FACTORIZATION OF POLYNOMIALS IN HYPERBOLIC GEOMETRY AND DYNAMICS

MICHAEL FILASETA AND STAVROS GAROUFALIDIS

ABSTRACT. Using factorization theorems for sparse polynomials, we compute the trace field of Dehn fillings of the Whitehead link, and (assuming Lehmer's Conjecture) the minimal polynomial of the small dilatation pseudo-Anosov maps and the trace field of fillings of the figure-8 knot. These results depend on the degrees of the trace fields over $\mathbb{Q}$ being sufficiently large.

CONTENTS

1. INTRODUCTION

1.1. Factorization problems in dynamics and hyperbolic geometry.

Two problems that one encounters in dynamics and hyperbolic geometry are about number fields and their defining polynomials, namely the computation

- of the minimal polynomial of the largest positive eigenvalue of a Perron-Frobenius matrix, and of
- of the trace fields of hyperbolic Dehn-fillings.

In both problems the number fields are generated by a solution of a one-variable specialization $p(x^m, x^n)$ of a polynomial $p(x, y) \in \mathbb{Z}[x, y]$ for some integers m and n. This leads to the question of the factorization of $p(x^m, x^n)$ for $p(x, y) \in \mathbb{Z}[x, y]$. It is customary to factorize a polynomial with integer coefficients into its cyclotomic part, its reciprocal non-cyclotomic part and its non-reciprocal part, defined in detail in Section 2. Thus, the above problem reduces to the factorization of the cyclotomic, reciprocal and non-reciprocal parts of $p(x^m, x^n)$. The cyclotomic part is well-understood; see for example the work of Granville and Rudnick [GR07, Section 3]. The non-reciprocal part is also well-understood by the work of Schinzel [Sch70]; see also [Fil99] and [FMV19, Theorem 1.1]. On the other hand, the factorization of the reciprocal part of a polynomial is not generally known, abstractly or concretely.

In special circumstances regarding the trace fields of hyperbolic Dehn-fillings, one can bypass the detailed problem of the factorization of $p(x^m, x^n)$, and assuming Lehmer's Conjecture, obtain a qualitative result asserting that each irreducible factor has degree bounded below by $C \max\{|m|, |n|\}$ for some constant that depends on p; see [GJ]. Furthermore, such results are also possible unconditionally by using the work of Dimitrov [Dim], though the special circumstances become more restrictive.

In the current paper, we will use the above described factorization methods in two sample problems. In a subsequent paper [Fil], an approach is developed to obtain information about the factorization of polynomials of the form $f_0(x) + f_1(x)x^n + \cdots + f_{r-1}(x)x^{(r-1)n} + f_r(x)x^{rn}$, replacing the role of Theorem 2.1 below and leading to weaker results than those in this paper but for polynomials associated with more general trace fields of hyperbolic Dehn-fillings.

1.2. The trace field of hyperbolic Dehn fillings.

The fundamental group of an oriented hyperbolic 3-manifold M embeds as a discrete subgroup Γ of $\mathrm{PSL}(2, \mathbb{C})$ and the embedding is well-defined up to conjugation [Thu77]. Discreteness implies that the subfield of the complex numbers generated by the traces of the elements of Γ is a number field, the so-called *trace field* of M. For a detailed discussion, see [MR03, Thm.3.1.2].

If the hyperbolic manifold M has a cusp, i.e., a torus boundary component, then all but finitely many fillings of a hyperbolic manifold are hyperbolic. This is the content of Thurston's hyperbolic Dehn filling theorem [Thu77, NZ85]. Dehn fillings are parametrized by a rational number m/n. A natural question is to ask how the trace field of the filled manifold $M_{m/n}$ depends on the filling m/n.

Using ideal triangulations of hyperbolic manifolds and their gluing equations and character varieties, one can reduce the problem of computing the trace field of an $M_{m/n}$ (for fixed m and large n) to the factorization of a *sparse polynomial* $p(x^m, x^n)$ where $p(x, y) \in \mathbb{Z}[x, y]$ is a polynomial of positive y-degree. This is explained in detail in Section A of the appendix.

For example, consider the hyperbolic manifold W with two cusps which is the complement of the Whitehead link shown in Figure 1.

Neumann-Reid show in [NR92, Thm. 6.2, Eqn. (6.7)] that the trace field of $W_{m/n}$ is given by $\mathbb{Q}(x - 1/x)$ where x is a suitable non-cyclotomic root of the polynomial

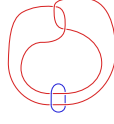$$F_{m,n}^W(x) = (x(x+1))^m x^{4n} - (x-1)^m. \tag{1}$$

FIGURE 1. The Whitehead link.

It is easy to see that $x^2 + 1$ is a root of $F_{m,n}^W(x)$. Theorem 1.1 below proves that the quotient is an irreducible polynomial in $\mathbb{Z}[x]$ for every fixed m and sufficiently large n.

A 2-variable polynomial of degree 1 in y whose specialization is (1) is given by

$$P_m^W(x, y) = (x + 1)^m y - (x - 1)^m.$$

Section 2 deals with the non-reciprocal factors of specializations of the above polynomial given by $y = x^{4n+m}$ where n and m are positive relatively prime integers with m odd and n large.

Our first result concerns fillings of the Whitehead link.

Theorem 1.1. *Let m be a fixed positive odd integer. There is an integer $N = N(m)$ such that if $n \in \mathbb{Z}$ with $n \geq N$ and $\gcd(n, m) = 1$, then $F_{m,n}^W(x)$ is $x^2 + 1$ times an irreducible polynomial.*

It is conceivable that $N(m) = 1$ for all m. Our approach provides an explicit although impractical value for $N(m)$ for a given m, namely

$$N(m) = \frac{5^{8\binom{2m}{m}+8m-7}}{2} - \frac{m}{4}.$$

A corollary of the above theorem is the determination of the invariant trace field $F_{W(m/n)}$ of the hyperbolic manifold $W(m/n)$ obtained by m/n surgery on the Whitehead link W.

Theorem 1.2. *For m a positive odd integer and n an integer $> N(m)$, as defined above, with $\gcd(n, m) = 1$, we have $F_{W(m/n)} = \mathbb{Q}(z)$ where $z = x - 1/x$ with x a root of*

$$((x(x + 1))^m x^{4n} - (x - 1)^m)/(x^2 + 1).$$

The degree of $F_{W(m/n)}$ is $2n + m - 1$, and a defining polynomial $T_{m,n}(z)$ of $F_{W(m/n)}$ over $\mathbb{Q}$ satisfies linear recursions with respect to m and n with coefficients in $\mathbb{Q}[z]$. Specifically, we can take

$$
\begin{aligned}
T_{m,n}(z) &= (z + 2)\, T_{m-1,n}(z) - z\, T_{m-2,n}(z) \quad \text{for } m \geq 2, \\
T_{m,n}(z) &= (z^2 + 2)\, T_{m,n-1}(z) - T_{m,n-2}(z) \quad \text{for } n \geq 2,
\end{aligned}
\tag{2}
$$

with initial conditions

$$T_{0,0}(z) = 0, \quad T_{1,0}(z) = 1, \quad T_{0,1}(z) = z, \quad T_{1,1} = z^2 + z + 1. \tag{3}$$

1.3. The minimal polynomial of small dilatation pseudo Anosov maps.

Consider the 2-variable Laurent polynomial

$$P^T(x, y) = y + y^{-1} - (x + x^{-1} + 1). \tag{4}$$

This is the Teichmuller polynomial of the simplest pseudo-Anosov braid $\sigma_1\sigma_2^{-1}$ studied in [McM00, p.552]. The specialization $P^T(x, x^g)$ appears in [McM15, Thm.1.1] in connection with the minimum value of the spectral radius of all reciprocal Perron-Frobenius $g \times g$ matrices. The specialization $P_{a,b}^T(x) := P^T(x^a, x^b)$ for positive integers a and b (where a is within 2 from a large integer g and b is small) appears in relation to the smallest dilatation number of pseudo-Anosov genus g fiberings [AD10, Sec.1.1], and also in [LT11, Hir10].

Clearing the denominators in $P^T(x, y)$ to obtain a polynomial in $\mathbb{Z}[x, y]$ gives

$$xyP^T(x, y) = xy^2 + x - x^2y - y - xy.$$

We will be interested in the polynomial

$$G_{a,b}^T(x) = \frac{x^a x^b P^T(x^a, x^b)}{x^{\min\{a,b\}}} = \frac{x^{a+2b} + x^a - x^{2a+b} - x^b - x^{a+b}}{x^{\min\{a,b\}}} \tag{5}$$

in $\mathbb{Z}[x]$ having constant term ± 1.

Computations suggest that $G_{a,b}^T(x)$ has the following cyclotomic factors.

(I) If (a, b) is of the form (a_1d_1, b_1d_1) where $d_1 \in \mathbb{Z}^+$ and (a_1, b_1) is congruent to one of the pairs $(1, 0)$, $(3, \pm 2)$, and $(5, 0)$ modulo 6, then $G_{a,b}^T(x)$ is divisible by $\Phi_{6d_1}(x)$.

(II) If (a, b) is of the form (a_2d_2, b_2d_2) where $d_2 \in \mathbb{Z}^+$ and (a_2, b_2) is congruent to one of the pairs $(2, \pm 1)$, $(4, \pm 3)$, $(6, \pm 3)$ and $(8, \pm 1)$ modulo 10, then $G_{a,b}^T(x)$ is divisible by $\Phi_{10d_2}(x)$.

(III) If (a, b) is of the form (a_3d_3, b_3d_3) where $d_3 \in \mathbb{Z}^+$ and (a_3, b_3) is congruent to one of the pairs $(3, \pm 2)$, $(4, \pm 3)$, $(8, \pm 3)$, and $(9, \pm 2)$ modulo 12, then $G_{a,b}^T(x)$ is divisible by $\Phi_{12d_3}(x)$.

(Here, $\Phi_n(x)$ is the n-th cyclotomic polynomial.) A given pair (a, b) can occur in several cases. For example, if $(a, b) = (448, 441)$, then (I) does not arise since b is odd so that b_1 cannot be 0 or ± 2 modulo 6. However, each of (II) and (III) can arise in two ways. For (II), we see that $(448, 441) \equiv (8, 1) \pmod{10}$ so taking $d_2 = 1$ we obtain $\Phi_{10}(x)$ is a factor of $G_{a,b}^T(x)$; and $(448, 441) = (64 \cdot 7, 63 \cdot 7)$ where $(64, 63) \equiv (4, 3) \pmod{10}$ so taking $d_2 = 7$ we obtain $\Phi_{70}(x)$ is a factor of $G_{a,b}^T(x)$. For (III), we see that $(448, 441) \equiv (4, -3) \pmod{12}$ so taking $d_3 = 1$ we obtain $\Phi_{12}(x)$ is a factor of $G_{a,b}^T(x)$; and $(448, 441) = (64 \cdot 7, 63 \cdot 7)$ where $(64, 63) \equiv (4, 3) \pmod{12}$ so taking $d_3 = 7$ we obtain $\Phi_{84}(x)$ is a factor of $G_{a,b}^T(x)$. Thus, $G_{448,441}^T(x)$ has four cyclotomic factors. Indeed, a computation shows that

$$G_{448,441}^T(x) = \Phi_{10}(x)\Phi_{70}(x) \cdot \Phi_{12}(x)\Phi_{84}(x) \cdot (\text{non-cyclotomic irreducible polynomial}). \tag{6}$$

Setting $C_{a,b}^T(x)$ to be the product of the distinct cyclotomic polynomials arising from (I), (II) and (III), we will show that, for large a/b or large b/a, we have $G_{a,b}^T(x)$ is $C_{a,b}^T(x)$ times a non-cyclotomic irreducible polynomial under the assumption of Lehmer's Conjecture on the smallest Mahler measure of a non-cyclotomic irreducible polynomial with integer coefficients. More precisely, we establish the following.

Theorem 1.3. *Let a and b be positive integers. Then the following hold.*

(a) The cyclotomic part of $G_{a,b}^T(x)$ is $C_{a,b}^T(x)$.

(b) If a and b are distinct, then the polynomial $G_{a,b}^T(x)$ is the product of irreducible reciprocal factors.

(c) Assuming Lehmer's Conjecture, there exists an absolute constant C such that if

$$\max\{a/b, b/a\} > C,$$

then the polynomial $G_{a,b}^T(x)/C_{a,b}^T(x)$ is irreducible.

In particular, if g is a sufficiently large integer, then Lehmer's Conjecture implies that $x^g P^T(x, x^g)/C_{1,g}^T(x)$ is an irreducible polynomial of degree $2g - 2\epsilon_g$ where $\epsilon_g = 1$ if 6 divides g and 0 otherwise.

2. Factoring $f(x)x^n + g(x)$

2.1. **Background on factorization.** Let us begin by recalling some standard terminology regarding factorization. We define a non-zero polynomial $w(x) \in \mathbb{R}[x]$ as *reciprocal* if $w(x) = \pm x^{\deg w} w(1/x)$. For example, $x+1$, $x-1$ and $x^3 - 3x^2 + 3x - 1$ are all reciprocal. Observe that $w(0) \neq 0$ for a reciprocal polynomial $w(x)$; to see this simply observe that if x divides $w(x)$, then the degree of $x^{\deg w} w(1/x)$ is less than the degree of $w(x)$ so $w(x) \neq \pm x^{\deg w} w(1/x)$. The terminology reciprocal is motivated by the fact that an (easily seen) equivalent definition for $w(x)$ being reciprocal is that $w(0) \neq 0$ and if α is a root of $w(x)$ with multiplicity some positive integer k, then $1/\alpha$ is a root of $w(x)$ with multiplicity k. Observe that if $w(x)$ is a reciprocal factor of a non-zero polynomial $F(x) \in \mathbb{R}[x]$, then $w(x)$ divides $x^{\deg F} F(1/x)$.

Important examples of reciprocal polynomials are given by the classical cyclotomic polynomials, that is the irreducible factors of $x^k - 1$ where k is a positive integer. There is one irreducible factor $\Phi_k(x)$ of $x^k - 1$ that does not appear as a factor of $x^\ell - 1$ for ℓ a positive integer $< k$, and that irreducible factor is called the kth cyclotomic polynomial. It has $\zeta = e^{2\pi i/k}$ as a root.

Given a polynomial $F(x) \in \mathbb{Z}[x]$, we refer to the non-reciprocal part of $F(x)$ as the factor that remains after we remove each reciprocal factor of $F(x)$ that is irreducible over the integers (so the gcd of the coefficients is 1) and that has a positive leading coefficient. Note that a non-zero constant polynomial in $\mathbb{Z}[x]$ is reciprocal, and, as irreducibility is over the integers, it is irreducible if and only if it is prime. For example, the non-reciprocal part of

$$F(x) = (-2x + 2)(x^6 + x^5 + x^4 + 3x^3 + x^2 + x + 1)$$

is obtained by first rewriting and completing the factorization to

$$F(x) = -2(x - 1)(x^3 + x^2 + 1)(x^3 + x + 1)$$

and then removing the irreducible reciprocal factors with a positive leading coefficient, namely 2 and $x - 1$. Thus, the non-reciprocal part of $F(x)$ in this example is

$$-x^6 - x^5 - x^4 - 3x^3 - x^2 - x - 1.$$

As this example shows, the non-reciprocal part of $F(x)$ can itself be a reciprocal polynomial (but its irreducible factors must be non-reciprocal).

For $w(x) = \sum_{j=0}^r a_j x^j \in \mathbb{R}[x]$, we use the notation

$$\|w\| = \sqrt{a_0^2 + a_1^2 + \cdots + a_r^2}.$$

Thus, $\|w\|$ may be viewed as a way for us to give some notion of a size to a polynomial.

For $u(x)$ and $v(x)$ in $\mathbb{Z}[x]$, we define $\gcd_{\mathbb{Z}}(u(x), v(x))$ as follows. Write

$$u(x) = \pm \prod_{j=1}^{r} g_j(x)^{k_j} \quad \text{and} \quad v(x) = \pm \prod_{j=1}^{r} g_j(x)^{\ell_j},$$

where the $g_j(x)$ are distinct irreducible polynomials in $\mathbb{Z}[x]$ with positive leading coefficients and the exponents k_j and ℓ_j are all non-negative integers. Then

$$\gcd_{\mathbb{Z}}(u(x), v(x)) = \prod_{j=1}^{r} g_j(x)^{\min\{k_j, \ell_j\}}.$$

The example

$$\gcd_{\mathbb{Z}}\big(-5(2x+2)^2(x^2-3)(x^3+x+1), -10(2x+2)^3(x^2-3)\big) = 5(2x+2)^2(x^2-3)$$

illustrates this definition.

Schinzel [Sch65, Sch68], capitalizing on an idea of Ljunngren [Lju60], showed how one can obtain information on the factorization of the non-reciprocal part of a polynomial. For the proof of Theorem 1.1, we make use of the following result from [FFK00, p.635], which is a variation of a result that appears in [Sch65].

Theorem 2.1. *Let $f(x)$ and $g(x)$ be in $\mathbb{Z}[x]$ with $f(0) \neq 0$, $g(0) \neq 0$, and $\gcd_{\mathbb{Z}}(f(x), g(x)) = 1$. Let r_1 and r_2 denote the number of non-zero terms in $f(x)$ and $g(x)$, respectively. If*

$$n \geq \max \left\{ 2 \times 5^{2N-1}, 2 \max \big\{ \deg f, \deg g \big\} \left(5^{N-1} + \frac{1}{4} \right) \right\}$$

where

$$N = 2\|f\|^2 + 2\|g\|^2 + 2r_1 + 2r_2 - 7,$$

then the non-reciprocal part of $f(x)x^n + g(x)$ is irreducible or identically one unless one of the following holds:

  (i) The polynomial $-f(x)g(x)$ is a pth power for some prime p dividing n.
  (ii) For either $\varepsilon = 1$ or $\varepsilon = -1$, one of $\varepsilon f(x)$ and $\varepsilon g(x)$ is a 4th power, the other is 4 times a 4th power, and n is divisible by 4.

Note that when (i) or (ii) hold in the above theorem, $f(x)x^n + g(x)$ is reducible by an apparent factorization.

2.2. **Proof of Theorem 1.1.** We set $f(x) = (x+1)^m$, $g(x) = -(x-1)^m$ and

$$F_{k,m}(x) = f(x)x^k + g(x) = (x+1)^m x^k - (x-1)^m,$$

where k is a positive integer. Observe that, since m is odd, $\gcd(4n+m, m) = \gcd(n, m)$. Our goal is to show that if $k = 4n + m$ is sufficiently large and $\gcd(k, m) = 1$, then $F_{k,m}(x)$ has $x^2 + 1$ as a factor and $F_{k,m}(x)/(x^2+1)$ is irreducible. We apply Theorem 2.1 with n replaced by k. For $k = 4n + m$ and $\gcd(k, m) = 1$, we show the following.

  • Each of (i) and (ii) in Theorem 2.1 do not hold.
  • The only cyclotomic factor of $F_{k,m}(x)$ is $x^2 + 1$, which has multiplicity 1.
  • The polynomial $F_{k,m}(x)$ has no irreducible reciprocal non-cyclotomic factors.

Theorem 2.1 will then imply that $F_{k,m}(x)/(x^2 + 1)$ is irreducible for $k = 4n + m$ sufficiently large and $\gcd(n, m) = 1$, completing the proof.

Suppose $k = 4n + m$ and $\gcd(k, m) = 1$. The polynomial $-f(x)g(x) = (x + 1)^m(x - 1)^m$ is a pth power for a prime p if and only if $p|m$. If $p|m$, then the condition $\gcd(k, m) = 1$ implies $p \nmid k$. Therefore, (i) with n replaced by k, does not hold. Furthermore, one sees that since m is odd, the polynomials $\pm f(x) = \pm(x + 1)^m$ and $\pm g(x) = \mp(x - 1)^m$ cannot be a fourth power. Thus, (ii) does not hold.

Next, we show that the only cyclotomic factor of $F_{k,m}(x)$ is $x^2 + 1$. To do this, we first note that if $w(x)$ is any irreducible reciprocal factor of $F_{k,m}(x)$, then $w(x)$ divides

$$x^{\deg F_{k,m}} F_{k,m}(1/x) = x^{k+m}\left(\left(\frac{1}{x} + 1\right)^m \frac{1}{x^k} - \left(\frac{1}{x} - 1\right)^m\right)$$

$$= -(1 - x)^m x^k + (x + 1)^m.$$

Thus, $w(x)$ must be a divisor of

$$(1 - x)^m F_{k,m}(x) + (x + 1)^m x^{\deg F_{k,m}} F_{k,m}(1/x) = -(1 - x)^m(x - 1)^m + (x + 1)^{2m}.$$

Since m is odd, we deduce that $w(x)$ divides $(x + 1)^{2m} + (x - 1)^{2m}$.

Assume now that $\zeta = e^{2\pi i/s}$, where $s \in \mathbb{Z}^+$, is a root of $F_{k,m}(x)$. Since cyclotomic polynomials are reciprocal, we obtain that ζ must be a root of $(x + 1)^{2m} + (x - 1)^{2m}$. Hence, $\zeta \neq 1$ and

$$\left(\frac{\zeta + 1}{\zeta - 1}\right)^{2m} = -1.$$

This implies that $(\zeta + 1)/(\zeta - 1)$ is a $(4m)^{\text{th}}$ root of unity. Setting $\theta = 2\pi/s$, we see that

$$\frac{\zeta + 1}{\zeta - 1} = \frac{e^{i\theta} + 1}{e^{i\theta} - 1} = \frac{e^{i\theta/2} + e^{-i\theta/2}}{e^{i\theta/2} - e^{-i\theta/2}} = \frac{\cos(\theta/2)}{i\sin(\theta/2)} = -i\cot(\theta/2).$$

Since $(\zeta + 1)/(\zeta - 1)$ is a root of unity, this last expression is non-zero and necessarily purely imaginary. Also, $\theta = 2\pi/s \in (0, \pi]$. Therefore, $(\zeta + 1)/(\zeta - 1) = -i$, and we must have $\cot(\theta/2) = 1$. We see then that $s = 4$ and $\zeta = i$. Observe that, since $k = 4n + m$, we can deduce that

$$\frac{F_{k,m}(\zeta)}{(\zeta - 1)^m} = \left(\frac{\zeta + 1}{\zeta - 1}\right)^m \zeta^m \zeta^{4n} - 1 = (-i)^m i^m i^{4n} - 1 = 1 - 1 = 0.$$

Thus, $x^2 + 1$ is a factor of $F_{k,m}(x)$. Since

$$F'_{k,m}(x) = m(x + 1)^{m-1}x^k + k(x + 1)^m x^{k-1} - m(x - 1)^{m-1},$$

we also obtain

$$\frac{F'_{k,m}(\zeta)}{(\zeta - 1)^{m-1}} = m\left(\frac{\zeta + 1}{\zeta - 1}\right)^{m-1} \zeta^m \zeta^{4n} + k\left(\frac{\zeta + 1}{\zeta - 1}\right)^{m-1}(\zeta + 1)\zeta^{m-1}\zeta^{4n} - m$$

$$= m(-i)^{m-1}i^m i^{4n} + k(-i)^{m-1}(i + 1)i^{m-1}i^{4n} - m = (k + m)i + (k - m) \neq 0.$$

Thus, $(x^2 + 1)^2$ is not a factor of $F_{k,m}(x)$, and $F_{k,m}(x)/(x^2 + 1)$ has no cyclotomic factors.

We now assume that $F_{k,m}(x)$ has an irreducible reciprocal non-cyclotomic factor. Calling this factor $w(x)$, we recall that $w(x)$ must divide $(x+1)^{2m} + (x-1)^{2m}$. Equivalently, we have

$$(x+1)^{2m} \equiv -(x-1)^{2m} \pmod{w(x)}. \tag{7}$$

Since $w(x)$ divides $F_{k,m}(x)$, we also have

$$(x+1)^m x^k \equiv (x-1)^m \pmod{w(x)}. \tag{8}$$

Squaring both sides of (8) and substituting from (7), we see that

$$-(x-1)^{2m} x^{2k} \equiv (x-1)^{2m} \pmod{w(x)}.$$

Hence, the polynomial $w(x)$ divides $(x-1)^{2m}(x^{2k}+1)$. As $w(x)$ is irreducible and non-cyclotomic and as all the irreducible factors of $(x-1)^{2m}(x^{2k}+1)$ are cyclotomic, we obtain a contradiction. Thus, the polynomial $F_{k,m}(x)$ has no irreducible reciprocal non-cyclotomic factors. The proof is complete. $\square$

2.3. **Proof of Theorem 1.2.** The main part of the theorem is a direct consequence of the work of Neumann-Reid from [NR92, Thm. 6.2, Eqn. (6.7)] which was mentioned in the introduction combined with Theorem 1.1. What is left to explain is the stated recursion (2).

We want to justify that

$$(x^2+1)x^{2n+m-1}T_{m,n}\left(x - \frac{1}{x}\right) = F_{m,n}^W(x), \tag{9}$$

where $T_{m,n}(z)$ is defined by the recursion (2). Recall $z = x - 1/x$. One checks directly that (9) holds for $(m,n) \in \{(0,0),(0,1),(1,0),(1,1)\}$. Suppose (9) holds when (m,n) is replaced by $(m-1,n)$ and $(m-2,n)$. Then making use of the recursion for $T_{m,n}(z)$ with $z = x - 1/x$, we obtain

$$(x^2+1)\,x^{2n+m-1}T_{m,n}(z)$$

$$= (x^2+1)\,x^{2n+m-1}(z+2)\,T_{m-1,n}(z) - (x^2+1)\,x^{2n+m-1}\left(x - \frac{1}{x}\right)T_{m-2,n}(z)$$

$$= (x^2+1)\,x^{2n+(m-1)-1}(x^2-1+2x)\,T_{m-1,n}(z) - (x^2+1)\,x^{2n+(m-2)-1}(x^3-x)\,T_{m-2,n}(z)$$

$$= (x^2-1+2x)\,F_{m-1,n}^W(x) - (x^3-x)\,F_{m-2,n}^W(x).$$

Thus, we want to show

$$(x^2-1+2x)\,F_{m-1,n}^W(x) - (x^3-x)\,F_{m-2,n}^W(x) = F_{m,n}^W(x).$$

This identity is easily verified from the definition of $F_{m,n}^W(x)$ on noting that

$$(x^2+2x-1)(x^2+x) - (x^3-x) = \big(x(x+1)\big)^2$$

and

$$(x^2+2x-1)(x-1) - (x^3-x) = (x-1)^2.$$

The above shows that (9) holds if it holds for (m, n) replaced by $(m - 1, n)$ and $(m - 2, n)$. A similar argument shows that (9) holds if it holds for (m, n) replaced by $(m, n - 1)$ and $(m, n - 2)$. This is enough to deduce that (9) holds in general.   □

3. Factoring fewnomials

3.1. The cyclotomic part of $G_{a,b}^T(x)$.
In this section, we prove Theorem 1.3 (a). Suppose $\zeta = \zeta_n = e^{2\pi i/n}$ is a root of $G_{a,b}^T(x)$, and hence

$$\zeta^{a+2b} + \zeta^a - \zeta^{2a+b} - \zeta^b - \zeta^{a+b} = 0. \tag{10}$$

The strategy will be as follows. We will show that

(∗) there are positive integers n_0, d_0, a_0 and b_0 such that $n_0 \leq 12$, $n = n_0 d_0$, $a = a_0 d_0$ and $b = b_0 d_0$.

Then

$$\zeta^a = \zeta_{n_0 d_0}^{a_0 d_0} = \zeta_{n_0}^{a_0} \quad \text{and} \quad \zeta^b = \zeta_{n_0 d_0}^{b_0 d_0} = \zeta_{n_0}^{b_0}$$

so that (10) implies

$$\zeta_{n_0}^{a_0+2b_0} + \zeta_{n_0}^{a_0} - \zeta_{n_0}^{2a_0+b_0} - \zeta_{n_0}^{b_0} - \zeta_{n_0}^{a_0+b_0} = 0. \tag{11}$$

As $n_0 \leq 12$, to obtain all the solutions to (11), we begin by calculating each possibility for $1 \leq n_0 \leq 12$, $1 \leq a_0 \leq n_0$ and $1 \leq b_0 \leq n_0$ for which (11) holds. This can be accomplished by checking for each such n_0, a_0 and b_0 whether $x^{a_0+2b_0} + x^{a_0} - x^{2a_0+b_0} - x^{b_0} - x^{a_0+b_0}$ is divisible by $\Phi_{n_0}(x)$, as (11) will hold if and only if this divisibility by $\Phi_{n_0}(x)$ holds. Once we determine the set $\mathcal{T}$ of all triples (n_0, a_0, b_0) with $1 \leq n_0 \leq 12$, $1 \leq a_0 \leq n_0$ and $1 \leq b_0 \leq n_0$ satisfying (11), we deduce that all solutions to (11) with $n_0 \leq 12$ are given by triples (n_0, a_0, b_0) of positive integers satisfying

$$a_0 \equiv a_0' \pmod{n_0}, \quad b_0 \equiv b_0' \pmod{n_0}, \quad \text{and} \quad (n_0, a_0', b_0') \in \mathcal{T}. \tag{12}$$

One can reverse these steps to see that (12) implies (11) implies (10), where $n = n_0 d_0$, $a = a_0 d_0$ and $b = b_0 d_0$ for some positive integer d_0. We deduce then that $G_{a,b}^T(x)$ is divisible by $\Phi_n(x)$ if and only if $n = n_0 d_0$, $a = a_0 d_0$ and $b = b_0 d_0$ where $d_0 \in \mathbb{Z}^+$ and (12) holds. Following a direct computation of $\mathcal{T}$ as above, the divisibility of $G_{a,b}^T(x)$ by $C_{a,b}^T(x)$ then follows. What remains to be shown for part (a) of Theorem 1.3, is that if (10) holds, then (∗) holds. Furthermore, we need to justify that each of the irreducible polynomials $\Phi_n(x)$ that divides $G_{a,b}^T(x)$ appears as a factor in $G_{a,b}^T(x)$ with multiplicity exactly one.

For k a positive integer relatively prime to n, let ϕ_k be the automorphism of $\mathbb{Q}(\zeta)$ fixing $\mathbb{Q}$ given by $\phi_k(\zeta) = \zeta^k$. Let $d = \gcd(a, n)$, and define positive integers a' and n' by $a = da'$ and $n = dn'$. Then $\gcd(a', n') = 1$. Letting

$$a'' = a' + n' \prod_{\substack{p|d \\ p\nmid a'}} p,$$

one can see that $\gcd(a'', n) = 1$ by considering separately the three cases where a prime divides n', where a prime divides d but neither n' nor a', and where a prime divides both d and a'. Note that in the latter case, since $\gcd(a', n') = 1$, we have the prime does not divide

n'. Since $\gcd(a'', n) = 1$, there exists a $k \in \mathbb{Z}$ such that $ka'' \equiv 1 \pmod{n}$. Note that $ka'' \equiv 1 \pmod{n}$ implies $\gcd(k, n) = 1$. Since a'' and a' differ by a multiple of n', we obtain

$$\zeta_n^{ka} = \zeta_{n'}^{ka'} = \zeta_{n'}^{ka''} = \zeta_{n'}.$$

We deduce from $\phi_k\big(P^T(\zeta^a, \zeta^b)\big) = 0$ that

$$\zeta^{kb} + \zeta^{-kb} = \zeta_n^{ka} + \zeta_n^{-ka} + 1 = \zeta_{n'} + \zeta_{n'}^{-1} + 1. \tag{13}$$

In particular, if $n' > 6$, then

$$2 \geq |\zeta^{kb} + \zeta^{-kb}| = |\zeta_{n'} + \zeta_{n'}^{-1} + 1| = \cos(2\pi/n') + \cos(-2\pi/n') + 1 > 2,$$

which is impossible. Thus, $n' \leq 6$. Recall $\gcd(k, n) = 1$. Let $k' \in \mathbb{Z}$ satisfy $kk' \equiv 1 \pmod{n}$.

If $n' = 6$, then (13) implies $\zeta^{kb} + \zeta^{-kb} = 2$. Thus, $\zeta^{kb} = 1$. Applying $\phi_{k'}$, we deduce that $\zeta^b = 1$. As $\zeta_n^b = \zeta_{n'd}^b = \zeta_{6d}^b$, we deduce that b is a multiple of $6d$. Thus, at this point we have $n = n'd = 6d$, $a = a'd$ and $b = b'd$ for some positive integer b' divisible by 6. Taking $d_0 = d$ and $n_0 = 6$, we see that $(*)$ holds in this case.

If $n' = 5$, then (13) implies

$$\zeta^{kb} + \zeta^{-kb} = \zeta_5 + \zeta_5^{-1} + 1 = \frac{1 + \sqrt{5}}{2}.$$

Letting $\alpha_1 = (1 + \sqrt{5})/2$ and $\alpha_2 = (1 - \sqrt{5})/2$, we see that ζ^{kb} is a root of

$$(x^2 - \alpha_1 x + 1)(x^2 - \alpha_2 x + 1) = x^4 - x^3 + x^2 - x + 1 = \Phi_{10}(x).$$

Thus, $\Phi_{10}(\zeta^{kb}) = 0$, and applying $\phi_{k'}$, we see that $\Phi_{10}(\zeta^b) = 0$. We deduce that $n/\gcd(n, b) = 10$ so that $n = 10d'$ and $b = b'd'$ for some positive integers d' and b'. Also, $n = n'd = 5d$ implies $d = 2d'$ so that $a = a'd = 2a'd'$. Taking $d_0 = d'$ and $n_0 = 10$, we see that $(*)$ holds in this case.

If $n' = 4$, then using (13) and applying $\phi_{k'}$ gives $\zeta^b + \zeta^{-b} = 1$, so ζ^b is a root of $x^2 - x + 1 = \Phi_6(x)$. Thus, $n/\gcd(b, n) = 6$, so there are positive integers d' and b' such that $n = 6d'$ and $b = b'd'$. Since $n = n'd = 4d$, we also see that there is a positive integer d'' such that

$$d' = 2d'', \quad n = 12d'', \quad d = 3d'', \quad a = a'd = 3a'd'', \quad \text{and} \quad b = b'd' = 2b'd''.$$

Therefore, with $d_0 = d''$ and $n_0 = 12$, we obtain $(*)$ in this case.

If $n' = 3$, then 3 divides n. In this case, using (13) and applying $\phi_{k'}$ leads to $\zeta^b + \zeta^{-b} = 0$, so $\zeta^b = \pm i$. We deduce $n/\gcd(b, n) = 4$. Since 3 divides n, we can write $n = 12d'$ for some positive integer d'. Then $\gcd(b, n) = 3d'$ so that $b = 3b'd'$ for some positive integer b'. Since $n = n'd = 4d$, we have $d = 3d'$. Hence, $a = a'd = 3a'd'$. Thus, using $d_0 = d'$ and $n_0 = 12$, we see $(*)$ holds in this case.

If $n' = 2$, then 2 divides n. Here, using (13) and applying $\phi_{k'}$ gives $\zeta^b + \zeta^{-b} = -1$, so ζ_b is a root of $x^2 + x + 1 = \Phi_3(x)$. Thus, $n/\gcd(b, n) = 3$, so 3 also divides n. We write $n = 6d'$. Then

$$\gcd(b, n) = 2d', \quad b = 2b'd', \quad d = 3d', \quad \text{and} \quad a = 3a'd',$$

where a' and b' are positive integers. With $n_0 = 6$ and $d_0 = d'$, we see that $(*)$ holds in this case as well.

If $n' = 1$, then (13) implies $\zeta^{kb} + \zeta^{-kb} = 3$, which is impossible since the left-hand side is at most 2. So the case $n' = 1$ cannot occur. This finishes the proof that (10) implies $(*)$.

To finish the proof of Theorem 1.3 (a), we still need to address the multiplicity of the cyclotomic factors. Assume now that $\zeta = \zeta_n$ is a root with multiplicity > 1 for $G_{a,b}^T(x)$. Setting $H(x) = H_{a,b}(x)$ to be the numerator in (5), we deduce $H(\zeta) = H'(\zeta) = 0$. Since also $\zeta H'(\zeta) = 0$, we deduce that ζ is a root of

$$U(x) := (a + 2b)x^{a+2b} + ax^a - (2a + b)x^{2a+b} - bx^b - (a + b)x^{a+b}. \tag{14}$$

By what we have shown above, we know that either (I), (II) or (III) holds.

In the case of (I), we have $n = 6d_1$ so that $\zeta^{d_1} = \zeta_6$. We deduce $\zeta^a = \zeta^{a_1 d_1} = \zeta_6^{a_1}$ and, similarly, $\zeta^b = \zeta_6^{b_1}$. Now, it is simply a matter of substituting in the four possible values of (a_1, b_1) modulo 6 for (a, b) into the *exponents* of $U(x)$ in (14) and verify that $U(x)$ does not have $\Phi_6(x)$ as a factor, giving a contradiction. For example, if $(a_1, b_1) \equiv (3, 2) \pmod 6$, then

$$U(x) = (a + 2b)x^7 + ax^3 - (2a + b)x^8 - bx^2 - (a + b)x^5 = 0.$$

The remainder when $U(x)$ is divided by $\Phi_6(x) = x^2 - x + 1$ is

$$(a + 2b)x - a - (2a + b)(x - 1) - b(x - 1) + (a + b)(x - 1) = b(x + 1).$$

As the remainder must be identically 0 for $\Phi_6(x)$ to divide $U(x)$, we deduce $b = 0$, contradicting that $b \in \mathbb{Z}^+$. A very similar argument works for each of the four possibilities for (a_1, b_1) modulo 6 in (I); more precisely, in each case, the coefficient of x in the remainder being 0 implies that either a or b is 0, giving a contradiction.

In the case of (II), we obtain $\zeta^{d_2} = \zeta_{10}$ so that $\zeta^a = \zeta_{10}^{a_2}$ and $\zeta^b = \zeta_{10}^{b_2}$. One similarly checks each of the remainders obtained by substituting the eight possibilities for (a_2, b_2) for (a, b) in the exponents of $U(x)$ and dividing by $\Phi_{10}(x)$. As $\deg \Phi_{10}(x) = 4$, the remainders will have degree at most 3 with coefficients possibly depending on a and b. In each case, the coefficient of x^3 or the coefficient of x^2 being 0 implies that a or b is 0, giving a contradiction. For example, in the case $(a_2, b_2) = (4, -3) \pmod{10}$, the remainder of $U(x)$ divided by $\Phi_{10}(x)$ is $-2bx^3 + (b - a)x^2 - bx + a + b$, so a contradiction is obtained since the coefficient of x^3 being 0 implies $b = 0$.

In the case of (III), we deduce $\zeta^{d_3} = \zeta_{12}$ so that $\zeta^a = \zeta_{12}^{a_3}$ and $\zeta^b = \zeta_{12}^{b_3}$. We consider the remainders obtained by substituting each of the eight possibilities for (a_3, b_3) modulo 12 for (a, b) in the exponents of $U(x)$ and dividing by $\Phi_{12}(x)$. Note that $\deg \Phi_{12}(x) = 4$. In each case, the coefficient of x^3 in the remainder is non-zero if a and b are non-zero, so we obtain a contradiction.

Theorem 1.3 (a) follows. □

Comment: We opted for a self-contained argument above, in part because of the simplicity of the argument. There is a nice general algorithm for establishing the cyclotomic factors of polynomials given by Granville and Rudnick [GR07, Section 3]. This leads to narrowing down consideration to m^{th} roots of unity where m divides 30. The multiplicity of the roots would also need to be considered separately as done here. Another approach would be to take advantage of the fact that replacing x and y with cyclotomic numbers in (4) allows one to rewrite $P^T(x, y) = 0$ as a sum of three cosine values equal to 0, where one depends on x, one depends on y and one is $\cos(2\pi/3)$. Then a computational step in the recent interesting work by Kedlaya, Kolpakov, Poonen and Rubinstein [KKPR, Theorem 5.1] can be applied, where again the multiplicity of the roots would still need to be considered.

3.2. **The non-reciprocal part of $G^T(x^a, x^b)$.** In this section, we establish Theorem 1.3 (b). For distinct a and b, one checks that the exponents appearing in the numerator of $G^T(x^a, x^b)$ in the last expression in (5) are distinct; in other words, $G^T(x^a, x^b)$ consists of exactly five terms with coefficients ± 1. Furthermore, the polynomial $G^T(x^a, x^b)$ is reciprocal. A reciprocal polynomial cannot have exactly one irreducible non-reciprocal factor, so the non-reciprocal part of $G^T(x^a, x^b)$ is either reducible or identically 1. To establish Theorem 1.3 (b), we justify that the non-reciprocal part of $G^T(x^a, x^b)$ is not reducible.

A recent paper by Murphy, Vincent and the first author [FMV19, Theorem 1.2] provides a description of every polynomial $f(x)$ consisting of five terms and coefficients from $\{\pm 1\}$ that has a reducible non-reciprocal part. Although this reference is ideal for our situation, the result in [FMV19] needs to be unraveled as it indicates that such an $f(x)$ must come from a "modification" of one of 13 possible explicit classifications. The details of how to interpret the result are in [FMV19]. We give some explanation here as well by using as a concrete example one of the more complicated of the 13 classifications for such an $f(x)$.

Let

$$F(x,y) = x^5y^2 - x^3y^2 - x^3y - xy - 1 = (x^3y + x^2y + 1)(x^2y - xy - 1). \qquad (15)$$

Then one of the 13 classifications noted above from [FMV19] is that $f(x)$ has a reducible non-reciprocal part if $f(x)$ is of the form $G(x^t, x^u)$ where $G(x, y)$ is a modification of the polynomial $F(x, y)$ and t and u are positive integers. We first describe what these modifications look like by indicating how they are constructed. For a general polynomial $H(x, y) \in \mathbb{Z}[x, y]$, define

$$\widetilde{H}(x,y) = x^k y^\ell H(1/x, 1/y),$$

where k and ℓ are integers chosen as small as possible so that $\widetilde{H}(x, y) \in \mathbb{Z}[x, y]$. If $H(x, y) = \pm\widetilde{H}(x, y)$, we say that $H(x, y)$ is reciprocal. Set $S_1 = \{\pm F(x, y)\}$. Given S_j with $j \geq 1$, we construct S_{j+1} as follows. For each $F_0(x, y) \in S_j$, we begin by factoring it in $\mathbb{Z}[x, y]$ as $F_0(x, y) = F_1(x, y)F_2(x, y)$, where $F_1(x, y)$ and $F_2(x, y)$ are irreducible non-reciprocal polynomials. A check can be done, as one proceeds, to see that starting with any $F(x, y)$ from Theorem 1.2 in [FMV19], each $F_0(x, y) \in S_j$ for every j can be factored in this way. In other words, for the purposes of Theorem 1.2 in [FMV19], which we are using, each $F_0(x, y)$ in each S_j always factors as a product of exactly two irreducible non-reciprocal polynomials. The ordering of these two factors is irrelevant but to be fixed for each $F_0(x, y) \in S_j$ in what follows. We set

$$F_0^*(x,y) = F_1(x,y)\widetilde{F}_2(x,y)$$

and

$$S_{j+1} = S_j \bigcup \left(\bigcup_{F_0 \in S_j} \{ \pm \widetilde{F}_0(x,y)\} \right) \bigcup \left(\bigcup_{F_0 \in S_j} \{ \pm F_0^*(x,y), \pm F_0(-x,y), \pm F_0(x,-y)\} \right).$$

A key point is that there will be a $J \in \mathbb{Z}^+$ such that $S_J = S_{J+1}$ and as a consequence we obtain $S_j = S_J$ for all $j \geq J$. We construct the sets S_j until such a J occurs. Then the set S_J corresponds to the set of all modifications of $F(x, y)$. For $F(x, y)$ defined by (15), we obtain $J = 5$ and $|S_J| = 32$.

Next, we need to determine whether there are choices for a and b for which $G^T(x^a, x^b)$ is of the form given by $G(x^t, x^u)$ for each $G(x, y) \in S_J$. We simplified the process by only

looking at such $G(x, y)$ with two positive coefficients and three negative coefficients, as in $G^T(x^a, x^b)$. For $F(x, y)$ defined by (15), there were 8 such polynomials in S_J. Fix $G(x, y)$ as one of these. We then want to compare the degrees of the positive terms in $G(x^t, x^u)$ with the positive terms in $G^T(x^a, x^b)$ and the negative terms in $G(x^t, x^u)$ with the negative terms in $G^T(x^a, x^b)$. In the way of an explicit example, for $F(x, y)$ as in (15), one of the elements of S_J is $G(x, y) = x^5y^2 - x^4y - x^2y - x^2 + 1$. Observe that $G(x^t, x^u) = x^{5t+2u} - x^{4t+u} - x^{2t+u} - x^{2t} + 1$. We set $c = -\min\{a, b\}$ to be an unknown in the definition of $G^T(x^a, x^b)$ in the last expression in (5). In order for $G^T(x^a, x^b)$ to be of the form $G(x^t, x^u)$, then it is necessary and sufficient for

$$\{a + 2b + c, a + c\} = \{5t + 2u, 0\}$$

and

$$\{2a + b + c, b + c, a + b + c\} = \{4t + u, 2t + u, 2t\}.$$

Although it is easy in this case to compare sizes of the elements to determine, for example, that $a + 2b + c = 5t + 2u$ and $a + c = 0$, we simply made all possible equations from the equality of these sets, allowing 2 possibilities for the first set equality and 6 possibilities for the second set equality. Thus, for this choice of $F(x, y)$ and $G(x, y)$, we had 12 systems of equations to solve in integers a, b, c, t and u. We used Maple 2019.2 to run through all of the choices for $F(x, y)$ and $G(x, y)$ as described above, and none of resulting systems of equations had solutions with non-zero a and b. Thus, Theorem 1.3 (b) follows.

3.3. **Proof of Theorem 1.3.** We have already proven parts (a) and (b) of the theorem. For the last part, we need to assume Lehmer's Conjecture [Leh33]. Recall the Mahler measure of a polynomial $p(x_1, \ldots, x_r)$ in r variables is given by

$$M(p(x_1, \ldots, x_r)) = \exp\left(\int_0^1 \int_0^1 \cdots \int_0^1 \log|p(e^{2\pi it_1}, e^{2\pi it_2}, \ldots, e^{2\pi it_r})|\, dt_1\, dt_2 \ldots dt_r\right).$$

For a vector $\vec{s} = \langle s_1, s_2, \ldots, s_r \rangle$ of integers, we define $H(\vec{s}) = \max_{1 \le j \le r}\{|s_j|\}$. Now, given a vector $\vec{a} = \langle a_1, a_2, \ldots, a_r \rangle$ of positive integers, we consider all non-zero vectors $\vec{s} = \langle s_1, s_2, \ldots, s_r \rangle$ of integers perpendicular to $\vec{a}$, so satisfying $\sum_{j=1}^r s_j a_j = 0$, and define $q(\vec{a})$ to be the minimum value of $H(\vec{s})$ over all such $\vec{s}$. Lawton [Law83, Theorem 2] has shown

$$\lim_{q(\vec{a}) \to \infty} M(p(x^{a_1}, \ldots, x^{a_r})) = M(p(x_1, \ldots, x_r)).$$

Lehmer's Conjecture asserts that

$$M(p(x)) \ge c = 1.176280818\ldots,$$

where

$$c = M(x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1).$$

A computation gives $M(xyP^T(x, y)) = 1.28573\ldots$. We only require this numerical estimate, but we note that, as a consequence of work of Rogers and Zudilin [RZ14], an explicit expression of the value of $M(xyP^T(x, y))$ can be given in terms of an L-series of a conductor 15 elliptic curve. Since $C_{a,b}^T(x)$ is the cyclotomic factor of $G_{a,b}^T(x)$, Lawton's theorem implies that for a/b or b/a sufficiently large (so that $q(\langle a, b \rangle)$ is large), one has

$M(G_{a,b}^T(x)/C_{a,b}^T(x)) = M(x^{a+b}P^T(x^a, x^b))$ is near $1.28573\dots$ and hence $< c^2$. Mahler measure behaves multiplicatively on a product of polynomials. Thus, if $G_{a,b}^T(x)/C_{a,b}^T(x)$ were reducible, it would have a factor with Mahler measure less than c violating Lehmer's Conjecture. This completes the proof of Theorem 1.3 (c). □

Appendix A. Dehn fillings of the Whitehead link

In this section, which is not needed for the results of the paper, we recall the computation of the trace field of Dehn fillings of the Whitehead link, due to Neumann-Reid [NR92]. The computation works for every cusped hyperbolic manifold and uses standard material on ideal triangulations, gluing equations and character varieties.

A.1. **Ideal triangulations, gluing equations and character varieties.** An ideal tetrahedron is the convex hull of four points in the boundary $\partial\mathbb{H}^3$ of 3-dimensional hyperbolic space $\mathbb{H}^3$ [Thu77]. In the upper half-space model $\mathbb{H} = \mathbb{C} \times (0, \infty)$, the boundary can be identified with the 2-dimensional sphere $\mathbb{C} \cup \{\infty\}$. Setting three of the four points of an ideal tetrahedron to 0, 1 and ∞ allows the last point to be a complex number $z \in \mathbb{C} \setminus \{0, 1\}$. This number is the *shape* of the ideal tetrahedron, equal to a cross ratio of four points in $\mathbb{C}$, and it is well-defined up to a six-fold orbit ambiguity.

Ideal tetrahedra were used by Thurston as building blocks of cusped hyperbolic 3-manifolds as follows. Start from a topological ideal triangulation $\mathcal{T}$ of an oriented 3-manifold M with torus boundary components (such a triangulation always exists) and choose shape parameters $z_1, \dots, z_N$, one for each ideal tetrahedron. Then, one can write down a system of gluing equations around each edge of the ideal triangulation. Each equation implies that a Laurent monomial in z_i and $w_i = 1 - z_i$ is equal to ± 1. The solution to the system of equations is an affine variety $G(\mathcal{T})$ in $(\mathbb{C} \setminus \{0, 1\})^N$. If M has c cusps, then typically $G(\mathcal{T})$ is a c-dimensional variety, although it is possible that $G(\mathcal{T})$ is empty. At any rate, each solution to the gluing equations gives via the developing map a representation of $\pi_1(M)$ (the fundamental group of M) to $\mathrm{PSL}(2, \mathbb{C})$, the isometry group of $\mathbb{H}^3$.

If in addition one imposes a completeness equation around each cusp of M (these equations also have the same shape as the gluing equations of the edges of $\mathcal{T}$), and finds a solution of the logarithmic system of equations, this obtains a concrete description of the hyperbolic structure of M in terms of the shapes of $\mathcal{T}$. In this case, the set of edge and cusp equations is zero-dimensional and the shapes are algebraic numbers.

This method of describing hyperbolic manifolds may sound abstract. However, Weeks developed a program `SnapPea` that uses ideal triangulations and numerically finds a hyperbolic structure. A modern version of the program, `SnapPy`, is available from [CDW]. Among other things, `SnapPy` gives certified exact arithmetic computations. For more information on the combinatorics of ideal triangulations of 3-manifolds, see [NZ85].

A.2. **Fillings of the Whitehead link.** In this section, we review the results from [NR92] regarding fillings of the complement of the Whitehead link (shown on the left of Figure 1). The starting point is Thurston's observation that the complement of the Whitehead link W is a hyperbolic manifold obtained by face-pairings of a regular ideal octahedron [NR92, Fig.10]. The ideal octahedron can be decomposed into four ideal tetrahedra, each of shape

$\sqrt{-1}$ [NR92, Fig.11]. This gives an ideal triangulation $\mathcal{T}$ of W with four tetrahedra. The gluing equations variety $G(\mathcal{T})$ is an affine surface. Neumann-Reid [NR92, Sec.6.2] prove that the subset $G(\mathcal{T})^{\mathrm{par}}$ of $G(\mathcal{T})$ which consists of solutions that are complete at the red cusp (of Figure 1) is a rational curve parametrized by

$$\mathbb{C}^* \longrightarrow G(\mathcal{T})^{\mathrm{par}}, \qquad x \mapsto (z_1, z_2, z_3, z_4) = (x, -x^{-1}, x, -x^{-1})$$

The curve $G(\mathcal{T})^{\mathrm{par}}$ contains the special point $x = i$ corresponding to the hyperbolic structure on W. The (square of the) holonomy around the meridian and longitude of the blue cusp are rational functions $\mu(x)$ and $\lambda(x)$ of x on the curve $G(\mathcal{T})^{\mathrm{par}}$. If $W(m/n)$ denotes the Dehn filling on the blue cusp of the Whitehead link W, then one adds the equation

$$\mu(x)^m \lambda(x)^n = 1 \tag{16}$$

Since $G(\mathcal{T})^{\mathrm{par}}$ is a curve, if μ is a nonconstant function, it follows that $\mu(x)^{-m}$ and $t = \lambda(x)$ are polynomially dependent, so $p_m(t, \mu(x)^{-m}) = 0$ for some polynomial p_m. This brings (16) to the form

$$p_m(t, t^n) = 0 \tag{17}$$

as stated in the introduction. In the particular case of the Whitehead link, Neumann-Reid [NR92, Eqn. 6.7] prove that (16) is simply

$$(x(x+1))^m x^{4n} - (x-1)^m = 0.$$

Finally, to describe the trace field of $W(m/n)$, Neumann-Reid [NR92, p. 299] use the face-pairing of the ideal octahedron (4 pairs of faces, identified pairwise) and compute explicitly the four corresponding matrices of $\mathrm{PSL}(2, \mathbb{C})$. The entries of these matrices are polynomials in $x - x^{-1}$, and the trace field that they generate is $\mathbb{Q}(x - x^{-1})$.

We furthermore should point out a theorem of Hodgson-Meyerhoff-Weeks concerning pairs of *scissors congruent* hyperbolic manifolds (M, M'), that is pairs of non-isometric hyperbolic manifolds that are obtained by the same set of ideal tetrahedra, assembled together in a combinatorially different manner.

Theorem A.1. [HMW92] *For coprime integers $(4m, n)$, the pair*

$$\bigl(W(4m/n), -W(4m/(-n-2m))\bigr)$$

is geometrically similar and has a common 2-fold cover.

Here, $-M$ denotes the orientation reversed manifold of M.

References

[AD10]   John Aaber and Nathan Dunfield, *Closed surface bundles of least volume*, Algebr. Geom. Topol. **10** (2010), no. 4, 2315–2342.

[CDW]   Marc Culler, Nathan Dunfield, and Jeffrey Weeks, *SnapPy, a computer program for studying the topology of 3-manifolds*, Available at http://snappy.computop.org.

[Dim]   Vesselin Dimitrov, *A proof of the Schinzel-Zassenhaus conjecture on polynomials*, Preprint 2019, arXiv:1912.12545.

[FFK00] Michael Filaseta, Kevin Ford, and Sergei Konyagin, *On an irreducibility theorem of A. Schinzel associated with coverings of the integers*, Illinois J. Math. **44** (2000), no. 3, 633–643.

[Fil]   Michael Filaseta, *On the factorization of lacunary polynomials*, Preprint 2022, arXiv:2207.11648.

[Fil99] ———, *On the factorization of polynomials with small Euclidean norm*, Number theory in progress, Vol. 1 (Zakopane-Kościelisko, 1997), de Gruyter, Berlin, 1999, pp. 143–163.

[FMV19] Michael Filaseta, Robert Murphy, and Andrew Vincent, *Computationally classifying polynomials with small Euclidean norm having reducible non-reciprocal parts*, Number theory week 2017, Banach Center Publ., vol. 118, Polish Acad. Sci. Inst. Math., Warsaw, 2019, pp. 245–259.

[GJ]   Stavros Garoufalidis and BoGwang Jeon, *On the trace fields of hyperbolic dehn fillings*, Preprint 2021, arXiv:2103.00767.

[GR07]   Andrew Granville and Zeév Rudnick, *Torsion points on curves*, Equidistribution in number theory, an introduction, NATO Sci. Ser. II Math. Phys. Chem., vol. 237, Springer, Dordrecht, 2007, pp. 85–92.

[Hir10] Eriko Hironaka, *Small dilatation mapping classes coming from the simplest hyperbolic braid*, Algebr. Geom. Topol. **10** (2010), no. 4, 2041–2060.

[HMW92] Craig Hodgson, Robert Meyerhoff, and Jeffrey Weeks, *Surgeries on the Whitehead link yield geometrically similar manifolds*, Topology '90 (Columbus, OH, 1990), Ohio State Univ. Math. Res. Inst. Publ., vol. 1, de Gruyter, Berlin, 1992, pp. 195–206.

[KKPR]   Kiran Kedlaya, Alexander Koplakov, Bjorn Poonen, and Michael Rubinstein, *Space vectors forming rational angles*, Preprint 2020, arXiv:2011.14232.

[Law83] Wayne M. Lawton, *A problem of Boyd concerning geometric means of polynomials*, J. Number Theory **16** (1983), no. 3, 356–362.

[Leh33] Derrick Lehmer, *Factorization of certain cyclotomic functions*, Ann. of Math. (2) **34** (1933), no. 3, 461–479.

[Lju60] Wilhelm Ljunggren, *On the irreducibility of certain trinomials and quadrinomials*, Math. Scand. **8** (1960), 65–70.

[LT11]   Erwan Lanneau and Jean-Luc Thiffeault, *On the minimum dilatation of pseudo-Anosov homeomorphisms on surfaces of small genus*, Ann. Inst. Fourier (Grenoble) **61** (2011), no. 1, 105–144.

[McM00] Curtis McMullen, *Polynomial invariants for fibered 3-manifolds and Teichmüller geodesics for foliations*, Ann. Sci. École Norm. Sup. (4) **33** (2000), no. 4, 519–560.

[McM15] ———, *Entropy and the clique polynomial*, J. Topol. **8** (2015), no. 1, 184–212.

[MR03]   Colin Maclachlan and Alan Reid, *The arithmetic of hyperbolic 3-manifolds*, Graduate Texts in Mathematics, vol. 219, Springer-Verlag, New York, 2003.

[NR92]   Walter Neumann and Alan Reid, *Arithmetic of hyperbolic manifolds*, Topology '90 (Columbus, OH, 1990), Ohio State Univ. Math. Res. Inst. Publ., vol. 1, de Gruyter, Berlin, 1992, pp. 273–310.

[NZ85]   Walter Neumann and Don Zagier, *Volumes of hyperbolic three-manifolds*, Topology **24** (1985), no. 3, 307–332.

[RZ14]   Mathew Rogers and Wadim Zudilin, *On the Mahler measure of $1 + X + 1/X + Y + 1/Y$*, Int. Math. Res. Not. IMRN (2014), no. 9, 2305–2326.

[Sch65] Andrzej Schinzel, *On the reducibility of polynomials and in particular of trinomials*, Acta Arith. **11** (1965), 1–34.

[Sch68] ———, *Reducibility of polynomials and covering systems of congruences*, Acta Arith. **13** (1967/1968), 91–101.

[Sch70] ———, *Reducibility of lacunary polynomials. I*, Acta Arith. **16** (1969/70), 123–159.

[Thu77] William Thurston, *The geometry and topology of 3-manifolds*, Universitext, Springer-Verlag, Berlin, 1977, Lecture notes, Princeton.

Department of Mathematics, University of South Carolina, Columbia, SC 29208, USA
http://www.math.sc.edu/~filaseta
    Email address: filaseta@mailbox.sc.edu

International Center for Mathematics, Department of Mathematics, Southern University of Science and Technology, Shenzhen, China
http://people.mpim-bonn.mpg.de/stavros
    Email address: stavros@mpim-bonn.mpg.de