$. This automorphism generates the Galois group Gal $(\mathbb{F}_q/\mathbb{F}_p)$. For a matrix $A = (a_{i,j})$ over $\mathbb{F}_q$, let $\varphi(A)$ be the matrix $(\varphi(a_{i,j}))$.

Lemma 4.3 *Let $F = F(p,m)$ be a fundamental block. Consider a matrix in construction consisting of the following three blocks:*

$$\begin{array}{cc} \alpha F & \beta F \\ \gamma F & \cdot \end{array}$$

with α, β, $\gamma \in \mathbb{F}_q$. Then the recurrent rule produces the following matrix:

$$\begin{array}{cc} \alpha F & \beta F \\ \gamma F & \delta F \end{array}$$

with $\delta = \varphi(m)\alpha + \beta + \gamma$.

Proof: Denote $-m$ with λ. There is only one element x where one can start to apply the recurrent rule:

$$\begin{array}{cccccc} \dots & \dots & \lambda^{p-3}\alpha & \beta & \dots & \dots \\ \dots & \dots & \lambda^{p-2}\alpha & \beta & \dots & \dots \\ \lambda^{p-3}\alpha & \lambda^{p-2}\alpha & \lambda^{p-1}\alpha & \beta & \lambda\beta & \lambda^2\beta \\ \gamma & \gamma & \gamma & x & \cdot & \cdot \\ \dots & \dots & \lambda\gamma & \cdot & \cdot & \cdot \\ \dots & \dots & \lambda^2\gamma & \cdot & \cdot & \cdot \end{array}$$

Applying the recurent rule along the first row and along the first column to be completed yelds:

$$\begin{array}{cccccc} \dots & \dots & \lambda^{p-3}\alpha & \beta & \dots & \dots \\ \dots & \dots & \lambda^{p-2}\alpha & \beta & \dots & \dots \\ \lambda^{p-3}a & \lambda^{p-2}\alpha & \lambda^{p-1}\alpha & \beta & \lambda\beta & \lambda^2\beta \\ \gamma & \gamma & \gamma & \delta & \delta & \delta \\ \dots & \dots & \lambda\gamma & \delta & \cdot & \cdot \\ \dots & \dots & \lambda^2\gamma & \delta & \cdot & \cdot \end{array}$$

where $\delta = (-m)^{p-1}\alpha * m + \beta + \gamma = m^p\alpha + \beta + \gamma = \varphi(m)\alpha + \beta + \gamma$ in $\mathbb{F}_q$. The recurrent rule is linear, so a constant δ row together with a constant δ column generate δF. □

Theorem 4.4 *Recall that $G(d,q,m)$ is the $p^d \times p^d$ matrix computed by the recurrent rule over the finite field $\mathbb{F}_q$ and $F = F(q,m) = G(1,q,m)$ is the fundamental block. Then for all $d \geq 1$:*

$$G(d,q,m) = \varphi^{d-1}(F) \otimes \varphi^{d-2}(F) \otimes \cdots \otimes \varphi(F) \otimes F.$$

Proof: The proof works by induction over d. For $d = 1$ this is true by definition. Suppose that $G(d,q,m)$ fulfills the statement and consider $G(d+1,q,m)$. Being computed by the same recurent rule, the $p \times p$ left upper minor of $G(d+1,q,m)$ is a copy of F. Applying Lemma 4.3 for $(\alpha,\beta,\gamma) = (0,0,1)$ or $(0,1,0)$ one gets that a copy of F continued by a first row of ones $F^{111\ldots1}$ horizontally generates copies of F like $FFFF\ldots F$ and that this happens also vertically if the first column of F is downwards extended with ones. Thus in the block-wise representation of $G(d+1,q,m)$ with $p \times p$ blocks, the first line and the first column consist of copied fundamental blocks:

$$\begin{array}{ccccc} F & F & F & F & \ldots \\ F & b(1,1)F & b(1,2)F & b(1,3)F & \ldots \\ F & b(2,1)F & \cdot & \cdot & \ldots \\ F & b(3,1)F & \cdot & \cdot & \ldots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{array}$$

Here the $b(i,j)$ are such that all $b(k,0) = 1$, $b(0,n) = 1$ and $b(i+1,j+1) = \varphi(m)b(i,j) + b(i+1,j) + b(i,j+1)$. One gets that $G(d+1,q,m) = X \otimes F$ where the matrix X over $\mathbb{F}_q$ satisfies the following conditions: (i) X is a $p^d \times p^d$ matrix, (ii) X has elements $b(i,j)$ as above. This means that $X = G(d,q,m')$ for $m' = \varphi(m)$, so by induction, denoting $F(q,\varphi(m)) = F'$:

$$X = \varphi^{d-1}(F') \otimes \varphi^{d-2}(F') \otimes \cdots \otimes \varphi(F') \otimes F'.$$

Observe that $F' = F(q,\varphi(m)) = \varphi(F(q,m)) = \varphi(F)$ because φ is an automorhism and one applies φ inductively. We hold:

$$X = \varphi^{d}(F) \otimes \varphi^{d-1}(F) \otimes \cdots \otimes \varphi^2(F) \otimes \varphi(F).$$

We substitute this X in $G(d+1,q,m) = X \otimes F$ and we are done. □

Corollary 4.5 *Let $\mathbb{F}_q$ be a finite field of characteristic p and $m \in \mathbb{F}_q$ such that the fundamental block $F(q,m) \in \mathcal{M}_{p\times p}(\mathbb{F}_q)$ contains at least a zero. In this case the set $\mathcal{G}(q,m)$ exists as $\lim_{d\to\infty} \mathcal{G}(d,q,m)$ and is self-similar.*

Proof: For any matrix A over $\mathbb{F}_q$, let $\delta(A)$ be the matrix obtained by substituting every non-zero element with one. Let $\iota(B)$ be the set associated with the matrix B. Then:

$$\mathcal{G}(d,q,m) = \iota\delta(G(d,q,m) = \iota\delta(\bigotimes_{i=d-1}^{0} \varphi^i(F)) = \iota(D^{\otimes d}),$$

where $D = \delta(F)$ is a $\{0,1\}$-matrix, $F = F(q,m)$ is the fundamental block, and φ is Frobenius' automorphism extended for matrices. Now the principle of substitution works. □

Lemma 4.6 *If $\mathbb{F}_q$ is the prime field $\mathbb{F}_p$ and $m \in \mathbb{F}_p$, the fundamental block $F(p,m)$ contains zeros if and only if $m \neq -1$. In this situation it contains in the row $i = 1$ exactly one zero:*

$$a(1,k) = 0 \;\leftrightarrow\; \mathbb{F}_p \models k = -(m+1)^{-1}.$$

Note: in general there are many other zeros in the fundamental block.

Proof: The element $a(1,k) = km + (k+1) = k(m+1) + 1$ which is zero only for $k = -(m+1)^{-1}$. This element exists if and only if $m \neq -1$ in $\mathbb{F}_p$. Every corresponding k has a representative between 1 and $p-1$ inclusively. If $m = -1$ the matrix $F(p,-1)$ contains only ones. □

Now the main result follows from Remark 3.3 and from the Lemma 4.4:

Corollary 4.7 *For all primes p and all $m \in \mathbb{F}_p \setminus \{-1\}$ the set $\mathcal{G}(p,m)$ is self-similar. For $m = -1$ the set $\mathcal{G}(p,m)$ is the full square.*

Corollary 4.8 *The Pascal Triangle modulo p is the set $\mathcal{G}(p,0)$. The Passoja-Lakhtakia Carpet modulo p is the set $\mathcal{G}(p,1)$. Consequently, both sets are self-similar.*

Example 4.9 The following example shows the matrix $G(2,3,1)$ which is a step in the construction for the celebrated Sierpinski Carpet $\mathcal{G}(3,1)$. For the first citation concerning Sierpinski's Carpet, see [11]. The zeros are not displayed.

$$\begin{array}{cccccccccc}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & & -1 & 1 & & -1 & 1 & & -1 \\
1 & -1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 \\
1 & 1 & 1 & & & & -1 & -1 & -1 \\
1 & & -1 & & & & -1 & & 1 \\
1 & -1 & 1 & & & & -1 & 1 & -1 \\
1 & 1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 \\
1 & & -1 & -1 & & 1 & 1 & & -1 \\
1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1
\end{array}$$

5 Multiplicative inverse means mirroring

Definition 5.1 For a matrix A we define the mirroring ΣA using the definition of a matrix as a family of column-vectors. If $A = (\vec{a}_1, \ldots, \vec{a}_n)$ then $\Sigma A = (\vec{a}_n, \ldots, \vec{a}_1)$.

Definition 5.2 For $m \neq 0$ we define the operator $\mathcal{O}$ acting on the fundamental block $F(q,m)$ in the following way:

$$\text{For } i = 0 \text{ to } p-1, \text{ one divides the row } i \text{ by } (-m)^i.$$

The result is denoted by $\mathcal{O}F(q,m)$.

Lemma 5.3 *For all finite fields $\mathbb{F}_q$ and for all $m \in \mathbb{F}_q \setminus \{0\}$ the following identity holds:*

$$\mathcal{O}F(q,m) = \Sigma F(q, m^{-1}).$$

Proof: The Lemma follows from the following claims:

1. The first row and the last column of $\mathcal{O}F(q,m)$ consist of ones only.
2. For every connected 2×2 sub-block of $\mathcal{O}F(q,m)$:

$$\begin{array}{cc} A & B \\ C & D \end{array}$$

   is true that $C = m^{-1}B + A + D$.

The first claim follows from Lemma 4.1 and from the definition of the operator $\mathcal{O}$: one divides every row with the corresponding element of the last column.

We prove the second claim. Let $(a,\ b \mid c,\ d)$ be the corresponding elements in $F(q,m)$; they fulfill:

$$d = ma + b + c.$$

Using the definition of $\mathcal{O}F(q,m)$, we see that:

$$A = \mu a, \quad B = \mu b,$$

$$C = (-m)^{-1}\mu c, \quad D = (-m)^{-1}\mu d,$$

where $\mu = (-m)^i$ for some i. It follows that:

$$C = (-m)^{-1}\mu c = (-m)^{-1}\mu(d - ma - b) = (-m)^{-1}\mu d + \mu a - (-m)^{-1}\mu b = D + A + m^{-1}B.$$

□

For the next Corollary recall from the proof of Corollary 4.5 that $\delta F(q, m)$ is the matrix obtained by substituting every element of $F(q, m)$ with 1 if and only if it is $\neq 0$. Recall the notation $F(q, m) = (a(i, j))$. Denote the elements of $F(q, m^{-1})$ with $s(i, j)$.

Lemma 5.4 *The following statements follow directly from Lemma 5.3:*

1. *For all* $0 \leq i, j \leq p - 1$*:*
$$s(i, p - 1 - j) = a(i, j)(-m)^{-i}.$$
2. *For all* $0 \leq i, j \leq p - 1$*:*
$$a(i, j)(-m)^{-i} = a(p - 1 - j, p - 1 - i)(-m)^{j+1-p}.$$
3. *If* $m \in \mathbb{F}_q \setminus \{0\}$ *then:*
$$\delta F(q, m) = \delta\Sigma F(q, m^{-1}) = \Sigma\delta F(q, m^{-1}).$$
4. *If* $m \in \mathbb{F}_q \setminus \{0\}$ *the matrix* $\delta F(q, m)$ *allows two diagonal symmetries.*
5. *If* $m \neq 0$ *and* $F(q, m)$ *contains zeros, then:*
$$\deg(m/\mathbb{F}_p) \leq \frac{p-1}{2}.$$

Proof:

1. This is nothing as Lemma 5.3 written element by element.
2. This is the symmetry of $F(q, m^{-1})$ through its first diagonal: just write the elements of $F(q, m^{-1})$ as functions of the row-number and the corresponding element of $F(q, m)$. Concretely one has:
$$s(i, p - 1 - j) = a(i, j)(-m)^{-i},$$
as in the first statement,
$$s(i, p - 1 - j) = s(p - 1 - j, i),$$
because of the symmetry of $F(p, m^{-1})$ through its first diagonal, and
$$s(p - 1 - j, i) = a(p - 1 - j, p - 1 - i)(-m)^{j+1-p},$$
which is another instance of the first statement. Apply the transitivity.
3. It follows from the first statement:
$$a(i, j) = 0 \ \leftrightarrow \ s(i, p - 1 - j) = 0.$$
4. For the reflexion through the first diagonal it is nothing to prove, because the recurrent law is symmetric. The symmetry through the second diagonal follows from the second statement:
$$a(i, j) = 0 \ \leftrightarrow \ a(p - 1 - j, p - 1 - i) = 0.$$

5. Recall that the set of zeros of the fundamental block $F(q,m)$ is symmetric through both diagonals, so if zeros exist, there will be a zero $a(i,j)$ with at least one coordinate $\leq (p-1)/2$. But the value of $a(i,j)$ is a polynomial in m with coefficients in $\mathbb{F}_p$ and of degree $\min(i,j)$.

□

Example 5.5 The last condition occurring here implies the existence of relatively less values of m generating self-similar sets in arbitrary finite fields that are not whole squares. Look at the case $\mathbb{F}_{19^2} = \mathbb{F}_{361}$ seen as $\mathbb{F}_{19}[x]$ where $x^2+1=0$. Encode the element $ax+b$ in the natural number $19a+b$. We do not mention both m and m^{-1} because they produce mirrored carpets. Also, if m has been already mentioned, we do not mention its Frobenius m^{19}, because it produces the same carpet. So, up to Frobenius and multiplicative inverse, one has non-trivial self-similar carpets over $\mathbb{F}_{361}$ if and only if m is equal with one of the following 29 elements: 0, 1, 2, 3, 4, 6, 7, 8, 9, 14, 19, 21, 35, 47, 52, 53, 56, 63, 69, 76, 78, 88, 92, 102, 130, 136, 137, 148, 168.

6 $\mathbb{F}_p$ as a field of self-similar carpets

6.1 Symmetry groups

For studying the groups of symmetries of the set $\mathcal{G}(p,m)$ is enough to understand the symmetries for the fundamental block $F(p,m)$. All groups of symmetries we are looking for are subgroups of the dihedral group of symmetries D_8 of the square.

Definition 6.1 The dihedral group D_{2n} is the group with presentation:

$$\langle r, f \mid r^n = 1, f^2 = 1, frf = r^{-1} \rangle,$$

and is the group of symmetries of the regular polygon with n sides. The generators r and f are the rotation with angle $2\pi/n$ and the reflection through the x-axis. The group has $2n$ elements.

The group with two elements S_2 can be embeded in D_8 as subgroup generated by f or every other reflexion. Klein's group K_4 is the four-element group $S_2 \times S_2$. One can embed K_4 in D_8 as subgroup generated by the reflexions through the diagonals of the square.

We start with the most non-symmetric case, the case of Pascal's Triangle:

Lemma 6.2 *If $m = 0$ the group of symmetries consists of two elements: the identity and the reflection through the first diagonal.*

Proof: In $F(p,0)$ for $0 \leq i,j \leq p-1$:

$$a_{i,j} = 0 \ \leftrightarrow \ p \,|\, f(i,j) = \binom{i+j}{i} \ \leftrightarrow \ i+j \geq p.$$

So exactly the elements situated strictly below the second diagonal are 0 and all other elements are $\neq 0$. □

Theorem 6.3 *Let p be a prime.*

1. *$\mathcal{G}(p,0)$: the Pascal Triangle modulo p is symmetric through the first diagonal only and has a group of symmetries isomorphic with S_2.*
2. *$\mathcal{G}(p,1)$: the Passoja-Lakhtakia Carpet modulo p has the group D_8 as group of symmetries.*

3. *$\mathcal{G}(p,-1)$: the full square has the group D_8 as group of symmetries.*

4. *If $p \geq 5$ and $m \in \mathbb{F}_p \setminus \{-1,0,1\}$, $\mathcal{G}(p,m)$ is a self-similar set whose group of symmetries is generated by the reflexions through the diagonals of the unit square and is isomorphic with Klein's group K_4.*

Proof: The case $m = 0$ follows completely from Lemma 6.2. Let now $m \in \mathbb{F}_p \setminus \{0\}$, let K be the group generated by the symmetries through the both diagonals (isomorphic with Klein's group K_4) and let G be the group of symmetries of $\mathcal{G}(p,m)$. From Lemma 5.4 it follows that $K \leq G \leq D_8$. If $m = -1$ then $\mathcal{G}(p,-1)$ is the full square and trivially $G = D_8$. If $m = 1$ than it follows from Lemma 5.4 that:

$$\delta F(p,1) = \Sigma \delta F(p,1),$$

so G contains also the reflexion through the vertical median of the square and is strictly bigger than K. But K has already 4 elements, hence $G = D_8$.

Conversely, suppose that $G = D_8$. We exclude the trivial case $m = -1$. From Lemma 6.2 it follows that $m \neq 0$. From Lemma 4.6 it follows that $F(p,m)$ has only a zero in the second row ($i = 1$), which is $a(1,k) = 0$ for a $0 < k < p-1$ such that $k = -(m+1)^{-1}$ in $\mathbb{F}_p$. If $a(1,k)$ is not the central element of the row $i = 1$ then there would be two zeros in this row: $a(1,k)$ and its mirored image through Σ, which is a contradiction with Lemma 4.6. It follows that $-(m+1)^{-1} = (p-1)/2$ in $\mathbb{F}_p$, so $(m+1)^{-1} = 2^{-1}$ and $m = 1$. □

Corollary 6.4 *If $p > 3$ and $m \in \mathbb{F}_p \setminus \{-1\}$ there are at least two zeros in $F(p,m)$.*

Proof: In fact one can prove a little bit more. If $m \in \{-2, -2^{-1}\}$ then the unique zero of the second row $i = 1$ lies on the intersection of this row with one of the diagonals, so its orbit under the action of G has two elements. If $m \in \mathbb{F}_p \setminus \{-2, -2^{-1}, -1, 0\}$ then the orbit has four elements.

□

In fact for the case $m = 0$ the existence of many zeros is evident. For $m \in \{-2, -2^{-1}, 1\}$ we prove in the next sub-sections that in general there are much more zeros than four.

6.2 Diagonal Carpets

For $m = -2$ one has $a(1,1) = 0$. In the looking glass, for $m = -2^{-1}$ one has $a(1,p-2) = 0$. We prove that in these cases all the elements of odd index on the corresponding diagonal are zero.

Definition 6.5

$$D^+ = \{(i,i) \mid 0 < i < p-1 \ \wedge \ 2 \not| i\}.$$
$$D^- = \{(i,j) \mid i + j = p-1 \ \wedge \ 2 \not| i\}.$$

Theorem 6.6 *If $p \geq 5$ be a prime, then:*

1. *In $F(p,-2)$ if $(i,i) \in D^+$ then $a(i,i) = 0$.*

2. *In $F(p,-2^{-1})$ if $(i,j) \in D^-$ then $a(i,j) = 0$.*

3. *The elements with even coordinates on the respective diagonals are all different from 0.*

Proof:

1. We prove that for $m = -2 \in \mathbb{Z}$ the recurrent function $f : \mathbb{N} \times \mathbb{N} \to \mathbb{Z}$ defined in Section 2 has the property $f(2s+1, 2s+1) = 0$ for all $s \in \mathbb{N}$. This follows from the following identity:

$$\sum_{a=0}^{n} \binom{n}{a} \binom{2n-a}{n-a} (-2)^a = \begin{cases} (-1)^s \binom{2s}{s}, & \text{if } n = 2s, \\ 0, & \text{if } n = 2s+1. \end{cases}$$

   This identity can be proved using Zeilberger's Algorithm, see [9] and [4]. In fact, after running the software from [4], one gets the recurrent formula:

$$4(n+1)S(n) + (n+2)S(n+2) = 0,$$

   where $S(n)$ is the sum on the left side of the equality. Starting with $S(0) = 1$ and $S(1) = 0$ one gets the result by induction. The author thanks Prof. Dr. Wolfram Koepf for kindly running his Maple package "Hypergeometric Summation" at author's request. Please note that this identity is not the Reed - Dawson Identity, although similar. Our identity seems to have been previously unknown.

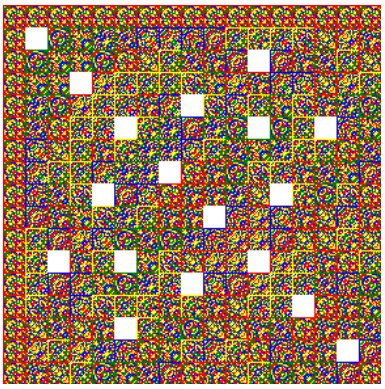
2. This follows from the case $m = -2$ and from Lemma 5.3. Note that the corresponding values of $f(n, k)$ are no more 0 in $\mathbb{Z}$ but become 0 in $\mathbb{F}_p$.

3. For n even, $f(n, n)$ is not divisible by p. □

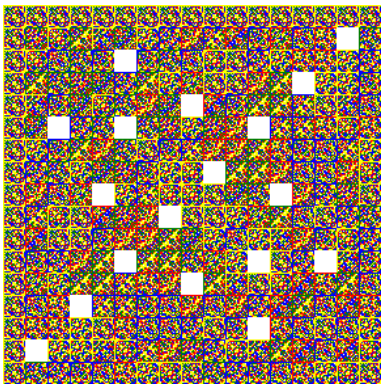
We note that those are not the only zeros in general: starting with $p = 11$ there are a lot of other zeros for $m \in \{-2, -2^{-1}\}$. One can now also prove a slight improvement of 6.4:

Corollary 6.7 *Let $m \neq -1$. For $p = 7$ there are at least three zeros in $F(p, m)$, and for $p \geq 11$ there are at least four zeros in $F(p, m)$.*

Proof: The only one problem was $m \in \{-2, -2^{-1}\}$, which is now trivial applying Theorem 6.6. □



$\mathcal{G}(2, 17, 15)$. Observe that $15 = -2$ in $\mathbb{F}_{17}$.



$\mathcal{G}(2, 17, 8)$. Observe that $8 = -2^{-1}$ in $\mathbb{F}_{17}$.

6.3 Passoja-Lakhtakia Carpets

The only one fully symmetric case with p odd and $m = 1$ is worth for a closer look.

Definition 6.8 Call $N = \{(i, j) \,|\, a(i, j) = 0\}$ the set of zeros of $F(p, 1)$. The set:

$$C = \{(\frac{p-1}{2}, i)\,;\, (i, \frac{p-1}{2}) | \, 0 \leq i \leq p-1 \ \wedge \ 2 \not| i\}$$

shall be called the Cross, and $S = N \setminus C$ shall be called the set of sporadic zeros. We call the elements of the cross regular zeros.

We see now that the elements of the Cross are really zeros of $F(p, 1)$.

Corollary 6.9 *If p is an odd prime, the fundamental block $F(p, 1)$ has the following properties:*

1. *For all $0 \leq k \leq p-1$:*
$$a(p-1, k) = (-1)^k.$$
2. *For all n and k with $0 \leq n, k \leq p-1$,*
$$a(n, k) = (-1)^n a(n, p-1-k).$$
3. *The Cross C consists of zeros of $F(p, 1)$.*

Proof:

1. This is exactly Lemma 4.1.
2. According to Lemma 5.3,
$$\mathcal{O}F(p, 1) = \Sigma F(p, 1).$$
If $k = 2s$, $\mathcal{O}$ operates by multiplication with 1, so the even rows are centrally symmetric. If $k = 2s + 1$, $\mathcal{O}$ operates by multiplication with -1, so odd rows are antisymmetric.
3. This follows easily from the last statement because for k and p odd:
$$a(k, \frac{p-1}{2}) = (-1)^k a(k, (p-1) - \frac{p-1}{2}) = -a(k, \frac{p-1}{2}),$$
implies $a(k, \frac{p-2}{2}) = 0$. Apply now the symmetry of $\delta F(p, 1)$. □

Example 6.10 Here one sees only the border and the zeros of $F(13,1)$:

$$\begin{array}{cccccccccccccc}
+1 & +1 & +1 & +1 & +1 & +1 & +1 & +1 & +1 & +1 & +1 & +1 & +1 & +1 \\
+1 & \cdot & \cdot & \cdot & \cdot & \cdot & 0 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & -1 \\
+1 & \cdot & 0 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 0 & \cdot & \cdot & +1 \\
+1 & \cdot & \cdot & \cdot & \cdot & \cdot & 0 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & -1 \\
+1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & +1 \\
+1 & \cdot & \cdot & \cdot & \cdot & \cdot & 0 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & -1 \\
+1 & 0 & \cdot & 0 & \cdot & 0 & \cdot & 0 & \cdot & 0 & \cdot & 0 & \cdot & +1 \\
+1 & \cdot & \cdot & \cdot & \cdot & \cdot & 0 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & -1 \\
+1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & +1 \\
+1 & \cdot & \cdot & \cdot & \cdot & \cdot & 0 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & -1 \\
+1 & \cdot & 0 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 0 & \cdot & \cdot & +1 \\
+1 & \cdot & \cdot & \cdot & \cdot & \cdot & 0 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & -1 \\
+1 & -1 & +1 & -1 & +1 & -1 & +1 & -1 & +1 & -1 & +1 & -1 & +1 & -1 & +1
\end{array}$$

For the primes $p = 3$, 5, 7, 11, 19 there are only regular zeros in $F(p,1)$. 13 is the first odd prime with sporadic zeros, followed by 17. By all other primes tried out by the author there are lots of sporadic zeros in the fundamental block $F(p,1)$.

7 Commentaries

1. According to [2] the Kronecker product of matrices was called so by K. Hensel in [1] where he said that he had learnt it in Kronecker's lectures. Kronecker seems to have never published something about it. The first known appearance of this matrix product in the literature was in a paper by J. G. Zehfuß in [14].

2. Can we better understand the sporadic zeros for $\mathbb{F}_p$ and $m = 1$? The same question for $\mathbb{F}_q$ and arbitrary $m \in \mathbb{F}_q$.

3. Is it true that two zeros of the fundamental block cannot have a common edge? The fundamental block contains sometimes neighbors with common edge and equal value: take for example $\mathbb{F}_{11}$ and $m = 1$, where $a_{4,2} = a_{4,3} = a_{3,3} = a_{3,4} = 8$. The author found some cases of zeros with common vertex in a fundamental block, but no case with common edge.

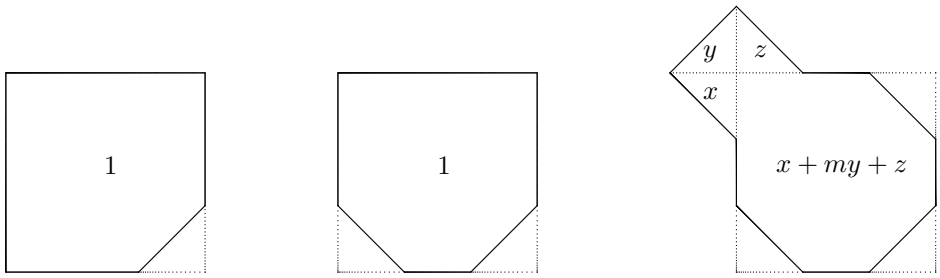
4. Sets $\mathcal{G}(d,q,m)$ can be graphically represented if one associates a list of colours to the elements of $\mathbb{F}_q$. One can define per default that white corresponds to 0. Call this representation a coloured carpet.

5. $\mathcal{G}(d,p,1)$ has a symmetrical representation with colours if the list of colours satisfies:

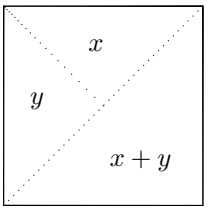
$$\forall\, k \in \mathbb{F}_p \ \mathrm{color}(k) = \mathrm{color}(p-k).$$

   This follows from the Corollary 6.9.

6. Coloured carpets can be also realized as tilings using for $m \neq 0$ following coloured tiles,



and for $m = 0$ following coloured tiles:



7. For some integer n with prime-decomposition $n = p_1^{k_1} \dots p_s^{k_s}$, the ring $\mathbb{Z}/n\mathbb{Z}$ is isomorphic with the product of finite rings $\mathbb{Z}/p_1^{k_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p_s^{k_s}\mathbb{Z}$. From this reason, coloured carpets over $\mathbb{Z}_n$ are overlappings of carpets modulo p^k. Can we understand the carpets modulo prime-powers? Experiments show that they are generally not self-similar and that they have a very sophisticated structure.

References

[1] **K. Hensel**: *Über Gattungen, welche durch Composition aus zwei anderen Gattungen entstehen.* Crelle Journal 105, 329 - 344, 1889.

[2] **Harold V. Henderson, Friedrich Pukelsheim, Shayle R. Searle** *On the history of the Kronecker product.* Journal of Linear and Multilinear Algebra 14, 113 - 120, 1983.

[3] **Jarkko Kari**: *Theory of cellular automata: A survey.* Theoretical Computer Science 334, 3 - 33, 205.

[4] **Wolfram Koepf**: *Hypergeometric Summation. An Algorithmic Approach to Summation and Special Function Identities.* Vieweg, Braunschweig/Wiesbaden, 1998. http://www.mathematik.uni-kassel.de/ koepf/hyper.html

[5] **Benoit B. Mandelbrot**: *The fractal geometry of nature.* W. H. Freeman and Company, San Francisco, 1977, 1982.

[6] **Dann E. Passoja, Akhlesh Lakhtakia**: *Carpets and rugs: an exercise in numbers.* Leonardo, 25, 1, 1992, 69 - 71.

[7] **Dann E. Passoja, Akhlesh Lakhtakia**: *Variations on a Persian theme.* Journal of Recreational Mathematics, 24, 1, 1 - 5, 1992.

[8] **Mihai Prunescu**: *Undecidable properties of recurrent double sequences.* Notre Dame Journal of Formal Logic, 49, 2, 143 - 151, 2008.

[9] **Marko Petkovsek, Herbert Wilf and Doron Zeilberger**: $A = B$. A K Peters. Ltd, 1997. http://www.cis.upenn.edu/ wilf/AeqB.html.

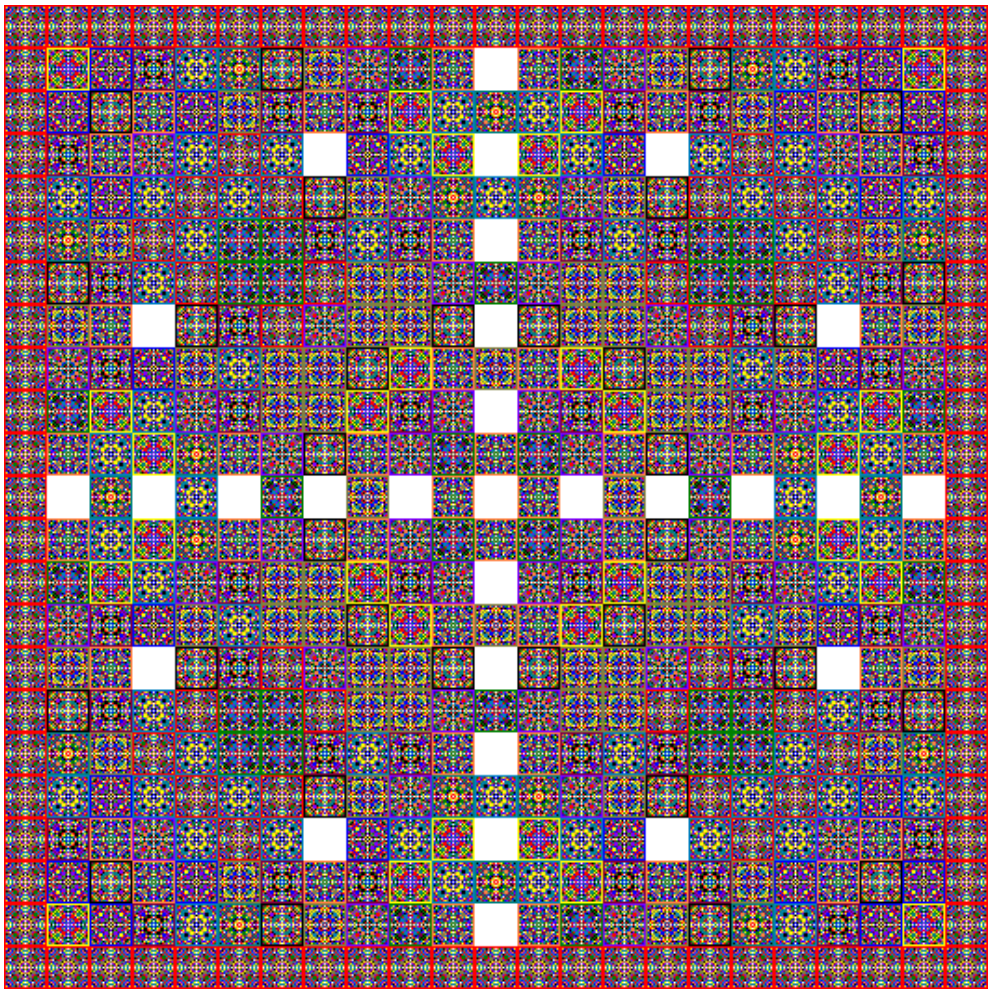
[10] **N. J. Rose**: *The Pascal triangle and Sierpinski's tree.* Mathematical Calendar, Releigh, N. C, Rome Press, 1981.

[11] **Waclaw Sierpinski**: *Sur une courbe cantorienne qui contient une image biunivoque et continue de toute courbe donne.* C. R. Acad. Sci, Paris, Sr. 162, 629, 1916.

[12] **Herbert S. Wilf**: *Generatingfunctionology.* Academic Press, 1990, 1994.

[13] **Stephen J. Willson**: *Cellular automata can generate fractals.* Discrete Applied Mathematics, 8, 1984, 91 - 99.

[14] **J. G. Zehfuß**: *Über eine gewisse Determinante.* Zeitschrift für Mathematik und Physik, 3, 298 - 301, 1858.



$\mathcal{G}(2, 23, 1)$ coloured such that $\forall\, k \in \mathbb{F}_{23}$ $\;\text{colour}(k) = \text{colour}(23 - k)$.