ACTA ARITHMETICA
155.1 (2012)

Schinzel's problem: Imprimitive covers and the monodromy method

by

MICHAEL D. FRIED (Irvine, CA, and Billings, MT) and
IVICA GUSIĆ (Zagreb)

1. Schinzel's problem and our particular case. For $f, g \in \mathbb{C}[x]$, *Schinzel's problem* was to describe those cases when

(1.1) $f(x) - g(y)$ factors nontrivially as a polynomial in two variables.

The topic is in [Sc71]; [Fr11] has many relevant references. With K a number field, let $\mathcal{O}_K$ be its ring of integers, $\boldsymbol{p}$ a prime ideal of $\mathcal{O}_K$, and $\mathcal{O}_K/\boldsymbol{p}$ its residue class field. Davenport's problem considered when, nontrivially,

(1.2) the ranges of f and g are identical on almost all $\mathcal{O}_K/\boldsymbol{p}$.

The most trivial cases are where $g(x) = f(ax + b)$ for some $a, b \in \bar{\mathbb{Q}}$, the algebraic numbers. When $K = \mathbb{Q}$, mostly that relation forces $a, b \in K$. For example this holds when f is *indecomposable* (not a composite of lower degree polynomials). With the indecomposability assumption, solutions to Davenport's and Schinzel's problems were essentially the same (solved in [Fr73, Thm. 1]; see [Fr11, Thm. 4.1]).

Cases where a, b are not in K are important to Davenport's problem, but not to Schinzel's. Though Schinzel's problem is our main focus, in §2.4 the indecomposable case reappears in Prob. 1.3, our case of Schinzel's problem. The dihedral group, D_n, with n even, the example of §1.3, will aid a reader unaccustomed to branch cycles. Compare our goals with the §1.4 conjecture.

1.1. Branch cycles. We start by assuming $f = f_1 \circ f_2$, and $\deg(f_i) > 1$, $i = 1, 2$: f *decomposes*. For Schinzel's problem (1.1) consider these extensions of what is a trivial relation between f and g (allowing a switch of f and g):

2010 *Mathematics Subject Classification*: Primary 141130, 20B15, 20C15, 30F10; Secondary 12D05, 12E30, 12F10, 20E22.
Key words and phrases: Davenport's problem, Schinzel's problem, factorization of variables separated polynomials, Riemann's existence theorem, wreath products, imprimitive groups.

DOI: 10.4064/aa155-1-3

(1.3a) Composition reducibility: $f_1(x) - g(y)$ factors.
(1.3b) A particular case of composition reducibility: $g = f_1 \circ g_2$.

[Fr87, Def. 2.1] calls an example of (1.1) *newly reducible*—nontriviality for Schinzel's problem—if the composite reducibility (1.3a) does not hold. We call the corresponding (f, g) a *Schinzel pair.*

We here consider the problem left by R. Avanzi and U. Zannier [AZ03], and the seconnd author [Gu10]. Consider those f for which there is a $g = \alpha \circ f$, with $\alpha \in \mathrm{PGL}_2(\mathbb{C})$, satisfying an essential condition for possible Schinzel pairs: The Galois closures of the covers $f, g : \mathbb{P}^1_x \to \mathbb{P}^1_z$ are the same. Then, from those find (f, g) that are Schinzel pairs.

Let $\mathbb{P}^1_z$ be the Riemann sphere, uniformized by the variable z. Any rational function $f \in \mathbb{C}(x)$ gives an analytic map (a *cover*) $\mathbb{P}^1_x \to \mathbb{P}^1_z$. If the degree of f is n, then *branch points* of f are the values of z over which there are fewer than n distinct points. For example, $z = \infty$ is a branch point of any polynomial $f \in \mathbb{C}[x]$ with $\deg(f) > 1$, because only ∞ lies over ∞. We denote the branch points of f by $\boldsymbol{z}_f = \{z_1, \dots, z_r\}$.

Refer to $f_X : X \to \mathbb{P}^1_z$, a compact Riemann surface cover, as *Galois* if the automorphisms that commute with f_X have cardinality $\deg(f_X)$. We often simplify f_X to f if there will be no misunderstanding. The *Galois* closure of f is the smallest Galois cover, $\hat{f} : \hat{X} \to \mathbb{P}^1_z$, that factors through f. It always exists. The group of automorphisms, G_f, of $\hat{X}$ commuting with $\hat{f}$ is the (geometric) *monodromy group* of f.

The Galois correspondence associates to the cover f_X a (faithful) coset (or permutation) representation $T_f : G_f \to S_n$. We label $G(T_f, 1)$ a subgroup (up to conjugation by G_f) defining the cosets. These are the elements of G_f that fix the integer 1 in the representation T_f. Similarly, any cover $f' : X' \to \mathbb{P}^1_z$ through which $\hat{f}$ factors corresponds to a coset representation (possibly not faithful) of G_f.

Whatever the branch points $\boldsymbol{z}$, for any cover $f : X \to \mathbb{P}^1_z$ of compact Riemann surfaces, these produce conjugacy classes $\mathbf{C} = \mathrm{C}_1, \dots, \mathrm{C}_r$ in the geometric monodromy $G_f \le S_n$. Denote $\mathbb{P}^1_z \setminus \{\boldsymbol{z}\}$ by $U_{\boldsymbol{z}}$. [Fr11, §5.3.2] explains using *classical generators* of the fundamental group of $U_{\boldsymbol{z}}$. These figure in why you can select respective representatives $\sigma_i \in \mathrm{C}_i$, $i = 1, \dots, r$, to have these properties:

(1.4a) *Generation*: $\langle \sigma_i \mid i = 1, \dots, r \rangle = G_f := G \le S_n$.
(1.4b) *Product-one*: $\sigma_1 \cdots \sigma_r = 1$.

For fixed $\mathbf{C}$, the set of $\boldsymbol{\sigma}$ satisfying (1.4) is the *Nielsen class*, $\mathrm{Ni}(G, \mathbf{C})$, of $(G, \mathbf{C})$. Equivalences on Nielsen classes correspond to equivalences between covers.

To get started we need only one: *absolute equivalence.* That means you mod out on Nielsen classes by the action of the subgroup of S_n, $N_{S_n}(G, \mathbf{C})$, that normalizes G and permutes (with multiplicity) the conjugacy classes in $\mathbf{C}$. The absolute equivalence class of $\boldsymbol{\sigma} \in \mathrm{Ni}(G, \mathbf{C})$ is

$$\{\alpha\boldsymbol{\sigma}\alpha^{-1} \mid \alpha \in N_{S_n}(G, \mathbf{C})\}.$$

Denote these equivalence classes, running over $\boldsymbol{\sigma} \in \mathrm{Ni}(G, \mathbf{C})$, by $\mathrm{Ni}(G, \mathbf{C})^{\mathrm{abs}}$.

The index, $\mathrm{ind}(\sigma)$, of a permutation $\sigma \in S_n$ is just n minus the number of disjoint cycles in the permutation. Example: an n-cycle in S_n has index $n-1$, and an involution has index equal to the number of disjoint 2-cycles in it. The *genus*, $\mathbf{g}_X$, of X given by f_X with branch cycles in a given Nielsen class is well defined. The Riemann–Hurwitz formula says

$$2(n + \mathbf{g}_X - 1) = \sum_{i=1}^{r} \mathrm{ind}(\sigma_i). \tag{1.5}$$

Two covers $f_i : X_i \to \mathbb{P}^1_z$ are in the same *absolute class* if there is a continuous (1-1) map $\psi : X_1 \to X_2$ so that $f_1 = f_2 \circ \psi$.

Further, the disjoint cycles of σ_i correspond to points of X lying over z_i. A disjoint cycle length is the ramification index of the point over z_i. An r-tuple, $\boldsymbol{\sigma}$, satisfying (1.4) is a *branch cycle description* of f. [Fr11, App. A] explains *classical generators* of the fundamental group of $U_{\boldsymbol{z}}$ and how from them you get the following.

PROPOSITION 1.1. *There is a* 1-1 *correspondence between elements of* $\mathrm{Ni}(G, \mathbf{C})^{\mathrm{abs}}$ *and absolute equivalence classes of covers* $f : X \to \mathbb{P}^1_z$ *in the Nielsen class, with any fixed set of* r *distinct branch points* $\boldsymbol{z}$.

We refer to Prop. 1.1 as R(iemann's)E(xistence)T(heorem) or RET. §2.1 uses special classical generators that work for our particular problem.

1.2. Reduced Galois equivalence. Denote the functions $x \mapsto ax + b$, $a \in \mathbb{C}^*$, $b \in \mathbb{C}$, by $\mathbb{A}(\mathbb{C})$. If $f, g \in \mathbb{C}[x]$, and $g(x) = \alpha \circ f \circ \beta(x)$ (resp. $f \circ \beta$), $\alpha, \beta \in \mathbb{A}(\mathbb{C})$, we say f and g are *reduced* (resp. *affine*) *equivalent.* Call $f \in \mathbb{C}[x]$ *cyclic* if f is reduced equivalent to $x^{\deg(f)}$. Consider the following for (f, g) reduced, but not affine equivalent:

(1.6a) f is not cyclic and $f, g : \mathbb{P}^1_x \to \mathbb{P}^1_z$ have the same Galois closures.

(1.6b) f is not a composition of some polynomial with a nontrivial cyclic polynomial and $f(x) - g(y)$ is newly reducible.

We say the polynomials f and g satisfying (1.6a) are reduced *Galois equivalent.* With slight modification, the name makes sense for any pair of covers $f : X_f \to \mathbb{P}^1_z$, $g : X_f \to \mathbb{P}^1_z$, if they have the same Galois closure covers. As in §1.1 let $G_f(T_f, 1)$ and $G_f(T_g, 1)$ be the subgroups of G_f corresponding to the covers f and g.

For a cover represented by a noncyclic polynomial, there is a unique branch cycle, σ_∞ (attached to $z=\infty$), that has exactly one disjoint cycle (of length n).

PROPOSITION 1.2. *If either of* (1.6) *holds, then translating f by a constant, we may assume $a=\zeta_v=e^{2\pi i/v}$, $v\neq 1$, and that $g=\zeta_v f$. Then a acts as a permutation u_a of the finite branch points of f.*

If (1.6a) *holds, then $z\mapsto az+b$ gives a cyclic cover $\mu:\mathbb{P}^1_z\to\mathbb{P}^1_u$ with group $\langle a^*\rangle=\mathbb{Z}/v$ where the following holds: The composite covers $\mu\circ\hat f$ and $\mu\circ\hat g$ are also the same and Galois. If $\sigma^*_\infty\in G_{\mu\circ\hat f}$ is a branch cycle over ∞ for $\mu\circ\hat f$, then we can take its natural image in $\langle a^*\rangle$ to be a^*, and $\sigma_\infty=(\sigma^*_\infty)^v$.*

Denote by $c_{\rm AZ}$ conjugation by σ^*_∞. It has trivial action on σ_∞ and no element of S_n represents $c_{\rm AZ}$. Up to conjugacy in G_f we can choose $c_{\rm AZ}$ to take $G_f(T_f,1)$ to $G_f(T_g,1)$. Identify $G_{\mu\circ\hat f}$ with the union of G_f cosets $\bigcup_{j=0}^{v-1}(\sigma^*_\infty)^jG_f$ (Rem. 1.4*).*

About the proof of Proposition 1.2. This is a special case of [Fr11, Prop. 7.28]. It stems from [Fr73, Prop. 2], which says—under the newly reducible assumption—that the Galois closures of f and g are the same. This general result has no dependence on the form of f and g, except that their fiber product is newly reducible. Since their Galois closures are the same, their branch points are also identical.

As σ_∞ is a power of σ^*_∞, $c_{\rm AZ}$ acts trivially on it. Since σ^*_∞ normalizes G_f, it might be in $N_{S_n}(G_f)$. Yet, as it centralizes σ_∞, it would have to be a power of σ_∞ (for the calculation see [Fr70, Step 1, proof of Lem. 9]), contrary to it having order $v\cdot n$.

The covers f and g correspond to representations of G on cosets of $G_f(T_f,1)$ and $G_f(T_g,1)$. They are conjugate in G_f if and only if f and g are absolutely equivalent covers: the same as f and g being affine equivalent. By assumption they are not. So no element of S_n represents $c_{\rm AZ}$. Choose the conjugates $G_f(T_f,1)$ and $G_f(T_g,1)$ so that σ^*_∞ conjugates one to the other. ■

PROBLEM 1.3. Characterize branch cycles $\boldsymbol{\sigma}$ (covers f_X) satisfying either of (1.6). For polynomials this includes $\mathbf{g}_X=0$, but it makes sense without restricting $\mathbf{g}_X$.

REMARK 1.4 ($c_{\rm AZ}$ leaves $\mathbf{C}$ invariant). The covers f and g in Prop. 1.2 have the same Galois closures. So, $c_{\rm AZ}$ must permute the conjugacy classes in $\mathbf{C}$—preserving multiplicity—just like the elements of $N_{S_n}(G,\mathbf{C})$.

Once we have identified the operator c_{AZ} as in §1.3 or §2, we can form $G_{\mu\circ\hat f}$ by taking a formal element σ^*, and forming the union of the left cosets of G_f. Multiplying coset elements comes from this formula for $\sigma', \sigma'' \in G_f$:

$$(\sigma^*_\infty)^{j'}\sigma'(\sigma^*_\infty)^{j''}\sigma'' = (\sigma^*_\infty)^{j'+j''}c_{AZ}^{-j''}(\sigma')\sigma''.$$

EXAMPLE 1.5. For $f \in \mathbb{C}[x]$ and $a = -1$ in Prop. 1.2, f and $-f$ define absolutely equivalent covers if and only if f is affine equivalent to an odd f^*: $f^*(-x) = -f^*(x)$. That happens for odd degree in the general case of §1.3. Define the nth Chebyshev polynomial, T_n, from $T_n(\cos(\theta))$ being the real part of $(e^{i\theta})^n = e^{ni\theta}$. For n odd, T_n is odd since $(-e^{i\theta})^n = -(e^{i\theta})^n$.

1.3. Dihedral example, D_n, n even. Consider the semidirect product

$$\mathbb{Z}/n \times^s A := \mathbb{A}_n(A) \quad \text{with } A \le (\mathbb{Z}/n)^*.$$

Regard it as the group of 2×2 matrices:

(1.7a) $\left\{\begin{pmatrix} a & b \\ 0 & 1\end{pmatrix} \mid a \in A,\ b \in \mathbb{Z}/n\right\}$. For $A = \{\pm1\}$, denote $\mathbb{A}_n(A)$ by D_n.

(1.7b) Each element of $\mathbb{A}_n(A)$ is a product $\begin{pmatrix} 1 & b \\ 0 & 1\end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & 1\end{pmatrix}$.

[Fr11, §7.2.1] (entitled "Writing equations") gives the modern—but discusses the historical—view of the subgroups of $\mathbb{A}_n(A)$ playing the role of $G_{\mu\circ\hat{f}}$ in Prop. 1.2. The set of involutions (order 2 elements) in $\mathbb{A}_n(A)$ has the form

$$I_n(A) = \left\{\begin{pmatrix} a & b \\ 0 & 1\end{pmatrix} \mid a^2 = 1\ (a \ne 1) \text{ and } b(a+1) = 0\right\}.$$

LEMMA 1.6. *Assume $2\,|\,n \ge 4$. Then the distinct conjugacy classes, $\mathrm{C}_{-1,0}$ and $\mathrm{C}_{-1,1}$, with representations $\sigma_1 = \begin{pmatrix} -1 & 1 \\ 0 & 1\end{pmatrix}$ and $\sigma_2 = \begin{pmatrix} -1 & 0 \\ 0 & 1\end{pmatrix}$, comprise $I_n(\{\pm1\})$. An automorphism $c_n(\{\pm1\})$ of D_n is given by*

$$\begin{pmatrix} 1 & b \\ 0 & 1\end{pmatrix} \mapsto \begin{pmatrix} 1 & b \\ 0 & 1\end{pmatrix} \quad \textit{and} \quad \begin{pmatrix} -1 & b \\ 0 & 1\end{pmatrix} \mapsto \begin{pmatrix} -1 & b-1 \\ 0 & 1\end{pmatrix}, \quad b \in \mathbb{Z}/n.$$

The lemma follows easily by computation, with $c_n(\{\pm1\})^2$ the same as conjugation by $\sigma_\infty = \begin{pmatrix} -1 & -1 \\ 0 & 1\end{pmatrix}$. Now with $v = 2$, $\zeta_v = -1$, we describe D_n^* so that it fits the conclusion of Prop. 1.2 as $G_{\mu\circ f}$. Use σ_i, $i = 1, 2$, from Lem. 1.6. As generators, D_n^* has σ_1 and σ^*_∞, the latter satisfying these conditions:

$$(1.8)\qquad \begin{aligned} &(\sigma^*_\infty)^2 = \sigma_\infty \quad (\sigma^*_\infty \text{ has order } 2n),\\ &(\sigma^*_\infty)^k\begin{pmatrix} -1 & 0 \\ 0 & 1\end{pmatrix}(\sigma^*_\infty)^{-k} = \begin{pmatrix} -1 & -k \\ 0 & 1\end{pmatrix}. \end{aligned}$$

Denote the representation from permutations in (1.9) by T_f. It comes from acting on (left) cosets of $\langle\sigma_2\rangle$. Another representation, T_g, comes from cosets of $\langle\sigma_1\rangle$.

The corresponding cover—given by a degree n Chebyshev polynomial—appears in Prop. 1.2 with $r = 3$ and $A = \{\pm1\}$. Assume that $2\,|\,n \ge 4$. With the elements acting as permutations—from the left—on the integers $\{0, 1, \ldots, n-1\}$ modulo n, we have

$$(1.9)\qquad \begin{aligned} \sigma_1 &= (1\ n)(2\ n-1)\cdots(n/2\ n/2+1),\\ \sigma_2 &= (1\ n-1)(2\ n-2)\cdots(n/2-1\ n/2+1),\\ \sigma_\infty := \sigma_3 &= (1\ 2\ \ldots\ n-1\ n)^{-1} = \begin{pmatrix} 1 & -1 \\ 0 & 1\end{pmatrix}. \end{aligned}$$

We now apply RET (Prop. 1.1) to (1.9) to produce a polynomial pair (f, g) with these properties for any even $n \geq 4$:

(1.10a) all irreducible factors of $f(x) - g(y)$ have degree 2; but in this case
(1.10b) (1.1) is newly reducible only for $n = 4$.

For finite branch points take any pair $(z', -z')$. For simplicity we will set $z' = 1$. As in §1.1, f (resp. g) corresponds to the permutation representation T_f (resp. T_g).

The respective indices of the σ_i s in (1.9) are $n/2$, $n/2-1$, and $n-1$. Plug these into (1.5) and conclude that the genus of the cover—call it f—is 0. Similarly for a cover g from T_g. Now use this characterization: $f : X \to \mathbb{P}^1_z$ is absolutely equivalent to a polynomial cover if X has genus 0, and precisely one point lies over $z = \infty$.

RET and the Galois correspondence give the following:

(1.11a) The irreducible factors of $f(x) - g(y)$ correspond 1-1 to the orbits of $G(T_g, 1)$ in T_f (on the cosets of $D_n(T_f, 1)$), all length 2.
(1.11b) The representation $T_{\mu \circ f}$ corresponding to $\mu \circ f : X \to \mathbb{P}^1_u$, having monodromy D_n^*, is on the $2n$ cosets of $D_n^*(T_f, 1)$.
(1.11c) Composing c_{AZ} (as in §2.4) in Prop. 1.2 with $T_{\mu \circ f}$ is equivalent to $T_{\mu \circ g}$.

Finally, D_n maps to $D_{n/2}$, with a compatible representation on the cosets of $\langle \sigma_1 \rangle$. Then f is a composite of degree 2 and $n/2$ polynomials. When $n/2 = n'$ is odd, use Ex. 1.5 to see that the replacement for (1.11) (as in [Fr11, Lem. 7.4]) has a factor of degree 1, and the rest of degree 2. So, unless $\deg(f) = 4$, f is not newly reducible.

We use the principle "dragging a cover by its branch points" ([Fr11, §6.1]) to produce a new cover from $f : X \to \mathbb{P}^1_z$ with the same branch cycles, but finite branch points placed at any distinct points in $\mathbb{C}$. We require ζ_v to permute the finite branch points. Example: for the orbit condition (2.2), we may assume f has finite branch points ζ_v^j, $j = 1, \ldots, v$. Then $\mu \circ f$ has branch points 0, 1 and ∞.

Problem 1.7. As in (1.11c), compute branch cycles, $\sigma_0^*, \sigma_1^*, \sigma_\infty^*$ for $\mu \circ f$.

Hints for Problem 1.7. Take the branch cycle for ∞ as σ_∞^* using (3.5). The shape of the branch cycle for σ_1^* is a product of $(n + n - 2)/2 = n - 1$ disjoint 2-cycles, from juxtaposing contributions of σ_1 and σ_2; and σ_0^* is a product of n disjoint v-cycles.

The Nielsen class $\mathrm{Ni}(D_n, \mathbf{C})^{\mathrm{abs}}$ with the three conjugacy classes represented in (1.9) has six elements, indicated by the order of those conjugacy classes in a representing 3-tuple. This is common when $r = 3$, but for $r \geq 4$, the braid group enters, as used in [Fr11, §6.4] to dramatic effect. So, here inspection can produce the desired $\sigma_0^*, \sigma_1^*, \sigma_\infty^*$ satisfying generation and product-one in (1.4).

For, however, a general polynomial f with only the knowledge that u_a in Prop. 1.2 permutes the branch points, solving this problem requires *classical generators* (as in §2) for the covers f and $\mu \circ f$, and then a relation between these as in §3.1. ∎

1.4. The conjecture of [Gu10]. Our tentative conjecture is that §1.3 (with $n = 4$) gives the only case of Schinzel pairs of the form $(f, \zeta_v f)$. As the argument of [Fr70, p. 47] shows, this is true if and only if σ_∞ generates a normal subgroup in G.

Precisely: The conjugation $\sigma_i \sigma_\infty \sigma_i^{-1} = \sigma_\infty^k$ by a finite branch cycle implies σ_i has the same index as multiplication by $k \in (\mathbb{Z}/n)^*$ on $\mathbb{Z}/n$. Possibilities for a genus 0 cover (using (1.5)) show that f is equivalent to a Chebyshev (or cyclic) polynomial, with well understood branch cycles. Then, the Nielsen class—according to §1.3—must be $\mathrm{Ni}(D_4, \mathbf{C})^{\mathrm{abs}}$ with $\mathbf{C} = \mathrm{C}_{-1,0} \cup \mathrm{C}_{-1,1} \cup \mathrm{C}_\infty$, as in Lem. 1.6.

2. The group formulation of conditions (1.6). A conclusion from Prop. 1.2 is that (as in the last hint to Prob. 1.7)

$$\boldsymbol{z}_f = \zeta_v \boldsymbol{z}_f = \boldsymbol{z}_g. \tag{2.1}$$

Consider any polynomial f satisfying (2.1), and one further condition:

(2.2) u_a has one orbit on finite branch points: $r - 1 = v$.

That is, $\boldsymbol{z}_f$ are the vertices of a regular v-gon on a circle around the origin.

§2.1 sets up the procedure for computing branch cycles for $\zeta_v f$ from those of f. §2.2 then characterizes possible branch cycles when you add (1.6a), the Galois closure assumption for the pair $(f, \zeta_v f)$. §2.3 notes that we can adjust the method to handle Prop. 1.2 without condition (2.2).

2.1. The effect of u_a on branch cycles when (2.1) holds. Let $\mathbb{A}^0_{r-1}$ consist of all distinct $r-1$-tuples in $\mathbb{C}$. Assume (2.2). Then, given branch cycles for f relative to classical generators of $\pi_1(U_{\boldsymbol{z}_f}, z_0)$, it makes sense to compute branch cycles for $\zeta_v f$ relative to the same classical generators.

Since we have assumed that $z = 0$ is not a branch point, we can use it as a basepoint, and the paths of the Appendix where $r - 1 = 6$—listed as $\bar\sigma_1, \dots, \bar\sigma_{r-1}, \bar\sigma_\infty$. We can compose a cover $f : X \to \mathbb{P}^1_z$ with any $\alpha \in \mathrm{PGL}_2(\mathbb{C})$. We make an increasing sequence of assumptions, starting with:

(2.3) Suppose $\alpha(\boldsymbol{z}_f) = \boldsymbol{z}_f$, that is, α permutes the branch points.

We only do the next lemma for the case we use in the rest of the paper, and with the classical generators $\bar\sigma_1, \dots, \bar\sigma_r = \bar{\boldsymbol{\sigma}}$ of the Appendix.

LEMMA 2.1. *We can explicitly compute the effect of α on an explicit set of classical generators to find branch cycles for $\alpha \circ f$ from branch cycles for f. Assume α is multiplication by ζ_v under assumption* (2.2) *and $\boldsymbol{\sigma}$ are branch cycles for f relative to $\bar{\boldsymbol{\sigma}}$ above. Then, relative to $\bar{\boldsymbol{\sigma}}$, branch cycles for $\zeta_v f$ are*

$$(\sigma_2, \dots, \sigma_{r-1}, \sigma_1, \sigma_1^{-1}\sigma_r\sigma_1). \tag{2.4}$$

Proof. Rotation through an angle of $2\pi/v$ sends $\bar{\sigma}_i$ to $\bar{\sigma}'_i = \bar{\sigma}_{i+1}$, $i = 1, \dots, r-2$, and $\bar{\sigma}_{r-1}$ to $\bar{\sigma}'_{r-1} = \bar{\sigma}_1$. Similarly, $\bar{\sigma}_r$ (on the meridian halfway between $\bar{\sigma}_r$ and $\bar{\sigma}_1$) rotates to the meridian halfway between $\bar{\sigma}_1$ and $\bar{\sigma}_2$.

Here is the deal! The branch cycles for $\alpha \circ f$ relative to $\bar{\boldsymbol{\sigma}}'$ are $\boldsymbol{\sigma}$, the same as those for f computed relative to the $\bar{\sigma}_1, \dots, \bar{\sigma}_r$. Write $\bar{\sigma}_1, \dots, \bar{\sigma}_r$—up to isotopy—as words in $\bar{\sigma}'_1, \dots, \bar{\sigma}'_r$. Then, plug $\boldsymbol{\sigma}$ in to get the branch cycles for $\alpha \circ f$. To do that we only need to express σ_r by the following formula. Up to isotopy

$$\bar{\sigma}_1\bar{\sigma}'_r = \bar{\sigma}_r\bar{\sigma}_1. \tag{2.5}$$

Explanation: The left side deforms on $U_{\boldsymbol{z}_f}$—without moving z_0, or touching any points of the paths outside of $\bar{\sigma}_r, \bar{\sigma}_1, \bar{\sigma}'_r$—to a "circle" based at z_0 around z_1 and ∞. This is homotopic to a deformation of the right side of (2.5) that does the same. ∎

2.2. Adding the Galois closure condition. Suppose we have $(G, \mathbf{C})$, with two (faithful) permutation representations $T_i : G \to S_{n_i}$, $i = 1, 2$. (Our example will have $n_1 = n_2 = n$.) Then, we have two absolute Nielsen classes: $\mathrm{Ni}(G, \mathbf{C})^{\mathrm{abs},i}$, $i = 1, 2$. Assume, too, we have representative classes ${}_i\boldsymbol{\sigma} \in \mathrm{Ni}(G, \mathbf{C})^{\mathrm{abs},i}$, and, as in Prop. 1.1, these define covers $f_i : X_i \to \mathbb{P}^1_z$, $i = 1, 2$, with branch points $\boldsymbol{z}$, relative to specific classical generators.

We must add *inner equivalence* to *absolute equivalence* on Nielsen classes (§1.1), $\mathrm{Ni}(G, \mathbf{C})^{\mathrm{in}} := \mathrm{Ni}(G, \mathbf{C})/G$, to formulate the criterion that the f_i s have the same Galois closure covers. That is, mod out by just G acting inside $N_{S_n}(G, \mathbf{C})$.

[Fr11, §B.2.1] uses examples to show how absolute and inner classes relate—starting from the canonical maps $\psi_{\mathrm{in,abs}} : \mathrm{Ni}(G, \mathbf{C})^{\mathrm{in}} \to \mathrm{Ni}(G, \mathbf{C})^{\mathrm{abs}}$ —to the main ingredient of [FV91, Main Thm.]. The following is a natural addendum.

PROPOSITION 2.2. *The covers f_1 and f_2 have the same Galois closures if there exists $\boldsymbol{\sigma} \in \mathrm{Ni}(G, \mathbf{C})^{\mathrm{in}}$ for which $\psi_{\mathrm{in,abs},i}(\boldsymbol{\sigma}) = {}_i\boldsymbol{\sigma}$, $i = 1, 2$. The following characterizes there being a polynomial f in $\mathrm{Ni}(G, \mathbf{C})^{\mathrm{abs}}$ with $g = \zeta_v f$ satisfying* (1.6a) (*Galois closure condition*)*, with branch points $\boldsymbol{z}$ satisfying the one-orbit condition* (2.2)*:*

(2.6a) *G has an automorphism, conjugation by σ^*_∞, as in Prop.* 1.2*, with*

(2.6b) $\boldsymbol{\sigma} \in \mathrm{Ni}(G, \mathbf{C})^{\mathrm{abs}}$ *of genus* 0 (*à la* (1.5)), $r-1=v$, *and* (2.4) *holds. There is an analog for more general orbits of* ζ_v. *See* §2.3.

We note two points about the §1.3 example. First: We checked separately that we got reduciblity (for all n). Then, that it gave newly reducible, so a Schinzel pair (as in (1.6b)) just in the case $n = 4$. Still, both came directly from branch cycles. It is easy to generalize those conditions to apply to Prop. 2.2.

Second: In §1.3 conjugation by σ_∞^* permutes two distinct conjugacy classes. §2.4 shows we must have something like that to get Schinzel pairs.

2.3. Characterizing the f in Prop. 1.2 in general. Although more intricate, we can generalize (2.4) to any number of orbits for multiplication by ζ_v on branch points. It is possible that with more than one orbit, we might have the origin as a branch point. We hope to complete the one orbit case of this paper in a later publication. There we will treat the generalization of (2.4).

2.4. Equivalent representations. We continue the 2nd observation at the end of §2.2. Assume in Prop. 1.2 that $\sigma_\infty^* = \sigma^*$ satisfies the following condition:

(2.7) Conjugation, c_{σ^*}, by σ^* preserves all conjugacy classes.

Indeed, we aim at generality for future use. Assume a finite group G has an outer automorphism γ (in place of c_{σ^*}) *preserving classes*—the conclusion of (2.7).

Then, Prop. 2.4 shows f could not possibly give new Schinzel pairs. Applied to the conditions of Prop. 2.2 it does produce a variables separated factorization $f(x)-g(y)$, but this is not newly reducible: (1.3a) holds. It still may contribute to Davenport's problem (1.2) where, if the range values are assumed with the same multiplicities, the representations T_f and T_g satisfy the conclusion of Lem. 2.3.

Applying any automorphism γ to any permutation representation $T : G \to S_n$ sends it to another representation:

$$T_\gamma : \sigma \mapsto T \circ \gamma(\sigma), \quad \sigma \in G.$$

Denote the stabilizer of an integer in T by $G(T, 1)$ and the number of fixed integers of $T(\sigma)$ by $\mathrm{tr}(T(\sigma))$, its *trace*.

LEMMA 2.3. *Consider a representation* $T : G \to S_n$. *Assume* γ *preserves classes. Then* $\mathrm{tr}(T(\sigma)) = \mathrm{tr}(T_\gamma(\sigma))$ *for all* $\sigma \in G$.

Proof. We are comparing the cosets of $G(T, 1)$ fixed by σ (multiplying on the left) with the cosets fixed by $\gamma(\sigma)$. Since conjugation by γ preserves the conjugacy class of σ, we see that $\gamma(\sigma) = \sigma'\sigma(\sigma')^{-1}$ for some $\sigma' \in G$.

The fixed cosets of $\sigma'\sigma(\sigma')^{-1}$ are the same as the fixed cosets of σ on the conjugates of those cosets by σ'. But, if $T(\sigma')(1) = k$, then σ' conjugates those cosets to the cosets of $G(T,k)$. Now, σ fixes exactly the same number of $G(T,1)$ cosets as it fixes of $G(T,k)$ cosets. We are done. ∎

Suppose we start with a fixed faithful transitive permutation representation T_f, coming from a cover of nonsingular curves $f : X_f \to Y$ (over $\mathbb{C}$). Apply the Galois correspondence. It gives a 1-1 correspondence between (nonsingular) covers $f' : X' \to Y$ through which f factors, up to absolute equivalence, and groups $G(T,1) \le G' \le G$. Each G' corresponds to a system of imprimitivity of the permutation representation. This generalizes the notion of composition factors of a polynomial (or rational function).

Proposition 2.4. *Assume γ and T as above, with $g : X_g \to Y$ corresponding to T_γ. Then the* (*normalization of the*) *fiber product $X_f \times_Y X_g$ is reducible. This applies to the permutation representation T' attached to any G' with $G(T,1) < G' < G$. In particular, if T is not primitive, then $X_f \times_Y X_g$ is not newly reducible.*

So, if (f,g) is a polynomial pair from Prop. 1.2, *with $G = G_f$, $\gamma = c_{\sigma^*_\infty}$, then $f(x) - g(y)$ is reducible* (*as in* (1.1)), *but not newly reducible.*

Proof. [Fr11, §2.3] discusses Galois theory and fiber products. Including that we naturally form the Galois closure of a degree n cover from a component of the fiber product of the cover with itself, taken n times. Thus, the two topics go together: use of normalization (which for curves means the results are nonsingular), and how this generalizes the case of two polynomials (f,g) as in the last statement.

This paper's case (over the complexes) is easier than in [Fr11], over any characteristic zero field. The point is to have Galois theory turn statements relating two covers into statements comparing two permutation representations. For example, consider this statement: $X_f \times_Y X_g$ is reducible, which [Fr11, §2.1] shows generalizes saying (1.1). The translation is that

(2.8) $\quad G_f(T_g,1)$ has more than one orbit in the representation T_f.

This exactly generalizes (1.11a) in §1.3, except we computed directly that all orbits there had length 2 (for $n > 2$). Here, a short argument from group theory applies: [Fr73, Lem. 3] and assiduously redone in [Fr11, Rem. 4.3], titled "Davenport without f indecomposable." It says (2.8) follows from the weaker condition

(2.9) $\quad \mathrm{tr}(T_f(\sigma)) > 0$ if and only if $\mathrm{tr}(T_g(\sigma)) > 0$ for all $\sigma \in G$.

Similarly, consider how we figured that only for $n = 4$ would the §1.3 example be newly reducible. In our general case we assumed T is not primitive. So, there is a representation T' on the cosets of a group properly between

$G(T,1)$ and G. According to Lem. 2.3, this produces the two representations T' and T'_γ to which we can apply the reducibility result above. We only need, in the last sentence, where (f,g) are polynomials, the fact that f decomposes under the hypotheses of Prop. 1.2. This is in the paragraphs above [Fr11, Rem. 7.7, at the end of §7.2.3] (called "Ritt I") where we revamped how [AZ03] treated the indecomposable case. ■

3. Searching for $(G, \mathbf{C})$ that give Schinzel pairs. These short comments suggest tools for dealing with what remains unsolved here, or with related problems. §3.1 and §3.2 are additions to the wreath product comments of [Fr11, §7.2.4]. §3.2 focuses on our main case: $G_\mu = \mathbb{Z}/v$.

3.1. Comments on [Ba02]. Suppose we have any sequence of covers

$$X \xrightarrow{f} \mathbb{P}^1_x \xrightarrow{\mu} \mathbb{P}^1_u.$$

[BF86] and [Tr93] provide results for more general problems where the target of f is not necessarily genus 0. Simplifying, however, for our special case is the work of [Ba02, Chap. V], called "Nielsen graphs."

(3.1) From branch cycles for $\mu \circ f$ (relative to its base's classical generators), we can compute branch cycles for f.

In the other direction, branch cycles for f and μ give information on branch cycles for $\mu \circ f$. We naturally identify the monodromy group $G_{\mu\circ f}$ with a subgroup of the *wreath product* $G_f \wr G_\mu$ of G_f and G_μ, a completely general statement.

For general μ of degree v, $G_f \wr G_\mu$ is naturally the semidirect product $(G_f)^v \times^s G_\mu$. Suppose $G_\mu \le S_v$. Denote the ith copy of G_f in $(G_f)^v$ by $G_{f,i}$, $i = 1, \dots, v$. Then, here is the action of $\gamma \in G_\mu$:

$$(\sigma_1, \dots, \sigma_v) \in (G_f)^v \mapsto (\sigma_{(1)\gamma}, \dots, \sigma_{(v)\gamma}).$$

It permutes the coordinates of $(G_f)^v$ according to the permutation effect of γ.

Suppose f and μ are both polynomial covers. By [Fr70, Lem. 15], $G_{\mu\circ f}$ will be the full wreath product under the following conditions:

(3.2) The images of the finite branch points of f under μ are all distinct and also distinct from the (finite) branch points of μ.

If the conditions of [Fr70, Lem. 15] do not hold, then $G_{\mu\circ f}$ may be a *proper* subgroup of $G_f \wr G_\mu$, but still satisfying these conditions:

(3.3) $G_{\mu\circ f}$ maps surjectively onto G_μ, and its intersection with $(G_f)^v$ projects surjectively onto each $G_{f,i}$, $i = 1, \dots, v$.

3.2. The case $G_\mu = \mathbb{Z}/v$. To simplify notation we use a superscript $*$-notation for elements in $G_{\mu\circ f} := G^*$. Our basic assumptions will be:

(3.4a) $\mu(z) = z^v$ is a cyclic cover of degree $v > 1$.
(3.4b) f is in a genus 0 Nielsen class, totally ramified over $z = \infty$.
(3.4c) the finite branch points of f fall into s orbits of (exact) length v under multiplication by $e^{2\pi i/v}$.

From (3.4c), **C** has $r - 1 = s \cdot v$ conjugacy classes in it corresponding to finite branch points. From (3.4a), the branch points in each $e^{2\pi i/v}$ orbit go to the same value of u under μ. Finally, from (3.4b), $\mu \circ f$ totally ramifies over ∞, corresponding to a branch cycle σ^*_∞ that has order $n \cdot v = n^*$.

A description of branch cycles for the cover $\mu \circ f$ includes a branch cycle at ∞, given by an $n \cdot v$-cycle σ^*. We now set up notation for σ^*. Identify v copies of $\{1, \dots, n\}$ as $\{1_i, \dots, n_i\}$, the integers on which $G_{f,i}$ acts, $i = 1, \dots, v$. With no loss of generality, up to renaming the letters—using the fact that $(\sigma^*_\infty)^v = \sigma_\infty$—we can take σ^*_∞ as

(3.5) $$(1_1\ 1_2\ \dots\ 1_d\ 2_1\ \dots\ 2_d\ \dots\ n-1_1\ \dots\ n-1_d\ n_1\ \dots\ n_d).$$

Then σ_∞ generates the intersection of $\langle\sigma^*_\infty\rangle$ with $(G_f)^v$.

In our situation, as in Prop. 1.2, the actual $G_{\mu\circ\hat{f}} := G_{f^*}$ is the smallest subgroup of the full wreath product, $G_f \wr \mathbb{Z}/v = (G_f)^v \times^s \mathbb{Z}/v$, satisfying the wreath conditions (3.3).

3.3. New nonpolynomial Schinzel pairs. Prop. 2.4 produces general fiber products of covers that may not have genus 0. With its extra hypothesis, however, these are not newly reducible. To expand our understanding of Schinzel pairs we might drop the condition they come from polynomials or even that they come from genus 0 covers. Yet, they produce new fiber products, from a pair of covers $f : X \to \mathbb{P}^1_z$ and $g = \zeta_v f$, for which $f(x) - g(y)$ is newly reducible.

Ex. 3.1 uses genus 0 covers, given by rational functions, rather than polynomials. Again $v = 2$, but $\zeta_2 = -1$ has two orbits on four finite branch points.

Example 3.1. Here $r = 4$. Use the "dragging a cover by its branch points" principle of §1.3 to place the branch points at $-1, -2, +2, +1$ to correspond to branch cycles $(\sigma_1, \sigma_2, \sigma_2, \sigma_1)$ as given in (1.9). The Nielsen class here contains the two conjugacy classes labeled $\mathrm{C}_{-1,0}, \mathrm{C}_{-1,1}$, both twice, but it does not include an n-cycle. The group is still D_n; the Galois closure has genus 1 (not 0 as in §1.3).

Many—as a function of n—covers in the Nielsen class correspond to different branch cycles. Yet, only two give a $g = -f$ with the same Galois closure. To be precise we must give classical generators replacing those of the Appendix. They are almost the same "lolly-pop" paths from the origin through -1, -2, $+2$, $+1$ except that you cannot allow the lolly-pop that passes around -2 to go through -1. Instead, take a little blip to the right around -1 before continuing onto the rest of the lolly-pop. Similarly for the lolly-pop through $+2$, a little blip to the left around $+1$.

Now we suggest how to get new groups, but with covers of genus > 0.

PROBLEM 3.2. Extend the automorphism c_n of Lem. 1.6 to other subgroups of $\mathbb{A}(n)$ to produce new, newly reducible fiber products analogous to the case of $n = 4$ of §1.3.

Appendix. Regular polygon classical generators. The paths $\delta_i \sigma_i^* \delta_i^{-1}$ (including that with subscript $r = \infty$, going around ∞) in Fig. 1 satisfy all the conditions of *classical generators* based at $z_0 = 0$. Our notation is compatible with that of [Fr11, App. B.1], except we here use very regular paths, with punctures (except at ∞) arranged on a regular 6-gon.

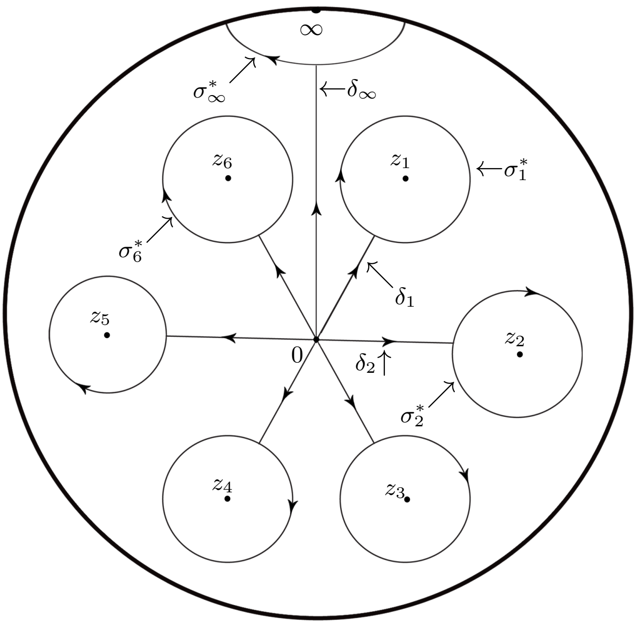

Fig. 1. $r = 7$, with 6 branch points on a regular polygon

References

[AS85] M. Aschbacher and L. Scott, *Maximal subgroups of finite groups*, J. Algebra 92 (1985), 44–80.

[AZ03] R. M. Avanzi and U. M. Zannier, *The equation $f(X) = f(Y)$ in rational functions $X = X(t)$, $Y = Y(t)$*, Compos. Math. 139 (2003), 263–295.
[Ba02] P. L. Bailey, *Incremental ascent of a modular tower via branch cycle designs*, PhD thesis, Univ. of California at Irvine, http://math.uci.edu/~mfried/paplist-mt/pBaileyThesis2002.pdf.
[BF86] R. Biggers and M. D. Fried, *Irreducibility of moduli spaces of cyclic unramified covers of genus g curves*, Trans. Amer. Math. Soc. 295 (1986), 59–70.
[Fr70] M. D. Fried, *On a conjecture of Schur*, Michigan Math. J. 17 (1970), 41–55.
[Fr71] —, *On the Diophantine equation $f(x) - y = 0$*, Acta Arith. 19 (1971), 79–87.
[Fr73] —, *The field of definition of function fields and a problem in the reducibility of polynomials in two variables*, Illinois J. Math. 17 (1973), 128–146.
[Fr87] —, *Irreducibility results for separated variables equations*, J. Pure Appl. Algebra 48 (1987), 9–22.
[Fr11] —, *Variables separated equations: Strikingly different roles for the branch cycle lemma and the finite simple group classification*, Sci. China Math. 55 (2012), 1–72.
[FV91] M. D. Fried and H. Völklein, *The inverse Galois problem and rational points on moduli spaces*, Math. Ann. 290 (1991), 771–800.
[Gu10] I. Gusić, *Reducibility of $f(x) - cf(y)$*, preprint, 2010.
[Sc71] A. Schinzel, *Reducibility of polynomials*, in: Actes du Congrès International des Mathématiciens (Nice, 1970), Tome 1, Gauthier-Villars, Paris, 1971, 491–496.
[Tr93] R. J. Trudeau, *Introduction to Graph Theory*, Dover, New York, 1993.

Michael D. Fried
Emeritus, UC Irvine
3547 Prestwick Rd.
Billings, MT 59101, U.S.A.
E-mail: mfried@math.uci.edu

Ivica Gusić
FKIT
University of Zagreb
Marulicev trg 19
Zagreb, Croatia
E-mail: igusic@fkit.hr

Received on 11.4.2011
and in revised form on 11.8.2011 (6668)