Polynomial Roots with Common Tails

Gregory Dresden, Saimon Islam, Prakriti Panthi,
Anukriti Shrestha, and Jiahao Zhang

April 17, 2019

Abstract

How many irreducible polynomials have real roots which, when expressed as simple continued fractions, all have common tails? We show how to identify all such polynomials (they have degree at most six), and we establish connections to linear fractional transforms, Galois groups, and some factoring techniques that date back hundreds of years.

In a recent paper [7] based on an undergraduate honors thesis, Alexandra Hobby and David Hobby pointed out an interesting feature of the polynomial $x^3 + 6x^2 + 9x + 1$. This function has three real roots, and when we write them as continued fractions (using the standard notation as explained later), we obtain

$$\begin{aligned} -3.5320888\ldots &= [-4; 2, \quad 7, 3, 2, 3, 1, 1, \ldots] \\ -2.3472963\ldots &= [-3; 1, 1, 1, \quad 7, 3, 2, 3, 1, 1, \ldots] \\ -0.1206147\ldots &= [-1; 1, \quad 7, 3, 2, 3, 1, 1, \ldots]. \end{aligned}$$

Hobby and Hobby noted that all three continued fractions have "common tails," and they asked how many other polynomials have roots with this same behavior. Back in the mid 1800s, Serret [12, 13] gave appropriate conditions for polynomials of degree 2 and 3 to have roots with common tails. In their recent work, Hobby and Hobby found examples of such polynomials with degrees 4 and 6, and they wondered if there were others. In this article we finish the problem: we prove definitively that such polynomials can only be of degrees 2, 3, 4, or 6, and we describe how to identify all such polynomials. But before we go any further, let us review some standard definitions and preliminary theorems.

1 Preliminaries.

Recall that a *simple continued fraction*, typically called a *continued fraction*, is a number of the form

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}},$$

where a_0 is an integer and $a_1, a_2, a_3, \ldots$ are positive integers. It is well known that a real number is irrational if and only if the continued fraction expression is infinite (and in that case the expression is unique). For more details on continued fractions, see [6]. We will use the standard notation of $[a_0; a_1, a_2, a_3, \ldots]$ to refer to the continued fraction above.

We will say that two irrational numbers have *common tails* if their simple continued fraction expansions are eventually identical (after allowing for a possible offset). Along these lines, we will say that *a polynomial has common tails* if all its roots are distinct irrational real numbers with common tails.

As will become clear in a moment, we also want to define *linear fractional transforms*, which are functions of the form $(ax+b)/(cx+d)$ such that $ad-bc \neq 0$. These functions form a group under composition, and we will be interested in the particular group of such functions with integer coefficients a, b, c, d satisfying $ad - bc = \pm 1$. If we map each such $(ax+b)/(cx+d)$ to the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, then we find that this particular group of functions is isomorphic to the projective group of matrices $\overline{\Gamma} = \mathrm{PGL}(2, \mathbb{Z})$, which is often referred to as the *extended modular group*. A particularly nice feature of this isomorphism is that composition of functions can be rewritten in terms of multiplication of matrices. This correspondence allows us to use the function notation $(ax+b)/(cx+d)$ and the matrix notation $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ interchangeably, with the understanding that $(ax+b)/(cx+d)$ is the same function as $(-ax-b)/(-cx-d)$, and so likewise we understand that $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is considered the same object as $\begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$ in $\mathrm{PGL}(2, \mathbb{Z})$. We will use $\overline{\Gamma}$ and $\mathrm{PGL}(2, \mathbb{Z})$ interchangeably to refer to the group of such objects (either functions or matrices) with a, b, c, d integers and with determinant $ad - bc = \pm 1$.

So, why are we interested in linear fractional transforms? The following theorem reveals a very useful connection between common tails and these particular linear fractional transforms in the extended modular group $\overline{\Gamma}$. It was proved by Serret [12, §16, pp. 34–35] in his popular algebra books from the mid nineteenth century, by Hardy and Wright [6, §10.11, pp. 141–143] in the mid twentieth century, and doubtless by many others.

Theorem 1 (Serret; Hardy and Wright)**.** *Two irrational numbers r_1 and r_2 have common tails if and only if $r_2 = (ar_1 + b)/(cr_1 + d)$ with $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ an element of $\overline{\Gamma} = \mathrm{PGL}(2, \mathbb{Z})$; that is, a, b, c, d are integers such that $ad - bc = \pm 1$.*

Many authors say that two such irrational numbers r_1 and r_2 from Theorem 1 are *equivalent*.

Theorem 1 lets us move from talking about "polynomials whose roots all have common tails" to talking about "polynomials whose roots are related by elements of $\overline{\Gamma} = \mathrm{PGL}(2, \mathbb{Z})$," and so our next task is to understand more about this extended modular group $\overline{\Gamma}$.

2 The Extended Modular Group.

Although much has been written about this extended modular group $\overline{\Gamma} = \mathrm{PGL}(2, \mathbb{Z})$ (see, for example, [8] and [14]), we need only the following two results on $\overline{\Gamma}$. Both of these results follow immediately from theorems by Yılmaz Özgür and Şahin [15, Theorem 2.3] and Dresden [3]. (For proofs, see [2].) Our first result limits the size of finite subgroups in $\overline{\Gamma}$.

Theorem 2. *Any finite nontrivial subgroup of $\overline{\Gamma} = \mathrm{PGL}(2, \mathbb{Z})$ is of size two, three, four, or six. The groups of size two are conjugate in $\overline{\Gamma}$ to either $\{x, -x\}$ or $\{x, 1/x\}$ or $\{x, -1/x\}$. All groups of size three in $\overline{\Gamma} = \mathrm{PGL}(2, \mathbb{Z})$ are conjugate in $\overline{\Gamma}$ to the cyclic group*

$$G_3 = \left\{ x,\ \frac{-1}{x+1},\ \frac{-x-1}{x} \right\}.$$

Likewise, all groups of size four are conjugate in $\overline{\Gamma}$ *to the dihedral group*

$$G_4 = \left\{ x,\ \frac{1}{x},\ -x,\ \frac{-1}{x} \right\},$$

and all groups of size six are conjugate in $\overline{\Gamma}$ *to the dihedral group*

$$G_6 = \left\{ x,\ \frac{-1}{x+1},\ \frac{-x-1}{x},\ \frac{1}{x},\ \frac{-x}{x+1},\ -x-1 \right\}.$$

We note in our definitions above that G_6 contains G_3. Our second result on the extended modular group tells us more about this relationship.

Proposition 1. *If a group of size six in* $\overline{\Gamma} = \mathrm{PGL}(2, \mathbb{Z})$ *contains* G_3*, then the group must be* G_6*.*

These results on the finite subgroups of $\overline{\Gamma}$ will assist us in identifying polynomials with common tails, as we now show in the next section.

3 Polynomials with common tails.

Recall that Theorem 1 allows us to change our conversation from "polynomials whose roots all have common tails" to "polynomials whose roots are related by elements of $\overline{\Gamma} = PGL(2, \mathbb{Z})$." With this in mind, given a polynomial f we define Γ_f to be the set of linear fractional transforms $m(x) = (ax+b)/(cx+d)$ in $\overline{\Gamma}$ that take some root r_i of f to some root r_j for some particular i and j. This set Γ_f is clearly nonempty (as it always contains the element $m(x) = x$), and the following theorem gives us a bit more.

Theorem 3. *Suppose* f *of degree at least three is an irreducible polynomial with rational coefficients and with real roots, all with common tails. Then,* f *is of degree 3, 4, or 6, and the set* Γ_f *both permutes the roots of* f *and is a subgroup of* $\overline{\Gamma}$ *conjugate to* G_3*,* G_4*, or* G_6 *respectively.*

Proof. Given $f(x)$ as stated, we label the roots $\{r_1, r_2, \ldots, r_n\}$ where $n \geq 3$ is the degree of f. With Γ_f defined as above, we can now establish the following.

1. We claim that Γ_f has at least n elements. Since r_1 has common tails with each distinct root r_i, by Theorem 1 there are maps that take r_1 to each r_i.

2. We claim that for $(ax+b)/(cx+d)$ with integer coefficients and $ad - bc \neq 0$, the polynomial $g(x) = f((ax+b)/(cx+d)) \cdot (cx+d)^n$ has the same degree n as f. There are just two cases to check. If $c = 0$, then a, d are both nonzero and so $g(x) = f\left(\frac{a}{d}x + \frac{b}{d}\right) \cdot d^n$ which clearly has the same degree as f. If $c \neq 0$, then a a brief calculation shows that the coefficient of x^n in $g(x)$ is $f(a/c) \cdot c^n$, and since f is irreducible of degree at least 3 then $f(a/c)$ is nonzero and hence g is indeed of degree n.

3. We claim that a linear fractional transform m_{ij} in Γ_f that takes some root r_i to some root r_j must in fact take *every* root back to a root (that is to say, it must be a *permutation* on the complete set of roots $\{r_1, r_2, \ldots, r_n\}$). If we write $m_{ij}(x) = (ax+b)/(cx+d)$ and we recall that it takes r_i to r_j, then $f(m_{ij}(x)) \cdot (cx+d)^n$ is a polynomial (still of degree n) with r_i as a root. Of course, f itself has r_i as a root, so by the uniqueness of minimal polynomials we know that f is a (nonzero) constant multiple of $f(m_{ij}(x)) \cdot (cx+d)^n$. Thus, they have exactly the same

roots, and hence m_{ij} takes each root $r_1, r_2, \ldots, r_n$ back into that same collection of roots. But m_{ij} is a linear fractional transform with determinant ± 1 and hence it is invertible (in fact, its inverse corresponds precisely to the matrix inverse of the corresponding matrix for m_{ij}) so m_{ij} is a one-to-one map from $\{r_1, r_2, \ldots, r_n\}$ back into itself, and hence is a permutation of that set of roots.

4. We now claim that Γ_f is closed under composition. Suppose m and m' are both in Γ_f, so both act as permutations on the roots. Their composition is still a linear fractional transform and is still a permutation on the roots, hence is still in Γ_f.

5. Next, we claim Γ_f has exactly n elements. Suppose m and m' are both in Γ_f and both take r_1 to the same root r_i. Then, $m^{-1}(m'(x))$ takes r_1 back to r_1. We write $m^{-1}(m'(x))$ as $(ax+b)/(cx+d)$, and since $m^{-1}(m'(r_1))$ equals r_1, we get the equation $(ar_1+b)/(cr_1+d) = r_1$. This becomes $cr_1^2 + (d-a)r_1 - b = 0$, and since r_1 is algebraic of degree at least 3, we get that $c = 0$, $d-a = 0$, and $b = 0$, which means $(ax+b)/(cx+d)$ simplifies to $(ax+0)/(0x+a) = ax/a$. This could be $1x/1$ or $(-1)x/(-1)$, but either way it reduces to the identity map x, and so $m^{-1}(m'(x)) = x$ and thus $m(x) = m'(x)$. Hence, the map (let's call it m_{1i}) that takes r_1 to r_i is unique. Combined with step 1, we see that we have a bijection from the set $\{r_1, \ldots, r_n\}$ to the set Γ_f by the map that takes r_i to m_{1i}, and so Γ_f has exactly n elements.

6. Finally, since Γ_f is a nonempty and finite subset of $\overline{\Gamma}$ (by step 5) that is closed under the group operations, it is actually a subgroup of $\overline{\Gamma}$ and so by Theorem 2 it is conjugate to either G_3, G_4, or G_6 and hence has degree 3, 4, or 6, respectively; the same can be said about the degree of $f(x)$.

□

Example 1. Let us consider the polynomial $f(x) = x^3+6x^2+9x+1$ from the opening paragraph of this article. Hobby and Hobby showed (by direct computation in [7]) that the map $(3x+7)/(-x-2)$ and its inverse $(-2x-7)/(x+3)$ permute the roots and have associated determinant 1. Thanks to Theorem 3, we can conclude that the complete set Γ_f of all such linear fractional transforms is a group of size three, hence must be these two maps along with the identity. We also know from Theorem 2 that Γ_f is conjugate to G_3, and so there exists a $\sigma \in \overline{\Gamma}$ such that $\Gamma_f = \sigma^{-1} \circ G_3 \circ \sigma$, or in other words,

$$\left\{x,\ \frac{3x+7}{-x-2},\ \frac{-2x-7}{x+3}\right\} = \sigma^{-1} \circ \left\{x,\ \frac{-1}{x+1},\ \frac{-x-1}{x}\right\} \circ \sigma.$$

Although Theorem 2 is not constructive, it is a fairly simple task to find σ; if we write $\sigma(x) = (sx+t)/(ux+v)$, then we can look to solve

$$\frac{3x+7}{-x-2} = \sigma^{-1} \circ \frac{-1}{x+1} \circ \sigma = \frac{-(st+tu+uv)x - (t^2+tv+v^2)}{(s^2+su+u^2)x + (uv+sv+st)}. \tag{1}$$

We can set the two expressions (s^2+su+u^2) and $-(t^2+tv+v^2)$ equal to (plus or minus) the corresponding entries in $(3x+7)/(-x-2)$. The second equality gives us $t^2+tv+v^2 = \pm 7$, a type of *positive definite binary quadratic form* (see [1] for details on binary quadratic forms). For our purposes, we can rewrite this as $(2t+v)^2 + 3v^2 = \pm 28$ which becomes easy to solve. (A similar method applies for s and u.) We find $s = -1, t = -3, u = 0, v = 1$ as one possible solution to (1) and so $\sigma(x) = -x-3$ is one such desired function.

As we now turn our attention from subgroups of $\overline{\Gamma}$ back to polynomials with common tails, we know from Theorem 3 that we need only look at polynomials of degrees 2, 3, 4, or 6. The first two cases were covered by Serret in the nineteenth century; we will review those results and then use them in our work on polynomials of degree 4 and 6. For the quartics, we will call upon a factoring technique of Descartes from the seventeenth century, and then for the sextics we will bring in a bit of invariant theory.

4 Serret's work on quadratic polynomials.

Serret used what we call Theorem 1 to prove the following, which can be found in [12, §26, pp. 57–58].

Theorem 4 (Serret)**.** *Let f be an irreducible monic polynomial of degree two with rational coefficients and real roots. Then f has roots with common tails if and only if there exist rational P and integers a, c with*

$$f(x) = x^2 + Px - \left(\frac{Pa}{c} + \frac{a^2 \pm 1}{c^2}\right) \qquad \textit{and} \qquad c|(a^2 \pm 1) \tag{2}$$

The following examples illustrate how to use this theorem.

Example 2. We start with $f(x) = x^2 + (21/2)x + 9/2$. By applying equation (2), we find that f will have common tails if and only if we can find integer solutions to the *indefinite* binary quadratic form $2a^2 + 21ac + 9c^2 = \mp 2$ such that $c|(a^2 \pm 1)$. A quick search reveals that $a = 191, c = -19$ is one such solution, with $c|(a^2 - 1)$.

Example 3. We continue with $f(x) = x^2 + (21/2)x + 9/4$. This does not have common tails (the roots are $[-11; 1, 2, 1, \overline{1, 3, 1, 9, 3, 1}]$ and $[-1; \overline{1, 3, 1, 1, 3, 9}]$), but as we now show it takes some effort to prove this with Theorem 4. If we attempt to apply equation (2), we get $9/4 = -((21/2)a/c + (a^2 \pm 1)/c^2)$ with $c|(a^2 \pm 1)$. The equation simplifies to $4a^2 + 42ac + 9c^2 = \mp 4$, and using the standard methods for solving binary quadratic forms (as seen in [4, Chapter 4]) we discover that $4a^2 + 42ac + 9c^2 = -4$ has no integer solutions but $4a^2 + 42ac + 9c^2 = 4$ has infinitely many solutions $\pm(a_k, c_k)$, where

$$(a_k, c_k) = (1, 0) \cdot \begin{pmatrix} -7 & 32 \\ -72 & 329 \end{pmatrix}^k, \qquad k \in \mathbb{Z}.$$

It remains to show that $c_k \nmid (a_k^2 - 1)$ for all k. By carefully analyzing the powers of the matrix above, we can show that if 2^i is the largest power of 2 that divides c_k, then $a_k \equiv 1 \pm (2^{i-2} + 2^{i-1})$ mod 2^i. This implies $a_k^2 - 1 \equiv 2^{i-1}$ mod 2^i and so since 2^i divides c_k and not $a_k^2 - 1$, we have $c_k \nmid (a_k^2 - 1)$. Hence, there are no solutions to (2) and so Theorem 4 tells us this polynomial does not have common tails.

Suffice it to say, Theorem 4 is rather difficult to use. Fortunately, the situation is much easier for polynomials of higher degree, as we show next.

5 Serret's work on cubic polynomials.

This is the second case considered by Serret. To begin with, given a cubic $x^3 + Px^2 + Qx + R$ we recall that its discriminant Δ can be written as

$$\Delta = -(4Q^3 + 27R^2) + 18PQR + P^2Q^2 - 4P^3R. \tag{3}$$

With this in mind, and so long as $\Delta \neq 0$ (which is the same as saying that the polynomial has no repeated roots), Serret [13, §511, p. 468] defined

$$a = \frac{\sqrt{\Delta} - (9R - PQ)}{2\sqrt{\Delta}}, \qquad b = \frac{-(a^2 - a + 1)}{c}, \qquad c = \frac{6Q - 2P^2}{2\sqrt{\Delta}}, \qquad d = 1 - a. \tag{4}$$

Serret went on to show that $m(x) = (ax+b)/(cx+d)$ is of order three under composition, permutes the roots of the cubic, and has associated determinant $ad - bc = 1$. Thus, thanks to Theorem 1, Serret concluded the following.

Theorem 5 (Serret)**.** *Given a polynomial $x^3 + Px^2 + Qx + R$ with real coefficients and three distinct irrational roots, the roots will have common tails if and only if the four quantities a, b, c, d defined in (4) are all integers.*

It is typical (but not required) to apply Serret's theorems to cubics with rational coefficients P, Q, R. However, the theorem still holds for irrational coefficients, a fact that we will exploit a bit later in Section 8 on sextics.

Example 4. We return to the polynomial $f(x) = x^3 + 6x^2 + 9x + 1$ as seen in the opening paragraph of this article. Using (4) we get a, b, c, d equal to $3, 7, -1, -2$, respectively, and so the roots are permuted by $(3x+7)/(-x-2)$; thus we recover the same map discovered by Hobby and Hobby in Example 1. Since a, b, c, d are all integers, Theorem 5 confirms that the roots all have common tails.

6 Cubics, Quartics, and Sextics.

Suppose we have a cubic polynomial with roots permuted by G_3; that is to say, if r is a root, so also are $-1/(r+1)$ and $(-r-1)/r$. This would be the polynomial

$$\left(x - r\right)\left(x - \frac{-1}{r+1}\right)\left(x - \frac{-r-1}{r}\right).$$

If we expand and carefully group the terms, we obtain

$$x^3 - Ax^2 - (A+3)x - 1, \qquad \text{such that} \quad A = \frac{r^3 - 3r - 1}{r(r+1)}.$$

With this in mind, we define $p_3(x; A) = x^3 - Ax^2 - (A+3)x - 1$, and thanks to our construction, *any* monic cubic polynomial whose roots are permuted by G_3 must equal $p_3(x; A)$ for some A. Furthermore, if A is chosen such that $p_3(x; A)$ has real roots and is irreducible over $\mathbb{Q}$, then $p_3(x; A)$ has common tails.

Likewise, we can describe all monic quartic polynomials with roots permuted by G_4 by starting with

$$\left(x - r\right)\left(x - \frac{1}{r}\right)\left(x - (-r)\right)\left(x - \frac{-1}{r}\right)$$

and expanding to obtain

$$x^4 - 2Ax^2 + 1, \qquad \text{such that} \quad 2A = \frac{r^4 + 1}{r^2},$$

and so it is natural to define $p_4(x; A) = x^4 - 2Ax^2 + 1$.

Finally, we can apply the same method with G_6 and we are led to the polynomial

$$p_6(x;A) = x^6 + 3x^5 - Ax^4 - (5+2A)x^3 - Ax^2 + 3x + 1,$$

such that $A = (1 + 3r - 5r^3 + 3r^5 + r^6)/(r^2(1+r)^2)$.

We have noted that any monic cubic polynomial whose roots are permuted by G_3 must equal $p_3(x;A)$ for some A. The same applies to G_4 and G_6 with the polynomials $p_4(x;A)$ and $p_6(x;A)$. Surprisingly, *every* nonquadratic polynomial with common tails is related to p_3, p_4 or p_6, as the following theorem illustrates.

Theorem 6. *Suppose $f(x)$ of degree $n = 3, 4,$ or 6 is an irreducible polynomial with rational coefficients and with real roots, all with common tails. Then there exists $A \in \mathbb{Q}$ and $\sigma \in \overline{\Gamma}$ such that $f(x)$ is an appropriate multiple of $p_n(\sigma(x); A)$.*

The phrase "appropriate multiple" in the statement of the theorem is necessary as $\sigma(x)$ has the form $(sx+t)/(ux+v)$ and so we would need to multiply $p_n(\sigma(x); A)$ by $(ux+v)^n$ to assure ourselves that we actually have a polynomial on our hands.

Before proving Theorem 6, it might first be helpful to revisit a familiar polynomial.

Example 5. For $f(x) = x^3 + 6x^2 + 9x + 1$ from Examples 1 and 4, we can verify that Theorem 6 applies in this case by writing $f(x) = -p_3(\sigma(x); A)$ for $\sigma(x) = -x - 3$ and $A = -3$. This is, of course, the same $\sigma(x)$ that we saw in Example 1.

Proof of Theorem 6. Let $n = 3, 4,$ or 6 be the degree of f, and let Γ_f be the associated subgroup of $\overline{\Gamma}$ from Theorem 3. We know from that theorem that Γ_f is conjugate in $\overline{\Gamma}$ to G_n; let $\sigma \in \overline{\Gamma}$ be that element such that $\Gamma_f = \sigma^{-1} \cdot G_n \cdot \sigma$. (This is the same construction as we saw in Example 1.) Let $X = \{r_1, r_2, \ldots, r_n\}$ be the solution set of $f(x)$. Obviously, $\sigma \circ X$ is the solution set for $f(\sigma^{-1}(x))$. Now, apply G_n to $\sigma \circ X$ with $G_n = \sigma \circ \Gamma_f \circ \sigma^{-1}$ and we get $G_n \circ \sigma \circ X = \sigma \circ \Gamma_f \circ X$. But Γ_f permutes the roots of $f(x)$, so $\Gamma_f \circ X = X$. Then $G_n \circ \sigma \circ X = \sigma \circ X$. This means G_n also permutes the roots of $f(\sigma^{-1}(x))$. By our discussion above concerning the construction of the polynomials p_3, p_4, and p_6, this means $f(\sigma^{-1}(x))$ must have the same roots as $p_n(x; A)$ for some A. This means $f(x)$ has the same roots as $p_n(\sigma(x); A)$, and so $f(x)$ is an appropriate multiple of $p_n(\sigma(x); A)$, as desired. $\square$

7 Quartics with Common Tails.

Serret made the following observation on quadratics in [12, §26, p. 59], right after what we call Theorem 4:

> Il faut remarquer que les racines de l'équation (2) donnent lieu à des fractions continues qui se terminent par les mêmes quotients, lors même que la quantité P serait irrationnelle.

which translates to

> Note that the roots of equation (2) give rise to continued fractions that end in the same quotients, even though the quantity P is irrational.

Here's a particularly nice application of this fact. The quartic polynomial $f(x) = x^4 - 4x^2 + 1$ factors as

$$x^4 - 4x^2 + 1 = (x^2 + \sqrt{2}x - 1)(x^2 - \sqrt{2}x - 1) \tag{5}$$

and each of those quadratic factors fits the format of equation (2) in Theorem 4, using $P = \pm\sqrt{2}$, $a = 0$, and $c = 1$. Hence, each factor has roots with common tails, but note that each root of one factor is the negative of a root of the other factor, and so all four roots must have common tails. A quick computation of our four roots as continued fractions confirms this:

$$\begin{aligned}
-1.93185\ldots &= [-2; 14, \quad 1, 2, 15, 10, 1, 18, 1, 1, 21, \ldots];\\
-0.517638\ldots &= [-1; 2, 13, \quad 1, 2, 15, 10, 1, 18, 1, 1, 21, \ldots];\\
0.517638\ldots &= [0; 1, 1, 13, \quad 1, 2, 15, 10, 1, 18, 1, 1, 21, \ldots];\\
1.93185\ldots &= [1; 1, 13, \quad 1, 2, 15, 10, 1, 18, 1, 1, 21, \ldots].
\end{aligned}$$

Of course, to apply Serret's Theorem 4 to quartics in this manner we need to first guarantee that we can always find a factorization like equation (5), and as it turns out an old method of Descartes [11, p. 209] from 1637 allows us to do exactly that. To this end, we set up the *resolvent cubic* of a quartic, as follows. Given $f(x) = x^4 + Px^3 + Qx^2 + Rx + S$, we first write $g(x) = f(x - P/4)$, known as the *depressed quartic* as it has no x^3 term. Then, given this $g(x) = x^4 + a_2x^2 + a_1x + a_0$, we define the resolvent cubic to be $h(y) = y^3 + 2a_2y^2 + (a_2^2 - 4a_0)y - a_1^2$. For u a nonzero root of this resolvent cubic, Descartes gave the following factorization for the original quartic $f(x)$:

$$(x^2 + (P/2 + \sqrt{u})x + (s + t\sqrt{u})) \cdot (x^2 + (P/2 - \sqrt{u})x + (s - t\sqrt{u})), \tag{6}$$

where the numbers s and t are defined as

$$s = \frac{Q + u}{2} - \frac{P^2}{8}, \qquad t = \frac{sP - R}{2u}. \tag{7}$$

With this, we can now establish the following.

Theorem 7. *Let f be an irreducible quartic polynomial with rational coefficients and four real roots. Then f has common tails if and only if the following two statements hold:*

1. *The resolvent cubic has three distinct rational roots.*
2. *For each nonzero root u of the resolvent cubic, the values s, t from (7) obey the following: if we write $t = -a/c$ for a,c relatively prime integers, then c divides $a^2 \pm 1$ and $s = tP/2 - (a^2 \pm 1)/c^2$ for some particular choice of the $\pm$ sign.*

We note that *this is much easier* than Serret's Theorem 4 for quadratics, because in that theorem (as seen in Example 2 and 3) we had to search for the integers a and c (or prove they didn't exist) either by brute force or through the theory of binary quadratic forms. In this Theorem 7 for quartics, our test for common tails uses entirely elementary methods: calculate the resolvent cubic, use the rational root test to find any nonzero rational roots u, then use (7) to find the rational numbers s and t, and then read $-a$ and c from the numerator and denominator of t. Perhaps an example will help illustrate this technique.

Example 6. Consider $f(x) = x^4 + 2x^3 - 19x^2 - 20x - 5$. The depressed quartic is $f(x - 1/2) = x^4 - (41/2)x^2 + 1/16$, with resolvent cubic $y^3 - 41y^2 + 420y = y(y - 20)(y - 21)$. If we take the first nonzero root $u = 20$ of the resolvent cubic, Descartes's method lets us factor $f(x)$ as

$$\left(x^2 + (1 + \sqrt{20})x + \sqrt{20}/2\right) \cdot \left(x^2 + (1 - \sqrt{20})x - \sqrt{20}/2\right),$$

with $s = 0$ and $t = 1/2$. We choose $a = -1$, $c = 2$ and we verify that $c|a^2 + 1$ and that $s = tP/2 - (a^2 + 1)/c^2$ with $P = 2$ and using the $+$ in the $a^2 \pm 1$ terms. Next, using the other nonzero root $u = 21$, Descartes's method now gives us

$$\left(x^2 + (1 + \sqrt{21})x + (1/2 + \sqrt{21}/2)\right) \cdot \left(x^2 + (1 - \sqrt{21})x + (1/2 - \sqrt{21}/2)\right),$$

with $s = 1/2$ and $t = 1/2$. We again choose $a = -1$, $c = 2$, and we verify that $c|a^2 - 1$ and $s = tP/2 - (a^2 - 1)/c^2$, this time using the negative sign in the $a^2 \pm 1$ terms. We conclude that our polynomial $f(x)$ does indeed have roots with common tails.

Interestingly, we can write $f(x)$ as $p_4(2x + 1; 41)/16$, which does not satisfy Theorem 6, and also as $p_4((x + 1)/x; 11/10) \cdot (-5x^4)$, which does.

Before proving our Theorem 7, we need to establish the following statement about polynomials of degree 4 with common tails.

Proposition 2. *Suppose f is an irreducible quartic polynomial with rational coefficients and real roots, all with common tails. Then the Galois group of $f(x)$ is dihedral of size 4.*

Proof. By Theorem 6, we know $f(x)$ is an appropriate multiple of $p_4(\sigma(x); A)$ for some σ and A. Since $\sigma \in \overline{\Gamma}$ is invertible, the splitting fields for $p_4(x; A)$ and $p_4(\sigma(x); A)$ are actually the same (the inclusions in both directions are easy to see), and hence their Galois groups are the same. Fortunately, the Galois group for $p_4(x; A)$ is easy to calculate. The four roots are $\frac{1}{2}(\pm\sqrt{2A + 2} \pm \sqrt{2A - 2})$, and so its splitting field is $\mathbb{Q}(\sqrt{2A + 2}, \sqrt{2A - 2})$, and it is a standard exercise in many algebra textbooks ([5, p. 548] or [11, p. 204]) to show that the Galois group for this kind of field is a dihedral group of size 4. $\square$

We are now ready to prove our theorem.

Proof of Theorem 7. First, suppose our quartic f has common tails. By Proposition 2 the Galois group of f is dihedral of size 4, and so by [9, Theorem 1] the resolvent cubic of f must have three distinct rational roots.

(We have to be a bit careful here; the resolvent cubic in [9] differs slightly from the "Descartes" resolvent cubic we are using, in that the roots of one cubic are shifted, by the constant a_2, from the roots of the other cubic. However, we are only interested in whether or not we have three *distinct rational* roots and so this slight difference is immaterial to us.)

For u a nonzero root of that resolvent cubic, we consider the first factor in the expression (6):

$$x^2 + (P/2 + \sqrt{u})x + (s + t\sqrt{u}). \tag{8}$$

Since $f(x)$ has common tails, then so also does (8). As we mentioned earlier, Serret observed that his derivation of (2) from Theorem 1 worked equally well for a quadratic with irrational coefficients, and so given this we must have P', a, c with $c|(a^2 \pm 1)$ and

$$x^2 + P'x - \left(\frac{P'a}{c} + \frac{a^2 \pm 1}{c^2}\right) = x^2 + (P/2 + \sqrt{u})x + (s + t\sqrt{u}).$$

Comparing the linear terms gives us $P' = P/2 + \sqrt{u}$, and so from the constant terms we have

$$-\left(\left(\frac{P}{2} + \sqrt{u}\right)\left(\frac{a}{c}\right) + \frac{a^2 \pm 1}{c^2}\right) = s + t\sqrt{u}. \tag{9}$$

Now, f being irreducible means (8) must have irrational coefficients and so in particular $\sqrt{u} \notin \mathbb{Q}$. Thus we can compare the coefficients of $\sqrt{u}$ in (9) which gives us $t = -a/c$ and thus $s = tP/2 - (a^2 \pm 1)/c^2$ as desired.

Conversely, suppose f satisfies conditions 1 and 2 of the theorem. From condition 2, it's easy to show (by brute force if necessary) that the roots of each quadratic in (6) are permuted by $m(x) = \dfrac{ax - \frac{a^2 \pm 1}{c}}{cx - a}$ with the appropriate choice of sign, and hence by Theorem 1 each quadratic in (6) has common tails. Since condition 1 tells us the resolvent cubic has three distinct roots, at least two of them are nonzero (let's call them u_1 and u_2), and each of these give us a distinct and separate factorization in (6). If the first factorization (using u_1) in (6) gives us two quadratics with roots r_1, r_2 and roots r_3, r_4, then the second factorization (using u_2 in place of u_1) will give us two quadratics with either r_1, r_3 and r_2, r_4 as roots, or r_1, r_4 and r_2, r_3 as roots. From our first factorization (with u_1) we have that r_1, r_2 have common tails as do r_3, r_4. From the second factorization (with u_2) we have that either r_1, r_3 have common tails or r_1, r_4 have common tails, but in either case we conclude that all four roots r_1, r_2, r_3, r_4 of our original quartic f have common tails. □

8 Sextics with common tails

We now start working on our theorem to identify sextics with common tails. This will require a few definitions. First, given a monic polynomial with roots $\{r_1, r_2, \dots\}$ we recall that its discriminant Δ is defined as

$$\Delta = \prod_{i<j} (r_i - r_j)^2. \tag{10}$$

While this can always be expressed in terms of the polynomial's coefficients (as seen in (3) for the cubic case), it is not practical to do so for the sextic. In all cases, the discriminant is positive so long as the roots are distinct real numbers.

Next, given an element m of order three in $\overline{\Gamma} = \mathrm{PGL}(2, \mathbb{Z})$, we know from applying Theorem 2 that there exists $\sigma_m \in \overline{\Gamma}$ such that the group $\{x, m(x), m^2(x)\}$ equals $\sigma_m^{-1} \cdot G_3 \cdot \sigma_m$. We recall that although Theorem 2 is not constructive, it is a fairly simple task to use the technique from Example 1 to find such a conjugator element σ_m in $\overline{\Gamma}$. With this in mind, we are ready for our final theorem.

Theorem 8. *Given a monic irreducible sextic polynomial f with rational coefficients and real roots, it has common tails if and only if the following are true.*

1. *The sextic f factors over $\mathbb{Q}(\sqrt{\Delta})$ into two monic cubics f_1 and f_2.*
2. *At least one of the cubics f_1 and f_2 satisfies the conditions of Theorem 5; in particular, the cubic has common tails, and the values a, b, c, and d in (4) are all integers.*
3. *For $m(x)$ the order-three transform $(ax + b)/(cx + d)$ with a, b, c, d from part 2, and for $\sigma_m(x) \in \overline{\Gamma}$ a conjugator as defined above, the numerator of the rational polynomial $f(\sigma_m^{-1}(x))$ is palindromic.*

Before diving into the proof of Theorem 8, it might be instructive to work through an example.

Example 7. We begin with the monic polynomial

$$f(x) = \left(735x^6 - 735x^5 - 203x^4 + 515x^3 - 239x^2 + 45x - 3\right)/735,$$

which factors over $\mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(\sqrt{345})$ into the two monic cubics

$$f_1(x) = x^3 \;+\; \frac{-15+\sqrt{345}}{30}x^2 \;-\; \frac{3+\sqrt{345}}{42}x \;+\; \frac{10+\sqrt{345}}{245},$$
$$f_2(x) = x^3 \;+\; \frac{-15-\sqrt{345}}{30}x^2 \;-\; \frac{3-\sqrt{345}}{42}x \;+\; \frac{10-\sqrt{345}}{245}.$$

Both cubics satisfy the conditions of Theorem 5 with a, b, c, d equal to $-2, 1, -7, 3$, respectively, and so with $m(x)$ equal to $(-2x+1)/(-7x+3)$ we now wish to find a function σ_m such that

$$m(x) \;=\; (-2x+1)/(-7x+3) \;=\; \sigma_m^{-1}(x) \;\circ\; -1/(x+1) \;\circ\; \sigma_m(x).$$

We use the same technique as in Example 1 to find that $\sigma_m(x) = (3x-1)/(-x)$ meets our needs. We note that

$$f(\sigma_m^{-1}(x)) = \frac{3x^6 + 9x^5 - 31x^4 - 77x^3 - 31x^2 + 9x + 3}{-735(x+3)^6},$$

which does indeed have a palindromic numerator. We conclude that this polynomial has six roots with common tails, and a quick calculation confirms this:

$$\begin{aligned}
-0.866885\ldots &= [-1; 7, \quad 1, 1, 19, 1, 5, 2, 4, 1, 1, 721, 1, 1, 3, \ldots];\\
0.162508\ldots &= [0; 6, 6, \quad 1, 1, 19, 1, 5, 2, 4, 1, 1, 721, 1, 1, 3, \ldots];\\
0.301468\ldots &= [0; 3, 3, 6, \quad 1, 1, 19, 1, 5, 2, 4, 1, 1, 721, 1, 1, 3, \ldots];\\
0.362418\ldots &= [0; 2, 1, 3, 6, \quad 1, 1, 19, 1, 5, 2, 4, 1, 1, 721, 1, 1, 3, \ldots];\\
0.446278\ldots &= [0; 2, 4, 6, \quad 1, 1, 19, 1, 5, 2, 4, 1, 1, 721, 1, 1, 3, \ldots];\\
0.594213\ldots &= [0; 1, 1, 2, 6, \quad 1, 1, 19, 1, 5, 2, 4, 1, 1, 721, 1, 1, 3, \ldots].
\end{aligned}$$

We can also verify that Theorem 6 applies to $f(x)$ now that we know it has common tails, and we would like to use $\sigma_m(x) = (3x-1)/(-x)$ from earlier in this example. A quick calculation reveals the following satisfying formula:

$$f(x) = p_6\left(\frac{3x-1}{-x};\; 31/3\right) \cdot (-x^6/245).$$

We are now ready for our proof.

Proof of Theorem 8. To begin, we suppose f is a monic irreducible sextic polynomial with rational coefficients and six common tails. We will prove that this implies parts 1, 2, and 3 of our theorem. By Theorem 6, $f(x)$ is an appropriate multiple of $p_6(\sigma(x); A)$ for some $\sigma \in \overline{\Gamma}$ and some rational A. To be precise, there is some $\sigma(x) = (sx+t)/(ux+v)$ in $\overline{\Gamma}$, some rational A, and some rational B such that

$$f(x) = p_6(\sigma(x); A) \cdot (ux+v)^6 \cdot B, \tag{11}$$

where the constant B is chosen to make the right-hand side of (11) monic. Now, $p_6(x; A)$ has two interesting properties. First, the discriminant of $p_6(x; A)$ is $\Delta = 2^6(A+6)^4(A-3/4)^3$, which can be verified by using (10) with the six roots given by having G_6 act on a single root r. And second, $p_6(x; A)$ factors over $\mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(\sqrt{A-3/4})$ as

$$p_6(x; A) = p_3(x; -3/2 + \sqrt{A-3/4}) \cdot p_3(x; -3/2 - \sqrt{A-3/4}).$$

Surprisingly, we can say almost exactly the same about f. First, since the discriminant of a polynomial is invariant under linear fractional transforms $(sx+t)/(ux+v)$ with $sv - tu = \pm 1$ (see [10, Theorem 2.39]), the discriminant of f from (11) is the same as the discriminant for $p_6(x; A)$, namely, $\Delta = 2^6(A+6)^4(A-3/4)^3$. Second, thanks to the factorization of $p_6(x; A)$ over $\mathbb{Q}(\sqrt{A-3/4})$ given above, we can apply it to the right-hand side of (11) to obtain $f(x) = f_1(x) \cdot f_2(x)$, with

$$\begin{aligned} f_1(x) &= p_3(\sigma(x); -3/2 + \sqrt{A - 3/4}) \cdot (ux + v)^3 \cdot B_1 \\ f_1(x) &= p_3(\sigma(x); -3/2 - \sqrt{A - 3/4}) \cdot (ux + v)^3 \cdot B_2, \end{aligned} \tag{12}$$

where B_1 and B_2 are chosen so as to make the right-hand sides of (12) into monic polynomials. These two monic polynomials f_1 and f_2 have coefficients in $\mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(\sqrt{A - 3/4})$, and so this satisfies part 1 of our theorem.

For part 2, we know that since f_1 and f_2 are factors of the sextic f, they each are (monic, by definition) cubics with common tails and thus must satisfy the conditions of Theorem 5. For part 3, we let $m(x) = (ax + b)/(cx + d)$ be the linear fractional transform with coefficients a, b, c, d from (4) and Theorem 5 for the polynomial f_1, and we let σ_m be an element in $\overline{\Gamma}$ (thanks to Theorem 2) such that $\{x, m(x), m^2(x)\} = \sigma_m^{-1} \circ G_3 \circ \sigma_m$. Now, we know $m(x)$ and $m^2(x)$ are in Γ_{f_1} which means they're also in Γ_f (we are using the definition of Γ_f from Section 3). This means $\sigma_m^{-1} \circ G_3 \circ \sigma_m$ is in Γ_f, which means $\sigma_m \circ \Gamma_f \circ \sigma_m^{-1}$ contains G_3, and so thanks to Proposition 1 we have $\sigma_m \circ \Gamma_f \circ \sigma_m^{-1} = G_6$ which in particular contains $1/x$. Now, since Γ_f permutes the roots of $f(x)$, we have that $G_6 = \sigma_m \circ \Gamma_f \circ \sigma_m^{-1}$ permutes the roots of $f(\sigma_m^{-1}(x))$ and since $1/x$ is one of those permutations, then the numerator of $f(\sigma_m^{-1}(x))$ must be palindromic.

For the other direction, suppose f is a monic irreducible sextic with rational coefficients satisfying parts 1, 2, and 3 given in the theorem. We know at least one of the monic cubic factors (call it f_1) has three roots r_1, r_2, r_3 with common tails by part 2, with appropriate map $m(x) = (ax+b)/(cx+d)$ with a, b, c, d derived from the coefficients of $f_1(x)$ as seen in (4). We now show that the other factor (call it f_2 with roots r_4, r_5, r_6) produces the same values a, b, c, d from (4) and hence has common tails as well. From our definition of the discriminant in (10), we know $\sqrt{\Delta}$ is in the splitting field for $f(x)$, and $\sqrt{\Delta} \notin \mathbb{Q}$, so there exists an element ϕ in the Galois group of f such that $\phi(\sqrt{\Delta}) = -\sqrt{\Delta}$. We claim that ϕ applied to the coefficients of f_1 (we write this as f_1^{ϕ}) equals f_2. We know $f_1(r_1) = 0$, which means $\phi(f_1(r_1)) = 0$ which becomes $f_1^{\phi}(\phi(r_1)) = 0$, and so (since $\phi(r_1)$ is still a root of $f(x)$) the monic cubic f_1^{ϕ} is still a factor of f but it's not f_1, so by the uniqueness of minimal polynomials it must be f_2. Now we know $f_2 = f_1^{\phi}$, so the values in (4) from the coefficients of f_2 must be $\phi(a), \phi(b), \phi(c), \phi(d)$ with a, b, c, d from the coefficients of f_1. Of course, these values a, b, c, d are integers, and hence $\phi(a), \phi(b), \phi(c), \phi(d)$ equal a, b, c, d and so our roots r_4, r_5, r_6 of f_2 have common tails as well.

Turning our attention to $f(\sigma_m^{-1}(x))$, its roots are $\sigma_m(r_1), \ldots, \sigma_m(r_6)$ and since $f(\sigma_m^{-1}(x))$ is palindromic these roots are permuted by $1/x$, and since f is irreducible none of these roots are fixed by $1/x$. This means at least one element of $\{\sigma_m(r_1), \sigma_m(r_2), \sigma_m(r_3)\}$ has common tails with at least one element of $\{\sigma_m(r_4), \sigma_m(r_5), \sigma_m(r_6)\}$, and since σ_m is in $\overline{\Gamma} = \mathrm{PGL}(2, \mathbb{Z})$, then by Theorem 1 we can say the same about $\{r_1, r_2, r_3\}$ and $\{r_4, r_5, r_6\}$. We conclude that all six roots have common tails. □

9 Conclusion.

We have only scratched the surface of what can be discovered in the topic of polynomials with roots with common tails! For example, suppose we were to use a more general definition of continued fractions, perhaps of the form

$$b_0 + \cfrac{a_1}{b_1 + \cfrac{a_2}{b_2 + \cfrac{a_3}{b_3 + \cdots}}}.$$

Would this give us a larger class of polynomials with roots with common tails?

Acknowledgment. The authors express their gratitude to the editor and the anonymous referees for their numerous comments which have greatly improved the article. We very much appreciate their patience.

References

[1] Buell, D. (1989). *Binary Quadratic Forms.* New York: Springer-Verlag.

[2] Dresden, G., Panthi, P., Shrestha, A., Zhang, J. (2018). Finite subgroups of the extended modular group. `arxiv.org/abs/1802.02000`

[3] Dresden, G. (2004). There are only nine finite groups of fractional linear transformations with integer coefficients. *Math. Mag.* 77(3): 211–218. doi.org/10.2307/3219118

[4] Flath, D. (1989). *Introduction to Number Theory.* New York: John Wiley & Sons.

[5] Gallian, J. (2010). *Contemporary Abstract Algebra*, 7th ed. Belmont, CA: Brooks/Cole.

[6] Hardy, G., Wright, E. (1979). *An Introduction to the Theory of Numbers*, 5th ed. New York: Oxford Univ. Press.

[7] Hobby, A., Hobby, D. (2015). Roots with common tails. `arxiv.org/abs/1508.07490v1`

[8] Jones, G., Thornton, J. (1986). Automorphisms and congruence subgroups of the extended modular group. *J. London Math. Soc. (2).* 34(1): 26–40. doi.org/10.1112/jlms/s2-34.1.26

[9] Kappe, L., Warren, B. (1989). An elementary test for the Galois group of a quartic polynomial. *Amer. Math. Monthly.* 96(2): 133–137. doi.org/10.2307/2323198

[10] Olver, P. (1999). *Classical Invariant Theory.* Cambridge, UK: Cambridge Univ. Press.

[11] Rotman, J. (2002). *Advanced Modern Algebra.* Upper Saddle River, NJ: Pearson.

[12] Serret, J. (1877). *Cours d'algèbre supérieure. Tome I*, 4th ed. Paris, France: Gauthier-Villars. Reprinted in 1992, Sceaux, France: Éditions Jacques Gabay.

[13] Serret, J. (1879). *Cours d'algèbre supérieure. Tome II*, 4th ed. Paris, France: Gauthier-Villars. Reprinted in 1992, Sceaux, France: Éditions Jacques Gabay.

[14] Singerman, D. (1985). $\mathrm{PSL}(2,q)$ as an image of the extended modular group with applications to group actions on surfaces. *Proc. Edinburgh Math. Soc. (2).* 30(1): 143–151. doi.org/10.1017/S001309150001806X

[15] Yılmaz Özgür, N., Şahin, R. (2003). On the extended Hecke groups $\overline{H}(\lambda_q)$. *Turkish J. Math.* 27(4): 473–480.

GREG DRESDEN received his Ph.D. from the University of Texas in 1997 and now teaches at Washington and Lee University in the mountains of Virginia. When not thinking about math, he enjoys playing piano and spending time with family.
Mathematics Department, Washington and Lee University, Lexington, VA 24450
dresdeng@wlu.edu

SAIMON ISLAM is currently an undergraduate Mathematics major receiving his B.S. degree from Washington and Lee University. He enjoys watching anything with Nicholas Cage or James Spader, and quoting Arnold Schwarzenegger.
Mathematics Department, Washington and Lee University, Lexington, VA 24450
islams19@mail.wlu.edu

PRAKRITI PANTHI is a junior at Washington and Lee working towards a B.S. degree in Mathematics and Economics. She enjoys playing badminton, hiking, reading fiction and rereading the Harry Potter series.
Mathematics Department, Washington and Lee University, Lexington, VA 24450
panthip20@mail.wlu.edu

ANUKRITI SHRESTHA is a senior at Washington and Lee majoring in Integrated Engineering (Chemistry) and Mathematics. She plans to pursue a Ph.D. in Chemical Engineering after graduation. She likes spending her free time reading mystery novels and hanging out with dogs.
Mathematics Department, Washington and Lee University, Lexington, VA 24450
shresthaa19@mail.wlu.edu

JIAHAO ZHANG is a Math major and East Asian Study minor at Washington and Lee University. He likes playing basketball and reading ancient Chinese poems in his spare time.
Mathematics Department, Washington and Lee University, Lexington, VA 24450
zhangj20@mail.wlu.edu