Combinatorial Relationship Between Finite Fields and Fixed Points of Functions Going Up and Down

Emerson León, Julián Pulido

June, 2023

Abstract

Abstract We explore a combinatorial bijection between two seemingly unrelated topics: the roots of irreducible polynomials of degree m over a finite field $\mathcal{F}_p$ for a prime number p and the number of points that are periodic of order m for a continuous piece-wise linear function $g_p : [0,1] \to [0,1]$ that *goes up and down p times* with slope $\pm p$.

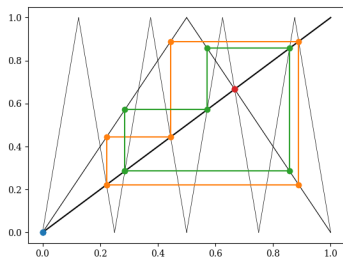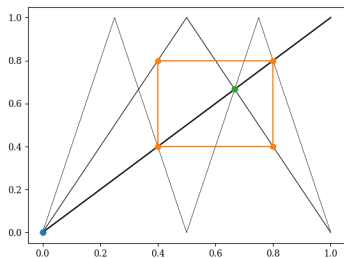- ▶ Combinatorial Relationship
- ▶ Explicit bijection B_α
  - ▶ The permutation π_{p^n}
  - ▶ Main theorem
- ▶ Generalizations:
  - ▶ Homeomorphisms
  - ▶ Other up and down patterns

Functions going up and down

Let $g_p : [0, 1] \rightarrow [0, 1]$ a continuous function piecewise linearly defined on the intervals $I_k := \left[\frac{k}{p}, \frac{k+1}{p}\right]$ for $0 \leq k \leq p - 1$, with I_k increasing from 0 to 1 for k even, and linearly decreasing from 1 to 0 on I_k for k odd.

Denote by g_p^n to the function obtained by taking g_p composed with itself n times. g_p^n has p^n fixed points.

A point x is called to be *periodic of order m* if $g_p^m(x) = x$, and $g_p^i(x) \neq x$ for $i = 1, 2, \ldots, m - 1$.

Example: Functions g_2, g_2^2 and g_2^3 with its fixed points.

Combinatorial Relationship

Theorem
The number $J_p(m)$ of points $x \in \mathrm{FP}(g_p^m)$ periodic of order m is equal to the number of roots of monic irreducible polynomials of degree m over the finite field $\mathcal{F}_p$.

Proof.
Both values can be computed by Möbius inversion formula. They satisfy the relation $\sum_{d|n} J_p(d) = \sum_{d|n} m I_p(d) = p^n$, in both cases (where $I_p(m)$ denotes the number of irreducible polynomials of degree m over $\mathcal{F}_p$ and the sum represent all elements of $\mathcal{F}_{p^n}$.) Then we find that $J_p(m) = m I_p(m) = \sum_{d|n} \mu(n/d) p^d$. $\qquad\qquad\square$

Corollary
There is a bijection $B : \mathrm{FP}(g_p^n) \to \mathcal{F}_{p^n}$, such that $B(x)^p = B(g_p(x))$ for every $x \in \mathrm{FP}(g_p^n)$.

We provide here one such bijection, connecting some of the structure of both worlds.

Bijection via permutation π_{p^n}

We want to get a bijective proof. For this we construct a permutation map $\pi_{p^n} : \{0, 1, \ldots, p^n - 1\} \to \{0, 1, \ldots, p^n - 1\}$ that help us to create our bijection B, as follows:

Definition

Take π_{p^1} the identity map from 0 to $p - 1$. Then if $ap^{n-1} \leq k < (a+1)p^{n-1}$,

$$\pi_{p^n}(k) = \begin{cases} \pi_{p^{n-1}}(k - ap^{n-1}) + ap^{n-1} & \text{for } a \text{ even} \\ \pi_{p^{n-1}}(p^{n-1} - (k - ap^{n-1}) - 1) + ap^{n-1} & \text{for } a \text{ odd.} \end{cases}$$

Some examples for $p = 2$ and $p = 3$ of how π_{p^n} permute the numbers $0, 1, \ldots, p^n - 1$:

$\pi_{2^1} : 0, 1$
$\pi_{2^2} : 0, 1, 3, 2$
$\pi_{2^3} : 0, 1, 3, 2, 6, 7, 5, 4$
$\pi_{2^4} : 0, 1, 3, 2, 6, 7, 5, 4, 12, 13, 15, 14, 10, 11, 9, 8$

Main Theorem

Definition (Bijection B_α)

Let α be a primitive root (i. e. a generator of the multiplicative group) of $\mathcal{F}_{p^n}$ and $0 = x_0 < x_1 < \cdots < x_{p^n-1}$ be the fixed points of g_p^n. We define the bijection $B_\alpha : \mathrm{FP}(g_p^n) \to \mathcal{F}_{p^n}$ by $B_\alpha(x_0) = 0 \in \mathcal{F}_{p^n}$ or $B_\alpha(x_k) = \alpha^{\pi_{p^n}(k)}$ for all other $k > 0$.

Theorem

The function B_α is a bijection such that $(B_\alpha(x_k))^p = B_\alpha(g_p(x_k))$ for any fixed point $x_k \in \mathrm{FP}(g_p^n)$.

Proposition

The bijection $B_\alpha : \mathrm{FP}(g_p^n) \to \mathcal{F}_{p^n}$ satisfy that $B_\alpha(x_i)B_\alpha(x_j) = B_\alpha(x_r)$ with

$$r = \pi_{p^n}^{-1}((\pi_{p^n}(i) + \pi_{p^n}(j)) \mod p^n - 1),$$

for any $0 < i, j < p^n$, where the class representative modulo $p^n - 1$ must be taken from 1 to $p^n - 1$.

Bijection B_α for $p = 2$, $n = 4$, and $\alpha^4 + \alpha + 1 = 0$ in $\mathcal{F}_{2^4}$

| i	x_i	$g_p(x_i)$	$\pi_{p^n}(i)$	$B_\alpha(x_i)$
0	0.0	0.0	0	0
1	0.1176470588	0.2352941176	1	α
2	0.1333333333	0.2666666666	3	α^3
3	0.2352941176	0.4705882352	2	α^2
4	0.2666666666	0.5333333333	6	$\alpha^3 + \alpha^2$
5	0.3529411764	0.7058823529	7	$\alpha^3 + \alpha + 1$
6	0.4	0.8	5	$\alpha^2 + \alpha$
7	0.4705882352	0.9411764705	4	$\alpha + 1$
8	0.5333333333	0.9333333333	12	$\alpha^3 + \alpha^2 + \alpha + 1$
9	0.5882352941	0.8235294117	13	$\alpha^3 + \alpha^2 + 1$
10	0.6666666666	0.6666666666	15	1
11	0.7058823529	0.5882352941	14	$\alpha^3 + 1$
12	0.8	0.3999999999	10	$\alpha^2 + \alpha + 1$
13	0.8235294117	0.3529411764	11	$\alpha^3 + \alpha^2 + \alpha$
14	0.9333333333	0.1333333333	9	$\alpha^3 + \alpha$
15	0.9411764705	0.1176470588	8	$\alpha^2 + 1$
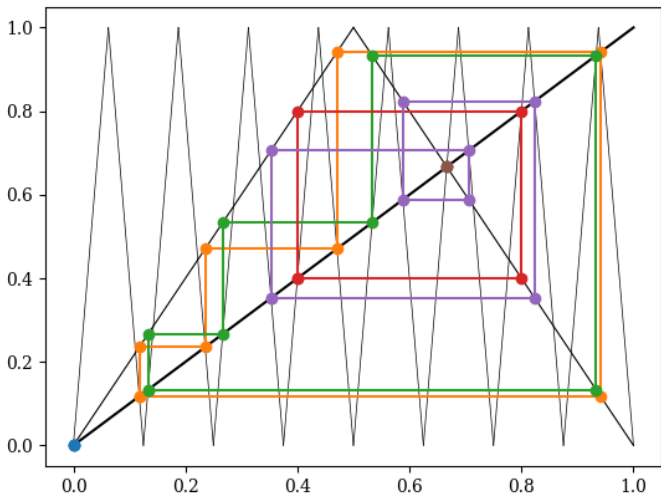
Example: Function g_2^4 with its fixed points.

More examples: p=3

$\pi_{3^1} : 0, 1, 2$

$\pi_{3^2} : 0, 1, 2, 5, 4, 3, 6, 7, 8$

$\pi_{3^3} : 0, 1, 2, 5, 4, 3, 6, 7, 8, 17, 16, 15, 12, 13, 14, 11, 10, 9,$
$\qquad 18, 19, 20, 23, 22, 21, 24, 25, 26$
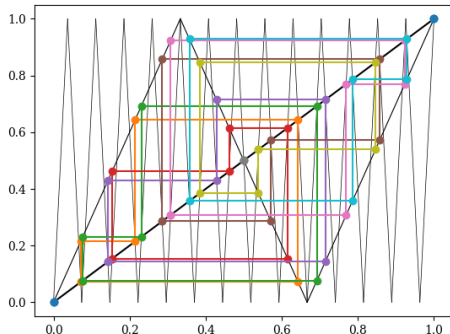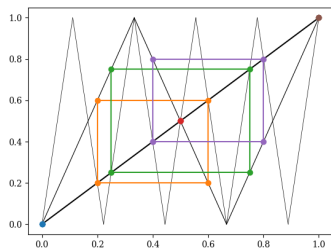
Example: Functions g_3, g_3^2 and g_3^3 with its fixed points.

g_p and its periodic points in base p

To prove the main theorem we need to understand g_p, its periodic points, and π_{p^n} in *base p*, .

Proposition

If $x = \sum_{i \geq 1} \frac{a_i}{p^i}$ for $0 \leq a_i \leq p - 1$, then

$$g_p(x) = \begin{cases} \sum_{i \geq 1} \frac{a_{i+1}}{p^i}, & \text{if } a_1 \text{ is even.} \\ \sum_{i \geq 1} \frac{p-1-a_{i+1}}{p^i}, & \text{if } a_1 \text{ is odd.} \end{cases}$$

Proposition

Let $x_0 < x_1 < \ldots < x_{p^n-1}$ be the fixed points of the function g_p^n. Then, for $k < p^n$ we have that $x_k = \frac{k}{p^n-1}$ if k is even, or $x_k = \frac{k+1}{p^n+1}$ if k is odd.

g_p and its periodic points in base p

Proposition

The expression in base p of $x = \frac{k}{p^n - 1}$ is periodic, where the first n digits represent k in base p and $a_{n+i} = a_i$. Also, if $x = \frac{k+1}{p^n + 1}$, its expression in base p has period $2n$, where the first n digits represent k in base p, while the next n digits are complementary of the first n digits, that is $a_{n+i} = p - 1 - a_i$.

Example

The function g_2 permutes the fixed points in $\mathrm{FP}(g_2^3)$ as follows:

$$0.\overline{000}_2 \to 0.\overline{000}_2$$
$$0.\overline{001110}_2 \to 0.\overline{011100}_2 \to 0.\overline{111000}_2 \to 0.\overline{001110}_2$$
$$0.\overline{010}_2 \to 0.\overline{100}_2 \to 0.\overline{110}_2 \to 0.\overline{010}_2$$
$$0.\overline{101010}_2 \to 0.\overline{101010}_2$$

π_{p^n} in base p

Proposition

If $k = (a_1 a_2 \ldots a_n)_p$ (where $k < p^n$), then $\pi_{p^n}(k) = (b_1 b_2 \ldots b_n)_p$ where $b_1 = a_1$, and $b_i = a_i$ when $b_1 + \cdots + b_{i-1}$ is even or $b_i = p - 1 - a_i$ when $b_1 + \cdots + b_{i-1}$ is odd.

Notice that for p odd, taking $p - 1$ complement doesn't change the parity of the digits, and therefore we could use the parity of $a_1 + \cdots + a_{i-1}$ to create the two cases in the previous proposition. In case $p = 2$ things are a little bit different.

Proposition

If $p = 2$ and $i = (a_1 a_2 \ldots a_n)_2$, then $\pi_{p^n}(i) = (b_1 b_2 \ldots b_n)_2$ where $b_1 = a_1$, and $b_i = 0$ if $a_{i-1} = a_i$ or $b_i = 1$ otherwise.

Sketch of Proof of the Main Theorem

We need to check that $(B_\alpha(x_k))^p = B_\alpha(g_p(x_k))$ for any $x_k \in \mathrm{FP}(g_p^n)$. We can analyze every step in base p to check that the following diagram commutes, where fr is the Frobenius Map $fr : x \mapsto x^p$.

$$
\begin{array}{ccc}
\mathrm{FP}(g_p^n) & \xrightarrow{\ B_\alpha\ } & \mathcal{F}_{p^n} \\
{\scriptstyle g_p}\downarrow & & \downarrow{\scriptstyle fr} \\
\mathrm{FP}(g_p^n) & \xrightarrow[\ B_\alpha\ ]{} & \mathcal{F}_{p^n}
\end{array}
$$

If $k = (a_1 \ldots a_n)_p < p^n$, then $x_k = (0.\overline{a_1 \ldots a_n a_1' \ldots a_n'})_p$ where $a_i' = a_i$ in case that $(a_1 \ldots a_n)_p$ is even, or $a_i' = p - 1 - a_i$ if $(a_1 \ldots a_n)_p$ is odd.

Denote $\pi_{p^n}(k) = (b_1 b_2 \ldots b_n)_p$,. Then $b_1 = a_1$, and $b_i = a_i$ when $b_1 + \cdots + b_{i-1}$ is even or $b_i = p - 1 - a_i$ when $b_1 + \cdots + b_{i-1}$ is odd.

Also $(B_\alpha(x_k))^p = \alpha^{p(b_1 \ldots b_n)_p} = \alpha^{(b_1 \ldots b_n 0)_p} = \alpha^{(b_2 \ldots b_n b_1)_p}$, since $\alpha^{p^n} = \alpha$ in the finite field $\mathcal{F}_{p^n}$.

We need to consider two cases, depending if a_1 is even or odd.

Also cases depending if $p = 2$ or p is odd...

Generalizations: Other functions going up and down

We want to extend our Theorem to other functions $f_p : [u, v] \to [u, v]$ going up and down p times. We restrict to the case that there is a continuous bijection $h : [0, 1] \to [u, v]$ that is a homeomorphism between both functions g_p and f_p (so that $f_p \circ h = h \circ g_p$). In this case we can easily extend our results to f_p as well.

Theorem

If $f_p : [u, v] \to [u, v]$ is such that there is a continuous bijection $h : [0, 1] \to [u, v]$ so that $f_p \circ h = h \circ g_p$, then there is a bijection $B_f : \mathrm{FP}(f_p^n) \to \mathcal{F}_{p^n}$ so that $(B_f(y_i))^p = B_f(f_p(y_i))$ for any fixed point $y_i \in \mathrm{FP}(f_p^n)$.
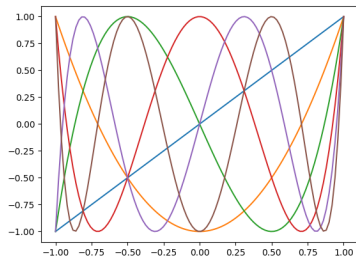
As an example we will see how to extend our results to *Chebyshev Polynomials.*

Example: Chebyshev Polynomials

Definition (Chebyshev polynomials)

The family of Chebyshev polynomials $T_k \in \mathbb{R}[x]$ can be defined recursively by $T_0(x) = 1$, $T_1(x) = x$, and $T_{k+1}(x) = 2xT_k(x) - Tk - 1(x)$.

The next polynomials in the sequence are $T_2(x) = 2x^2 - 1$, $T_3(x) = 4x^3 - 3x$, $T_4(x) = 8x^4 - 8x^2 + 1$, $T_5(x) = 16x^5 - 20x^3 + 5x$, and $T_6(x) = 32x^6 - 48x^4 + 18x^2 - 1$.

Proposition

The Chebyshev polynomial T_n is the expressions for $\cos(n\theta)$ in terms of $\cos(\theta)$, namely it holds that $\cos(n\theta) = T_n(\cos(\theta))$.

Example: Chebyshev Polynomials

Then $T_m \circ T_n = T_{mn}$ and also $T_p^n = T_{p^n}$.
T_m goes up and down m times in the interval [-1,1]

Proposition

The continuous bijection $h : [0,1] \to [-1,1]$ is given by
$h(x) = \cos(\pi x)$. It holds that $T_p \circ h = h \circ g_p$ for any value of p.

Theorem

There is a bijection $B_f : \mathrm{FP}(T_p^n) \to \mathcal{F}_{p^n}$ so that
$(B_f(y_i))^p = B_f(T_p(y_i))$ for any fixed point $y_i \in \mathrm{FP}(T_p^n)$.
If $x_i \in FP(g_{p^n})$ then $y_i = h(x_i) = \cos(\pi x_i) \in FP(T_{p^n}(x) - x)$.

Corollary

If p is odd, then $T_p^n(x) - x =$
$2^{p^n-1}(x-1) \prod_{k=1}^{(p^n-1)/2} \left(x - \cos\left(\frac{(2k-1)\pi}{p^n+1} \right) \right) \left(x - \cos\left(\frac{2k\pi}{p^n-1} \right) \right).$

Generalization: piecewise linear functions going up or down

Definition
Let p be a prime number, and $I \subseteq \{0, 1, 2, \ldots, p-1\}$. The function $g_{p,I} : [0, 1] \to [0, 1]$ given by

$$g_{p,I}(x) = \begin{cases} px - k, & \text{for } \frac{k}{p} \leq x < \frac{k+1}{p} \text{ with } k \in I. \\ k + 1 - px, & \text{for } \frac{k}{p} \leq x < \frac{k+1}{p} \text{ with } k \notin I. \end{cases}$$

In this case $g_{p,I}$ is a piece-wise linear function where I denotes the set of indices k where $g_{p,I}$ is increasing.

If I are all even numbers, then $g_{p,I} = g_p$. If I includes all indices, then $g_{p,I} = \{px\}$ (the fractionary part of px).

Definition
The set $I_{p^n} \subseteq \{0, 1, 2, \ldots, p^n - 1\}$ is the set of indices where $g_{p,I}^n$ is increasing on the interval $(\frac{k}{p^n}, \frac{k+1}{p^n})$.

We can generalize our theorems for all functions $g_{p,I}$.

Generalization for functions $g_{p,I}$

Definition

The permutation $\pi_{p^n,I}$ is defined recursively as follows: take $\pi_{p^1,I}$ the identity map from 0 to $p-1$. Then to define $\pi_{p^n,I}$, if $ap^{n-1} \leq k < (a+1)p^{n-1}$ take

$$\pi_{p^n,I}(k) = \begin{cases} ap^{n-1} + \pi_{p^{n-1},I}(k - ap^{n-1}) \text{ for } a \in I \\ ap^{n-1} + \pi_{p^{n-1},I}(p^{n-1} - (k - ap^{n-1}) - 1) \text{ for } a \notin I \end{cases}$$

Let α be a primitive root and let $x_0 < x_1 < \cdots < x_{p^n-1}$ be the fixed points of $g_{p,I}^n$. We define $B_{\alpha,I} : \mathrm{FP}(g_{p,I}^n) \to \mathcal{F}_{p^n}$ by $B_\alpha(x_{\pi_{p^n,I}(0)}) = 0 \in \mathcal{F}_{p^n}$ or $B_\alpha(x_k) = \alpha^{\pi_{p^n,I}(k)}$ for all other $k > 0$.

Theorem

The function $B_{\alpha,I}$ is a bijection and satisfy that $B_{\alpha,I}(x_k)^p = B_{\alpha,I}(g_{p,I}(x_k))$ for any fixed point $x_k \in \mathrm{FP}(g_{p,I}^n)$.
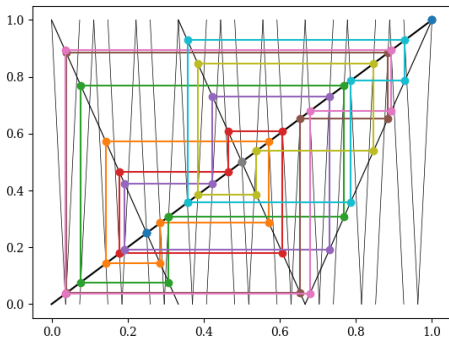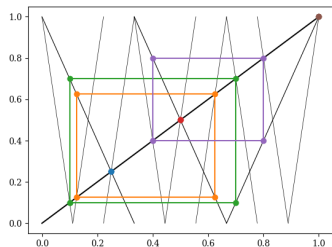
Example: $p = 3$, $I = \{2\}$

For $p = 3$, and $I = \{2\}$, then $\pi_{p^n, I}$ permutes as follows:

$\pi_{3^1, I} : 0, 1, 2$

$\pi_{3^2, I} : 2, 1, 0, 5, 4, 3, 6, 7, 8$

$\pi_{3^3, I} : 8, 7, 6, 3, 4, 5, 0, 1, 2, 17, 16, 15, 12, 13, 14, 9, 10, 11,$
$\quad\quad 20, 19, 18, 23, 22, 21, 24, 25, 26$

Fixed points of $g_{3^2, I}$ and $g_{3^3, I}$, with orbits under $g_{3, I}$.

Thank you!

Article, slides and interactive visualization can be found at
https://emersonjleon.pythonanywhere.com/math