FACTORIZING GLEASON POLYNOMIALS MODULO 2

XAVIER BUFF, WILLIAM FLOYD, SARAH KOCH, AND WALTER PARRY

Abstract. Among the connected components of the interior of the Mandelbrot set are those that are hyperbolic. These components consist of parameters $c \in \mathbb{C}$ for which the critical point $z_0 = 0$ of $f_c : z \mapsto z^2 + c$ is attracted to an attracting periodic cycle. Every hyperbolic component contains a unique center; that is, a parameter $c$ for which the critical point $z_0$ is periodic. For a given $n \geq 1$, the Gleason polynomial for period $n$ is the monic polynomial $G_n \in \mathbb{Z}[c]$ whose roots are exactly the centers of the hyperbolic components of period $n$. It is unknown if $G_n$ factors over $\mathbb{Z}$. In this article, we factor $G_n$ modulo 2. We prove the following remarkable fact: the number of irreducible factors of $G_n$ modulo 2 is equal to the number of real roots that $G_n$ has in $\mathbb{C}$.

1. Introduction

Let $k = \mathbb{Q}$ be the field of rational numbers or $k = \mathbb{F}_2$ be the finite field with 2 elements. Let $\overline{k}$ be an algebraic closure of $k$.

Given $c \in \overline{k}$, denote by $f_c \in k[z]$ the quadratic polynomial

$$f_c(z) := z^2 + c.$$ 

A point $z \in \overline{k}$ is a periodic point for $f_c$ if $f_c^n(z) = z$ for some positive integer $n$. The least such integer is called the period of $z$.

If $z$ is periodic of period $n \geq 1$ for $f_c$, then $(c, z)$ is a zero of the polynomial $F_n \in k[c, z]$ defined by

$$F_n(c, z) := f_c^n(z) - z.$$ 

An elementary induction shows that $F_n$ has integer coefficients, degree $2^{n-1}$ with respect to $c$ and degree $2^n$ with respect to $z$. The coefficient of $c^{2^{n-1}}$ is 1 and the coefficient of $z^{2^n}$ is 1. If $m$ divides $n$, then $F_m(c, z) = 0$ implies $F_n(c, z) = 0$. In addition, the polynomial

$$F_m(0, z) = z^{2^m} - z \in \overline{k}[z]$$

has simple roots, so that $F_m$ is square-free. Thus, if $m$ divides $n$, then $F_m$ divides $F_n$ in $k[c, z]$. It follows that there exists a sequence $(\Phi_n \in k[c, z])_{n \geq 1}$ such that

$$F_n(c, z) = \prod_{m|n} \Phi_m(c, z).$$

The polynomial $\Phi_n$ is called the $n$-th dynatomic polynomial.

Let $\mu : \mathbb{N} \setminus \{0\} \to \{-1, 0, 1\}$ be the Möbius function, and let $(\delta_n)_{n \geq 1}$ be the sequence of integers defined by

$$\delta_n := \sum_{m|n} \mu(m) 2^{\frac{n}{m}}.$$ 

Date: August 22, 2022.

The research of the third author was supported in part by the NSF.
Then, the polynomial $\Phi_n$ has degree $\delta_n/2$ with respect to $c$ and degree $\delta_n$ with respect to $z$. In this article, we are interested in the factorization of $\Phi_n$ in $k[c, z]$.

The following result is due to Bousch [B].

**Theorem 1.1.** If $k = \mathbb{Q}$, then for $n \geq 1$, the dynatomic polynomial $\Phi_n$ is irreducible in $\mathbb{Q}[c, z]$.

We shall see that when $k = \mathbb{F}_2$, the situation is radically different. Let $(\gamma_n)_{n \geq 1}$ be the sequence defined by

$$
\gamma_n := \frac{1}{2^n} \sum_{m | n, m \text{ odd}} \mu(m)2^\frac{m}{n}.
$$

**Theorem 1.2.** If $k = \mathbb{F}_2$, then for $n \geq 1$, the dynatomic polynomial $\Phi_n$ has exactly $\gamma_n$ irreducible factors in $\mathbb{F}_2[c, z]$ which are monic with respect to $c$. These are of the form $Q(z^2 + c - z)$ with $Q \in \mathbb{F}_2[c]$. If $n$ is odd, then each factor has degree $2n$ with respect to $z$ and degree $n$ with respect to $c$. If $n$ is even, then there are $\gamma_n$ factors of degree $n$ with respect to $z$ and degree $n/2$ with respect to $c$, and there are $\gamma_n - \gamma_n/2$ factors of degree $2n$ with respect to $z$ and degree $n$ with respect to $c$.

Our proof in §6 relies on studying the restriction of $\Phi_n$ to the slice $\{z = 0\}$. Note that $0$ is a critical point of $f_c$, i.e., $f_c'(0) = 0$.

**Remark 1.3.** For $k = \mathbb{F}_2$, all points are critical points since the derivative of $f_c$ identically vanishes.

A parameter $c \in \overline{k}$ is called a center of period $n$ if $0$ is a periodic point of period $n$ for $f_c$. The centers of period $n$ are the roots of the polynomial $G_n \in k[c]$ defined by

$$G_n(c) = \Phi_n(c, 0).$$

The polynomial $G_n$ is called the $n$-th Gleason polynomial. It has degree $\delta_n/2$.

The factorization of Gleason and related polynomials in $\mathbb{Q}[c]$ as well as in $\mathbb{F}_2[c]$ has recently attracted attention (see for example [CK1] and [CK2]); in particular, there are implications regarding the irreducibility over $\mathbb{C}$ of some dynamically defined curves in the space of quadratic rational maps (see for example [BEK]). Here is a long-standing conjecture whose origin is unknown to us. See Remark 3.5 in [M].

**Conjecture 1.4.** If $k = \mathbb{Q}$, then for $n \geq 1$, the polynomial $G_n$ is irreducible in $\mathbb{Q}[c]$.

In the following statement, $M$ is the Mandelbrot set. For the notion of primitive or satellite hyperbolic components, see [4.4]. The following result is due to Lutzky [L1], [L2]. We shall present a proof in §4.4 that differs from Lutzky’s proof (see §4.5 for a discussion of Lutzky’s proof).

**Theorem 1.5.** If $k = \mathbb{Q}$, then $G_n$ has exactly $\gamma_n$ roots in $\mathbb{R}$. When $n$ is odd, these $\gamma_n$ roots are centers of primitive components of $M$. When $n$ is even, $\gamma_n/2$ of these roots are centers of satellite components of $M$ and $\gamma_n - \gamma_n/2$ of these roots are centers of primitive components of $M$.

We shall prove that when $k = \mathbb{F}_2$, there is a parallel count for the number of monic irreducible factors of the $n$-th Gleason polynomial $G_n$. A polynomial $P \in k[c]$ of degree $d$ is centered if the coefficient of $c^{d-1}$ is equal to 0. Otherwise it is noncentered.
Theorem 1.6. If $k = \mathbb{F}_2$, then $G_n$ has exactly $\gamma_n$ monic irreducible factors in $\mathbb{F}_2[c]$. When $n$ is odd, those factors are the $\gamma_n$ irreducible centered polynomials of degree $n$ in $\mathbb{F}_2[c]$. When $n$ is even, those factors are the $\gamma_{n/2}$ irreducible noncentered polynomials of degree $n/2$ in $\mathbb{F}_2[c]$ together with the $\gamma_n - \gamma_{n/2}$ irreducible centered polynomials of degree $n$ in $\mathbb{F}_2[c]$.

This will be proved in §5.

Remark 1.7. Theorem 1.6 generalizes to cases where the degree $d$ is a power of a prime. We state this generalization without proof in Theorem 1.8. We introduce the following notation in order to include the statement of the theorem in this more general case.

Let $d = p^r$, where $p$ is a prime number, and $r$ is a positive integer. Let $\kappa_n$ and $\rho_n$ be the following sequences

$$
\kappa_n = -\frac{(d-1)p}{dn} \sum_{p|m|n} \mu(m)d^{\mp},
$$
and

$$
\rho_n = \frac{1}{dn} \sum_{m|n} \mu(m)d^{\mp} - \frac{(p-1)(d-1)}{dn} \sum_{p|m|n} \mu(m)d^{\mp}.
$$

Theorem 1.8. If $k = \mathbb{F}_d$, then $G_n$ has exactly $\rho_n$ monic irreducible factors in $\mathbb{F}_d[c]$. When $p$ does not divide $n$, those factors are the $\rho_n$ irreducible centered polynomials of degree $n$ in $\mathbb{F}_d[c]$. When $p$ does divide $n$, those factors are the $\kappa_n$ irreducible noncentered polynomials of degree $n/p$ in $\mathbb{F}_d[c]$ together with the $\rho_n - \kappa_n$ irreducible centered polynomials of degree $n$ in $\mathbb{F}_d[c]$.

Remark 1.9. One might hope that there is a corresponding generalization of Theorem 1.5 to multibrot sets associated to prime powers. Unfortunately, the choice of what hyperbolic components to count is not clear. For example, there are no hyperbolic components with real centers if $p$ is odd.

We thank the referee for many helpful comments.

2. SOME SEQUENCES OF INTEGERS

Recall that $\mu : \mathbb{N} \setminus \{0\} \to \{-1, 0, 1\}$ is the Mőbius function and that for $n \geq 1$,

$$
\delta_n := \sum_{m|n} \mu(m)2^{\mp},
$$
so that

$$
2^n = \sum_{m|n} \delta_m.
$$

It will be convenient to consider the sequence $(\varepsilon_n)_{n \geq 1}$ defined by

$$
\varepsilon_n := -\sum_{m|n \text{ even}} \mu(m)2^{\mp} \quad \text{so that} \quad \delta_n + \varepsilon_n = \sum_{m|n \text{ odd}} \mu(m)2^{\mp}.
$$

Lemma 2.1. The sequence $(\varepsilon_n)_{n \geq 1}$ is characterized by the recursion

$$(1) \quad \forall n \geq 1, \quad \varepsilon_{2n-1} = 0 \quad \text{and} \quad \varepsilon_{2n} = \delta_n + \varepsilon_n.
$$

Remark 2.2. This shows that the sequence $(\varepsilon_n)_{n \geq 1}$ takes nonnegative values.
Remark 2.3. This lemma asserts that any sequence satisfying recursion (1) is equal to the sequence \((\varepsilon_n)_{n \geq 1}\).

**Proof.** First, assume \(n \geq 1\). Since \(2n - 1\) does not have any even divisor, the sum defining \(\varepsilon_{2n-1}\) is empty, so that \(\varepsilon_{2n-1} = 0\). In addition,

\[
\delta_n + \varepsilon_n = \sum_{m \mid n} \mu(m)2^{\frac{m}{n}} - \sum_{m \mid n, m \text{ is odd}} \mu(m)2^{\frac{m}{n}}
\]

\[
= \sum_{m \mid n, m \text{ is odd}} \mu(m)2^{\frac{m}{n}}
\]

\[
= - \sum_{m \mid 2n, m \text{ is odd}} \mu(2m)2^{\frac{2m}{n}} \quad \text{since when } m \text{ is odd, } \mu(m) = -\mu(2m)
\]

\[
= - \sum_{m \mid 2n, k \mid 2n, k \text{ is even}} \mu(k)2^{\frac{2m}{n}} \quad \text{since when } 4 \mid k, \mu(k) = 0
\]

\[
= \varepsilon_{2n}.
\]

Second, assume \((\varepsilon'_n)_{n \geq 1}\) is a sequence satisfying recursion (1). Let \((u_n)_{n \geq 1}\) be the sequence defined by

\[
u_n := \varepsilon'_n - \varepsilon_n.
\]

Then, for \(n \geq 1\), we have that

\[
u_{2n-1} = \varepsilon'_{2n-1} - \varepsilon_{2n-1} = 0 \quad \text{and} \quad u_{2n} = \delta_n + \varepsilon'_n - \delta_n - \varepsilon_n = u_n.
\]

It follows by induction that the sequence \((u_n)_{n \geq 1}\) identically vanishes, so that the sequence \((\varepsilon'_n)_{n \geq 1}\) is equal to the sequence \((\varepsilon_n)_{n \geq 1}\). \(\square\)

It shall be convenient to consider three related sequences \((\alpha_n)_{n \geq 1}\), \((\beta_n)_{n \geq 1}\) and \((\gamma_n)_{n \geq 1}\) defined by

\[
\alpha_n := \frac{\delta_n}{n} = \frac{1}{n} \sum_{m \mid n} \mu(m)2^{\frac{m}{n}}, \quad \beta_n := \frac{\varepsilon_n}{n} = -\frac{1}{n} \sum_{m \mid n, m \text{ is even}} \mu(m)2^{\frac{m}{n}}
\]

and

\[
\gamma_n := \frac{\delta_n + \varepsilon_n}{2n} = \frac{1}{2n} \sum_{m \mid n, m \text{ is odd}} \mu(m)2^{\frac{m}{n}}.
\]

**Lemma 2.4.** The sequences \((\beta_n)_{n \geq 1}\) and \((\gamma_n)_{n \geq 1}\) are characterized by the recursion

\[
\forall n \geq 1, \quad \beta_{2n-1} = 0 \quad \text{and} \quad \beta_{2n} = \gamma_n = \frac{\alpha_n + \beta_n}{2}.
\]

**Proof.** This is an immediate consequence of Lemma 2.1. \(\square\)

### 3. Counting periodic sequences

#### 3.1. Symbolic dynamics

Let us consider the set \(\Sigma\) of sequences of 0’s and 1’s:

\[
\Sigma := \{0, 1\}^{\mathbb{N} \smallsetminus \{0\}}.
\]

A sequence in \(\Sigma\) shall be denoted by \(s = (s_n)_{n \geq 1}\). Consider the shift \(\sigma : \Sigma \to \Sigma\) defined by

\[
\sigma(s_1, s_2, s_3, \ldots) := (s_2, s_3, s_4, \ldots).
\]

Let \(\Theta \subset \Sigma\) be the subset of periodic sequences. Given \(n \geq 1\), set

\[
\tilde{\Theta}_n := \{s \in \Sigma : \sigma^n(s) = s\}.
\]
Note that $\hat{\Theta}_n \subset \Theta$ is the set of sequences which are periodic under iteration of $\sigma$ with period dividing $n$. Denote by $\Theta_n \subseteq \hat{\Theta}_n$ the subset of sequences which have exact period $n$, so that

$$\Theta = \bigcup_{n \geq 1} \Theta_n.$$

**Lemma 3.1.** For $n \geq 1$, $\text{card}(\Theta_n) = \delta_n$.

**Proof.** A sequence $s \in \hat{\Theta}_n$ is uniquely characterized by $(s_1, s_2, \ldots, s_n)$ which may be any element of $\{0, 1\}^n$. As a consequence $\text{card}(\hat{\Theta}_n) = 2^n$. In addition, $\hat{\Theta}_n = \bigcup_{m|n} \Theta_m$ so that $2^n = \sum_{m|n} \text{card}(\Theta_m)$.

It follows from the Möbius inversion formula that for $n \geq 1$,

$$\text{card}(\Theta_n) = \sum_{m|n} \mu(m)2^{\frac{n}{m}} = \delta_n. \quad \Box$$

Consider now the involution $\iota : \Sigma \to \Sigma$ defined by

$$\iota(s_1, s_2, s_3, \ldots) := (1 - s_1, 1 - s_2, 1 - s_3, \ldots).$$

Note that $\sigma$ and $\iota$ commute. A sequence $s \in \Sigma$ is reflexive if its orbit under iteration of $\sigma$ contains $\iota(s)$. Let $\Xi \subset \Sigma$ be the subset of reflexive sequences. A reflexive sequence is necessarily periodic since $\sigma^{om}(s) = \iota(s) \Rightarrow \sigma^{o(2m)}(s) = s$.

For $n \geq 1$, let $\Xi_n$ be the set of reflexive sequences of period $n$:

$$\Xi_n := \Xi \cap \Theta_n.$$

**Lemma 3.2.** For $n \geq 1$, $\text{card}(\Xi_n) = \varepsilon_n$.

**Proof.** Assume $s \in \Xi_n$ and $\sigma^{ok}(s) = \iota(s)$. Let $0 < m < n$ be congruent to $k$ modulo $n$, so that $\sigma^{om}(s) = \sigma^{ok}(s) = \iota(s)$. Note that $\sigma^{o(2m)}(s) = s$ so that $n$ divides $2m$. Since $0 < 2m < 2n$, we have $n = 2m$. As a consequence, for $n \geq 1$,

$$\text{card}(\Xi_{2n-1}) = 0.$$ 

For $n \geq 1$, set

$$\hat{\Xi}_n := \{s \in \Xi : \sigma^{on}(s) = s\} \quad \text{and} \quad \hat{\Xi}'_n := \{s \in \Xi : \sigma^{on}(s) = \iota(s)\}.$$

Since $\iota : \Sigma \to \Sigma$ does not have any fixed point, $\hat{\Xi}_n \cap \hat{\Xi}'_n = \emptyset$. Assume $s \in \hat{\Xi}_n$, i.e., $s$ is a reflexive sequence of period dividing $2n$. Let $m \geq 1$ be the smallest integer such that $\sigma^{om}(s) = \iota(s)$. Then $s$ has period $2m$ which divides $2n$, so that $m$ divides $n$. If $m$ divides $n$ and $n/m$ is odd, then $s \in \hat{\Xi}_n'$; and if $n/m$ is even, then $s \in \hat{\Xi}_n$. Thus, for $n \geq 1$,

(2) $\hat{\Xi}_2n = \hat{\Xi}_n' \cup \hat{\Xi}_n$ so that $\text{card}(\hat{\Xi}_2n) = \text{card}(\hat{\Xi}_n') + \text{card}(\hat{\Xi}_n)$.

A sequence $s \in \hat{\Xi}_n'$ is uniquely characterized by $(s_1, s_2, \ldots, s_n)$ which may be any element of $\{0, 1\}^n$. Thus

$$\text{card}(\hat{\Xi}_n') = 2^n = \sum_{m|n} \delta_m.$$
As in the previous proof,

\[ \hat{\Xi}_n = \bigcup_{m \mid n} \Xi_m \quad \text{so that} \quad \text{card}(\hat{\Xi}_n) = \sum_{m \mid n} \text{card}(\Xi_m). \]

In addition, since \( \text{card}(\hat{\Xi}_k) = 0 \) if \( k \) is odd, we have that

\[ \text{card}(\hat{\Xi}_{2n}) = \sum_{2m \mid 2n} \text{card}(\Xi_{2m}) = \sum_{m \mid n} \text{card}(\Xi_{2m}). \]

Thus, for \( n \geq 1 \),

\[ \sum_{m \mid n} \text{card}(\Xi_{2m}) = \text{card}(\hat{\Xi}_{2n}) \quad \text{from } 5 \]

\[ = \text{card}(\hat{\Xi}'_n) + \text{card}(\hat{\Xi}_n) \quad \text{from } 2 \]

\[ = \sum_{m \mid n} \delta_m + \sum_{m \mid n} \text{card}(\Xi_m) \quad \text{from } 3 \text{ and } 4 \]

so that for \( n \geq 1 \),

\[ \text{card}(\Xi_{2n}) = \delta_n + \text{card}(\Xi_n). \]

The sequence \((\text{card}(\Xi_n))_{n \geq 1}\) satisfies recursion (1), thus is equal to \((\varepsilon_n)_{n \geq 1}\).

\[ \square \]

### 3.2. Multiplication by 2 in \( \mathbb{R}/\mathbb{Z} \)

Consider the map \( \tau : \Sigma \to \mathbb{R}/\mathbb{Z} \) defined by

\[ \tau(s) := \sum_{j \geq 1} s_j 2^{-j} \pmod{1}. \]

Note that \( \tau : \Sigma \to \mathbb{R}/\mathbb{Z} \) is surjective (every angle in \( \mathbb{R}/\mathbb{Z} \) has a binary expansion and \( s \) is the corresponding sequence of digits) but not injective. For example, \((0,0,0,\ldots)\) and \((1,1,1,\ldots)\) have the same image by \( \tau \). However, if two distinct sequences are identified, one is eventually constant equal to 0 and the other is eventually constant equal to 1. It follows that the only periodic sequences which are identified are \((0,0,0,\ldots)\) and \((1,1,1,\ldots)\).

The map \( \tau : \Sigma \to \mathbb{R}/\mathbb{Z} \) semi-conjugates the shift \( \sigma : \Sigma \to \Sigma \) to the doubling map \( D : \mathbb{R}/\mathbb{Z} \to \mathbb{R}/\mathbb{Z} \) defined by

\[ D(\theta) := 2\theta, \]

that is, \( D \circ \tau = \tau \circ \sigma \). An angle \( \theta \in \mathbb{R}/\mathbb{Z} \) is periodic under iteration of \( D \) with period dividing \( n \) if and only if \( \theta \) can be written as \( m/(2^n - 1) \) with \( m \in \mathbb{Z}/(2^n - 1)\mathbb{Z} \). In addition, if \( s \in \hat{\Theta}_n \), i.e., if \( s \) is periodic with period dividing \( n \), then

\[ \tau(s) = \frac{m}{2^n - 1} \quad \text{with} \quad m := \sum_{j=1}^{n} s_j 2^{n-j} \in \mathbb{Z}/(2^n - 1)\mathbb{Z}. \]

The map \( \tau : \Sigma \to \mathbb{R}/\mathbb{Z} \) semi-conjugates the involution \( \iota : \Sigma \to \Sigma \) to the involution \( I : \mathbb{R}/\mathbb{Z} \to \mathbb{R}/\mathbb{Z} \) defined by

\[ I(\theta) := -\theta, \]

that is, \( I \circ \tau = \tau \circ \iota \). For \( n = 1 \), the doubling map \( D : \mathbb{R}/\mathbb{Z} \to \mathbb{R}/\mathbb{Z} \) has only 1 fixed point, namely 0, and this point is fixed by the involution \( I \). For \( n \geq 2 \), it follows from [3.1] that the doubling map has \( \delta_n \) periodic points of exact period \( n \), and that among those, \( \varepsilon_n \) have an orbit which is invariant by the involution \( I \). So, for \( n \geq 2 \), there are \( \alpha_n \) orbits of period \( n \) and \( \beta_n \) among them are invariant by the involution \( I \).
4. Quadratic polynomials in \( \mathbb{Q} \)

In this section, we are mainly concerned with the dynamics of the quadratic polynomials \( f_c : \mathbb{Q} \to \mathbb{Q} \) defined by
\[
f_c(z) := z^2 + c \quad \text{with} \quad c \in \mathbb{Q}.
\]
For \( c \in \mathbb{Q} \), the periodic points of \( f_c \) of period dividing \( n \) are the roots of the polynomial \( f_c^n(z) - z \in \mathbb{Q}[z] \) which has degree 2\(^n\). It shall therefore be convenient to consider the sequence \( (F_n(c, z) \in \mathbb{Q}[c, z])_{n \geq 1} \) of polynomials defined by
\[
F_n(c, z) := f_c^n(z) - z.
\]
Those polynomials satisfy the recursion
\[
F_1(c, z) = z^2 - z + c \quad \text{and} \quad F_{n+1}(c, z) = F_n(c, z)^2 + c.
\]
It follows that they have integer coefficients, degree 2\(^{n-1}\) with respect to \( c \) and degree 2\(^n\) with respect to \( z \). The coefficient of \( c^{2^{n-1}} \) is 1 and the coefficient of \( z^{2^n} \) is 1.

4.1. The dynamics of \( f_0 : z \mapsto z^2 \). The periodic points of \( f_0 \) of period dividing \( n \) are the roots of the polynomial \( F_n(0, z) = z^{2^n} - z \in \mathbb{Q}[z] \), whose roots are simple. The fixed points are 0 and 1. The periodic points of period \( n \geq 2 \) are roots of unity.

Let \( U \subset \mathbb{Q} \) be the multiplicative group of roots of unity. The transcendental map \( \mathbb{Q}/\mathbb{Z} \ni \theta \mapsto \exp(2\pi i \theta) \in U \) is a group isomorphism which conjugates the doubling map \( D : \mathbb{Q}/\mathbb{Z} \to \mathbb{Q}/\mathbb{Z} \) to the restriction \( f_0 : U \to U \). It conjugates the involution \( I : \mathbb{Q}/\mathbb{Z} \to \mathbb{Q}/\mathbb{Z} \) to the involution \( \iota : U \to U \) defined by \( \iota(z) = 1/z \).

It follows from \( \{3.2\} \) that for \( n \geq 2 \), the squaring map \( f_0 : \mathbb{Q} \to \mathbb{Q} \) has \( \delta_n \) periodic points of exact period \( n \), and that among those, \( \varepsilon_n \) have an orbit which is invariant by the involution \( \iota \).

4.2. The dynamics of \( f_{-2} : z \mapsto z^2 - 2 \). Consider the map \( \psi : \mathbb{Q}\setminus\{0\} \to \mathbb{Q} \) defined by
\[
\psi(z) := z + \frac{1}{z}.
\]
The map \( \psi \) is a ramified covering of degree 2. Each point in \( \mathbb{Q} \) has two distinct preimages in \( \mathbb{Q}\setminus\{0\} \) except 2 which has a single preimage at \( z = 1 \) and \( -2 \) which has a single preimage at \( z = -1 \). In addition,
\[
\psi \circ f_0(z) = z^2 + \frac{1}{z^2} = \left(z + \frac{1}{z}\right)^2 - 2 = f_{-2} \circ \psi(z).
\]
So, \( \psi \) semi-conjugates \( f_0 : \mathbb{Q}\setminus\{0\} \to \mathbb{Q}\setminus\{0\} \) to \( f_{-2} : \mathbb{Q} \to \mathbb{Q} \).

4.3. Real dynamics. A parameter \( c \in \mathbb{Q} \) is a center if 0 is periodic under iteration of \( f_c \). It is a center of period \( n \) if 0 has period \( n \) for \( f_c \). The centers of period \( n \) are precisely the roots of the Gleason polynomial \( G_n \in \mathbb{Q}[c] \) defined by
\[
G_n(c) := \Phi_n(c, 0).
\]

Example 4.1. We have that
\[
G_1(c) = c, \quad G_2(c) = 1 + c, \quad G_3(c) = 1 + c + 2c^2 + c^3.
\]
We shall say that $c$ is a real center if $c \in \mathbb{R}$. The kneading sequence of a real center $c$ is

$$\kappa(c) := (\kappa_n)_{n \geq 0} \in \{+,-,\star\}^\mathbb{N} \text{ with } \kappa_n = \begin{cases} + & \text{if } f_c^n(0) > 0 \\ \star & \text{if } f_c^n(0) = 0 \\ - & \text{if } f_c^n(0) < 0 \end{cases}$$

The kneading angle of a real center $c$ is the angle $\theta(c) := \tau(t(c)) \in \mathbb{R}/\mathbb{Z}$ where $t(c) := (t_n)_{n \geq 1} \in \Sigma$ is defined by

$$\forall n \geq 0 \quad t_{n+1} = \begin{cases} 0 & \text{if } \kappa_n = \star \\ t_n & \text{if } \kappa_n = + \\ 1 - t_n & \text{if } \kappa_n = - \end{cases}$$

**Example 4.2.** The polynomial $G_3$ has a unique real root $c_3$. We have that

$$\kappa(c_3) = (\star,-,+,\star,-,+,\ldots), \quad t(c_3) = (0,1,1,0,1,1,\ldots) \quad \text{and} \quad \theta(c_3) = \frac{3}{7}.$$

Note that by definition, the first digit in the binary expansion of $\theta(c)$ is a 0, so that this angle belongs to the arc $[0,1/2) \subset \mathbb{R}/\mathbb{Z}$. The following result is due to Milnor and Thurston [MT].

**Theorem 4.3.** If $c_1 < c_2$ are real centers, then $\theta(c_1) > \theta(c_2)$. If $c$ is a center of period $n$, then $\theta(c)$ is periodic of period $n$ for the doubling map $D : \mathbb{R}/\mathbb{Z} \rightarrow \mathbb{R}/\mathbb{Z}$. In addition, a periodic angle $\theta \in [0,1/2) \subset \mathbb{R}/\mathbb{Z}$ of period $n$ is the kneading angle of some real center of period $n$ if and only if $\theta \in \mathbb{R}/\mathbb{Z}$ is the closest angle to $1/2 \in \mathbb{R}/\mathbb{Z}$ within its orbit under iteration of $D$.

This result enables us to count the number of real centers of period $n$ as follows. The doubling map has a unique orbit of period 1. This orbit is reduced to the angle $0 \in \mathbb{R}/\mathbb{Z}$ which is the angle of the unique center of period 1: $c = 0$. So assume the period is $n \geq 2$. On the one hand, assume $O$ is an orbit for the doubling map $D : \mathbb{R}/\mathbb{Z} \rightarrow \mathbb{R}/\mathbb{Z}$ which is invariant by the involution $I : \mathbb{R}/\mathbb{Z} \rightarrow \mathbb{R}/\mathbb{Z}$. Then $O$ contains exactly two angles closest to $1/2 \in \mathbb{R}/\mathbb{Z}$, one in the arc $(0,1/2) \in \mathbb{R}/\mathbb{Z}$, the other in the arc $(-1/2,0) \in \mathbb{R}/\mathbb{Z}$ being its image by the involution $I$. According to Theorem 4.3, there is exactly one real center with kneading angle in $O$. According to §3.2, there are $\beta_n$ such orbits corresponding to $\beta_n$ real centers of period $n$. On the other hand, assume $O$ and $O'$ are two distinct orbits of period $n$ which are exchanged by the involution $I : \mathbb{R}/\mathbb{Z} \rightarrow \mathbb{R}/\mathbb{Z}$. The closest angle to $1/2 \in \mathbb{R}/\mathbb{Z}$ in one of the two orbits is contained in the arc $(0,1/2) \in \mathbb{R}/\mathbb{Z}$ and the closest angle to $1/2 \in \mathbb{R}/\mathbb{Z}$ in the other orbit is contained in the arc $(-1/2,0) \in \mathbb{R}/\mathbb{Z}$. According to Theorem 4.3, there is exactly one real center with kneading angle in $O \cup O'$. There are $(\alpha_n - \beta_n)/2$ such pairs of orbits corresponding to $(\alpha_n - \beta_n)/2$ real centers of period $n$. Thus, the total number of real centers of period $n$ is

$$\beta_n + \frac{\alpha_n - \beta_n}{2} = \frac{\alpha_n + \beta_n}{2} = \gamma_n = \frac{1}{2^n} \sum_{m \mid n \text{ odd}} \mu(m)2^\pi.$$

**4.4. Complex dynamics.** We shall prove Theorem 1.5 in this section. We have the following description of the kneading angle. Consider the family of quadratic polynomials $(f_c : \mathbb{C} \rightarrow \mathbb{C})_{c \in \mathbb{C}}$ defined by

$$f_c(z) := z^2 + c.$$
The Mandelbrot set $\mathcal{M}$ is the set of parameters $c$ such that the orbit $(f_c^n(0))_{n \geq 0}$ is bounded. Douady and Hubbard proved that the Mandelbrot set is connected. More precisely, let $\mathbb{D} \subset \mathbb{C}$ be the unit disk. There exists a conformal isomorphism $\phi_M : \mathbb{C} \setminus \mathcal{M} \to \mathbb{C} \setminus \mathbb{D}$ which satisfies $\phi_M(c) = c + O(1)$ as $c \to \infty$. For $\theta \in \mathbb{R}/\mathbb{Z}$, the curve
$$R(\theta) := \{ c \in \mathbb{C} \setminus \mathcal{M} : \text{argument}(\phi_M(c)) = 2\pi\theta \pmod{2\pi} \}$$
is called the external ray of $\mathcal{M}$ of angle $\theta$. If $\theta \in \mathbb{R}/\mathbb{Z}$ is periodic for the doubling map $D : \mathbb{R}/\mathbb{Z} \to \mathbb{R}/\mathbb{Z}$, then the ray $R(\theta)$ lands at a parameter $c \in \mathcal{M}$, i.e., $R(\theta) \cap \mathcal{M} = \{c\}$. Figure 1 shows the Mandelbrot set together with the rays of angle $1/3$, $2/3$, $3/7$ and $4/7$.

Assume now that $c_0$ is a center of period $n$. Then, $c_0$ is contained in the interior of $\mathcal{M}$. Let $\mathcal{H}_{c_0}$ be the connected component of the interior of the Mandelbrot set $\mathcal{M}$ containing $c_0$. Such a connected component $\mathcal{H}_{c_0}$ is called a hyperbolic component of $\mathcal{M}$. If $c \in \mathcal{H}_{c_0}$, the quadratic polynomial $f_c : z \mapsto z^2 + c$ has an attracting cycle of period $n$. The product $\lambda(c)$ of the derivatives of $f_c$ at the points of this cycle is called the multiplier of this cycle. To say that the cycle is attracting means that $\lambda(c) \in \mathbb{D}$. The map $\lambda : \mathcal{H}_{c_0} \to \mathbb{D}$ is a holomorphic isomorphism which extends as a homeomorphism $\lambda : \mathcal{H}_{c_0} \to \mathbb{D}$. The parameter $c_1 := \lambda^{-1}(1)$ is called the root of the hyperbolic component $\mathcal{H}_{c_0}$. The quadratic polynomial $f_{c_1}$ has a parabolic cycle, i.e., a cycle whose multiplier is a root of unity. If this multiplier is 1, then $\mathcal{H}_{c_0}$ is called a primitive component of $\mathcal{M}$. Otherwise, $\mathcal{H}_{c_0}$ is called a satellite component of $\mathcal{M}$. 

![Figure 1. The Mandelbrot set. The external rays $R(1/3)$ and $R(2/3)$ land at the root $c = -3/4$ of the satellite component $\mathcal{H}_{-1}$. The rays $R(3/7)$ and $R(4/7)$ land at the root $c = -7/4$ of the primitive component $\mathcal{H}_{c_3}$, where $c_3$ is the unique real center of period 3.](image-url)
If \( c_0 = 0 \), which corresponds to the unique center of period 1, the root is \( c_1 = 1/4 \) and there is a single ray landing at \( c_1 \): the ray \( R(0) \). If \( c_0 \) is a center of period \( n \geq 2 \), there are two rays landing at \( c_1 \). When \( c_0 \) is real, then \( c_1 \) is also real and when the period is not 1, the two rays landing at \( c_1 \) are \( R\left(\theta(c_0)\right) \) (which is contained in the upper half-plane) and \( R\left(-\theta(c_0)\right) \) (which is contained in the lower half-plane). The angles \( \theta(c_0) \in \mathbb{R}/\mathbb{Z} \) and \( -\theta(c_0) \in \mathbb{R}/\mathbb{Z} \) belong to the same orbit under iteration of the doubling map \( D: \mathbb{R}/\mathbb{Z} \to \mathbb{R}/\mathbb{Z} \) if and only if \( H_{c_0} \) is a satellite component of \( M \).

It follows from the count presented in §4.3 that among the \( \gamma_n \) real centers of period \( n \), \( \beta_n \) are centers of satellite components of \( M \) and \( \gamma_n - \beta_n \) are centers of primitive components of \( M \). Note that \( \beta_n \neq 0 \) only when \( n \) is even. In particular, if \( n \) is odd, the \( \gamma_n \) real centers of period \( n \) are centers of primitive components of \( M \). When \( n \) is even, \( \beta_n = \gamma_n/2 \). Thus, when \( n \) is even, among the \( \gamma_n \) centers of period \( n \), there are \( \gamma_{n/2} \) centers of satellite components and \( \gamma_n - \gamma_{n/2} \) centers of primitive components. This completes the proof of Theorem 1.5.

4.5. Lutzky’s proof. The original argument of Lutzky for counting the number of real centers may be illustrated by Figure 2.

![Figure 2](attachment:image.png)

**Figure 2.** The curves of points \((c, z) \in [-2, 1/2] \times [-2, 2]\) such that \( z \) is periodic of period \( n \) for \( f_c \). Red: \( n = 1 \); blue: \( n = 2 \), green: \( n = 3 \); pink: \( n = 4 \). The line of equation \( z = c \) is tangent to those curves at points whose first coordinate is a real center.

For \( c > 1/4 \), the polynomial \( f_c \) has no real periodic point and for \( c = -2 \), the semi-conjugacy in §4.2 shows that the polynomial \( f_{-2} \) has \( \alpha_n \) cycles of period \( n \). As \( c \) increases from \(-2\) to \( 1/4 \), the \( \alpha_n \) cycles must bifurcate in order to leave the real axis and become complex conjugate cycles. At a pitchfork bifurcation (which
corresponds to roots of satellite components of period \( n \), a single cycle bifurcates, contributing to one real center. At other bifurcations (which correspond to roots of primitive components), two cycles bifurcate, still contributing to only one real center. In addition, each pitchfork bifurcation comes from a bifurcation of period \( n/2 \). Thus, if \( \gamma_n' \) stands for the number of real centers of period \( n \) and \( \beta_n' \) stands for the number of pitchfork bifurcations of period \( n \), then for \( n \geq 1 \),

\[
\beta_{2n-1}' = 0, \quad \beta_{2n}' = \gamma_n' \quad \text{and} \quad \alpha_n = \beta_n' + 2(\gamma_n' - \beta_n'),
\]

which may be re-written as

\[
\beta_{2n-1}' = 0, \quad \beta_{2n}' = \gamma_n = \frac{\alpha_n + \beta_n'}{2}.
\]

According to Lemma 2.4, we have that \( \beta_n' = \beta_n \) and \( \gamma_n' = \gamma_n \) for \( n \geq 1 \) as required.

The justification that each bifurcation contributes to exactly one real center relies on the result of Milnor and Thurston stated previously.

5. Quadratic dynamics in \( \mathbb{F}_2 \)

In this section, we consider the case \( k = \mathbb{F}_2 \). Theorem 1.6 will be established at the end of the section. Let us recall that for \( n \geq 1 \), the finite field \( \mathbb{F}_{2^n} \) with \( 2^n \) elements is the splitting field of \( z^{2^n} - z \) over \( \mathbb{F}_2 \). The Fröbenius endomorphism \( f_0: \mathbb{F}_2 \to \mathbb{F}_2 \) is an automorphism of \( \mathbb{F}_2 \) over \( \mathbb{F}_2 \); it fixes \( \mathbb{F}_2 \) pointwise and satisfies

\[
f_0(z + w) = f_0(z) + f_0(w) \quad \text{and} \quad f_0(zw) = f_0(z)f_0(w).
\]

More precisely, any point \( z \in \mathbb{F}_2 \) is periodic for \( f_0 \). Such a point is periodic of period exactly \( n \) if and only if it is an element of \( \mathbb{F}_{2^n} \), which is not contained in \( \mathbb{F}_{2^{n-1}} \) for some proper positive divisor \( m \) of \( n \). The conjugates of a point \( z \) of period \( n \) are the points of its orbit under iteration of \( f_0 \): \( z, f_0(z), \ldots, f_0^{(n-1)}(z) \). This orbit is the Galois orbit of \( z \). The minimal polynomial of such a point has degree \( n \) and vanishes precisely on its Galois orbit.

The periodic points of period \( n \) are the roots of the dynatomic polynomial

\[
\phi_n(z) := \Phi_n(0, z) \in \mathbb{F}_2[z].
\]

The irreducible monic polynomials of degree \( n \) in \( \mathbb{F}_2[z] \) are the factors of \( \phi_n \). The polynomial \( \phi_n \) has degree \( \delta_n \) and simple roots (since it divides \( z^{2^n} - z \) whose derivative is \(-1\)). So, there are precisely \( \alpha_n = \delta_n/n \) monic irreducible polynomials of degree \( n \) in \( \mathbb{F}_2[z] \). Equivalently, there are \( \alpha_n \) Galois orbits of period \( n \) in \( \mathbb{F}_2 \).

5.1. Critical orbit for \( f_c \).

**Lemma 5.1.** Assume \( c \in \overline{\mathbb{F}_2} \). Then, for all \( n \geq 1 \),

\[
f_c^{\circ n}(0) = c_0 + c_1 + \ldots + c_{n-1} \quad \text{with} \quad c_j := f_0^{\circ j}(c).
\]

**Proof.** The proof goes by induction. For \( n = 1 \), we have that

\[
f_c(0) = c = c_0.
\]

And if

\[
f_c^{\circ n}(0) = c_0 + c_1 + \ldots + c_{n-1},
\]

then,

\[
f_c^{\circ (n+1)}(0) = c + f_0(f_c^{\circ n}(0)) = c + f_0(c_0) + f_0(c_1) + \cdots + f_0(c_{n-1}) = c_0 + c_1 + c_2 + \cdots + c_n. \quad \square
\]
5.2. Points in $\mathbb{F}_2$ are centers. We shall say that a Galois orbit is centered if the associated minimal polynomial is centered, and noncentered otherwise.

Let us recall that $c \in \mathbb{F}_2$ is a center of period $n$ if $0$ is periodic of period $n$ under iteration of $f_c$.

**Lemma 5.2.** Any point $c \in \mathbb{F}_2$ is a center. Let $n$ be the period of $c$ under iteration of $f_0$ and let $m$ be the period of $0$ under iteration of $f_c$. If the Galois orbit of $c$ is centered, then $m = n$. If the Galois orbit of $c$ is noncentered, then $m = 2n$.

**Proof.** For $j \geq 0$, set

$$c_j := f_0^{2^j}(c) \quad \text{and} \quad z_j := f_0^{2^j}(0) = c_0 + c_1 + \ldots + c_{j-1}. $$

On the one hand, if $c$ is periodic of period $n$ for $f_0$, we have that $c_{n+j} = c_j$ for all $j \geq 0$, and so

$$z_{2n} = 2(c_0 + c_1 + \ldots + c_{n-1}) = 0. $$

Thus, $0$ is periodic for $f_c$ and the period $m$ divides $2n$. On the other hand, if $z_m = 0$ for some $m \geq 1$, then

$$f_0^{2m}(c) = c_m = z_m + c_m = z_{m+1} = z_m^2 + c = c. $$

Thus, the period $n$ of $c$ for $f_0$ divides $m$. Since $m$ divides $2n$ and $n$ divides $m$, this forces either $m = n$ or $m = 2n$.

Let $P$ be the minimal polynomial of $c$. Its roots are the points $c_0, c_1, \ldots, c_{n-1}$. As a consequence, $0$ is periodic of period $n$ for $f_c$ if and only if $z_n = 0$, i.e., if and only if $c_0 + c_1 + \ldots + c_{n-1} = 0$, i.e., if and only if $P$ is centered. □

5.3. From dynamical plane to parameter space. Let $\iota : \mathbb{F}_2 \setminus \{0\} \to \mathbb{F}_2 \setminus \{0\}$ be the involution defined by

$$\iota(\vartheta) = \frac{1}{\vartheta}. $$

Assume $\vartheta \in \mathbb{F}_2 \setminus \{0\}$. Then,

$$\vartheta + \iota(\vartheta) = 0 \iff \vartheta^2 + 1 = 0 \iff \vartheta = 1. $$

We may therefore consider the map $\psi : \mathbb{F}_2 \setminus \mathbb{F}_2 \to \mathbb{F}_2 \setminus \{0\}$ defined by

$$\psi(\vartheta) := \frac{1}{\vartheta + \iota(\vartheta)} = \frac{\vartheta}{\vartheta^2 + 1}. $$

The involution $\iota$ and the map $\psi$ commute with $f_0$. So, they send Galois orbits to Galois orbits.

**Lemma 5.3.** The map $\psi : \mathbb{F}_2 \setminus \mathbb{F}_2 \to \mathbb{F}_2 \setminus \{0\}$ is surjective and each fiber contains two distinct points; those are exchanged by the involution $\iota$.

**Proof.** Assume $c \in \mathbb{F}_2 \setminus \{0\}$. Then, $\psi(\vartheta) = c$ if and only if $\vartheta^2 - \vartheta/c + 1 = 0$. The discriminant of this quadratic polynomial is $1/c^2 \neq 0$. So, there are two distinct roots. The product of the roots is $1$. So, they are exchanged by $\iota$. □

**Lemma 5.4.** Assume $\vartheta \in \mathbb{F}_2 \setminus \mathbb{F}_2$ and $c = \psi(\vartheta)$. Let $n$ be the period of $\vartheta$ for $f_0$ and let $m$ be the period of $c$ for $f_0$. If $\vartheta$ is conjugate to $1/\vartheta$, then $n = 2m$ and the minimal polynomial of $c$ is noncentered. Otherwise $n = m$ and the minimal polynomial of $c$ is centered.
Proof. By assumption, the Galois orbit of $\vartheta$ contains $n$ points and the Galois orbit of $c$ contains $m$ points. Since $\psi$ commutes with $f_0$, it sends the Galois orbit of $\vartheta$ to the Galois orbit of $c$. According to Lemma 5.3, the fibers of $\psi : \mathbb{F}_2 \setminus \mathbb{F}_2 \to \mathbb{F}_2 \setminus \{0\}$ contain exactly two points which are exchanged by the involution $\iota$. So, if the Galois orbit of $\vartheta$ is preserved by the involution $\iota$, then its image by $\psi$ contains $m = n/2$ points. Otherwise it contains $m = n$ points.

Lemma 5.5. Assume $\vartheta \in \overline{\mathbb{F}}_2 \setminus \mathbb{F}_2$ and $c = \psi(\vartheta)$. Then, for $n \geq 1$,

$$f_c^n(0) = \frac{\vartheta + \vartheta^2 + \vartheta^3 + \cdots + \vartheta^{2^n - 1}}{\vartheta^{2^n} + 1}.$$

Proof. For $n \geq 0$, set

$$c_n := f_0^n(c) = \frac{\vartheta^{2^n}}{\vartheta^{2^n+1} + 1} = \frac{\vartheta^{2^n}}{(\vartheta^{2^n} + 1)^2}.$$  

According to Lemma 5.1, we have that for $n \geq 0$,

$$f_c^n(0) = c_0 + c_1 + \cdots + c_{n-1}.$$  

Now, the proof goes by induction. For $n = 1$, we have that

$$f_c(0) = c = \frac{1}{\vartheta + 1/\vartheta} = \frac{\vartheta}{\vartheta^2 + 1}.$$  

And if

$$f_c^n(0) = \frac{\vartheta + \vartheta^2 + \vartheta^3 + \cdots + \vartheta^{2^n - 1}}{\vartheta^{2^n} + 1},$$  

then

$$f_c^{n+1}(0) = f_c^n(0) + c_n$$

$$= \frac{\vartheta + \vartheta^2 + \cdots + \vartheta^{2^n - 1}}{\vartheta^{2^n} + 1} + \frac{\vartheta^{2^n}}{(1 + \vartheta^{2^n})(\vartheta^{2^n} + 1)}$$

$$= \frac{(\vartheta + \vartheta^2 + \cdots + \vartheta^{2^n - 1})(\vartheta^{2^n} + 1) + \vartheta^{2^n}}{(1 + \vartheta^{2^n})(\vartheta^{2^n} + 1)}$$

$$= \frac{(\vartheta + \vartheta^2 + \cdots + \vartheta^{2^n - 1}) + \vartheta^{2^n} + (\vartheta^{2^n+1} + \cdots + \vartheta^{2^{n+1} - 1})}{\vartheta^{2^{n+1} + 1}}.$$  

Lemma 5.6. Assume $\vartheta \in \overline{\mathbb{F}}_2 \setminus \mathbb{F}_2$ is periodic of period $n \geq 2$ for $f_0$ and $c = \psi(\vartheta)$. Then, $0$ is periodic of period $n$ for $f_c$.

Proof. According to Lemma 5.5, for $j \geq 1$,

$$f_c^j(0) = \frac{\vartheta + \vartheta^2 + \vartheta^3 + \cdots + \vartheta^{2^j - 1}}{\vartheta^{2^j} + 1} = \frac{\vartheta^{2^j} - \vartheta}{(\vartheta - 1)(\vartheta^{2^j} + 1)} = f_c^{2^j}(\vartheta) - \vartheta = f_c^j(0) - \vartheta.$$  

Thus, $f_c^j(0) = 0$ if and only if $j$ is a multiple of $n$. 

5.4. Counting orbits. For $n \geq 1$, let $\alpha'_n$ be the number of Galois orbits in $\mathbb{F}_2 \setminus \{0\}$ which have period $n$, and let $\beta'_1$ be the number of those orbits which are invariant by the involution $\iota$. Then, $\alpha'_1 = \beta'_1 = 1$ since the only fixed point of $f_0$ in $\mathbb{F}_2 \setminus \{0\}$ is 1. And $\alpha'_n = \alpha_n$ for $n \geq 2$. 

Lemma 5.7. We have that
\[ \beta'_1 = 1 \quad \text{and} \quad \forall n \geq 1 \quad \begin{cases} 
\beta'_n = \alpha'_n + \beta'_n \\
\beta'_{2n+1} = 0.
\end{cases} \]

Proof. The only fixed point of \( \iota \) is 1, which is a fixed point of \( f_0 \). So, \( \beta'_1 = 1 \) and if a Galois orbit is preserved by \( \iota \), then its cardinality must be even. It follows that \( \beta'_{2n+1} = 0 \). Next, a Galois orbit of period \( n \) for \( f_0 \) is the image by \( \psi \) of
- either a Galois orbit of period 2\( n \) which is invariant by \( \iota \),
- or two distinct Galois orbits of period \( n \) which are exchanged by \( \iota \).

It follows that
\[ \alpha'_n = \beta''_n + \alpha'_n - \beta'_n \]
so that
\[ \beta''_n = \alpha'_n + \beta'_n. \]

□

Lemma 5.8. We have that \( \beta''_n = \beta_n \) for \( n \geq 2 \).

Proof. Consider the sequence \( (\beta''_n)_{n \geq 1} \) defined by
\[ \beta''_1 := 0 \quad \text{and} \quad \forall n \geq 2 \quad \beta''_n := \beta'_n. \]

Note that \( \alpha'_1 + \beta'_1 = 2 = \alpha_1 + \beta''_1 \), so that for \( n \geq 1 \),
\[ \alpha'_n + \beta''_n = \alpha_n + \beta''_n. \]

Thus, according to Lemma 5.7
\[ \forall n \geq 1, \quad \beta''_{2n-1} = 0 \quad \text{and} \quad \beta''_{2n} = \beta''_{2n} = \frac{\alpha'_n + \beta'_n}{2} = \frac{\alpha_n + \beta''_n}{2}. \]

According to Lemma 2.4, we have that \( \beta''_n = \beta_n \) for \( n \geq 1 \).

□

Lemma 5.9. For \( n \geq 1 \), the \( n \)-th Gleason polynomial has \( \gamma_n \) monic irreducible factors in \( \mathbb{F}_2[c] \).

Proof. For \( n \geq 1 \), let \( \gamma'_n \) be the number of Galois orbits of centers of period \( n \) in \( \mathbb{F}_2[c] \). For \( n = 1 \), we have \( \gamma'_1 = 1 = \gamma_1 \). For \( n \geq 2 \), according to Lemma 5.6, the Galois orbits of centers of period \( n \) are the images by \( \psi \) of the Galois orbits of period \( n \) for \( f_0 \). According to Lemma 5.4, the centered ones are the images of the Galois orbits which are not invariant by the involution \( \iota \). There are \( (\alpha_n - \beta_n)/2 \) such orbits. The noncentered ones are the images of the Galois orbits which are invariant by the involution \( \iota \). There are \( \beta_n \) such orbits. Therefore,
\[ \gamma'_n = \frac{\alpha_n - \beta_n}{2} + \beta_n = \frac{\alpha_n + \beta_n}{2} = \gamma_n. \]

This completes the proof of Theorem 1.6

6. Dynatomic polynomials in \( \mathbb{F}_2[c, z] \)

We finally prove Theorem 1.2. The proof relies on the following observation. Recall that for \( n \geq 1 \),
\[ F_n(c, z) := f^n_c(z) - z. \]

Lemma 6.1. For \( n \geq 1 \), we have the following equality in \( \mathbb{F}_2[c, z] \):
\[ F_n(c, z) = H_n(z^2 + c - z) \quad \text{with} \quad H_n(c) := F_n(c, 0). \]
Proof. Observe that for \( n \geq 1 \),
\[
H_{n+1}(c) = f_c^{\circ(n+1)}(0) = (f_c^{\circ n}(0))^2 + c = H_n^2(c) + c.
\]
We shall prove the result by induction on \( n \geq 1 \). For \( n = 1 \), we have that
\[
F_1(c, z) = f_c(z) - z = z^2 + c - z.
\]
So, the result holds.

Let us now assume that for some \( n \geq 1 \),
\[
F_n(c, z) = H_n(z^2 + c - z).
\]
Then,
\[
F_{n+1}(c, z) = \left( F_n(c, z) + z \right)^2 + c - z
= \left( H_n(z^2 + c - z) + z \right)^2 + c - z
= H_n^2(z^2 + c - z) + z^2 + c - z = H_{n+1}(z^2 + c - z).
\]
This completes the proof by induction.

For \( n \geq 1 \), we now have
\[
F_n(c, z) = \prod_{m \mid n} \Phi_m(c, z) \quad \text{and} \quad H_n(c) = \prod_{m \mid n} G_m(c).
\]
As a consequence, for \( n \geq 1 \),
\[
\Phi_n(c, z) = G_n(z^2 + c - z).
\]
On the one hand, it follows that if \( P(c) \) divides \( G_n(c) \), then \( P(z^2 + c - z) \) divides \( \Phi_n(c, z) \). Thus, \( \Phi_n \) has at least \( \gamma_n \) irreducible factors which are monic with respect to \( c \). On the other hand, if \( Q(c, z) \) is a factor of \( \Phi_n(c, z) \) which is monic with respect to \( c \), then \( Q(c, 0) \) is a monic factor of \( G_n(c) \). This shows that \( \Phi_n(c, z) \) has at most \( \gamma_n \) factors which are monic with respect to \( c \). Thus, \( \Phi_n(c, z) \) has exactly \( \gamma_n \) factors which are monic with respect to \( c \). Theorem 1.2 now follows easily from Theorem 1.6.

APPENDIX A. ITINERARIES OF ROOTS OF LOW-DEGREE GLEASON POLYNOMIALS

In this appendix, we present for each period \( n \in [1, 8] \) two tables. The first table corresponds to \( k = \mathbb{Q} \). It contains:

- the (approximate) value of the real center of period \( n \),
- the initial segment of its kneading sequence (to be repeated periodically with period \( n \)),
- the kneading angle \( \theta(c) \) with its binary expansion and
- the cycles in \( \mathbb{Z}/(2^n - 1)\mathbb{Z} \) of \( (2^n - 1)\theta(c) \) and \( -(2^n - 1)\theta(c) \).

The second table corresponds to \( k = \mathbb{F}_2 \). It contains:

- the minimal polynomials \( P \in \mathbb{F}_2[c] \) of the centers of period \( n \),
- the coefficients of \( c^k \) of \( P(c) \) and
- the minimal polynomials of the numbers \( \vartheta \in \mathbb{F}_2 \) such that \( P \circ \psi(\vartheta) = 0 \).

For periods 9 and 10, we only present the first table.
A.1. Period 1.

\[ G_1(c) = c \quad \text{and} \quad \gamma_1 = 1. \]

\[
\begin{array}{c|ccc|c}
\hline
0 & (\ast) & 0/1 = & .6 & \{0\} \\
\hline
c & (0, 1) & \vartheta & \\
\hline
\end{array}
\]


\[ G_2(c) = 1 + c \quad \text{and} \quad \gamma_2 = 1. \]

\[
\begin{array}{c|ccc|c}
\hline
-1 & (\ast, -) & 1/3 = & .01 & \{1, 2\} \\
\hline
1 + c & (1, 1) & 1 + \vartheta + \vartheta^2 & \\
\hline
\end{array}
\]


\[ G_3(c) = 1 + c + 2c^2 + c^3 \quad \text{and} \quad \gamma_3 = 1. \]

\[
\begin{array}{c|ccc|c}
\hline
-1.754878 & (\ast, -, +) & 3/7 = & .0111 & \{1, 2, 4\} \{6, 5, 3\} \\
\hline
1 + c + c^2 & (1, 1, 0, 1) & (1 + \vartheta + \vartheta^2)(\vartheta^3 + \vartheta^4 + 1) & \\
\hline
\end{array}
\]


\[ G_4(c) = 1 + 2c^2 + 3c^3 + 3c^4 + 3c^5 + c^6 \quad \text{and} \quad \gamma_4 = 2. \]

\[
\begin{array}{c|ccc|c}
\hline
-1.940800 & (\ast, - , +) & 7/15 = & .0111 & \{1, 2, 4, 8\} \{14, 13, 11, 7\} \\
\hline
-1.310703 & (\ast, - , -) & 6/15 = 2/5 = & .0110 & \{3, 6, 12, 9\} \\
\hline
1 + c + c^4 & (1, 1, 0, 1) & (1 + \vartheta + \vartheta^2)(\vartheta^3 + \vartheta^4 + 1) & \\
1 + c + c^2 & (1, 1, 1) & 1 + \vartheta + \vartheta^2 + \vartheta^3 + \vartheta^4 & \\
\hline
\end{array}
\]

A.5. Period 5.

\[ G_5(c) = 1 + c + 2c^2 + 5c^3 + 14c^4 + 26c^5 + 44c^6 + 69c^7 + 94c^8 \\
+ 114c^9 + 116c^{10} + 94c^{11} + 60c^{12} + 28c^{13} + 8c^{14} + c^{15} \]

and

\[ \gamma_5 = 3. \]

\[
\begin{array}{c|ccc|c}
\hline
-1.985424 & (\ast, -, + , +) & 15/31 = & .0111 & \{1, 2, 4, 8, 16\} \{30, 29, 27, 23, 15\} \\
\hline
-1.860783 & (\ast, -, + , -) & 14/31 = & .0110 & \{3, 6, 12, 17\} \{28, 25, 19, 7, 14\} \\
\hline
-1.625414 & (\ast, -, -, -) & 13/31 = & .0110 & \{5, 10, 20, 9, 18\} \{26, 21, 11, 22, 13\} \\
\hline
1 + c^2 + c^5 & (1, 0, 1, 0, 1) & (1 + \vartheta + \vartheta^2 + \vartheta^4 + \vartheta^6)(\vartheta^3 + \vartheta^4 + \vartheta^5 + \vartheta + 1) & \\
1 + c^2 + c^3 & (1, 0, 0, 1, 0) & (1 + \vartheta + \vartheta^2 + \vartheta^3 + \vartheta^4 + \vartheta + 1) & \\
1 + c + c^2 + c^3 + c^5 & (1, 1, 1, 0, 1) & (1 + \vartheta + \vartheta^2 + \vartheta^3 + \vartheta^4)(\vartheta^3 + \vartheta^4 + \vartheta^5 + \vartheta^6 + 1) & \\
\hline
\end{array}
\]

\[ G_6(c) = 1 - c + c^2 + 3c^3 + 7c^4 + 17c^5 + 35c^6 + 75c^7 + 155c^8 + 298c^9 + 536c^{10} + 927c^{11} + 1525c^{12} + 2331c^{13} + 3310c^{14} + 4346c^{15} + 5258c^{16} + 5843c^{17} + 5892c^{18} + 5313c^{19} + 4219c^{20} + 2892c^{21} + 1672c^{22} + 792c^{23} + 293c^{24} + 78c^{25} + 13c^{26} + c^{27} \]

and

\[ \gamma_6 = 5. \]

\[
\begin{array}{|c|c|c|}
\hline
-1.996376 & (\ast,-,+,+,+,+) & \frac{31}{63} = .01111111 \quad \{1,2,4,8,16,32\} \quad \{62,61,59,55,47,31\} \\
-1.966773 & (\ast,-,+,+,+,-) & \frac{30}{63} = \frac{10}{21} = .0111110 \quad \{3,6,12,24,48,33\} \quad \{60,57,51,39,15,30\} \\
-1.907280 & (\ast,-,+,+,+,-) & \frac{29}{63} = .0111101 \quad \{5,10,20,40,17,34\} \quad \{58,53,43,23,46,29\} \\
-1.772893 & (\ast,-,+,+,+,+) & \frac{28}{63} = \frac{4}{9} = .011100 \quad \{7,14,28,56,49,35\} \\
-1.476015 & (\ast,-,+,+,-,-) & \frac{26}{63} = .011010 \quad \{11,22,44,25,50,37\} \quad \{52,41,19,38,13,26\} \\
\hline
\end{array}
\]


\[ \deg(G_7) = 63 \quad \text{and} \quad \gamma_7 = 9. \]

\[
\begin{array}{|c|c|c|}
\hline
-1.999906 & (\ast,-,+,+,+,+,) & \frac{127}{255} = .0111111 \quad \{1,2,4,8,16,32,64\} \quad \{126,125,123,119,111,95,63\} \\
-1.991814 & (\ast,-,+,+,+,+,-) & \frac{127}{255} = .0111110 \quad \{3,6,12,24,48,96,65\} \quad \{124,121,115,103,79,31,62\} \\
-1.977180 & (\ast,-,+,+,+,+,-) & \frac{127}{255} = .0111101 \quad \{5,10,20,40,80,33,66\} \quad \{122,117,107,87,47,94,61\} \\
-1.953706 & (\ast,-,+,+,+,+,-) & \frac{127}{255} = .0111100 \quad \{7,14,28,56,112,97,67\} \quad \{120,113,99,71,15,30,60\} \\
-1.927148 & (\ast,-,+,+,+,+,-) & \frac{127}{255} = .0111100 \quad \{9,18,36,72,17,34,68\} \quad \{118,109,91,55,110,93,59\} \\
-1.884804 & (\ast,-,+,+,+,+,-) & \frac{127}{255} = .0111100 \quad \{11,22,44,88,49,98,69\} \quad \{116,105,83,39,78,29,58\} \\
-1.832315 & (\ast,-,+,+,+,+,-) & \frac{127}{255} = .0111100 \quad \{13,26,52,104,81,35,70\} \quad \{114,101,75,23,46,92,57\} \\
-1.674066 & (\ast,-,+,+,+,+,-) & \frac{127}{255} = .0111100 \quad \{19,38,76,25,50,100,73\} \quad \{108,89,51,102,77,27,54\} \\
-1.574889 & (\ast,-,+,+,+,+,-) & \frac{127}{255} = .0111100 \quad \{21,42,84,41,82,37,74\} \quad \{106,85,43,86,45,90,53\} \\
\hline
\end{array}
\]

\[
\begin{array}{|c|c|c|}
\hline
1 + c + c^2 & (1,1,0,0,0,0,1) & (\vartheta + \vartheta^3 + \vartheta^5 + \vartheta + 1)(\vartheta + \vartheta^5 + \vartheta^6 + \vartheta + 1) \\
1 + c^2 + c^3 & (1,0,1,0,0,0,1) & (\vartheta + \vartheta^6 + \vartheta^7 + \vartheta^8 + \vartheta + 1)(\vartheta^4 + \vartheta^6 + \vartheta^8 + \vartheta^9 + \vartheta + 1) \\
1 + c + c^2 + c^3 + c^4 & (1,1,1,0,0,0,1) & (\vartheta + \vartheta^4 + \vartheta^5 + \vartheta^6 + \vartheta + 1)(\vartheta + \vartheta^5 + \vartheta^9 + \vartheta^7 + \vartheta + 1) \\
1 + c^2 + c^3 + c^4 + c^5 & (1,0,1,1,0,0,1) & (\vartheta^4 + \vartheta^5 + \vartheta^6 + \vartheta + 1)(\vartheta^4 + \vartheta^5 + \vartheta^9 + \vartheta^7 + \vartheta + 1) \\
1 + c^2 + c^3 + c^4 + c^5 & (1,1,1,0,1,0,1) & (\vartheta^4 + \vartheta^5 + \vartheta^6 + \vartheta + 1)(\vartheta^4 + \vartheta^5 + \vartheta^9 + \vartheta^7 + \vartheta + 1) \\
1 + c^2 + c^3 + c^4 + c^5 & (1,0,0,1,1,0,1) & (\vartheta^4 + \vartheta^5 + \vartheta^6 + \vartheta + 1)(\vartheta^4 + \vartheta^5 + \vartheta^9 + \vartheta^7 + \vartheta + 1) \\
1 + c + c^2 + c^3 + c^4 + c^5 & (1,1,0,1,0,1,1) & (\vartheta^4 + \vartheta^5 + \vartheta^6 + \vartheta + 1)(\vartheta^4 + \vartheta^5 + \vartheta^9 + \vartheta^7 + \vartheta + 1) \\
1 + c^2 + c^3 + c^4 + c^5 & (1,0,1,1,1,0,1) & (\vartheta^4 + \vartheta^5 + \vartheta^6 + \vartheta + 1)(\vartheta^4 + \vartheta^5 + \vartheta^9 + \vartheta^7 + \vartheta + 1) \\
1 + c^2 + c^3 + c^4 + c^5 & (1,1,1,1,0,0,1) & (\vartheta^4 + \vartheta^5 + \vartheta^6 + \vartheta + 1)(\vartheta^4 + \vartheta^5 + \vartheta^9 + \vartheta^7 + \vartheta + 1) \\
\hline
\end{array}
\]
### A.8. Period 8.

\[
\deg(G_s) = 120 \quad \text{and} \quad \gamma_8 = 16.
\]

\[
\begin{align*}
&1 + c^3 + c^4 \\
&1 + c + c^3 + c^4 + c^6 \\
&1 + c + c^3 + c^4 + c^5 \\
&1 + c^2 + c^3 + c^4 + c^5 \\
&1 + c + c^2 + c^3 + c^4 + c^5 + c^6 + c^8 \\
&1 + c + c^2 + c^3 + c^4 + c^5 + c^6 + c^8
\end{align*}
\]

<table>
<thead>
<tr>
<th>[a ]</th>
<th>[b ]</th>
<th>[c ]</th>
</tr>
</thead>
<tbody>
<tr>
<td>1, 0, 1, 0, 1, 1</td>
<td>1, 1, 1, 1, 1, 1</td>
<td>1, 0, 1, 0, 1, 1</td>
</tr>
<tr>
<td>1, 1, 0, 1, 0, 1, 0, 1, 1</td>
<td>1, 0, 1, 1, 0, 1, 0, 1, 1</td>
<td>1, 1, 1, 1, 1, 1, 1, 1, 1</td>
</tr>
<tr>
<td>1, 0, 1, 0, 1, 1, 1, 1, 1, 1</td>
<td>1, 0, 1, 0, 1, 1, 1, 1, 1, 1</td>
<td></td>
</tr>
<tr>
<td>1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1</td>
<td>1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1</td>
<td></td>
</tr>
<tr>
<td>1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

\[
\begin{align*}
\vartheta^0 + \vartheta^0 + \vartheta^3 + \vartheta^3 + 1 \\
(\vartheta^8 + \vartheta^9 + \vartheta^6 + \vartheta^3 + 1)(\vartheta^8 + \vartheta^6 + \vartheta^5 + \vartheta + 1) \\
(\vartheta^8 + \vartheta^9 + \vartheta^6 + \vartheta^5 + \vartheta + 1)(\vartheta^8 + \vartheta^6 + \vartheta^5 + \vartheta + 1) \\
(\vartheta^8 + \vartheta^9 + \vartheta^6 + \vartheta^5 + \vartheta + 1)(\vartheta^8 + \vartheta^9 + \vartheta^6 + \vartheta^5 + \vartheta + 1) \\
(\vartheta^8 + \vartheta^9 + \vartheta^6 + \vartheta^5 + \vartheta + 1)(\vartheta^8 + \vartheta^9 + \vartheta^6 + \vartheta^5 + \vartheta + 1) \\
(\vartheta^8 + \vartheta^9 + \vartheta^6 + \vartheta^5 + \vartheta + 1)(\vartheta^8 + \vartheta^9 + \vartheta^6 + \vartheta^5 + \vartheta + 1)
\end{align*}
\]

\[ \deg(G_9) = 252 \quad \text{and} \quad \gamma_9 = 28. \]

<table>
<thead>
<tr>
<th>Polynomial</th>
<th>Degree</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>((x, -, +, +, +, +, +, +, +, +, +))</td>
<td>251</td>
<td>(0.1111111)</td>
</tr>
<tr>
<td>((x, -, +, +, +, +, +, +, +, +))</td>
<td>251</td>
<td>(0.1111110)</td>
</tr>
<tr>
<td>((x, +, -, +, +, +, +, +, +, +))</td>
<td>121</td>
<td>(1, 2, 4, 8, 16, 32, 64, 128, 256)</td>
</tr>
<tr>
<td>((x, +, +, -, +, +, +, +, +, +))</td>
<td>121</td>
<td>(1, 2, 4, 8, 16, 32, 64, 128, 256)</td>
</tr>
<tr>
<td>((x, +, +, +, +, -, +, +, +, +))</td>
<td>121</td>
<td>(1, 2, 4, 8, 16, 32, 64, 128, 256)</td>
</tr>
<tr>
<td>((x, +, +, +, +, +, +, -, +, +))</td>
<td>121</td>
<td>(1, 2, 4, 8, 16, 32, 64, 128, 256)</td>
</tr>
<tr>
<td>((x, +, +, +, +, +, +, +, -, +))</td>
<td>121</td>
<td>(1, 2, 4, 8, 16, 32, 64, 128, 256)</td>
</tr>
<tr>
<td>((x, +, +, +, +, +, +, +, +, -))</td>
<td>121</td>
<td>(1, 2, 4, 8, 16, 32, 64, 128, 256)</td>
</tr>
<tr>
<td>((x, +, +, +, +, +, +, +, +, +, -))</td>
<td>121</td>
<td>(1, 2, 4, 8, 16, 32, 64, 128, 256)</td>
</tr>
<tr>
<td>((x, +, +, +, +, +, +, +, +, +, +, -))</td>
<td>121</td>
<td>(1, 2, 4, 8, 16, 32, 64, 128, 256)</td>
</tr>
<tr>
<td>((x, +, +, +, +, +, +, +, +, +, +, +, -))</td>
<td>121</td>
<td>(1, 2, 4, 8, 16, 32, 64, 128, 256)</td>
</tr>
</tbody>
</table>

\[
\text{deg}(G_{10}) = 495 \quad \text{and} \quad \gamma_{10} = 51.
\]


Institut de Mathématiques de Toulouse, Université Paul Sabatier, 118, route de Narbonne, 31062 Toulouse Cedex, France
Email address: xavier.buff@math.univ-toulouse.fr

Department of Mathematics, Virginia Tech, Blacksburg, VA 24061, U.S.A.
Email address: floyd@math.vt.edu

Department of Mathematics, University of Michigan, Ann Arbor, MI 48109, U.S.A.
Email address: kochsc@umich.edu

Department of Mathematics and Statistics, Eastern Michigan University, Ypsilanti, MI 48197, U.S.A.
Email address: walter.parry@emich.edu