Available online at http://scik.org
J. Math. Comput. Sci. 4 (2014), No. 2, 226-245
ISSN: 1927-5307

$\mathbf{Q_p}$-POLYNOMIAL ISOMETRIES OF $\mathbf{Z_p}$

MARTIAL AUFRANC

Académie d'Orléans-Tours, Lycée Pothier, Orléans 45000, France

Abstract. This paper is devoted to polynomial isometries of $\mathbf{Z}_p$ with coefficients in $\mathbf{Q}_p$. We reduce the study of such a map to finite numbers of polynomial bijections and of polynomial isometries of $\mathbf{Z}_p$ with coefficients in $\mathbf{Z}_p$, which are well-known. These numbers do not depend on the degree of the polynomial but on its "order", which we introduce here.

Keywords: p-adic analysis; isometries; polynomials; ultrametric spaces.

2010 AMS Subject Classification: 28D05, 13B25.

1. Introduction

If a set is an integral domain with an absolute value, we can compare isometries and polynomial maps. Isometries of $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$ and $\mathbf{C}$ are simple. Several authors have studied non-polynomial isometries and various types of maps in p-adic Analysis and Fractal Geometry (see for example [1,2,4,5,7,8,9]). Bishop [3] proved that all polynomial isometries of $\mathbf{Q}_p$ have degree one and characterized them.

Polynomial isometries of $\mathbf{Z}_p$ (with coefficients in $\mathbf{Z}_p$) are really more interesting ; for example, almost any degree is possible, even with coefficients in $\mathbf{F}_p$. They are classified relatively to

Received February 8, 2014

corresponding polynomial bijections and irreducible polynomials on $\mathbf{F}_p$ (see [1,2] and section 3). Roughly, this criterium is about the behaviors of the polynomial and its derivative on $\mathbf{F}_p$: we say that the complexity is 0.

Now, let f be a polynomial isometry of $\mathbf{Z}_p$ with coefficients in $\mathbf{Q}_p$. Recall that $\mathbf{Z}_p$ is a union of p disjoint balls. On each ball, f induces a map that preserves distances, and so we naturally deduce new polynomial isometries of $\mathbf{Z}_p$. This process will be successful if we obtain polynomials with coefficients in $\mathbf{Z}_p$ after a finite number of steps. In section 4.3, we reformulate f and define its order, which is the main tool to prove this result (section 4.5). Moreover, it gives an evaluation of the complexity of f (which is the number of steps used to study f); in particular, we establish in section 4.9 that the complexity is, asymptotically, a logarithmic function of the order. At the same time, we obtain the form of a polynomial isometry relative to its order and its "valuation" (which is defined in section 4.3).

This method is different from Anashin's one [1] who uses interpolation series and reduces the study of such an isometry to the study of a compatible and bijective function of $\mathbf{Z}/p^K\mathbf{Z}$ where K is a logarithmic function of the degree of f. Our result is different too, since the order and the complexity do not really depend on the degree: for a given order or complexity, the degree of a $\mathbf{F}_p$-polynomial isometry of $\mathbf{Z}_p$ can be arbitrarily large.

2. Notations and definitions

• p is a prime integer and $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ is the finite field of p elements.

• $\mathbf{Z}_p$ is the ring of the p-adic integers $a = (\bar{a}^n)_{n\in\mathbf{N}} = \bar{a}^0 + p\,\bar{a}^1 + p^2\bar{a}^2 + \ldots$, where the integers $\bar{a}^i$ satisfy $0 \leq \bar{a}^i \leq p-1$.

• $\mathbf{Q}_p$ is the field of the p-adic numbers: $\mathbf{Q}_p = \mathbf{Z}_p[\frac{1}{p}]$.

• The absolute value $|\,.\,|$ is defined in $\mathbf{Q}_p$ (and $\mathbf{Z}_p$) by:

$|0| = 0$, and for any $a \neq 0$, $|\,(\bar{a}^i)_{i\in\mathbf{Z}}\,| = p^{-k}$ where $k = \mathrm{Min}\{\, i \in \mathbf{Z} \mid \bar{a}^i \neq 0\,\}$.

This absolute value is ultrametric: $|a+b| \leq \mathrm{Max}(|a|,|b|)$, then $\mathbf{Z}_p$ is the union of the disjoint balls $B_{<1}(i)$ for $0 \leq i \leq p-1$.

• We define and use: $X = x^p - x$, $Y = X/p$ and $Z = z^{p-1} - 1$.

• A S-polynomial is a polynomial with coefficients in the set S.

• We use Landau symbols O, o, and $f \sim g$ means $f - g = o(g)$.

• For any $x \in \mathbf{R}$ there exists an unique integer n such that $n \leq x < n+1$. We use $n = \lfloor x \rfloor$, and $\lceil x \rceil = n+1$ if $x > n$, if not $x = n = \lceil x \rceil$.

For general properties in p-adic analysis, see for example [6,12].

3. $\mathbf{Z}_p$-polynomial isometries of $\mathbf{Z}_p$

Here is the main result about $\mathbf{Z}_p$-polynomial isometries of $\mathbf{Z}_p$ (see [1,2]), the study of which is reduced to the study of two $\mathbf{F}_p$-polynomials on $\mathbf{F}_p$.

Let $f\colon x \mapsto a_0 + a_1 x + \ldots + a_k x^k$, with $a_i \in \mathbf{Z}_p$. Reducing the powers of x using $x^p = x$ and replacing a_i with a_i mod p, we obtain a $\mathbf{F}_p$-polynomial map $\hat{f}$ on $\mathbf{F}_p$ with degree $\leq p-1$. By the same way, $\widehat{f'}$ is calculated.

Proposition 3.1. *f is an isometry of $\mathbf{Z}_p$ exactly when*

(1) $\hat{f}$ defines a bijection of $\mathbf{F}_p$, and (2) $\widehat{f'}$ has no root in $\mathbf{F}_p$.

Proof. If f is isometric, then we obtain *(1)* since $|f(i) - f(j)| = |\hat{f}(i) - \hat{f}(j)|$, and *(2)* since

$$|f(i+pz) - f(i+pz')| = |p(z-z')\widehat{f'}(i)| = |z-z'|/p.$$

Conversely, if $i \neq j$, $|f(i+pz) - f(j+pz')| = |\hat{f}(i) - \hat{f}(j)| = 1$, then f is an isometry. □

This criterium can be combined with some well-known results about permutational polynomials (see [10,11]) and other properties, to obtain a lot of interesting results: for example, f cannot be an isometry if the degree of $\hat{f}$ is 2, 3 when -3 is a square, 4 if $p \neq 7$, $q \geq 2$ if q divides $p-1$...But for our purpose, we will only use the following

Corollary 3.1. *There is no $\mathbf{F}_p$-polynomial isometry of $\mathbf{Z}_p$ with degree 2, 3 when $p \neq 3$, 4 when $p \geq 5$, q when $q \geq 2$ and q divides $p-1$.*

Proof. a) We use $|f(x) - f(y)| = |x-y||b_1 + b_2(x+y)|$, where $f = b_0 + b_1 x + b_2 x^2$ ($b_2 \neq 0$). With $x = 0$ and $y = p$ if $b_1 = 0$, else $x = 0$ and $y = -b_1/b_2$ we obtain $|f(x) - f(y)| < |x-y|$.

b) Without loss of generality, suppose $f(x) = x + a_2x^2 + a_3x^3$ with $p \neq 3$ and $a_3 \neq 0$. The absolute value of $\dfrac{f(y)-f(x)}{y-x} = h(x,y) = 1 + a_2(x+y) + a_3(x^2+xy+y^2)$ must be 1 for any p-adic integers $x \neq y$. Using $x = x' + y'$ and $y = -x' + y'$, $h(x,y) = 1 + 2a_2.y' + a_3(x'^2 + 3y'^2)$.

- If $p \geq 5$, since a_3 and 3 are invertible, we can use the translation: $x'' = x'$, $y'' = y' + \dfrac{a_2}{3a_3}$, and so $h(x,y) = z + a_3(x''^2 + 3y''^2)$. Consider ε: $t \mapsto t^2$ and η: $t \mapsto -\dfrac{z}{a_3} - 3t^2$, defined in $\mathbf{F}_p$. The sets $\mathrm{Im}(\varepsilon)$ and $\mathrm{Im}(\eta)$ have the same cardinal $(p+1)/2$, hence the equation $\varepsilon(x'') = \eta(y'')$ admits at least one solution in $\mathbf{F}_p \times \mathbf{F}_p$, and so $h(\alpha,\beta) = 0 \bmod p$ for a suitable couple (α,β) in $\mathbf{F}_p^2$. If $\alpha \neq \beta$, f is not bijective. If $\alpha = \beta$, $|f(\alpha) - f(\alpha+p)| < \dfrac{1}{p}$ and f is not isometric.

- If $p = 2$, we conclude easily since $h(1,3) = 0 \bmod 2$.

(- $x \mapsto a_0 \pm (x + x^3)$ are in fact the $\mathbf{F}_3$-polynomial isometries of $\mathbf{Z}_3$ of degree 3.)

c) If $p \geq 5$, the only normalized bijective $\mathbf{F}_p$-polynomials of degree 4 are defined for $p = 7$ and by $f(x) = x^4 \pm 3x$ (see [11]). But $\widehat{f'}(x) = -3(x^3 \pm 1)$, then $\widehat{f'}(1) = 0$ or $\widehat{f'}(3) = 0$.

d) There is no $\mathbf{F}_p$-polynomial bijection of $\mathbf{F}_p$ with degree $q \geq 2$ that divides $p-1$, hence no such isometry of $\mathbf{Z}_p$ (see [11] or use Newton's identities). □

Examples

a) $x \mapsto x + 2x^3 + 4x^6$ is an isometry of $\mathbf{Z}_5$.

b) $x \mapsto a_0 + \sum\limits_{i \geq 1} a_i x^i$ is an isometry of $\mathbf{Z}_2$ exactly when

$$a_1 = 1 \bmod 2 \text{ and } \sum_{i \geq 1} a_{2i+1} = \sum_{i \geq 1} a_{2i} = 0 \bmod 2.$$

4. $\mathbf{Q}_p$-polynomial isometries of $\mathbf{Z}_p$

4.1. Description

In this section, we tranform the expression of a $\mathbf{Q}_p$-polynomial f to introduce its order (section 4.3), which is our main tool to reduce the study of f to bijections of $\mathbf{F}_p$ and $\mathbf{Z}_p$-polynomial isometries of $\mathbf{Z}_p$. Separating the negative powers of p : $f(x) = P_0(x) + \dfrac{1}{p}P_1(x) + \ldots + \dfrac{1}{p^k}P_k(x)$ where P_1, P_2, ...,P_k are $\mathbf{F}_p$-polynomials, and P_0 is a $\mathbf{Z}_p$-polynomial.

Since: $\forall (x,y) \in \mathbf{Z}_p^2, \quad |f(x) - f(y)| = |x - y|$, we can consider that P_0 is a $\mathbf{F}_p$-polynomial without loss of generality. Observe that terms with any degree may disappear with this first reduction.

Now, using successive Euclidean divisions of each P_i by $X = x^p - x$:

$$\begin{aligned} f = \ & f_{0,0} + X f_{1,0} + X^2 f_{2,0} + X^3 f_{3,0} + \ldots + \frac{1}{p}(f_{0,1} + X f_{1,1} + X^2 f_{2,1} + X^3 f_{3,1} + \ldots) \\ & + \ldots + \frac{1}{p^k}(f_{0,k} + X f_{1,k} + X^2 f_{2,k} + X^3 f_{3,k} + \ldots), \end{aligned} \tag{4.1}$$

where $f_{i,j}$ are $\mathbf{F}_p$-polynomials with degree less than $p-1$.

For the next sections, we need some properties of X, Y and Z.

4.2. Some properties of $X = x^p - x$, $Y = X/p$ and $Z = z^{p-1} - 1$

First, recall the following well-known result (see [7] for a proof):

Lemma 4.1. *$X = x^p - x$ admits exactly p roots β_0, β_1, $\ldots$ β_{p-1} in $\mathbf{Z}_p$, with $\beta_i = i \bmod p$.*

Since the absolute value is ultrametric, we have: $B_{<1}(\beta_i) = B_{<1}(i)$. Hence we will use that $\mathbf{Z}_p = \bigcup_{0 \le i \le p-1} B_{<1}(\beta_i)$.

Eventually we need some developments of $Y = X/p$ and Z:

Lemma 4.2. *For any root β of X in $\mathbf{Z}_p$ and z in $\mathbf{Z}_p$:*

$$Y(\beta + pz) = -z + p\beta^{p-1}z + p^2\frac{p-1}{2}\beta^{p-2}z^2 + p^2\binom{p}{3}\beta^{p-3}z^3 + \ldots + p^{p-1}z^p$$

(with the convention $\beta^l = 0$ if $\beta = 0$).

Proof. No difficulty, using $\beta^p = \beta$. □

Using $Z^2 = z^{p-2}X(z) - Z$ and $zZ = X(z) = z^p - z$, we prove by induction:

Lemma 4.3. *a) If $p \ge 5$ and $3 \le n \le p-1$:*

$$Z^n = z^{p-n}X^{n-1} - z^{p-n+1}X^{n-2} + \ldots + (-1)^n z^{p-2}X + (-1)^{n+1}Z.$$

b) If $p = 3$: $Z^3 = X^2 - zX + Z$, and $\forall n \ge 4$, $Z^n = (-1)^n(((n-3)Z - 1)X^2 + zX - Z) + X^3(-)$.

c) If $p = 2$, $Z^3 = (Z-1)X + Z$, $Z^4 = X^2 + (1-2Z)X - Z$, and

$$\forall n \ge 5 : \ Z^n = (-1)^{n+1}(\binom{n-3}{2}Z - (n-3))X^2 + ((n-2)Z - 1)X + Z) + X^3(-).$$

d) More generally, for $\alpha \ge 1$, $2 \le \beta \le p-1$ and using $\bar{l} = l \bmod (p-1)$:

$$Z^{\alpha p} = X^{\alpha(p-1)} + \sum_{j=1}^{\alpha(p-1)-1} a_j z^{-\overline{j}} X^j + (-1)^{\alpha p+1}Z,$$

$$Z^{\alpha p+1} = (Z-\alpha)X^{\alpha(p-1)} + \sum_{j=1}^{\alpha(p-1)-1} a_j \overline{z^{-j}} X^j + (-1)^{\alpha p+2} Z,$$

$$Z^{\alpha p+\beta} = z^{p-\beta} X^{\alpha(p-1)+\beta-1} + \sum_{j=1}^{\alpha(p-1)+\beta-2} a_j \overline{z^{-j}} X^j + (-1)^{\alpha p+\beta+1} Z,$$

where $a_j = a'_j + b'_j Z$, $b'_j = 0$ *if* j *does not divide* $p-1$, a'_j *and* b'_j *are in* $\mathbf{F}_p$.

4.3 Order and valuation

Let f be a $\mathbf{Q}_p$-polynomial isometry of $\mathbf{Z}_p$ given by formula 4.1. Some terms can be easily eliminated. Then we reformulate f and define its order.

$*$ For any root β of X in $\mathbf{Z}_p$: $f(\beta) = f_{0,0}(\beta) + \frac{1}{p} f_{0,1}(\beta) + \ldots + \frac{1}{p^k} f_{0,k}(\beta) \in \mathbf{Z}_p$ hence, for any $1 \le i \le k$, X divides the $\mathbf{F}_p$-polynomial $f_{0,i}$, the degree of which is less than $p-1$. Then $f_{0,i} = 0$.

$*$ For any root β of X in $\mathbf{Z}_p$ and any z and z' in $\mathbf{Z}_p$, by Taylor's formula:

$$|f(\beta+pz) - f(\beta+pz')| = \frac{1}{p}|z-z'| = \frac{1}{p}|z-z'||f'(\beta) + p(z+z')\frac{f''(\beta)}{2} + \ldots|.$$

Choosing $z = p^\lambda$ and $z' = 0$ with λ large enough, we obtain:

$$|f'(\beta)| = 1 = |f'_{0,0}(\beta) - f_{1,0}(\beta) - \frac{1}{p} f_{1,1}(\beta) - \frac{1}{p^2} f_{1,2}(\beta) - \ldots \frac{1}{p^k} f_{1,k}(\beta)|.$$

For the same reasons: $f_{1,1} = f_{1,2} = \ldots = f_{1,k} = 0$ and $|f'_{0,0} - f_{1,0}| = 1$.

$*$ In the equation $|f(\beta+pz) - f(\beta+pz')| = \frac{1}{p}|z-z'|$, observe the following term using Lemma 4.2: $\frac{1}{p^j} X^{j+2}(\beta+pz) = \frac{1}{p^j}(-1)^{j+2}(pz)^{j+2} = 0 \bmod p^2$. Hence no term $\frac{1}{p^j} X^l f_{l,j}$ intervene in this equation when $l \ge j+2$, and we have the same conclusion with the condition $f(\mathbf{Z}_p) \subset \mathbf{Z}_p$.

To sum up:

Proposition 4.2. *Any* $\mathbf{Q}_p$*-polynomial isometry of* $\mathbf{Z}_p$ *has the form :*

$$f = f_{0,0} + X f_{1,0} + X^2 f_{2,0} + X^3 f_{3,0} + \ldots + pQ$$
$$+ \frac{1}{p}(X^2 f_{2,1} + X^3 f_{3,1} + \ldots) + .. + \frac{1}{p^k}(X^2 f_{2,k} + X^3 f_{3,k} + X^4 f_{4,k} + ..) + ...$$

where $f_{i,j}$ *are* $\mathbf{F}_p$*-polynomials with degree less than* $p-1$, $f'_{0,0} - f_{1,0}$ *does not vanish on* $\mathbf{F}_p$, *and* Q *is a* $\mathbf{Z}_p$*-polynomial.*

Moreover, there is no condition on $f_{l,j}$ *when* $l - j \ge 2$.

Hence we assume from now that $f_{l,j}=0$ if $l-j\geq 2$, and that $Q=0$. Then:

$$\begin{aligned} f= \quad & f_0+Xh_1+\frac{1}{p}X^2h_2+\frac{1}{p^2}(X^2f_2+X^3h_3)+\frac{1}{p^3}(X^2f_{2,3}+X^3f_3+X^4h_4) \\ & +\ldots+\frac{1}{p^k}(X^2f_{2,k}+X^3f_{3,k}+\ldots+X^{k-1}f_{k-1,k}+X^kf_k+X^{k+1}h_{k+1}) \end{aligned} \tag{4.2}$$

or: $f=f_0+p(Yh_1+Y^2h_2+..)+(Y^2f_2+Y^3f_3+..)+\frac{1}{p}(Y^2f_{2,3}+Y^3f_{3,4}+..)+...$ where we use $\mathbf{F}_p$-polynomials with degree less than $p-1$. Finally, we gather the terms with same powers of Y modulo $p-1$:

$$f=f_0+p\sum_{j=1}^{p-1}H_j+\sum_{j=1}^{p-1}F_j+\frac{1}{p}\sum_{j=1}^{p-1}F_{j,j+1}+\ldots+\frac{1}{p^r}\sum_{j=1}^{p-1}F_{j,j+r} \tag{4.3}$$

where, for $1\leq j\leq p-1$ and $1\leq l\leq r$:

$$H_j=Y^jh_j+Y^{j+p-1}h_{j+p-1}+Y^{j+2(p-1)}h_{j+2(p-1)}+\cdots$$

$$F_j=Y^jf_j(x)+Y^{j+p-1}f_{j+p-1}+Y^{j+2(p-1)}f_{j+2(p-1)}+\cdots$$

$$F_{j,j+l}=Y^jf_{j,j+l}+Y^{j+(p-1)}f_{j+(p-1),j+l+(p-1)}+\ldots,$$

with the former conditions : $f_1=f_{1,j}=0$ and $|f_0'-h_1|=1$ on $\mathbf{F}_p$.

Now we can define the order and the valuation of such a $\mathbf{Q}_p$-polynomial:

Definition 4.1. *If the last term in formula 4.3 does not vanish, we say that the* **order** *of f is r. If the last term in formula 4.2 does not vanish, we say that the* **valuation** *of f is k.*

Then the order of a $\mathbf{Q}_p$-polynomial is -1 or a natural. It does not depend on its degree, which can be as big as we wish (terms of expression 4.1 may miss in expression 4.3), and it does not depend on the biggest absolute value of its coefficients for the same reason.

Also, the valuation k is the "useful" biggest absolute value of its coefficients since extra terms $\frac{1}{p^{k'}}X^{l'}f_{l',k'}$ such that $l'\geq k'+2$ may miss in formula 4.2.

4.4 $\mathbf{Q}_p$-polynomial isometries of order -1

In this section, f is a $\mathbf{Q}_p$-polynomial of order -1: $f=f_0+p\sum_{j=1}^{p-1}H_j$,
where $H_j=Y^jh_j+Y^{j+p-1}h_{j+p-1}+\ldots$, f_0 and h_l are $\mathbf{F}_p$-polynomials with degrees less than $p-1$, and $|f_0'-h_1|=1$ on $\mathbf{F}_p$. Note that these conditions imply $f(\mathbf{Z}_p)\subset\mathbf{Z}_p$.

First, suppose that f is isometric:

- for any root β_i of X, $f(\beta_i) = f_0(\beta_i) = f(i) \bmod p$, then f_0 induces a bijection of $\mathbf{F}_p$;

- for any root β of X, the map $f_{|\beta}\colon z \mapsto (f(\beta+pz)-f(\beta))/p$ is a $\mathbf{Q}_p$-polynomial isometry of $\mathbf{Z}_p$. Using Lemma 4.2: $H_j(\beta+pz) = (-z+p\beta^{p-1}z+\ldots)^j(h_j(\beta)+pzh'_j(\beta)+\ldots)+\ldots$ Interestingly, $f_{|\beta}$ is a $\mathbf{Z}_p$-polynomial : $z \mapsto f'_0(\beta)z+\sum_{j=1}^{k+1}(-1)^j h_j(\beta)z^j+p(\ldots)$, hence is an isometry if and only if conditions of Proposition 3.1 are satisfied.

Conversely, suppose that f_0 induces a bijection of $\mathbf{F}_p$ and that each $f_{|\beta}$ is an isometry of $\mathbf{Z}_p$. For any distinct roots β and β' of X in $\mathbf{Z}_p$ and all z in $\mathbf{Z}_p$:

$$|f(\beta+pz)-f(\beta'+pz')| = |pf_{|\beta}(z)+(f_0(\beta)-f_0(\beta'))-pf_{|\beta'}(z')| = 1.$$

Then, for any z and z' in $\mathbf{Z}_p$, $|f(z)-f(z')| = |z-z'|$: f is an isometry of $\mathbf{Z}_p$. To sum up :

Proposition 4.3. *Let $f = f_0 + p\sum_{j=1}^{p-1} H_j$ be a $\mathbf{Q}_p$-polynomial of order -1. Then f is isometric exactly when:*

(a) f_0 is a bijection of $\mathbf{F}_p$,

(b) for any root β of X, $f_{|\beta}: z \mapsto f'_0(\beta)z+\sum_{j=1}^{k+1}(-1)^j h_j(\beta)z^j+p(\ldots)$ satisfies properties (1) and (2) of Proposition 3.1:

1) $\widehat{f_{|\beta}}\colon z \mapsto f'_0(\beta)z+\sum_{j=1}^{p-1}(-1)^j z^j(h_j(\beta)+h_{j+p-1}(\beta)+\ldots)$ is a bijection of $\mathbf{Z}_p$,

2) $\widehat{f'_{|\beta}}\colon z \mapsto f'_0(\beta)-h_1(\beta)+$

$$\sum_{j=1}^{p-1}(-1)^{j+1}z^j((j+1)h_{j+1}(\beta)+(j+p)h_{j+p}(\beta)+(j+2p-1)h_{j+2p-1}(\beta)+\ldots)$$

has no root in $\mathbf{F}_p$.

Corollary 4.2. *A $\mathbf{Q}_2$-polynomial $f = f_0 + X h_1 + \frac{X^2}{2}h_2 + \ldots$ of order -1 is an isometry of $\mathbf{Z}_2$ if, and only if:*

$$(i)\ f_0 \text{ is a bijection of } \mathbf{Z}_2 \qquad (ii)\ f'_0+h_1 \text{ has no root in } \mathbf{F}_2$$

$$(iii)\ h_2+h_4+h_6+\ldots = 0 \bmod 2 \qquad (iv)\ h_3+h_5+h_7+\ldots = 0 \bmod 2$$

Observe that the condition $|f'_0-h_1| = 1$ is included in (b)2) (using $z=0$).

Eventually, we established that the study of f is equivalent to the study of one bijection of $\mathbf{F}_p$ and (at most) p $\mathbf{Z}_p$-polynomial isometries of $\mathbf{Z}_p$. We say that the complexity of f is 1.

Examples of $\mathbf{Q}_p$-polynomial isometries of $\mathbf{Z}_p$ of order -1:

(i) $x \mapsto x+x^2+2x^3+x^4+\dfrac{X^2}{2}+\dfrac{X^3}{4}+\dfrac{X^4}{8}+\dfrac{X^6}{32}+\dfrac{X^7}{64}+\dfrac{X^8}{128}, \quad (p=2)$

(ii) $x \mapsto x+\dfrac{2}{9}(x^3-x)^3 = x+3.2Y^3, \quad (p=3)$

(iii) $x \mapsto x+\dfrac{1}{5^2}(3x^4+2x^2+2)(x^5-x)^3+\dfrac{1}{5^5}(x^2+2)(x^5-x)^6, \quad (p=5).$

4.5. The main tool

By the same arguments as in 4.4, we reduce the order of a $\mathbf{Q}_p$-polynomial step by step:

Proposition 4.4. *For $r \geq 0$, the study of a $\mathbf{Q}_p$-polynomial isometry of $\mathbf{Z}_p$ of order r can be reduced to the study of one bijection of $\mathbf{F}_p$ and at most p $\mathbf{Q}_p$-polynomial isometries of $\mathbf{Z}_p$ of order $\leq r-1$ and valuation $\leq r+1$.*

Iterating the process, the study of a $\mathbf{Q}_p$-polynomial isometry of $\mathbf{Z}_p$ of order r can be reduced to the study of at most $1+p+\ldots+p^{r+1}$ bijections of $\mathbf{F}_p$ and p^{r+2} $\mathbf{Z}_p$-polynomial isometries of $\mathbf{Z}_p$. This result will be improved in the next sections.

Proof: Let $f = f_0 + p\sum_{j=1}^{p-1} H_j + \sum_{j=1}^{p-1} F_j + \frac{1}{p}\sum_{j=1}^{p-1} F_{j,j+1} + \ldots + \frac{1}{p^r}\sum_{j=1}^{p-1} F_{j,j+r}$ given by formula 4.3. If f is an isometry of $\mathbf{Z}_p$, then f_0 clearly induces a bijection of $\mathbf{F}_p$ and, for any root β of X in $\mathbf{Z}_p$, $f_{|\beta}$ is an isometry of $\mathbf{Z}_p$.

Conversely, suppose that f_0 is a bijection of $\mathbf{F}_p$ and that the maps $f_{|\beta}$ preserve distances between points of $\mathbf{Z}_p$. Then $f(\beta) = f_0(\beta)$ belongs to $\mathbf{Z}_p$, and $|f_{|\beta}(z) - f_{|\beta}(0)| = |z|$ proves that $f_{|\beta}(z)$ belongs to $\mathbf{Z}_p$ for any root β of X and z in $\mathbf{Z}_p$. Hence, $|f(\beta+pz)-f(\beta)| \leq |z|/p$ gives $f(\mathbf{Z}_p) \subset \mathbf{Z}_p$. Eventually, as seen in section 4.4, we deduce that f is an isometry of $\mathbf{Z}_p$.

In order to conclude, we still have to evaluate $G_j(\beta+pz)$ where G_j represents H_j, F_j or $F_{j,j+l}$, using Lemma 4.2. This is nearly the same calculation as in 4.4, in which g_k represents h_k, f_k, or any $f_{k,k+l}$.

$$G_j(\beta+pz) = Y^j(\beta+pz)g_j(\beta+pz) + Y^{j+p-1}(\beta+pz)g_{j+p-1}(\beta+pz)+\ldots$$

$$= (-z+p\beta^{p-1}z+p^2(-)+\ldots)^j(g_j(\beta)+pzg'_j(\beta)+p^2(-)+\ldots)$$

$$+(-z+p\beta^{p-1}z+\ldots)^{j+p-1}(g_{j+p-1}(\beta)+pzg'_{j+p-1}(\beta)+\ldots)+\ldots$$

$$= (-1)^j z^j g_j(\beta) + (-1)^{j+p-1}z^{j+p-1}g_{j+p-1}(\beta)+\ldots+p(\ldots)+\ldots.$$

Using $F_{j,j+r}$ and $F_{j,j+r-1}$, the last terms of the expression of $f_{|\beta}$ are:

$$\frac{1}{p^{r+1}}\sum_{j=1}^{p-1}\left(Q_0(z)+Q_1(z)X(z)+Q_2(z)X^2(z)+\ldots\right)$$

$$+\frac{1}{p^r}\sum_{j=1}^{p-1}\left(R_0(z)+R_1(z)X(z)+R_2(z)X^2(z)+\ldots\right)+\frac{1}{p^{r-1}}(\ldots)+\ldots$$

where Q_l and R_l are $\mathbf{F}_p$-polynomials with degrees less than $p-1$ (we used successive Euclidean divisions by X in $\mathbf{F}_p$). Thanks to Proposition 4.2, the factors of X^0 and X^1 vanish since $r+1\geq 1$, then $Q_0=Q_1=0$. Note that, if $r\geq 1$, we have also: $R_0=R_1=0$.

Let rewrite $f_{|\beta}$ using $Y=X/p$: its order is less than $r-1$. □

We see that f and $f_{|\beta}$ have the same degree and the same "real" valuation (defined as the biggest power of $1/p$ in the expression 4.1 of f). The order is a better tool to elaborate a process as Proposition 4.4 does and to evaluate the complexity of an isometry. For example, we saw in section 4.4 that isometries of order -1 have complexity 1, while their "real" valuations and degrees can nearly be any integer. Moreover, if the "useful" valuation of f is k, the valuation of $f_{|\beta}$ is less than $r+1$, which is better linked to the order of f after the first reductions.

We study the links between valuation, order and complexity in section 4.9.

Example: $x\mapsto x+\frac{3}{2^3}(x^2-x)^3+\frac{1}{2^7}(x^2-x)^7=x+(Y^3+Y^7)+2Y^3$ is a $\mathbf{Q}_2$-isometry of $\mathbf{Z}_2$ of order 0. Indeed, $x\mapsto x$ is a bijection of $\mathbf{F}_2$, and $f_{|0}=f_{|1}=z\mapsto z+z^4+z^8$ are $\mathbf{Z}_2$-polynomial isometries of $\mathbf{Z}_2$.

We can now study $\mathbf{Q}_p$-polynomial isometries of $\mathbf{Z}_p$ with bigger orders.

4.6. $\mathbf{Q}_p$-polynomial isometries of $\mathbf{Z}_p$ of order 0

We have to go further in the calculations of the proof of Proposition 4.4.

Let G_j be H_j or F_j or any $F_{j,j+l}$: $\quad G_j=Y^jg_j+Y^{j+p-1}g_{j+p-1}+\ldots$

We define: $\tilde{G}_j(x,y)=\sum_{\alpha\geq 0}y^\alpha g_{j+\alpha(p-1)}(x)$,

$\sigma_0(G_j,\beta)=\tilde{G}_j(\beta,1)=(g_j+g_{j+(p-1)}+g_{j+2(p-1)}+\ldots)(\beta)$,

$\sigma_1(G_j,\beta)=\partial_2\tilde{G}_j(\beta,1)=(g_{j+(p-1)}+2g_{j+2(p-1)}+3g_{j+3(p-1)}+\ldots)(\beta)$, and so on:

$\sigma_q(G_j,\beta)=\frac{1}{q!}\partial_2^q\tilde{G}_j(\beta,1)$.

We omit β for simplicity when there is no ambiguity.

Proposition 4.5. *($p \geq 3$) Let $f = f_0 + p\sum_{j=1}^{p-1} H_j + \sum_{j=1}^{p-1} F_j$ be a $\mathbf{Q}_p$-polynomial of order 0. If f is an isometry of $\mathbf{Z}_p$, we have (modulo p):*

(i) $\sigma_0(F_j) = f_j + f_{j+p-1} + f_{j+2(p-1)} + \ldots = 0,$

(ii) $\sigma_1(F_j) = f_{j+p-1} + 2f_{j+2(p-1)} + 3f_{j+3(p-1)} + \ldots = 0,$

(iii) $\sigma_2(F_j) = f_{j+2(p-1)} + 3f_{j+3(p-1)} + 6f_{j+4(p-1)} + \ldots = 0,$

(iv) for $l = (1), 2$: $\sigma_3(F_l) - \sigma_4(F_l) + \sigma_5(F_l) + \ldots = 0$

$$= f_{l+3(p-1)} + 3f_{l+4(p-1)} + 6f_{l+5(p-1)} + 10f_{l+6(p-1)} + 15f_{l+7(p-1)} + \ldots.$$

With these conditions, f is an isometry of $\mathbf{Z}_p$ exactly when f_0 is a bijection on $\mathbf{F}_p$, $f_1 = 0$ and the following $\mathbf{Z}_p$-polynomials are isometries of $\mathbf{Z}_p$:

$$z \mapsto f_0'(\beta)z + \sum_{j=1}^{k+1}(-1)^j h_j(\beta)z^j - (\overline{\sigma_2(F_1,\beta) - \sigma_3(F_1,\beta) + \ldots}^{1})ZX(z)$$
$$+ \sum_{j=1}^{p-1}(-1)^j(\bar{\sigma}_0^1(F_j,\beta)z^j + \bar{\sigma}_1^1(F_j,\beta)z^{j-1}X(z)).$$

Proof. In order to obtain $f_{|\beta}$, we calculate:

$$F_j(\beta + pz) = (-z + p\beta^{p-1}z + p^2(..))^j(f_j(\beta) + pzf_j'(\beta) + p^2(...))$$

$$+(-z + p\beta^{p-1}z + p^2(..))^{j+p-1}(f_{j+p-1}(\beta) + pzf_{j+p-1}'(\beta) + p^2(...)) + \ldots$$

$$= (-z)^j(f_j + z^{p-1}f_{j+p-1} + z^{2(p-1)}f_{j+2(p-1)} + \ldots)$$

$$-p\beta^{p-1}(-z)^j(jf_j + z^{p-1}(j+p-1)f_{j+p-1} + z^{2(p-1)}(j+2(p-1))f_{j+2(p-1)} + \ldots)$$

$$+p(-1)^j z^{j+1}(f_j' + z^{p-1}f_{j+p-1}' + z^{2(p-1)}f_{j+2(p-1)}' + \ldots) + p^2(...).$$

We will use Z and Lemma 4.3.

$$f_j + z^{p-1}f_{j+p-1} + z^{2(p-1)}f_{j+2(p-1)} + \ldots = \sigma_0(F_j) + \sigma_1(F_j)Z + \sigma_2(F_j)Z^2 + \ldots$$

With simplified notations:

$$z^j(\sigma_0 + \sigma_1 Z + \sigma_2 Z^2 + \ldots + \sigma_j Z^j + \sigma_{j+1}Z^{j+1} + \ldots)$$

$$= \sigma_0 z^j + \sigma_1 z^{j-1}X(z) + \ldots + \sigma_j X^j(z) + X^j(z)(\sigma_{j+1}Z + \sigma_{j+2}Z^2 + \ldots),$$

and eventually:

$* F_1(\beta+pz) = -\sigma_0 z - \sigma_1 X - X.(\sigma_2 Z + \sigma_3 Z^2 + \ldots) + \ldots$

$$= -\sigma_0 z - (\sigma_1 + (\sigma_2 - \sigma_3 + \sigma_4 + \ldots)Z)X - (\sigma_3 - \sigma_4 + \sigma_5 + \ldots)z^{p-2}X^2 + X^3(\ldots) + \ldots$$

$* F_2(\beta+pz) = \sigma_0 z^2 + \sigma_1 zX + X^2(\sigma_2 + \sigma_3 Z + \sigma_4 Z^2 + \ldots) + \ldots$

$$= \sigma_0 z^2 + \sigma_1 zX + (\sigma_2 + (\sigma_3 - \sigma_4 + \ldots)Z)X^2 + X^3(\ldots) + \ldots$$

$* F_j(\beta+pz) = (-1)^j(\sigma_0(F_j,\beta)z^j + \sigma_1(F_j,\beta)z^{j-1}X + \sigma_2(F_j,\beta)z^{j-2}X^2 + X^3(\ldots)) + \ldots$ for $3 \leq j \leq p-1$.

Then: $f_{|\beta}(z) = f_0'(\beta)z + \frac{1}{p}\sum_{j=1}^{p-1} F_j(\beta+pz) + \ldots$ is a $\mathbf{Q}_p$-polynomial isometry of order -1 because of Proposition 4.2 (the coefficients of X^0 and X^1 vanish). The degrees of the polynomials are less than $p-1$, hence we get (i)and (ii),

and $\sigma_2(F_1) - \sigma_3(F_1) + \sigma_4(F_1) - \sigma_5(F_1) + \ldots = 0 \bmod p$.

Moreover, there is no isometry of $\mathbf{Z}_p$ of degree 2 (Corollary 3.1). To apply the same method to $f_{|\beta}$ leads to such isometries if the former coefficient of X^2 does not vanish modulo p. Then (iii) and (iv) by the same arguments.

Note that $jf_j + (j+p-1)f_{j+p-1} + \ldots = j\sigma_0(F_j) - \sigma_1(F_j) \bmod p$ and $f_j' + f_{j+p-1}' + \ldots = \sigma_0'(F_j) = 0 \bmod p$. Finally the conclusion since the extra terms disappear modulo p in $f_{|\beta}$.

For $l = 1$, equation (iv) can be deduced from (i)(ii)(iii) since $f_1 = 0$. □

Proposition 4.6. *($p = 2$) Let $f = f_0 + 2H_1 + F_1$ be a $\mathbf{Q}_2$-polynomial of order 0. If f is an isometry of $\mathbf{Z}_2$, we have (modulo 2):*

(i') $f_2 + f_4 + f_6 + \ldots = 0$, (ii') $f_3 + f_5 + f_7 + \ldots = 0$,

(iii') $f_3 + f_4 + f_7 + f_8 + f_{11} + f_{12} + \ldots = 0$, (iv') $f_5 + f_6 + f_9 + f_{10} + \ldots = 0$.

With these conditions, f is an isometry exactly when f_0 induces a bijection of $\mathbf{F}_2$, $f_1 = 0$, and the two following $\mathbf{F}_2$-polynomials are isometries of $\mathbf{Z}_2$:

$$z \mapsto f_0'(\beta)z + \sum_{j=1}^{k+1}(-1)^j h_j(\beta)z^j - \overline{(f_3 - 2f_4 + 3f_5 - 4f_6 + \ldots)(\beta)}^1 ZX(z)$$
$$-\overline{(f_2 - f_3 + f_4 - \ldots)(\beta)}^1 z - \overline{(f_2 - 2f_3 + 3f_4 - 4f_5 + \ldots)(\beta)}^1 X(z)$$

Proof: Here $p-1=1$ is odd. We use $Y(2z)=-z+2z^2$, $Y(1+2z)=z+2z^2$, Lemma 4.3, and we adapt the calculations of Proposition 4.5 by switching f_i with $(-1)^i f_i$ in $F_1(2z)$, or f_i with $(-1)^{i-1}f_i$ in $F_1(1+2z)$, to obtain (i') to (iv'). Finally we conclude as in Proposition 4.5. □

Now we see that these necessary conditions may imply that the polynomials f_i could vanish. In other words, the order cannot be 0 if the useful valuation k is too small:

Corollary 4.3. *There is no $\mathbf{Q}_p$-polynomial isometry of $\mathbf{Z}_p$ with order $r=0$ and valuation $k<3p$.*

Proof. For such an isometry, if $k<j+3(p-1)$ and $j\geq 2$, there are at most three non-zero terms in the expression of $F_j=\sum_{n\geq 0} Y^{j+n(p-1)}f_{j+n(p-1)}$. Then $F_j=0$ because of (i), (ii) and (iii) of Proposition 4.5.

For $j=1$, we already know that $f_1=0$, and we verify the same result considering $F_1=\sum_{n=1}^{3} Y^{1+n(p-1)}f_{1+n(p-1)}$: $f_1=f_p=f_{2p-1}=f_{3p-2}=0$.

Also, Proposition 4.5 (iv) gives $F_2=0$ if $F_2=\sum_{n=0}^{3} Y^{2+n(p-1)}f_{2+n(p-1)}$ has only four terms.

So the first possible non-zero term F_j in a polynomial isometry of order 0 is F_3 if $p\geq 5$ and $k\geq 3p$, or F_1 if $p=3$ and $k\geq 9$, or F_1 if $p=2$ and $k\geq 6$ thanks to Proposition 4.6. □

Examples of $\mathbf{Q}_p$-polynomial isometries of $\mathbf{Z}_p$ of order 0:

$$x\mapsto x+\frac{X^2}{2}+\frac{X^3}{4}+\frac{X^3}{8}+\frac{X^4}{16}+\frac{X^5}{32}+\frac{X^6}{64},\quad (p=2,k=6)$$

$$x\mapsto x+\frac{X^2}{2}+3\frac{X^3}{8}+\frac{X^6}{32}+\frac{X^7}{128},\quad x\mapsto x+\frac{X^3}{8}+3\frac{X^7}{128},\quad (p=2,k=7)$$

$$x\mapsto x+\frac{X^3}{3^2}+2\frac{X^3}{3^3}+\frac{X^9}{3^9},\quad (p=3,k=9)$$

4.7. $\mathbf{Q}_p$-polynomial isometries of $\mathbf{Z}_p$ of order 1

Again, we need to extend the calculations of Proposition 4.5. In particular, we will use that no $\mathbf{Z}_p$-polynomial isometries of $\mathbf{Z}_p$ with degree 3 exists if $p\neq 3$. For $p=3$, we just adapt the results of Proposition 4.5 switching f_i with $f_{i,i+1}$, as explained in the proof of Corollary 4.4.

Proposition 4.7. *($p \neq 3$) Let $f = f_0 + p\sum_{j=1}^{p-1} H_j + \sum_{j=1}^{p-1} F_j + \frac{1}{p}\sum_{j=1}^{p-1} F_{j,j+1}$ be a $\mathbf{Q}_p$-polynomial of order 1. If f is an isometry of $\mathbf{Z}_p$, then f_0 is a bijection of $\mathbf{F}_p$, $f_1 = f_{1,2} = 0$, and we have the following equalities modulo p if $p \geq 5$:*

(i) $\sigma_0(F_{j,j+1}) = f_{j,j+1} + f_{j+p-1,j+p} + \ldots = 0$,

(ii) $\sigma_1(F_{j,j+1}) = f_{j+p-1,j+p} + 2f_{j+2(p-1),j+2p-1} + \ldots = 0$,

(iii) $\sigma_2(F_{j,j+1}) = f_{j+2(p-1),j+2p-1} + 3f_{j+3(p-1),j+3p-2} + \ldots = 0$,

(iv) $\sigma_3(F_{j,j+1}) = f_{j+3(p-1),j+3p-2} + 4f_{j+4(p-1),j+4p-3} + \ldots = 0$,

(v) for $l = (1), 2, 3$: $\sigma_4(F_{l,l+1}) - \sigma_5(F_{l,l+1}) + \sigma_6(F_{l,l+1}) + \ldots = 0$

$$= f_{l+4(p-1),l+4p-3} + 4f_{l+5(p-1),l+5p-4} + 10f_{l+6(p-1),l+6p-5} + \ldots.$$

For $p = 2$, we obtain equations (i') to (iv') of Proposition 4.6 switching f_l with $f_{l,l+1}$, and two new equalities mod 2:

(v') $f_{6,7} + f_{10,11} + f_{14,15} + f_{18,19} + \ldots = 0$, *(vi')* $f_{7,8} + f_{11,12} + f_{15,16} + f_{19,20} + \ldots = 0$

Provided these conditions, f is an isometry exactly when the useful parts of $f_{|\beta}$ are $\mathbf{Z}_p$-polynomial isometries of $\mathbf{Z}_p$.

Proof. In order to obtain $f_{|\beta}$, let note $G_j = F_{j,j+1}$ and $g_l = f_{l,l+1}$, and calculate $F_{j,j+1}(\beta + pz)$. Using Lemma 4.3, we obtain the coefficients of X^0, X, X^2 (as in Proposition 4.5), and finally the coefficient of X^3:

$*$ for $j = 1$ and $p \geq 5$: $z^{p-3}(-\sigma_4 + \sigma_5 - \sigma_6 + \ldots)$,

$*$ for $j = 1$ and $p = 2$: $\sigma_5' + \sigma_6'(Z-2) + \sigma_7'(-3Z+3) + \sigma_8'(6Z-4) + \ldots)$ and the same equations with σ_l'',

$*$ for $j = 2$ and $p \geq 5$: $z^{p-2}(\sigma_4 - \sigma_5 + \sigma_6 - \sigma_7 + \ldots)$,

$*$ for $j = 3$ and $p \geq 5$: $\sigma_3 + (\sigma_4 - \sigma_5 + \sigma_6 - \sigma_7 + \ldots)Z$,

$*$ for $j \geq 4$ and $p \geq 5$: σ_3.

Now, for suitable polynomials, $f_{|\beta}$ is given by:

$$f_{|\beta}(z) = f_0'(\beta)z + \frac{1}{p^2}\left(G_1(\beta + pz) + G_2(\beta + pz) + \sum_{j=3}^{p-1} G_j(\beta + pz)\right) + \ldots$$

$$= \frac{1}{p^2}(Q_0 + Q_1X + Q_2X^2 + Q_3X^3 + \ldots) + \frac{1}{p}(R_0 + R_1X + R_2X^2 + \ldots) + S.$$

So we obtain a $\mathbf{Q}_p$-polynomial isometry. Then $Q_0 = Q_1 = R_0 = R_1 = 0$ because of Proposition 4.2. Moreover, the valuation of $f_{|\beta}$ is smaller than $3p$, then its order is -1 (Corollary 4.3), hence $Q_2 = 0$. Eventually, since no $\mathbf{Z}_p$-polynomial isometry of $\mathbf{Z}_p$ with degree 3 exists ($p \neq 3$), we obtain $Q_3 = 0 \bmod p$ considering $\left(f_{|\beta}\right)_{|\beta'}$. Eventually the result.

For $l = 1$, (i) to (iv) and $f_1 = 0$ give equation (v). □

Corollary 4.4. *If $p \neq 3$, there is no $\mathbf{Q}_p$-polynomial isometry of $\mathbf{Z}_p$ of order 1 and valuation $k \leq 4p$. There is no $\mathbf{Q}_3$-polynomial isometry of $\mathbf{Z}_3$ of order 1 and valuation $k \leq 9$.*

Proof. $*$ If $p \geq 5$, suppose that $k < j + 4(p-1)$ and $j \geq 3$: there are at most four non-zero terms in the expression $F_{j,j+1} = \sum_{n \geq 0} Y^{j+n(p-1)} f_{j+n(p-1)}$. Then $F_{j,j+1} = 0$ because of Proposition 4.7 (i) to (iv).

For $j = 1$, $f_{1,2} = 0$ then $f_{p,p+1} = f_{2p-1,2p} = f_{3p-2,3p-1} = f_{4p-3,4p-2} = 0$.

Proposition 4.7 (v) gives $F_{2,3} = \sum_{n=0}^{4} Y^{2+n(p-1)} f_{2+n(p-1)} = 0$ and $F_{3,4} = 0$.

So the first possible non-zero term $F_{j,j+1}$ should be $F_{4,5}$ when $k \geq 4p+1$ (with $f_{4+4(p-1),4p+1}$), then $k \geq 4p+1$.

If $p = 2$, equations (i') to (vi') give $F_{1,2} = \sum_{n=1}^{6} Y^{1+n} f_{1+n,2+n} = 0$, since the first non zero term should be $f_{8,9}$, then $k \geq 9$.

If $p = 3$, we have the same results as in Proposition 4.5 switching f_l with $f_{l,l+1}$, otherwise we obtain a polynomial isometry of order 0 and valuation $2 < 9$ (if the coefficient of X^2 does not vanish), which would contradict Corollary 4.3. The first possible non-zero term should be $f_{9,10}$, so $k \geq 10$. □

Examples of $\mathbf{Q}_p$-polynomial isometries of $\mathbf{Z}_p$ of order 1:

$* \; x \mapsto x + \dfrac{X^2}{2} + \dfrac{X^4}{2^5} + \dfrac{X^6}{2^6} + \dfrac{X^8}{2^9}, \quad (p = 2, k = 9)$

$* \; x \mapsto x + \dfrac{8}{3^3}X^3 + \dfrac{1}{3^4}(2X^3 + X^5) + \dfrac{1}{3^5}X^5 + \dfrac{2}{3^7}X^7 + \dfrac{1}{3^{10}}X^9, \quad (p = 3, k = 10)$

4.8. $\mathbf{Q}_p$-polynomial isometries of $\mathbf{Z}_p$ of order 2

Again, we extend the former calculations and use that no $\mathbf{Z}_p$-polynomial isometries of $\mathbf{Z}_p$ with degree 4 exists if $p \geq 5$.

Proposition 4.8. *($p \geq 5$) Let f be a $\mathbf{Q}_p$-polynomial of order 2:*

$$f = f_0 + p\sum_{j=1}^{p-1} H_j + \sum_{j=1}^{p-1} F_j + \frac{1}{p}\sum_{j=1}^{p-1} F_{j,j+1} + \frac{1}{p^2}\sum_{j=1}^{p-1} F_{j,j+2}.$$

If f is an isometry of $\mathbf{Z}_p$, then f_0 is a bijection of $\mathbf{F}_p$, $f_1 = f_{1,2} = f_{1,3} = 0$, and we have the following equalities modulo p:

(i) $\sigma_0(F_{j,j+2}) = \sigma_1(F_{j,j+2}) = \sigma_2(F_{j,j+2}) = \sigma_3(F_{j,j+2}) = \sigma_4(F_{j,j+2}) = 0$,

(ii) for $l = (1), 2, 3, 4$: $\sigma_5(F_{l,l+2}) - \sigma_6(F_{l,l+2}) + \sigma_7(F_{l,l+2}) + \ldots = 0$

$$= f_{l+5(p-1),l+5p-3)} + 5f_{l+6(p-1),l+6p-4)} + 15f_{l+7(p-1),l+7p-5)} + \ldots$$

Corollary 4.5. *There is no $\mathbf{Q}_p$-polynomial isometry of $\mathbf{Z}_p$ of order $r = 2$ and valuation $k \leq 5p+1$ if $p \geq 5$, $k \leq 13$ if $p = 3$, $k \leq 9$ if $p = 2$.*

Proof. Same proof as for Corollary 4.4 when $p \neq 3$. If $p = 3$, the coefficients of X^3 must vanish modulo p, otherwise we obtain isometries with order 0 and valuation 3. We calculate it:

in $F_{1,3}$: $\sigma_4 - \sigma_5 + \sigma_6 - \ldots + Z(\sigma_5 - 2\sigma_6 + 3\sigma_7 + \ldots)$

$$= f_{9,11} + 4f_{11,13} + \ldots + Z(f_{11,13} + 5f_{13,15} + \ldots)$$

in $F_{2,4}$: $z(\sigma_4 - \sigma_5 + \sigma_6 - \ldots) = f_{10,12} + 4f_{12,14} + \ldots$.

Eventually, the first non zero term should be $f_{12,14}$, hence $k \geq 14$. □

In fact, laborious calculations show that there is no $\mathbf{Q}_3$-polynomial isometry of $\mathbf{Z}_3$ of order 2 and valuation $k \leq 16$.

Examples of $\mathbf{Q}_p$-polynomial isometries of $\mathbf{Z}_p$ of order 2:

$$x \mapsto x + \frac{3X^2}{4} + \frac{X^4}{2^6} + \frac{X^6}{2^7} + \frac{X^8}{2^{10}}, \qquad (p = 2, k = 10)$$

$$x \mapsto 2x + \frac{X^2}{3} + \frac{X^3 + 2X^4}{3^3} + \frac{X^5}{3^6} + \frac{X^6 + 2X^5}{3^7} + \frac{X^7}{3^8} + \frac{2X^7 + 2X^8}{3^9} + \frac{2X^{10}}{3^{10}}$$
$$+ \frac{2(X^9 + X^{11})}{3^{11}} + \frac{X^{11} + X^{12} + X^{13}}{3^{12}} + \frac{X^{11} + 2X^{12} + X^{13}}{3^{13}} + \frac{1}{3^{14}}(X^{13} + X^{14})$$
$$+ \frac{X^{13} + X^{14} + 2X^{15} + X^{16}}{3^{15}} + \frac{2X^{15}}{3^{16}} + \frac{X^{15}}{3^{17}}, \qquad (p = 3, k = 17)$$

4.9. Valuation, order, and complexity

Let us come back to the expression 4.2 of a $\mathbf{Q}_p$-polynomial isometry of $\mathbf{Z}_p$. Propositions 4.2 and 4.4 can be really improved: many terms vanish thanks to Corollaries 4.2 to 4.5. We estimate

the complexity of $\mathbf{Q}_p$-polynomial isometries of any order, which permits simplifications of the expressions of the corresponding isometries.

From now, r, k and λ are respectively the order, the valuation and the complexity of a $\mathbf{Q}_p$-polynomial isometry f of $\mathbf{Z}_p$: the study of f is reduced to study if at most $n_b = 1+p+...+p^{\lambda-1}$ $\mathbf{F}_p$-polynomials are bijections of $\mathbf{F}_p$ and $n_i = p^\lambda$ $\mathbf{Z}_p$-polynomials are isometries of $\mathbf{Z}_p$.

We are going to define an increasing sequence (v_n) by choosing the best possible values such a way that: $k \leq v_n$ implies $r \leq n$. For example, using Corollary 4.5, we choose $v_1 = 5p+1$ if $p \geq 5$ and $v_1 = 4p+1$ if $p \leq 3$.

First, we conclude for $r \leq p-3$ and give the possible form of isometries.

Proposition 4.9. *We assume that $r \leq p-3$ (or $r \leq 1$ if $p \leq 3$).*

$*$ *If $k < 3p$, then $r = -1$, $\lambda = 1$ and $f = f_0 + Xh_1 + \sum_{j=1}^{k} \frac{1}{p^j} X^{j+1} h_{j+1}$.*

$*$ *If $p \neq 3$ and $k \leq 4p$, or $p = 3$ and $k \leq 9$, then $r \leq 0$ (so $v_0 = 4p$, or 9, and $\lambda = 2$), and*

$$f = f_0 + Xh_1 + \frac{1}{p} X^2 h_2 + \sum_{j=2}^{k} \frac{1}{p^j} (X^j f_j + X^{j+1} h_{j+1}).$$

$*$ *If $p \geq 5$ and $k \leq 5p+1$, (or $p = 2$ and $k \leq 9$, or $p = 3$ and $k \leq 13$), then $r \leq 1$ (so $v_1 = 5p+1$, or $4p+1$ if $p \leq 3$), $\lambda = 2$ and*

$$f = f_0 + Xh_1 + \frac{1}{p} X^2 h_2 + \frac{1}{p^2}(X^2 f_2 + X^3 h_3) + \sum_{j=3}^{k} \frac{1}{p^j}(X^{j-1} f_{j-1,j} + X^j f_j + X^{j+1} h_{j+1}).$$

$*$ *If $p \geq 5$ and $k \leq v_n$, then $r \leq n$ and $\lambda = 2$, where:*

for $n \leq p-5$, $v_n = 4p + n(p+1)$ if $n+3$ divides $p-1$, else $v_n = 3p + n(p+1)$,

$v_{p-4} = p^2 + p - 4$, $v_{p-3} = p^2 + p - 3$, and

$$\begin{aligned} f = {} & f_0 + Xh_1 + \frac{1}{p} X^2 h_2 + \frac{1}{p^2}(X^2 f_2 + X^3 h_3) + \frac{1}{p^3}(X^2 f_{2,3} + X^3 f_3 + X^4 h_4) + \dots \\ & + \frac{1}{p^{n+2}}(X^2 f_{2,n+2} + X^3 f_{3,n+2} + \dots + X^{n+2} f_{n+2} + X^{n+3} h_{n+3}) \\ & + \frac{1}{p^{n+3}}(X^3 f_{3,n+3} + X^4 f_{4,n+3} + \dots + X^{n+3} f_{n+3} + X^{n+4} h_{n+4}) + \dots \\ & + \frac{1}{p^k}(X^{k-n} f_{k-n,k} + X^{k-n+1} f_{k-n+1,k} + \dots + X^k f_k + X^{k+1} h_{k+1}). \end{aligned}$$

Proof. The first items are consequences of Corollaries 4.3 to 4.5.

Now, suppose $p \geq 5$ and $r = 3$, hence $k \geq v_1 + 1 = 5p+2$.

Let $f = f_0 + p \sum_{j=1}^{p-1} H_j + \sum_{j=1}^{p-1} F_j + \frac{1}{p} \sum_{j=1}^{p-1} F_{j,j+1} + \frac{1}{p^2} \sum_{j=1}^{p-1} F_{j,j+2} + \frac{1}{p^3} \sum_{j=1}^{p-1} F_{j,j+3}$.

Then $f_{|\beta} = \frac{1}{p^4}(Q_0 + Q_1 X + \dots + Q_5 X^5) + \frac{1}{p^3}(R_0 + \dots + R_4 X^4) + \dots$

where $Q_0 = Q_1 = R_0 = R_1 = 0$ according to Proposition 4.2.

Since $4 < 3p$, the order of $f_{|\beta}$ is -1, then $Q_2 = Q_3 = Q_4 = 0$, which gives the equalities of Proposition 4.8 relatively to $\mathbf{F}_p$-polynomials $f_{l,l+3}$. The first non zero term should be $f_{5p,5p+3}$, hence $k \geq 5p+3$, except when 5 divides $p-1$ (Corollary 3.1). In this last situation, $Q_5 = 0$ and, using Lemma 4.3 a) and the coefficients of X^{5-j} in Z^n, we have $\sigma_0 = ... = \sigma_5 = 0$ and $\sigma_6 - \sigma_5 + \sigma_7 - ... = 0$ for j from (1) to 5, eventually $k \geq 6p+3$.

Hence, $v_2 = 6p+2$ if 5 divides $p-1$, otherwise $v_2 = 5p+2$.

Suppose $r = n+1 \leq p-4$: the valuation k' of $f_{|\beta}$ satisfies $k' \leq r+1 < 3p$, hence the order of $f_{|\beta}$ is -1. With similar notations, $Q_0 = \ldots = Q_{n+2} = 0$. By Lemma 4.3 a), $\sigma_0 = \ldots = \sigma_{n+2} = 0$ and $\sigma_{n+3} - \sigma_{n+4} + \ldots = 0$ for $j = (1)$ to $n+2$, plus $Q_{n+3} = 0$ if $n+3$ divides $p-1$. The first non zero term should be $f_{n+3+(n+3)(p-1),2n+4+(n+3)(p-1)}$ with $k \geq n(p+1)+3p+1$ for the first case ($v_n = 3p+n(p+1)$); for the second one, $k \geq n(p+1)+4p+1$ and $v_n = 4p+n(p+1)$.

In particular, $v_{p-5} = p^2 - p$, for $p-2$ does not divide $p-1$.

If $r = p-3$, Corollary 3.1 gives $Q_0 = .. = Q_{p-1} = 0$. The first non-zero term should be $f_{1+(p+1)(p-1),p-2+(p+1)(p-1)}$, so $k \geq p^2+p-3$.

If $r = p-2$, we have the same equations (for example, $x \mapsto x + x^p$ is an isometry of degree p). Hence $k \geq p^2+p-2$ and $v_{p-3} = p^2+p-3$. □

Now, we estimate v_n and the corresponding complexity for $n \geq p-2$.

We first need to solve equations $Q_0 = Q_1 = \ldots = Q_N = 0$ for any natural $N \geq p$, where the first term of the expression of $f_{|\beta}$ is $\frac{1}{p^{r+1}}(Q_0 + Q_1 X + \ldots)$. As seen for $N = p-1$ in Proposition 4.9, we have to calculate the coefficient of X^N in $f_{|\beta}$, which is the coefficient of X^{N-j} in $F_{j,j+r}$.

The notation $\sigma_l + ...$ means $\sigma_l + a_2\sigma_{l+1} + a_3\sigma_{l+3} + \ldots$ for suitable a_i and $\sigma_l = \sigma_l(F_{j,j+r})$. By induction and using Lemma 4.3 e), we obtain:

Lemma 4.4. *Equations $Q_0 = Q_1 = \ldots = Q_N = 0$ imply:*

- *if $\alpha(p-1) < N < (\alpha+1)(p-1)$,*
  - *for all $1 \leq j \leq p-1$: $\sigma_0 = \sigma_1 = \ldots = \sigma_{N+\alpha-1} = 0 = \sigma_{N+\alpha} + ...$,*
  - *for all $(1) \leq j \leq N - \alpha(p-1)$: $\sigma_{N+\alpha+1} + ... = 0$,*
- *If $N = \alpha(p-1)$, for all $1 \leq j \leq p-1$: $\sigma_0 = ... = \sigma_{N+\alpha-1} = 0 = \sigma_{N+\alpha} + ...$*

Then the first non-zero term of such an isometry of order r should be

$f_{u+(N+\alpha+1)(p-1),u+(N+\alpha+1)(p-1)+r}$ (for the first case and $u = N-\alpha(p-1)+1$) or

$f_{1+(N+\alpha+1)(p-1),1+(N+\alpha)(p-1)+r}$ (for the second case since $f_1 = 0$).

Hence its valuation satisfies: $k \geq (N+1)p+r$. This is the main tool we use to build (v_n), which improves formula 4.2 for bigger values of the order, and gives an asymptotic evaluation of the complexity:

Proposition 4.10. *To study if a $\mathbf{Q}_p$-polynomial of order r is an isometry of $\mathbf{Z}_p$ can be reduced to study if at most n_b $\mathbf{F}_p$-polynomials are bijections of $\mathbf{F}_p$ and n_i $\mathbf{Z}_p$-polynomials are isometries of $\mathbf{Z}_p$, where $n_b \leq (1+p)(1+\frac{r}{3})$, $n_i \leq p^2+\frac{r}{3}(p^2-1)$, and where the complexity satisfies :* $\lambda \underset{r\to+\infty}{\sim} \log_p(r)$.

Proof. $*$ We proved in Proposition 4.9 that $v_{p-3} = p^2+p-3$. The same method gives similar results as long as the order of $f_{|\beta}$ satisfies $r' \leq -1$, where its valuation is $k' = r+1$ and $r' \leq r-1$ (Proposition 4.2). This happens as long as $p-1 \leq r \leq 3p-2$ since $k' < 3p$ and so $r' = -1$. Then $Q_0 = .. = Q_{r+1} = 0$ and $k \geq (r+2)p+r$ as seen after Lemma 4.4.

So, if $A_2 = p-2 \leq r < 3p-2 = A_3$, $v_r = (p+1)r+3p$ and $\lambda = 2$.

$*$ Let define V_2 on $[A_2,A_3[$ by $V_2(r) = (p+1)r+3p$. Let suppose that $q \geq 4$, $A_{q-1} < A_q$, $V_{q-1}(r) = v_r = \alpha_{q-1}r+\beta_{q-1}$ for r in $[A_{q-1},A_q[$ where the complexity λ is $q-1$. To build A_{q+1} and V_q on $[A_q,A_{q+1}[$ on which $\lambda = q$, we consider f of order $r = \gamma+1$, with $A_q \leq \gamma < A_{q+1}$ and such that the order r' of $f_{|\beta}$ satisfies $r' < A_q$, and so $k' = r+1 \leq V_{q-1}(A_q-1)$: then we choose $A_{q+1} = V_{q-1}(A_q-1)-1$. Then, $k' = r+1 \geq V_{q-1}(r'-1)+1 = \alpha_{q-1}(r'-1)+\beta_{q-1}+1$ when $r' \geq A_{q-1}$, and: $Q_0 = Q_1 = \ldots = Q_N = 0$ where $r+1-N = \lfloor \frac{r+\alpha_{q-1}-\beta_{q-1}}{\alpha_{q-1}} \rfloor + 1$. Then $k \geq (N+1)p+r$ as seen after Lemma 4.4 and finally we can choose $V_q(\gamma) = \alpha_q\gamma+\beta_q$ where $\alpha_q = (1-\frac{1}{\alpha_{q-1}})p+1$ and $\beta_q = (1+\frac{\beta_{q-1}-1}{\alpha_{q-1}})p$.

By induction, we built $(A_q)_{q\geq 3}$ and v such that $A_q \leq r < A_{q+1}$ implies $v_r = \alpha_q r+\beta_q$ with the former formulae.

$* \ \alpha_q = \dfrac{1-p^q}{1-p^{q-1}} \sim p$ and $\beta_q = (q+1)\dfrac{p^{q-1}(1-p)}{1-p^{q-1}} \sim q(p-1)$.

Now we estimate $A_q = \alpha_{q-2}(A_{q-1}-1)+\beta_{q-2}-1$, using $\dfrac{A_q}{1-p^{q-2}} - \dfrac{A_{q-1}}{1-p^{q-3}}$:

$A_q = (1-p^{q-2})\left(\frac{3p-2}{1-p} + \sum_{k=4}^{q} \frac{(1-p)kp^{k-3} - 2 + 2p^{k-2}}{(1-p^{k-3})(1-p^{k-2})}\right) \sim Lp^q$ with $L > 0$, which gives the estimation of λ since: $r \in [A_n, A_{n+1}[\Rightarrow \lambda = n$.

Finally, we estimate p^λ using $A_\lambda \leq r$, $n_b = 1 + p + \ldots + p^{\lambda-1}$ and $n_i = p^\lambda$. □

Conflict of Interests

The authors declare that there is no conflict of interests.

REFERENCES

[1] V. Anashin, Uniformly distributed sequences of p-adic integers, II. Discrete Math. Appl. 12 (2002), 527-590.

[2] V. Anashin, A. Khrennikov, Applied Algebraic Dynamics, de Gruyter Expositions in Mathematics. Walter de Gruyter GmbH & Co., Berlin-N.Y. (2009).

[3] E. Bishop, Isometries of the p-adic numbers, J. Ramanujan Math. Soc. 8 (1993), 1-5.

[4] E. S. Brussel, A family of p-adic isometries, fixed points, and the number three, arXiv math 0603387 (2006).

[5] J. Chauvineau, Quelques remarques sur les applications isométriques et la réparti-tion dans un corps p-adique, Séminaire Delange-Pisot-Poitou, Théorie des nombres, 6 (1964-65), 1-13.

[6] S. Katok, p-adic analysis in comparison with real, MASS Selecta: Teaching and Learning Advanced Undergraduate Mathematics, Providence (2003).

[7] G. H. Hardy, E. M. Wright, An Introduction to the Theory of Numbers, Oxford Science Publications (1990).

[8] M. Lapidus, M. Van Frankenhuijsen, Fractal geometry, complex dimensions and zeta functions: Geometry and spectra of fractal strings, 2nd edn. (Section 13.2), Springer (2013).

[9] M. Lapidus, H. Lu, Nonarchimedean Cantor set and string, J. Fixed Point Theory Appl. 3 (2008), 181-190.

[10] H. Lausch, W. Nobauer, Algebra of Polynomials, North-Holl. Publ. Co, American Elsevier (1973).

[11] R. Lidl R., H. Niederreiter, Finite Fields. Addison-Wesley Publ. Co. (1983).

[12] A. Robert, A course in p-adic analysis, Springer, New York (2000).