MARKOFF TRIPLES AND NIELSEN EQUIVALENCE IN $\mathbf{SL}_2(\mathbb{F}_p)$

DANIEL E. MARTIN

Abstract. In 2013, Darryl McCullough and Marcus Wanderley made a series of conjectures that describe the Nielsen equivalence classes and T_2-equivalence classes of pairs of generators for $\mathrm{SL}_2(\mathbb{F}_q)$ and the Markoff equivalence classes of triples in $\mathbb{F}_q^3$ that solve $x^2+y^2+z^2=xyz+\kappa$ for some $\kappa\in\mathbb{F}_q$. (The case $\kappa=0$ was originally conjectured by Baragar in 1991.) We prove that one of the McCullough–Wanderley conjectures, the "Q-Classification Conjecture" on Markoff triples, implies the others. Then we prove that the Q-Classification Conjecture holds if $q=p$ is a prime such that 24,504,480 does not divide p^2-1. More generally, for any integer d, we reduce the Q-Classification Conjecture for all primes $p\not\equiv\pm1 \bmod d$ to checking whether a roughly $2d\times 2d$ matrix with entries in $\mathbb{Q}[\kappa]$ is invertible. We (and SageMath) perform this invertibility check for all prime powers d up to 17, hence the modulus $24{,}504{,}480 = 2\,\mathrm{lcm}(1,2,\ldots,17)$.

1. Introduction

1.1. Statement of Results.

The primary result of this paper is the following:

Theorem 1.1. *Let p be prime such that $24{,}504{,}480 \nmid p^2-1$. For any $\kappa\in\mathbb{F}_p\backslash\{4\}$, there is a single orbit of solutions in $\mathbb{F}_p^3$ to $x^2+y^2+z^2=xyz+\kappa$ under the group generated by*

$$(x,y,z)\mapsto(yz-x,y,z),\ (x,y,z)\mapsto(x,xz-y,z) \text{ and } (x,y,z)\mapsto(x,y,xy-z),$$

other than the following exceptional orbits up to coordinate permutation, provided the elements exist in $\mathbb{F}_p$:

(1) the orbit of $(\sqrt{\kappa},0,0)$,
(2) the orbit of $(1,1,1)$ when $\kappa=2$,
(3) the orbit of $(1,0,\frac{1}{2}(1\pm\sqrt{5}))$ when $\kappa=\frac{1}{2}(5\pm\sqrt{5})$,
(4) or the orbits of $(1,0,\sqrt{2})$ and $(\frac{1}{2}(1+\sqrt{5}),1,1)$ when $\kappa=3$.

The modulus $24{,}504{,}480 = 2\,\mathrm{lcm}(1,2,\ldots,17)$ can be increased with further computation. For any positive integer d, we reduce the theorem above for all primes $p\not\equiv\pm1 \bmod d$ to an explicit matrix rank calculation. Performing this calculation for all prime powers d up to 17 proves the theorem above. This resolves the"Q-Classification Conjecture" of McCullough and Wanderley [MW13] for all primes that avoid the forbidden set of 2^7 congruence classes modulo $5\cdot7\cdot9\cdot11\cdot13\cdot16\cdot17$. (Sage code to verify the conjecture for a prime power input d can be found on the author's website: dem6.people.clemson.edu.)

Date: November 24, 2025.
2010 *Mathematics Subject Classification.* Primary: 11D25, 20H30, 37C85. Secondary: 05C25.
Key words and phrases. Markoff triples, Markoff graph, Nielsen equivalence, T-systems, linear groups over finite fields, product replacement graph.
This research is supported by NSF grant 2336000.

Bourgain, Gamburd, and Sarnak have obtained an asymptotic version of Theorem 1.1. In [BGS25] they prove that for any $\varepsilon > 0$, if x is sufficiently large then the density of primes $p < x$ for which Theorem 1.1 fails when $\kappa = 0$ is at most x^{ε}. As noted in [BGS16b] and [BGS25], and as detailed in a forthcoming paper [BGS26], their argument generalizes to arbitrary κ. Similar questions have also been addressed for variants and generalizations of the Markoff surface in [Bar96; Bar98] and [Fuc+24].

Setting $\kappa = 0$ yields the classical Markoff equation $x^2+y^2+z^2 = xyz$ (sometimes with $3xyz$ in place of xyz). In this case, the transitivity asserted by Theorem 1.1 was first conjectured to hold for all primes by Baragar in 1991 [Bar91]. Baragar's conjecture was resolved for all but finitely many primes (specifically $p > 10^{393}$ [Edd+25]) by a theorem of Chen [Che24], building on the work of Bourgain, Gamburd, and Sarnak [BGS16a; BGS16b; BGS25]. An alternative proof of Chen's theorem has been provided by the author in [Mar25], and it has been generalized to other Markoff-type equations by de Courcy-Ireland, Litman, and Mizuno in [CLM25].

Investigation into the classical Markoff equation ($\kappa = 0$) was historically motivated by Diophantine approximation. More precisely, the entries in solutions from $\mathbb{Z}^3$, called *Markoff numbers*, control the Markoff and Lagrange spectra [Mar79]. This phenomenon does not occur for nonzero κ—the more general Markoff equation has surprising connections to other disciplines. Over $\mathbb{C}$, the group action in Theorem 1.1 mirrors that of the monodromy group of Painlevé VI equations on $\mathbb{C}^2$ [Boa05] [PCI24]. And over $\mathbb{F}_p$ (and its extensions), the same group action mirrors that of Nielsen moves on $\mathrm{SL}_2(\mathbb{F}_p)$ generating pairs. Indeed, the small orbits indicated in (1–4) have been computed from both the Painlevé VI [DM00] [LT14] and $\mathrm{SL}_2(\mathbb{F}_p)$ [McC05] [MW13] perspectives without reference to one another.

Our motivation for considering arbitrary κ is to determine Nielsen classes of $\mathrm{SL}_2(\mathbb{F}_p)$, the subject of the McCullough–Wanderley conjectures. The secondary result of this paper is the following, proved as a consequence of Theorem 1.1.

Theorem 1.2. *Let p be prime with $12{,}252{,}240 \nmid p^2-1$. For any $\kappa \in \mathbb{F}_p \backslash \{4\}$, there is a single orbit of generating pairs (A, B) for $\mathrm{SL}_2(\mathbb{F}_p)$ with $\operatorname{tr} ABA^{-1}B^{-1} = \kappa - 2$ under the group generated by*

$$(A, B) \mapsto (A, AB),\ (A, B) \mapsto (B, A) \text{ and } (A, B) \mapsto (A^{-1}, B),$$

except when $\kappa = 0$ and $p \equiv 1 \bmod 4$, in which case there are two orbits.

This resolves the "Classification Conjecture," the "Trace Conjecture," and the "T-Classification Conjecture" of McCullough and Wanderley [MW13] for the same set of congruence classes as Theorem 1.1.

Our two theorems split the paper into two components. The remainder of the introduction exposits the relation between Theorems 1.1 and Theorem 1.2. Then in Section 2 we prove that the former implies the latter. In fact, Theorem 1.5 proves more generally that the McCullough–Wanderley conjectures are equivalent over $\mathbb{F}_q$ for any prime power q. The perspective is centered around Nielsen classes through the proof of Theorem 1.5 in Section 2. Then the perspective shifts to Markoff triples and does not return. Section 3 outlines the proof strategy for Theorem 1.1, and Sections 4–8 carry out the strategy.

1.2. **Background.** For an integer $n \geq 2$ and a group G, two n-tuples in G are called *Nielsen equivalent* if one can be obtained from the other via a sequence of

elementary Nielsen moves:

$$(g_1, ..., g_i, ..., g_n) \mapsto (g_1, ..., g_j^{\pm 1} g_i, ..., g_n), \tag{1.1}$$

$$(g_1, ..., g_i, ..., g_n) \mapsto (g_1, ..., g_i g_j^{\pm 1}, ..., g_n), \tag{1.2}$$

$$(g_1, ..., g_i, ..., g_j, ..., g_n) \mapsto (g_1, ..., g_j, ..., g_i, ..., g_n), \tag{1.3}$$

$$\text{or } (g_1, ..., g_i, ..., g_n) \mapsto (g_1, ..., g_i^{-1}, ..., g_n) \tag{1.4}$$

for distinct i and j. Nielsen moves provide a kind of Euclidean algorithm for the combinatorial group theorist. A survey on their history and utility can be found in [FRS95]. See also [Che+23] and [DM24] for more recent references and applications, and see [CF12, Chapter 9] and [Lus91] for specialized applications to knot theory and K-theory. Nielsen moves have also become important in computational group theory over the last few decades. Group-generating n-tuples are the vertices and elementary Nielsen moves are the edges of the *extended product replacement graph*, on which a random walk is known as the *product replacement algorithm* for generating random group elements [Pak01].

Nielsen moves naturally partition the set of n-tuples in G. The resulting *Nielsen equivalence classes* have been completely determined in a handful of cases (refer to [Pak01] for a list). In most of those cases, n strictly exceeds $d(G)$, the minimum size of a generating set for G. The extent of our knowledge when $n = d(G)$ is as follows: there is a unique Nielsen class when G is the fundamental group of a closed surface [Lou10] [Zie70], and Nielsen classes in abelian groups are completely determined [DG99] [Oan11]. The only other full account of Nielsen classes when $n = d(G)$ for an infinite family of groups is conjectural, due to McCullough and Wanderley [MW13]. Let us describe it.

Higman observed that if (g_1, g_2) and $(\tilde{g}_1, \tilde{g}_2)$ are Nielsen equivalent in G, then the *extended conjugacy classes* of the commutators, $\mathrm{cl}_G([g_1, g_2]) \cup \mathrm{cl}_G([g_2, g_1])$ and $\mathrm{cl}_G([\tilde{g}_1, \tilde{g}_2]) \cup \mathrm{cl}_G([\tilde{g}_2, \tilde{g}_1])$, are equal. This union is called the *Higman invariant* of a Nielsen class. The "Classification Conjecture" asserts that this is a complete invariant in the case $G = \mathrm{SL}_2(\mathbb{F}_q)$:

Conjecture 1.3 ("Classification Conjecture" [MW13])**.** *Nielsen classes of generating pairs in* $\mathrm{SL}_2(\mathbb{F}_q)$ *are uniquely determined by the Higman invariant.*

When $G = \mathrm{SL}_2(\mathbb{F}_q)$, all matrices in $\mathrm{cl}_G([g_1, g_2]) \cup \mathrm{cl}_G([g_2, g_1])$ have the same trace, so we also have a *trace invariant*. An equivalent version of the Classification Conjecture in terms of the trace invariant can be found in [MW13]. (The trace invariant is used in the phrasing of Theorem 1.2.)

McCullough and Wanderley also consider the coarser notion of equivalence determined by so-called T_n*-systems*. Their "T-Classification Conjecture" asserts that T_2-systems in $\mathrm{SL}_2(\mathbb{F}_q)$ are uniquely determined by the trace invariant. They prove that the Classification Conjecture implies the T-Classification Conjecture [MW13].

Finally, McCullough and Wanderley consider the triple in $\mathbb{F}_q^3$ associated to a pair of matrices $A, B \in \mathrm{SL}_2(\mathbb{F}_q)$:

$$(A, B) \mapsto (\operatorname{tr} A, \operatorname{tr} B, \operatorname{tr} AB). \tag{1.5}$$

A triple in $\mathbb{F}_q^3$ is called *essential* if it is the image of a pair (A, B) that generates $\mathrm{SL}_2(\mathbb{F}_q)$. To see the relation to Nielsen moves, let us recall a few facts relevant to the trace map above. First, Macbeath showed that the preimage of any triple

in $\mathbb{F}_q^3$ is a single nonempty $\mathrm{SL}_2(\mathbb{F}_{q^2})$-simultaneous conjugacy class of $\mathrm{SL}_2(\mathbb{F}_q)$ pairs [Mac69]. Second, we have Fricke's trace identity,

$$(\operatorname{tr} A)^2 + (\operatorname{tr} B)^2 + (\operatorname{tr} AB)^2 = (\operatorname{tr} A)(\operatorname{tr} B)(\operatorname{tr} AB) + \operatorname{tr}[A, B] + 2.$$

Third, we have already remarked that $\operatorname{tr}[A, B]$ is constant on Nielsen classes. When combined, these facts tell us that Nielsen moves permute solutions in $\mathbb{F}_q^3$ to the Markoff equation

$$x^2 + y^2 + z^2 = xyz + \kappa \tag{1.6}$$

for some fixed $\kappa \in \mathbb{F}_q$. We call such solutions *Markoff triples (with respect to κ)*. Comparing the Markoff equation to Fricke's trace identity, let us highlight the correspondence

$$\kappa = \operatorname{tr}[A, B] + 2,$$

to be used when translating between $\mathrm{SL}_2(\mathbb{F}_q)$ pairs and $\mathbb{F}_q$ triples.

It is straightforward to work out the action on triples corresponding to elementary Nielsen moves:

$$\begin{aligned} ((A, B) \mapsto (A, AB)) &\rightsquigarrow ((x, y, z) \mapsto (x, z, xz - y)), \\ ((A, B) \mapsto (B, A)) &\rightsquigarrow ((x, y, z) \mapsto (y, x, z)), \\ \text{and } ((A, B) \mapsto (A^{-1}, B)) &\rightsquigarrow ((x, y, z) \mapsto (x, y, xy - z)). \end{aligned} \tag{1.7}$$

All Nielsen moves are generated by these three. The last map, $(x, y, z) \mapsto (x, y, xy - z)$, is called a *Vieta involution*. The first- and second-coordinate Vieta involutions are defined similarly and can be obtained from the appropriate compositions of the three maps above. In light of this, two triples are called *Markoff equivalent* if one can be obtained from the other by a combination of Vieta involutions and coordinate permutations—those maps induced by Nielsen moves.

Conjecture 1.4 ("Q-Classification Conjecture" [MW13])**.** *The Markoff class of an essential triple $(x, y, z) \in \mathbb{F}_q^3$ is uniquely determined by $\kappa := x^2 + y^2 + z^2 - xyz$.*

As indicated in Theorem 1.1, the Vieta involutions alone produce the same Markoff classes. There is no need for coordinate permutations.

McCullough and Wanderley verified their conjectures computationally for $q \leq 101$, and they proved them for all q such that $q - 1$ is prime and $q + 1$ is thrice a prime (which may or may not constitute an infinite set) [MW13]. Our approach to these conjectures takes the Markoff perspective. We begin in Section 2 by proving the following:

Theorem 1.5. *The Q-Classification Conjecture implies the Classification and T-Classification Conjectures.*

This allows us to determine Nielsen classes in $\mathrm{SL}_2(\mathbb{F}_q)$ without real consideration for its group structure. Note that Theorem 1.5 is already known for certain special cases of q and κ [MW13] [Cam25], to be described shortly.

After Section 2 we focus on Markoff triples and the proof of Theorem 1.1, which is essentially the Q-Classification Conjecture. Again, see Section 3 for an overview of the proof.

2. Relations among the McCullough–Wanderley conjectures

We begin by relating the trace and Higman invariants.

Proposition 2.1 (Proposition 5.2 and Lemma 5.3 in [MW13]). *Among* $\mathrm{SL}_2(\mathbb{F}_q)$ *generating pairs, there is a unique Higman invariant (i.e. extended conjugacy class of the commutator) of any given trace in* $\mathbb{F}_q\backslash\{\pm 2\}$. *There is no Higman invariant of trace* 2, *and there are either one or two Higman invariants of trace* -2 *depending on whether* $q \equiv 3 \bmod 4$ *or* $q \equiv 1 \bmod 4$, *respectively.*

McCullough and Wanderley deduce from this that the Classification Conjecture implies the T- and Q-Classification Conjectures (Corollary 5.7 and Proposition 8.5 in [MW13]). The converse implications are more challenging and only partially known under additional hypotheses. Specifically, it is proved in [MW13] that the Q-Classification Conjecture implies the Classification Conjecture when q is even or when $4-\kappa$ is not a square in $\mathbb{F}_q$, and Campos-Vargas proved the implication for all $\kappa \in \mathbb{F}_p\backslash\{4\}$ when $q = p$ is a prime congruent to $3 \bmod 4$ [Cam25]. Our goal in this section is to prove the implication for arbitrary prime powers q and arbitrary $\kappa \in \mathbb{F}_q\backslash\{4\}$. To do so, we employ a similar proof strategy to that of McCullough and Wanderley. Let us describe it.

Let (A_1, B_1) and (A_2, B_2) be generating pairs for $\mathrm{SL}_2(\mathbb{F}_q)$ with the same Higman invariant. If the Q-Classification Conjecture holds, there is some sequence of Vieta involutions and coordinate permutations that transforms $(\operatorname{tr} A_2, \operatorname{tr} B_2, \operatorname{tr} A_2B_2)$ into $(\operatorname{tr} A_1, \operatorname{tr} B_1, \operatorname{tr} A_1B_1)$. This corresponds to a sequence of Nielsen moves applied to (A_2, B_2), but it may not end at (A_1, B_1). We only know that the endpoint $(\tilde{A}_1, \tilde{B}_1)$ satisfies $(\operatorname{tr} A_1, \operatorname{tr} B_1, \operatorname{tr} A_1B_1) = (\operatorname{tr} \tilde{A}_1, \operatorname{tr} \tilde{B}_1, \operatorname{tr} \tilde{A}_1\tilde{B}_1)$. We would like to say that this equality of triples implies (A_1, B_1) is Nielsen equivalent to $(\tilde{A}_1, \tilde{B}_1)$ and thus to (A_2, B_2)—that would prove the Classification Conjecture. So, naturally, we ask what can be said about two matrix pairs that correspond to the same triple. The answer comes primarily from the work of MacBeath [Mac69]. (Note that matrix pairs are called *conjugate* if they are simultaneously conjugate.)

Lemma 2.2 (Lemma 2.1(ii) in [MW13]). *Two pairs of generators for* $\mathrm{SL}_2(\mathbb{F}_q)$ *are Nielsen equivalent if they are* $\mathrm{SL}_2(\mathbb{F}_q)$*-conjugate.*

Theorem 2.3 (Theorem 3 in [Mac69]). *Let* $(\alpha, \beta, \gamma) \in \mathbb{F}_q^3$ *solve the Markoff equation for some* $\kappa \neq 4$. *If* q *is odd, there are exactly two* $\mathrm{SL}_2(\mathbb{F}_q)$*-conjugacy classes of matrix pairs with trace* (α, β, γ).

Returning to our setup in $\mathrm{SL}_2(\mathbb{F}_q)$, it follows immediately that (A_1, B_1) and $(\tilde{A}_1, \tilde{B}_1)$ must be Nielsen equivalent in the special case $q \equiv 1 \bmod 4$ and $\kappa = 0$ (or, equivalently, $\operatorname{tr} A_1^{-1}B_1^{-1}A_1B_1 = -2$). Indeed, the two Higman invariants of trace -2 identified in Proposition 2.1 must be the Higman invariants of the two conjugacy classes of matrix pairs identified in Theorem 2.3. Since (A_1, B_1) and $(\tilde{A}_1, \tilde{B}_1)$ have the same Higman invariant by hypothesis and both correspond to the same Markoff triple, they must lie in the same $\mathrm{SL}_2(\mathbb{F}_q)$-conjugacy class by Theorem 2.3. Thus (A_1, B_1) and $(\tilde{A}_1, \tilde{B}_1)$ are Nielsen equivalent by Lemma 2.2.

Outside of the special case $\kappa = 0$ and $q \equiv 1 \bmod 4$, we are not so lucky—there is only one Higman invariant of trace $\kappa - 2$, but there are two conjugacy classes of matrix pairs corresponding to the Markoff triple $(\operatorname{tr} A_1, \operatorname{tr} B_1, \operatorname{tr} A_1B_1)$. It is entirely possible that (A_1, B_1) and $(\tilde{A}_1, \tilde{B}_1)$ lie in different conjugacy classes,

rendering Lemma 2.2 inapplicable. Our strategy here is to show that the Nielsen class of (A_1, B_1) contains two distinct conjugacy classes corresponding to each (or any) Markoff triple, so it must contain $(\tilde{A}_1, \tilde{B}_1)$ and thus (A_2, B_2).

At this point, our proof diverges from that of McCullough and Wanderley. In Lemma 10.2 of [MW13], it is shown that (A, B) and (A^{-1}, B^{-1}) are not conjugate if $2 - \operatorname{tr} A^{-1}B^{-1}AB$ is not a square in $\mathbb{F}_q$. Since (A, B) and (A^{-1}, B^{-1}) correspond to the same Markoff triple and are evidently Nielsen equivalent, that completes McCullough and Wanderley's proof: the Q-Classification Conjecture implies the Classification Conjecture when $4 - \kappa$ is not a square. In our proof, we use instead the Nielsen equivalent pairs (A, B) and (B, A). It turns out that when $\kappa \in \mathbb{F}_q \backslash \{0, 4\}$ or when $\kappa = 0$ and $q \equiv 3 \bmod 4$, there exist generators A and B for $\mathrm{SL}_2(\mathbb{F}_q)$ such that (A, B) and (B, A) are not conjugate yet correspond to the same Markoff triple. That is the only missing ingredient to a complete proof.

We can construct such generators A and B from a specific kind of Markoff triple. It takes the form (α, α, γ) with γ satisfying the properties below.

Lemma 2.4. *Let $q > 353$, and let $p = \operatorname{char}(\mathbb{F}_q)$. If $\kappa \in \mathbb{F}_q \backslash \{0, 4\}$ or if $\kappa = 0$ and $q \equiv 3 \bmod 4$, there exists $\gamma \in \mathbb{F}_q \backslash \{0\}$ such that $\mathbb{F}_p(\gamma) = \mathbb{F}_q$, and neither $2 - \gamma$, $\kappa - \gamma^2$, $\kappa - 8 + 4\gamma - \gamma^2$, nor $-\kappa + \kappa\gamma - \gamma^2$ is a square in $\mathbb{F}_q$.*

Proof. When κ is not 0 or 4, none of the four polynomials in γ share any roots or have repeated roots. Consequently, the Weil bound on multiplicative character sums guarantees the existence of our desired γ for sufficiently large q. Since we wish to prove the lemma for all $q > 353$, let us check what "sufficiently large" means.

Let χ be the quadratic character on $\mathbb{F}_q^\times$ and set $\chi(0) = 0$. The form of the Weil bound we need is Theorem 11.23 in [IK21]: $|\sum_{\mathbb{F}_q} \chi(f(x))| \le (\deg(f) - 1)\sqrt{q}$ provided $f(x) \in \mathbb{F}_q[x]$ is not a square in $\overline{\mathbb{F}}_q[x]$ (or, more generally, not an n^{th} power if χ has order n). By expanding the products below and applying the Weil bound to each resulting sum, we get

$$\frac{1}{16} \sum_{\gamma \in \mathbb{F}_q} \Big((1 - \chi(2 - \gamma))(1 - \chi(\kappa - \gamma^2)) \\ \cdot (1 - \chi(\kappa - 8 + 4\gamma - \gamma^2))(1 - \chi(-\kappa + \kappa\gamma - \gamma^2)) \Big) \ge \frac{1}{16}(q - 56\sqrt{q}).$$

The argument in the sum above is 1 when neither $2 - \gamma$, $\kappa - \gamma^2$, $\kappa - 8 + 4\gamma - \gamma^2$, nor $-\kappa + \kappa\gamma - \gamma^2$ is a square and 0 otherwise, except that roots of the four polynomials are counted as $\frac{1}{2}$ or 0. As per the lemma statement, we wish to avoid these seven roots as well as 0 and elements from a proper subfield of $\mathbb{F}_q$. A crude over-count (provided q is at least 11) of the number of elements to be avoided is $\frac{3}{2}\sqrt{q}$, which is less than $\frac{1}{16}(q - 56\sqrt{q})$ when $q > 6400$. Thus when κ is not 0 or 4 and $q > 6400$, the desired γ exists.

When $\kappa = 0$ and $q \equiv 3 \bmod 4$, the requirement that $\kappa - \gamma^2$ and $-\kappa + \kappa\gamma - \gamma^2$ are not squares holds automatically. This makes the resulting bound on q much less than 6400. We omit details.

For prime powers smaller than 6400, the lemma can be verified by direct computation. Since the number of acceptable γ in $\mathbb{F}_q$ is roughly $\frac{1}{16}q$, a brute-force search is quick. □

We will need to know that the Markoff triple (α, α, γ) obtained from Lemma 2.4 is essential. For this we have McCullough and Wanderley's description of nonessential

triples in Section 11 of [MW13]. The theorem below provides a summary. Parts (1–4b) also appear as the "Main Theorem" in McCullough's unpublished manuscript [McC05], where additional proof details are provided. A full account is also provided in [Cam25].

Theorem 2.5 (Section 11 in [MW13]). *Let* $\varphi = \frac{1}{2}(1+\sqrt{5})$ *and* $\overline{\varphi} = \frac{1}{2}(1-\sqrt{5})$. *If* $\kappa \in \mathbb{F}_q \backslash \{4\}$, *then a Markoff triple with respect to* κ *is essential if and only if it is not among the following exceptions up to permuting or negating coordinates:*

(1) $(\sqrt{\kappa}, 0, 0)$,
(2) $(1,1,0)$ *or* $(1,1,1)$ *when* $\kappa = 2$,
(3a) $(\varphi, \varphi, \varphi)$, $(\varphi, \varphi, 1)$, *or* $(\varphi, 0, 1)$ *when* $\kappa = 2+\varphi$,
(3b) $(\overline{\varphi}, \overline{\varphi}, \overline{\varphi})$, $(\overline{\varphi}, \overline{\varphi}, 1)$, *or* $(\overline{\varphi}, 0, 1)$ *when* $\kappa = 2+\overline{\varphi}$,
(4a) $(\sqrt{2}, 0, 1)$ *or* $(\sqrt{2}, \sqrt{2}, 1)$ *when* $\kappa = 3$,
(4b) $(\varphi, \overline{\varphi}, 0)$, $(\varphi, \overline{\varphi}, -1)$, $(\varphi, 1, 1)$, *or* $(\overline{\varphi}, 1, 1)$, *when* $\kappa = 3$
(5) *or* (α, β, γ) *with* $\mathbb{F}_p(\alpha^2, \beta^2, \gamma^2, \kappa) \neq \mathbb{F}_q$, *where* $p = \mathrm{char}(\mathbb{F}_q)$.

Except for (5), each category above includes all triples in a single Markoff class up to permuting and negating coordinates. Of course, category (5) can account for many different Markoff classes if $\mathbb{F}_q$ has proper subfields. Note that the numbering above matches Theorem 1.1.

We now have all the pieces needed to equate the McCullough–Wanderley conjectures.

Theorem 1.5. *The Q-Classification Conjecture implies the Classification and T-Classification Conjectures.*

Proof. Assume the Q-Classification Conjecture. Let $\kappa \in \mathbb{F}_q \backslash \{4\}$, and assume $q \equiv 3 \bmod 4$ if $\kappa = 0$ (otherwise we are done by Lemma 2.2, Theorem 2.3, and Proposition 2.1). Assume that $\gamma \in \mathbb{F}_q$ from Lemma 2.4 exists (and fix one). Then there exists $\alpha \in \mathbb{F}_q$ with

$$\alpha^2 = \frac{\kappa - \gamma^2}{2 - \gamma}$$

because the right-side expression is a square by choice of γ. Thus (α, α, γ) is a Markoff triple for the given κ. We claim it is an essential triple. Indeed, it cannot fall into category (5) of Theorem 2.5 because $\mathbb{F}_p(\alpha^2, \gamma^2, \kappa) \supseteq \mathbb{F}_p(\gamma) = \mathbb{F}_q$, again by choice of γ. From categories (1–4b), the only nonessential triples of the form (α, α, γ) for which it is possible that neither $2-\gamma$ nor $\kappa-\gamma^2$ is a square are $\pm(1,1,0)$. As we insisted that $\gamma \neq 0$ in Lemma 2.4, (α, α, γ) must be essential.

By the Q-Classification Conjecture, any $\mathrm{SL}_2(\mathbb{F}_q)$ generating pair with commutator trace $\kappa - 2$ is Nielsen equivalent to a pair with trace (α, α, γ). So to prove our theorem it suffices to show that all pairs with trace (α, α, γ) are Nielsen equivalent. By Lemma 2.2 and Theorem 2.3, this follows if we can find two Nielsen equivalent pairs of trace (α, α, γ) that are not conjugate.

Observe that

$$\alpha^2 - 4 = \frac{\kappa - 8 + 4\gamma - \gamma^2}{2 - \gamma}$$

is also a square by choice of γ, so there exists $\zeta \in \mathbb{F}_q$ with

$$\zeta + \zeta^{-1} = \alpha. \tag{2.1}$$

Next, the choice of γ allows us to fix $\eta \in \mathbb{F}_q$ such that

$$\eta^2 = \frac{-\kappa + \kappa\gamma - \gamma^2}{\kappa - 8 + 4\gamma - \gamma^2} = \frac{\alpha^2 - \kappa}{\alpha^2 - 4}.$$

It does not matter which of the two choices of ζ or η we use. Finally, observe that

$$\frac{\alpha^2}{\eta^2} - 4 = \frac{(\gamma^2 - 4\gamma + \kappa)^2}{(2-\gamma)(-\kappa + \kappa\gamma - \gamma^2)}$$

is also a square, so there exists $\vartheta \in \mathbb{F}_q^\times$ with $\eta(\vartheta + \vartheta^{-1}) = \alpha$. Now here, the choice between the two possibilities for ϑ does matter. Any value of ϑ makes $(\zeta + \zeta^{-1}, \eta(\vartheta + \vartheta^{-1}), \eta(\zeta\vartheta + \zeta^{-1}\vartheta^{-1}))$ a Markoff triple, so one of the two values that solves $\eta(\vartheta + \vartheta^{-1}) = \alpha$ must make it (α, α, γ), while the other (replacing ϑ with ϑ^{-1}) makes it $(\alpha, \alpha, \alpha^2 - \gamma)$. We pick the one for which

$$\eta(\vartheta + \vartheta^{-1}) = \alpha \quad \text{and} \quad \eta(\zeta\vartheta + \zeta^{-1}\vartheta^{-1}) = \gamma. \tag{2.2}$$

The matrix pair

$$A = \begin{bmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{bmatrix}, \; B = \begin{bmatrix} \eta\vartheta & (\zeta^{-1} - \zeta)^{-1} \\ (\zeta^{-1} - \zeta)(\eta^2 - 1) & \eta\vartheta^{-1} \end{bmatrix} \in \mathrm{SL}_2(\mathbb{F}_q)$$

satisfies $(\operatorname{tr} A, \operatorname{tr} B, \operatorname{tr} AB) = (\alpha, \alpha, \gamma)$. The Nielsen equivalent pair (B, A) also has trace (α, α, γ), and we claim it is not $\mathrm{SL}_2(\mathbb{F}_q)$-conjugate to (A, B). To see this, we compute

$$\begin{bmatrix} \zeta^{-1} - \eta\vartheta & (\zeta - \zeta^{-1})^{-1} \\ \eta\vartheta - \zeta & (\zeta^{-1} - \zeta)^{-1} \end{bmatrix} (B, A) \begin{bmatrix} \zeta^{-1} - \eta\vartheta & (\zeta - \zeta^{-1})^{-1} \\ \eta\vartheta - \zeta & (\zeta^{-1} - \zeta)^{-1} \end{bmatrix}^{-1} \\ = \left(A, \begin{bmatrix} \eta\vartheta & \eta\vartheta - \zeta^{-1} \\ \zeta - \eta\vartheta & \eta\vartheta^{-1} \end{bmatrix} \right).$$

Call the last matrix C. The equation above shows that (B, A) and (A, C) are $\mathrm{SL}_2(\mathbb{F}_q)$-conjugate, so the claim follows if (A, B) and (A, C) are not conjugate. The centralizer of A is the subgroup of diagonal matrices. If $D \in \mathrm{SL}_2(\mathbb{F}_q)$ is diagonal, the top-right entry of DBD^{-1} is a square multiple of $(\zeta^{-1} - \zeta)^{-1}$. Thus DBD^{-1} could equal C only if $(\zeta^{-1} - \zeta)(\eta\vartheta - \zeta^{-1})$ is a square in $\mathbb{F}_q$. But

$$\begin{aligned} (\zeta^{-1} - \zeta)(\eta\vartheta - \zeta^{-1}) &= \zeta^{-1}\eta(\vartheta + \vartheta^{-1}) + 1 - \zeta^{-2} - \eta(\zeta\vartheta + \zeta^{-1}\vartheta^{-1}) \\ &= \zeta^{-1}\alpha + 1 - \zeta^{-2} - \gamma && \text{by (2.2)} \\ &= \zeta^{-1}(\zeta + \zeta^{-1}) + 1 - \zeta^{-2} - \gamma && \text{by (2.1)} \\ &= 2 - \gamma, \end{aligned}$$

which is not a square as per Lemma 2.4. Thus (A, B) and (B, A) cannot be $\mathrm{SL}_2(\mathbb{F}_q)$-conjugate. This completes the proof when γ from Lemma 2.4 exists.

As described below, the theorem is proved by direct computation when q and κ are such that γ from Lemma 2.4 does not exist. □

McCullough and Wanderley have already verified their conjectures for $q \leq 101$. For $q > 101$, there are exactly 37 pairs q, κ for which γ from Lemma 2.4 does not exist, and $q \leq 181$ in all but two of those pairs (namely $q = 353$ and $\kappa = 36$ or 181). Over such small fields, verifying Theorem 1.5 computationally is feasible: pick any generating pair (A, B) for $\mathrm{SL}_2(\mathbb{F}_q)$ with $\operatorname{tr}[A, B] = \kappa - 2$, and build the Nielsen

class of (A, B) until two non-conjugate pairs are found that correspond to the same Markoff triple. For example, in $\mathbb{F}_{353}$ with $\kappa = 181$, we find

$$\left(\begin{bmatrix} 296 & 0 \\ 0 & 161 \end{bmatrix}, \begin{bmatrix} 182 & 183 \\ 74 & 216 \end{bmatrix}\right) \quad \text{and} \quad \left(\begin{bmatrix} 296 & 0 \\ 0 & 161 \end{bmatrix}, \begin{bmatrix} 182 & 201 \\ 315 & 216 \end{bmatrix}\right).$$

Both pairs correspond to the essential Markoff triple $(104, 45, 45)$. They are not simultaneously conjugate because, as in the last proof, the top-right entries 183 and 201 from the second matrices are not square multiples of one another. To see that these pairs are Nielsen equivalent, let $\sigma_z \circ \tau_x$, τ_z, and σ_z denote the three Nielsen moves in (1.7), respectively. Then the composition $\sigma_z \circ \tau_x \circ (\sigma_z \circ \tau_z)^2 \circ (\sigma_z \circ \tau_x)^2 \circ \sigma_z$ maps the first matrix pair above to the second.

As a final remark, the map $(A, B) \mapsto (B, A)$ used in the proof of Theorem 1.5 is not a *special* (determinant 1) Nielsen move; it comes from the nontrivial coset in $\mathrm{Aut}(F_2)/\mathrm{SAut}(F_2)$, where F_2 is the free group on two letters and $\mathrm{SAut}(F_2)$ is the kernel of $\mathrm{Aut}(F_2) \xrightarrow{\mathrm{ab}} \mathrm{GL}_2(\mathbb{Z}) \xrightarrow{\det} \{\pm 1\}$. So for the computational group theorist, our results on the Q-Classification Conjecture do not fully determine connected components of the product replacement graph, but rather the *extended* product replacement graph. In the special case that $4 - \kappa$ is not a square, however, there is already McCullough and Wanderley's proof of Theorem 1.5, which uses the *special* Nielsen move $(A, B) \mapsto (A^{-1}, B^{-1})$.

3. Overview of the remaining sections

3.1. **The main definitions.** We introduce all but one of the objects central to the proof of Theorem 1.1 in advance. The definition that we skip for now is not as succinct as those below.

Notation 3.1. Let σ_x, σ_y, and σ_z denote the three Vieta involutions as in Theorem 1.1, let τ_x, τ_y, and τ_z denote the three coordinate transpositions indexed by their fixed coordinate, and let Γ denote the group generated by the σ_i and τ_j along with the double sign change $(x, y, z) \mapsto (x, -y, -z)$. Let Γ_x denote the stabilizer of the first coordinate (generated by τ_x, σ_y, and the double sign change).

Throughout the paper, R is an integral domain and F is its field of fractions. We use $\overline{F}$ to denote the algebraic closure of F and $\overline{R}$ to denote the integral closure of R in $\overline{F}$. There are reminders of this notation throughout.

The definitions below, just like the term *Markoff triple*, depend on the value of κ that determines the Markoff equation. Since we so rarely have occasion to consider two distinct values of κ at once (it only happens in the proof of Proposition 6.21), the subscript κ is suppressed in notation.

Notation 3.2. For a fixed $\kappa \in R$, let $\mathscr{M}(R) \subseteq R^3$ denote the set of Markoff triples.

Notation 3.3. For a fixed $\kappa \in R$, let $\mathscr{P}(R)$ denote those $f \in \overline{R}[x]$ such that

$$\sum_{\mathbf{t} \in \mathscr{O}} f(x) = 0$$

for any finite Γ-invariant subset $\mathscr{O} \subseteq \mathscr{M}(R)$. Note that "$x$" in the summation is shorthand for $x(\mathbf{t})$, where $x(\alpha, \beta, \gamma) = \alpha$.

The inclusion of $(x, y, z) \mapsto (-x, -y, z)$ in Γ guarantees $x^{2n+1} \in \mathscr{P}(R)$ for any $n \geq 0$. It is the even degree polynomials in $\mathscr{P}(R)$ that are hard to come by.

Definition 3.4. A *first-coordinate orbit* is a set of the form $\Gamma_x \cdot \mathbf{t}$ for some $\mathbf{t} \in \mathscr{M}(R)$. We use $\mathcal{O}_x$ to denote a generic first-coordinate orbit and $\mathcal{O}_\alpha$ for some $\alpha \in R$ to denote a generic first-coordinate orbit in which $x = \alpha$.

Definition 3.5. Let $\alpha \in R$, and let $\zeta \in \overline{R}$ solve $\zeta + \zeta^{-1} = \alpha$. The *(rotation) order* of α, denoted $\mathrm{ord}(\alpha)$, is the smallest positive even integer n such that $\zeta^n = 1$. If no such n exists, we say α has infinite order.

Insisting that α have even order is not standard in the literature, nor is it of theoretical importance in our work. It does, however, lead to cleaner propositions.

Notation 3.6. For $\kappa \in R$ and an integer $d \geq 2$, let $\mathscr{P}_x(R, d)$ denote those $f \in \overline{R}[x, y, z]$ such that $\sum_{\mathcal{O}_\alpha} f(\mathbf{t}) = 0$ whenever $\mathcal{O}_\alpha$ is finite and $2d \nmid \mathrm{ord}(\alpha)$. Also let $\mathscr{P}_x(R, \infty)$ denote those $f \in \overline{R}[x, y, z]$ such that $\sum_{\mathcal{O}_\alpha} f(\mathbf{t}) = 0$ for all but finitely many $\alpha \in R$.

3.2. **Proof strategy.** Let us turn to $R = \mathbb{F}_q$ and Theorem 1.1. Several small Γ-invariant subsets of $\mathscr{M}(\mathbb{F}_q)$ are identified for certain κ in Theorem 2.5. The Q-Classification Conjecture predicts that Γ acts transitively on all remaining Markoff triples. In particular, if $q = p$ is prime (to avoid case (5) of Theorem 2.5) and κ is neither 2 (to avoid case (2)), $2 + \varphi$ (to avoid case (3a)), $2 + \overline{\varphi}$ (to avoid case (3b)), 3 (to avoid case (4)), nor 4 (generally forbidden), then the Q-Classification Conjecture predicts that Γ should act transitively on $\mathscr{M}(\mathbb{F}_p)$ if $\left(\frac{\kappa}{p}\right) = -1$, and $\mathscr{M}(\mathbb{F}_p)$ should break into exactly two Γ-orbits if $\left(\frac{\kappa}{p}\right) = 1$, namely $\Gamma \cdot (\sqrt{\kappa}, 0, 0)$ (from case (1)) and everything else.

To limit the number of Γ-invariant subsets of $\mathscr{M}(\mathbb{F}_p)$, we plan to build up the rank of $\mathscr{P}(\mathbb{F}_p)$ from Notation 3.3. To see why this works, suppose $\mathcal{O}$ is Γ-invariant, and for $\alpha \in \mathbb{F}_p$ let $c_{\mathcal{O}}(\alpha)$ count the number of triples in $\mathcal{O}$ with first coordinate α. For any $f = f(x) \in \mathbb{F}_p[x]$,

$$\sum_{\mathbf{t} \in \mathcal{O}} f(x) = \sum_{\alpha \in \mathbb{F}_p} c_{\mathcal{O}}(\alpha) f(\alpha).$$

Provided f is an even polynomial, this shows that $f \in \mathscr{P}(\mathbb{F}_p)$ if and only if the vectors

$$\begin{bmatrix} f(0) \\ f(1) \\ \vdots \\ f(p-1) \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} c_{\mathcal{O}}(0) \\ c_{\mathcal{O}}(1) \\ \vdots \\ c_{\mathcal{O}}(p-1) \end{bmatrix}$$

are orthogonal for every Γ-invariant subset $\mathcal{O}$ of $\mathscr{M}(\mathbb{F}_p)$. So the more polynomials we produce in $\mathscr{P}(\mathbb{F}_p)$, the smaller its orthogonal complement, which means there are fewer possible Γ-invariant subsets. This is made precise in Theorem 4.7, which rephrases Theorem 1.1 and the Q-Classification Conjecture in terms of the expected orthogonal complement of $\mathscr{P}(\mathbb{F}_p)$.

This leads us to the last fundamental definition that is missing from Section 3.1. There is a polynomial reduction algorithm, call it Φ (the subscript κ is suppressed again), that is useful for producing elements of $\mathscr{P}(\mathbb{F}_p)$, and more generally $\mathscr{P}(R)$. The algorithm takes as input a multivariate polynomial $f = f(x, y, z)$ and outputs a univariate polynomial $\Phi(f) = \Phi(f)(x)$ satisfying $\sum_{\mathcal{O}} f(\mathbf{t}) = \sum_{\mathcal{O}} \Phi(f)(x)$ for any Γ-invariant set $\mathcal{O} \subseteq \mathscr{M}(R)$. Our strategy is to apply Φ to multivariate polynomials

for which it is easy to check that $\sum_{\mathbf{t}\in\mathcal{O}} f(\mathbf{t})$ vanishes when $R = \mathbb{F}_q$. For example, if $f = (x^q - x)yz^3$ then $\Phi(f)$ is in $\mathscr{P}(\mathbb{F}_q)$ because f is identically 0 on $\mathbb{F}_q^3$.

Let us define the output of Φ for monic monomial inputs from $R[x, y, z]$, where R is some integral domain. Arbitrary inputs are then handled by extending linearly. Consider the input $x^\ell y^m z^n$ with $\ell, m, n > 0$. For any $\mathcal{O} \subseteq \mathscr{M}(R)$, we have

$$\sum_{\mathbf{t}\in\mathcal{O}} x^\ell y^m z^n = \sum_{\mathbf{t}\in\mathcal{O}} x^{\ell-1} y^{m-1} z^{n-1}(x^2 + y^2 + z^2 - \kappa)$$

by virtue of $\mathbf{t}$ being a Markoff triple (we need not even assume $\mathcal{O}$ is Γ-invariant here). The total degree of $x^{\ell-1}y^{m-1}z^{n-1}(x^2 + y^2 + z^2 - \kappa)$ is one less than that of $x^\ell y^m z^n$. We denote a reduction of this form as ρ, so

$$\rho(x^\ell y^m z^n) = x^{\ell-1} y^{m-1} z^{n-1}(x^2 + y^2 + z^2 - \kappa).$$

Now consider a monomial with only two variables, say $y^m z^n$ with $m, n > 0$. If $\mathcal{O} \subset \mathscr{M}(R)$ is closed under the first-coordinate Vieta involution then

$$\begin{aligned}
\sum_{\mathbf{t}\in\mathcal{O}} y^m z^n &= \sum_{\mathbf{t}\in\mathcal{O}} (y^m z^n - xy^{m-1}z^{n-1}z + xy^{m-1}z^{n-1}) \\
&= \sum_{\mathbf{t}\in\mathcal{O}} y^{m-1}z^{n-1}(yz - x) + \sum_{\mathbf{t}\in\mathcal{O}} xy^{m-1}z^{n-1} \\
&= \sum_{\mathbf{t}\in\mathcal{O}} xy^{m-1}z^{n-1} + \sum_{\mathbf{t}\in\mathcal{O}} xy^{m-1}z^{n-1} && \text{by Vieta involution} \\
&= \sum_{\mathbf{t}\in\mathcal{O}} 2xy^{m-1}z^{n-1}. && (3.1)
\end{aligned}$$

Again, the total degree of $2xy^{m-1}z^{n-1}$ is one less than the degree of the input. We abuse notation and express a step of this form as

$$\sigma_x(y^m z^n) = 2xy^{m-1}z^{n-1}.$$

Of course σ_y and σ_z are defined analogously. Once all multivariate terms of f have been eliminated, what remains can be expressed in x alone using the coordinate permutations $\tau_x, \tau_y, \tau_z \in \Gamma$. Again we abuse notation and write

$$\tau_y(z^n) = x^n.$$

The final result is the desired univariate polynomial $\Phi(f)$ that satisfies

$$\sum_{\mathbf{t}\in\mathcal{O}} f(\mathbf{t}) = \sum_{\mathbf{t}\in\mathcal{O}} \Phi(f)(x) \text{ whenever } \Gamma\cdot\mathcal{O} = \mathcal{O}. \tag{3.2}$$

Our reduction algorithm is deterministic because for every monomial there is a unique prescribed operation. Note that the choice to combine "like terms" at any stage does not affect the output because we defined Φ on monomials and extended linearly. Also note that variable permutations need not be reserved for the final stage. For example, the result is the same whether we apply σ_x, $\tau_z \circ \sigma_y$, and $\tau_y \circ \sigma_z$ to the three terms of $yz + xz + xy$, respectively, or whether we permute variables in order to combine the three monomials first then apply σ_x to $3yz$. The general principle is below. It matches the relation between τ_i and σ_j viewed as elements of Γ.

Proposition 3.7. *For any $i, j \in \{x, y, z\}$, $\tau_i \circ \sigma_j = \sigma_{\tau_i(j)} \circ \tau_i$ on any applicable bivariate monomial, and $\tau_i \circ \rho = \rho \circ \tau_i$ on any trivariate monomial.*

Proof. Without loss of generality, let $j = x$. Then

$$\begin{aligned}(\tau_i \circ \sigma_x)(y^m z^n) &= \tau_i(2xy^{m-1}z^{n-1}) \\ &= 2\tau_i(x)\tau_i(y)^{m-1}\tau_i(z)^{n-1} \\ &= \sigma_{\tau_i(x)}(\tau_i(y)^m \tau_i(z)^n) \\ &= (\sigma_{\tau_i(x)} \circ \tau_i)(y^m z^n).\end{aligned}$$

The second claim is verified in similar fashion. □

We have already seen a few polynomials in $\overline{\mathbb{F}}_q[x, y, z]$ that evidently sum to 0 over Γ-invariant subsets of $\mathscr{M}(\mathbb{F}_q)$. All odd polynomials work due to the double sign change in Γ, as do the even polynomials $(x^{q+1} - x^2)y^{2n}$ (whose Φ reduction is also even) since $x^{q+1} - x^2$ is identically 0 on $\mathbb{F}_q$. Unfortunately, finding a formula for $\Phi((x^{q+1} - x^2)y^{2n})$ appears to be a serious challenge, and without one we cannot determine the rank of the reduced polynomials as n ranges. For $f \in \mathbb{F}_q[x, y, z]$, it is straightforward to find the coefficients of the largest powers of x in $\Phi(f)$. Indeed, Section 5 is devoted to proving such a formula (Theorem 5.11; see also (5.8) and Theorem 5.14). But the author has no formula for the coefficients of smaller powers. This makes it difficult to prove that the span of $\Phi((x^{q+1} - x^2)y^{2n})$ as n ranges includes polynomials of small degree, specifically anything of degree less than $\frac{1}{2}(q + 1)$.

In avoidance of this obstacle, we turn to a family of polynomials with much more variation in their degrees. The smallest example from this family is $f(x, y, z) = y^4 - y^2z^2 + \frac{1}{2}x^2y^2$. Before seeing its significance, here is its reduction:

$$\begin{aligned}y^4 - y^2z^2 + \tfrac{1}{2}x^2y^2 &\xmapsto{\tau_y} y^4 - x^2y^2 + \tfrac{1}{2}x^2y^2 = y^4 - \tfrac{1}{2}x^2y^2 \\ &\xmapsto{\sigma_z} y^4 - xyz \\ &\xmapsto{\rho} y^4 - (x^2 + y^2 + z^2) \\ &\xmapsto{\tau_y, \tau_z} x^4 - 3x^2.\end{aligned}$$

To see the utility of this polynomial, consider the following reduction of xf:

$$\begin{aligned}xf = xy^4 - xy^2z^2 + \tfrac{1}{2}x^3y^2 &\xmapsto{\sigma_z} 2y^3z - xy^2z^2 + x^2yz \\ &\xmapsto{\rho} 2y^3z - yz(x^2 + y^2 + z^2) + x^2yz \\ &\xmapsto{\tau_x} 2y^3z - x^2yz - y^3z - y^3z + x^2yz = 0.\end{aligned} \tag{3.3}$$

What makes this last reduction special is that it only uses operations that preserve the first coordinate. In other words, it avoids σ_x, τ_y, and τ_z. Thus if $\mathscr{O}_\alpha$ is some first-coordinate orbit, then

$$\alpha \sum_{\mathbf{t} \in \mathscr{O}_\alpha} f(\mathbf{t}) = \sum_{\mathbf{t} \in \mathscr{O}_\alpha} xf(\mathbf{t}) = \sum_{\mathbf{t} \in \mathscr{O}_\alpha} 0 = 0. \tag{3.4}$$

So if $\alpha \neq 0$, the left-side sum above must vanish. But then if 0 *never* appears as a coordinate in $\mathscr{M}(\mathbb{F}_q)$ (which happens when $\kappa = 0$ and $q \equiv 3 \bmod 4$), the sum of f over every first-coordinate orbit must vanish. Now, any Γ-invariant set $\mathscr{O} \subseteq \mathscr{M}(\mathbb{F}_q)$ can be viewed as a disjoint union of first-coordinate orbits, so this would imply $0 = \sum_{\mathscr{O}} f(\mathbf{t}) = \sum_{\mathscr{O}} \Phi(f)(x)$. But then $\Phi(f) = x^4 - 3x^2$ must lie in $\mathscr{P}(\mathbb{F}_q)$!...at least when $\kappa = 0$ and $q \equiv 3 \bmod 4$.

In pursuit of similar polynomials, we make extensive use of the partial reduction algorithm in (3.3), which is restricted to the operations ρ, σ_y, σ_z, and τ_x. We call this reduction algorithm Φ_x. Since Φ_x cannot reduce a monomial of the form $y^m z^n$, the output of Φ_x need not be univariate. Instead, it is some element of $R[x]+R[y,z]$ satisfying the analog of (3.2):

$$\sum_{\mathbf{t}\in\mathscr{O}_x} f(\mathbf{t}) = \sum_{\mathbf{t}\in\mathscr{O}_x} \Phi_x(f)(\mathbf{t}) \text{ whenever } \Gamma_x \cdot \mathscr{O}_x = \mathscr{O}_x. \tag{3.5}$$

To make the output of Φ_x well-defined, we adopt the convention that every monomial appearing in $\Phi_x(f)$ has degree in y at least that of z.

If $\operatorname{char}(R) \neq 2$, then the rotation order of 0 is 4 in R since 0 is the sum of a primitive fourth root of unity and its inverse. Recalling Notation 3.6, we conclude that $y^4 - y^2z^2 + \frac{1}{2}x^2y^2 \in \mathscr{P}_x(R,2)$. We generalize this example in Section 6: for integers d and n satisfying $d \,|\, n$ and $\operatorname{char}(R) \nmid d$, we find polynomials of degree $2n$ in $\mathscr{P}_x(R,d)$, one for each $\alpha \in R\backslash\{\pm 2\}$ with $2d \,|\, \operatorname{ord}(\alpha)$ and $\operatorname{ord}(\alpha) \,|\, 2n$. These polynomials turn out to be eigenvectors of eigenvalue α with respect to a certain linear map, just as (3.4) suggests $y^4 - y^2z^2 + \frac{1}{2}x^2y^2$ is an eigenvector of eigenvalue 0. Now, the example with $\alpha = 0$ and $d = 2$ was not widely applicable—only in the special case $\kappa = 0$ and $q \equiv 3 \bmod 4$ does $\mathscr{M}(\mathbb{F}_q)$ not possess a triples with 0 as an entry. But for larger d, building up $\mathscr{P}_x(R,d)$, particularly when $R = \overline{\mathbb{Z}}$, is more useful. Let's consider how the case $d = 4$ is relevant to all prime powers $q \not\equiv \pm 1 \bmod 8$. If $\mathfrak{p} \subset \overline{\mathbb{Z}}$ is a prime over $\operatorname{char}(\mathbb{F}_q)$ and $f \in \mathscr{P}_x(\overline{\mathbb{Z}},4)$ we can reduce $f \bmod \mathfrak{p}$ to produce a polynomial in $\mathscr{P}_x(\mathbb{F}_q,4)$ (Proposition 6.21). By Notation 3.6, the only first-coordinate orbits $\mathscr{O}_\alpha \subset \mathscr{M}(\mathbb{F}_q)$ on which $\sum_{\mathscr{O}_\alpha} f(\mathbf{t})$ is not guaranteed to vanish are those where $8 \,|\, \operatorname{ord}(\alpha)$. But since $q \not\equiv \pm 1 \bmod 8$ and all elements of $\mathbb{F}_q$ have rotation order dividing $q \pm 1$ (see Corollary 4.2), no such orbits exist. In particular, $\Phi(f) \in \mathscr{P}(\mathbb{F}_q)$.

For $q = p$ a prime not congruent to $\pm 1 \bmod 2d$, we are able to prove that the Φ reductions of $\mathscr{P}_x(\overline{\mathbb{Z}},d) \bmod \mathfrak{p}$ generate all but perhaps the smallest degree polynomials that are expected to be in $\mathscr{P}(\mathbb{F}_p)$. This is Corollary 6.20, the culmination of all the work in Sections 5 and 6. "Filling out" the rest of $\mathscr{P}(\mathbb{F}_p)$ so that it matches what Theorem 4.7 predicts is a computational task that we approach from two angles. First, in Section 7 we add polynomials of the form $\Phi((x^{p+1} - x^2)y^{2n})$ into $\mathscr{P}(\mathbb{F}_p)$. We only need a few of them, namely $n = 1,2,3,4$ for generic κ, and it is not too hard to find a complete formula for the Φ reductions when n is small. Second, in Section 8, we use computer assistance to compute the reductions of the smallest polynomials in $\mathscr{P}_x(\overline{\mathbb{Z}},d)$ and check that they span the expected space (see Algorithm 1). Working over $\overline{\mathbb{Z}}$ and projecting onto residue fields is the only way to fill out $\mathscr{P}(\mathbb{F}_p)$ for all $p \not\equiv \pm 1 \bmod 2d$ simultaneously. That is the purpose of considering $\mathscr{P}_x(\overline{\mathbb{Z}},d)$.

In summary, we proceed as follows:

- Section 4: Determine what $\mathscr{P}(\mathbb{F}_p)$ must equal for Theorem 1.1 to hold (Theorem 4.7).
- Section 5: Compute generic formulas for the top coefficients of $\Phi(f)$ (Theorems 5.11 and 5.14).
- Section 6: Find "eigenvectors" generalizing (3.3) (Theorem 6.10). Specialize Section 5's formula for $\Phi(f)$ to these eigenvectors (Theorem 6.17)

to prove that $\mathscr{P}_x(\overline{\mathbb{Z}}, d)$ contains polynomials of any sufficiently large degree (Corollary 6.20).

Section 7: Fill in the gaps (which are small; 2-, 3-, or 4-dimensional depending on κ) between what $\mathscr{P}_x(\overline{\mathbb{Z}}, d) \bmod \mathfrak{p}$ is expected to be and what Section 4 says $\mathscr{P}(\mathbb{F}_p)$ must be (Theorem 7.1).

Section 8: With help from SageMath, prove that $\mathscr{P}_x(\overline{\mathbb{Z}}, d)$ contains the small degree polynomials that are missing from Section 6 but expected in Section 7.

Theoretical work essentially stops after the proof of Lemma 7.2, at which point the paper becomes largely computational.

4. The conjectured space $\mathscr{P}(\mathbb{F}_p)$

The three preliminary results below are well-known. We provide proofs, albeit terse, for the sake of completeness.

Proposition 4.1. *Let $\mathcal{O}_\alpha \subseteq \mathscr{M}(R)$ be some first-coordinate orbit. If $\alpha^2 \neq 4$, let $\zeta, \eta \in \overline{F}$ solve $\zeta + \zeta^{-1} = \alpha$ and $(\alpha^2 - 4)\eta^2 = (\alpha^2 - \kappa)$. There exists $\vartheta \in \overline{F}$ such that*

$$\mathcal{O}_\alpha = \begin{cases} (\alpha, \eta(\zeta^n\vartheta + \zeta^{-n}\vartheta^{-1}, \eta(\zeta^{n+1}\vartheta + \zeta^{-n-1}\vartheta^{-1})) & \alpha^2 \neq 4, \kappa \\ (\alpha, \zeta^n\vartheta, \zeta^{n+1}\vartheta) & \alpha^2 = \kappa \\ (\alpha, \vartheta + n\sqrt{\kappa - 4}, \vartheta + (n+1)\sqrt{\kappa - 4}) & \alpha^2 = 4 \end{cases}$$

for $n \in \mathbb{Z}$, up to permuting or negating the second and third coordinates.

Proof. A quick check shows that a triple in any of the three given forms solves the Markoff equation. Conversely, any Markoff triple can be rewritten in one these three forms by solving for ζ, η, and ϑ.

Next, it may be computed directly that $\tau_x \circ \sigma_y$ increases n by exactly one in all three cases and $\sigma_y \circ \tau_x$ decreases n by exactly one on all three cases. Since Γ_x is generated by τ_x, σ_y, and $(x, y, z) \mapsto (x, -y, -z)$, we see that $\mathcal{O}_\alpha$ consists of the indicated triples up to permuting or negating the second and third coordinates. □

Corollary 4.2. *Let q be an odd prime power, and let χ be the quadratic character on $\mathbb{F}_q^\times$. If $\alpha \in \mathbb{F}_q \backslash \{\pm 2, \pm\sqrt{\kappa}\}$, then there are $q - \chi(\alpha^2 - 4)$ triples in $\mathscr{M}(\mathbb{F}_q)$ with first coordinate α, $\operatorname{ord}(\alpha)$ divides $q - \chi(\alpha^2 - 4)$, and every first-coordinate orbit $\mathcal{O}_\alpha$ has size $\operatorname{ord}(\alpha)$ or $2\operatorname{ord}(\alpha)$.*

Proof. Define $\chi(0) = 0$. By solving the Markoff equation for z, the number of triples with first two coordinates α and β is seen to be $1 + \chi(\beta^2(\alpha^2 - 4) - 4\alpha^2 + 4\kappa)$. Thus the number of triples with first coordinate α is a well-known sum:

$$\sum_{\beta \in \mathbb{F}_q} (1 + \chi(\beta^2(\alpha^2 - 4) - 4\alpha^2 + 4\kappa)) = q - \chi(\alpha^2 - 4)$$

as claimed.

Next consider some $\mathcal{O}_\alpha$ with $\zeta + \zeta^{-1} = \alpha$ so that $\operatorname{ord}(\alpha)$ is the multiplcative order of ζ if $-1 \in \langle\zeta\rangle$ and twice the multiplicative order of ζ otherwise. We have $\chi(\alpha^2 - 4) = -1$ if and only if $\zeta \notin \mathbb{F}_q$, in which case the image of ζ under the nontrivial element of $\operatorname{Gal}(\mathbb{F}_{q^2}/\mathbb{F}_q)$ is ζ^{-1}. That is, ζ is in the kernel of the norm map $\mathbb{F}_{q^2}^\times \to \mathbb{F}_q^\times$. This kernel has size $q + 1$, so $\operatorname{ord}(\alpha)$ divides $q + 1 = q - \chi(\alpha^2 - 4)$. The other possibility is $\zeta \in \mathbb{F}_q$, in which case $\operatorname{ord}(\alpha)$ divides the size of $\mathbb{F}_q^\times$, which is $q - 1 = q - \chi(\alpha^2 - 4)$. Finally, note that $\operatorname{ord}(\alpha)$ counts the number of elements

in Proposition 4.1 as n varies *and* as the sign of the second and third coordinates change (because $\operatorname{ord}(\alpha)$ is twice the multiplcative order of ζ when $-1 \notin \langle\zeta\rangle$). After transposing the second and third coordinates, this count can either double or stay the same. □

Corollary 4.3. *Let q be an odd prime power. If $\alpha \in \mathbb{F}_q \backslash \{\pm\sqrt{\kappa}\}$ has rotation order $q+1$ or $q-1$, then there is a unique first-coordinate orbit $\mathcal{O}_\alpha$ in $\mathscr{M}(\mathbb{F}_q)$.*

Proof. Let $(\alpha, \beta_1, \gamma_1), (\alpha, \beta_2, \gamma_2) \in \mathscr{M}(\mathbb{F}_q)$, and let $\zeta, \eta \in \mathbb{F}_{q^2}$ solve $\zeta + \zeta^{-1} = \alpha$ and $(\alpha^2 - 4)\eta^2 = (\alpha^2 - \kappa)$. Assume that $\operatorname{ord}(\alpha) = q \pm 1$ so that $\langle\zeta, -1\rangle$ is either $\mathbb{F}_q^\times$ or the kernel of the norm $\mathbb{F}_{q^2}^\times \to \mathbb{F}_q^\times$.

Observe that

$$\vartheta_i^{\pm 1} \coloneqq \frac{1}{2\sqrt{\alpha^2 - \kappa}} \left(\sqrt{\alpha^2 - 4}\beta_i \pm (2\gamma_i - \alpha\beta_i) \right)$$

satisfies $\eta(\vartheta_i + \vartheta_i^{-1}) = \beta_i$. If $\sqrt{\alpha^2 - 4} \in \mathbb{F}_q$, we see directly from the formula for $\vartheta_i^{\pm 1}$ that $\vartheta_1 \vartheta_2^{-1} \in \mathbb{F}_q^\times$. But $\sqrt{\alpha^2 - 4} \in \mathbb{F}_q$ also implies $\zeta \in \mathbb{F}_q^\times$. Thus ϑ_1 and ϑ_2 differ by a power of $\pm\zeta$, which shows $(\alpha, \beta_2, \gamma_2) \in \Gamma_x \cdot (\alpha, \beta_1, \gamma_1)$ by Proposition 4.1. If $\sqrt{\alpha^2 - 4} \notin \mathbb{F}_q$, then $\vartheta_1, \vartheta_2 \notin \mathbb{F}_q$. Using the formulas for ϑ_1 and ϑ_2, we can determine their images under the nontrivial automorphism of $\mathbb{F}_{q^2}/\mathbb{F}_q$: either $\vartheta_1^q = \vartheta_1^{-1}$ and $\vartheta_2^q = \vartheta_2^{-1}$ if $\sqrt{\alpha^2 - \kappa} \notin \mathbb{F}_q$ or $\vartheta_1^q = -\vartheta_1^{-1}$ and $\vartheta_2^q = -\vartheta_2^{-1}$ if $\sqrt{\alpha^2 - \kappa} \in \mathbb{F}_q$. Either way, $\vartheta_1 \vartheta_2^{-1}$ belongs to the kernel of the norm $\mathbb{F}_{q^2}^\times \to \mathbb{F}_q^\times$, which is generated by $\pm\zeta$. Again this gives $(\alpha, \beta_2, \gamma_2) \in \Gamma_x \cdot (\alpha, \beta_1, \gamma_1)$ by Proposition 4.1. □

Notation 4.4. Index the coordinates of $\mathbb{F}_q^q$ by $0, \ldots, q-1$, and let $\mathbf{e}_i$ be the i^{th} standard basis row vector. Let $\mathscr{P}^\perp(\mathbb{F}_q)$ denote the orthogonal complement of the image of $\mathscr{P}(\mathbb{F}_q)$ under the composition

$$\begin{aligned} \mathbb{F}_q[x] \to \mathbb{F}_q[x]/(x^q - x) &\xrightarrow{\sim} \mathbb{F}_q^q \\ x^i + (x^q - x) &\mapsto \mathbf{e}_i. \end{aligned}$$

Notation 4.5. Let

$$\mathbf{x} = \sum_{i=0}^{q} x^i \mathbf{e}_i^T,$$

and for $\alpha \in \mathbb{F}_q$ let $\mathbf{x}(\alpha)$ denote the vector $\mathbf{x}$ with x replaced by α.

Row vectors are used for polynomials and column vectors for inputs so that "$f(x)$" can be written as a matrix product in the form $\mathbf{f}(\mathbf{x})$.

Lemma 4.6. *For $\mathcal{O} \subseteq \mathscr{M}(\mathbb{F}_q)$ and $\alpha \in \mathbb{F}_q$, let $c_{\mathcal{O}}(\alpha)$ count the number of triples in $\mathcal{O}$ with first coordinate α. Then*

$$\mathscr{P}^\perp(\mathbb{F}_q) = \operatorname{span}\left\{ \sum_{\alpha \in \mathbb{F}_q} c_{\mathcal{O}}(\alpha)\mathbf{x}(\alpha) \;\middle|\; \Gamma \cdot \mathcal{O} = \mathcal{O} \right\}.$$

Proof. The proof is essentially an unwrapping of definitions. Let $\mathbf{f} \in \mathbb{F}_q^q$ correspond to some $f \in \mathbb{F}_q[x]$ as per Notation 4.4. By definition, $f \in \mathscr{P}(\mathbb{F}_q)$ if and only if $\sum_{\mathcal{O}} f(x) = 0$ whenever $\Gamma \cdot \mathcal{O} = \mathcal{O}$. We have defined each $c_{\mathcal{O}}(\alpha)$ so that

$$\sum_{\mathbf{t} \in \mathcal{O}} f(x) = \sum_{\alpha \in \mathbb{F}_q} c_{\mathcal{O}}(\alpha) f(\alpha) = \mathbf{f}\left(\sum_{\alpha \in \mathbb{F}_q} c_{\mathcal{O}}(\alpha)\mathbf{x}(\alpha) \right).$$

In particular, $\mathscr{P}^{\perp}(\mathbb{F}_q)$ contains the span in the lemma statement, and the orthogonal complement of the span is contained in $\mathscr{P}(\mathbb{F}_q)$. □

Combining Lemma 4.6 with Theorem 2.5 tells us what we should expect $\mathscr{P}^{\perp}(\mathbb{F}_q)$ to equal provided the Q-Classification Conjecture holds. Indeed, to obtain spanning vectors we need only compute the coefficients $c_{\mathscr{O}}(\alpha)$ for the various orbits listed in Theorem 2.5 and plug them into Lemma 4.6's formula. The vectors corresponding to cases (1–4b) are given below. As before, $\varphi := \frac{1}{2}(1+\sqrt{5})$ and $\overline{\varphi} := \frac{1}{2}(1-\sqrt{5})$.

$$\begin{aligned}
\mathbf{y}_\kappa &:= 2\mathbf{x}(0) + \tfrac{1}{2}(\mathbf{x}(\sqrt{\kappa}) + \mathbf{x}(-\sqrt{\kappa})) \\
\mathbf{y}_1 &:= \mathbf{x}(0) + \tfrac{3}{2}(\mathbf{x}(1) + \mathbf{x}(-1)) \\
\mathbf{y}_\varphi &:= 2\mathbf{x}(0) + \tfrac{3}{2}(\mathbf{x}(1) + \mathbf{x}(-1)) + \tfrac{5}{2}(\mathbf{x}(\varphi) + 5\mathbf{x}(-\varphi)) \\
\mathbf{y}_{\overline{\varphi}} &:= 2\mathbf{x}(0) + \tfrac{3}{2}(\mathbf{x}(1) + \mathbf{x}(-1)) + \tfrac{5}{2}(\mathbf{x}(\overline{\varphi}) + \mathbf{x}(-\overline{\varphi})) \\
\mathbf{y}_2 &:= 2\mathbf{x}(0) + \tfrac{3}{2}(\mathbf{x}(1) + \mathbf{x}(-1)) + 2(\mathbf{x}(\sqrt{2}) + \mathbf{x}(-\sqrt{2})) \\
\mathbf{y}_5 &:= 2\mathbf{x}(0) + 3(\mathbf{x}(1) + \mathbf{x}(-1)) + \tfrac{5}{2}(\mathbf{x}(\varphi) + \mathbf{x}(-\varphi)) + \tfrac{5}{2}(\mathbf{x}(\overline{\varphi}) + \mathbf{x}(-\overline{\varphi})).
\end{aligned} \tag{4.1}$$

As an example, $\mathbf{y}_2$ comes from the orbit in case (4a) of Theorem 2.5, in which 0 occurs eight times as a first coordinate, 1 and -1 occur six times each, and $\sqrt{2}$ and $\sqrt{2}$ occur eight times each. (The choice to scale by $\frac{1}{4}$ is made for the sake of computational convenience in Section 7.)

Computing coefficients for case (5) of Theorem 2.5 is more challenging, but we restrict to the case that $q = p$ is prime so the computation is unnecessary. This leaves only the orbit of essential triples. Since this orbit is the complement of the nonessential triples in $\mathscr{M}$, we can obtain its vector by subtracting those above (depending on κ) from $\sum_{\mathbb{F}_p} c_{\mathscr{M}}(\alpha)\mathbf{x}(\alpha)$. Hence we define

$$\begin{aligned}
\mathbf{y}_{\mathscr{M}} &:= \sum_{\alpha\in\mathbb{F}_p} c_{\mathscr{M}}(\alpha)\mathbf{x}(\alpha) \\
&= \sum_{\alpha\in\mathbb{F}_p} (p - \chi(\alpha^2-4)) \sum_{i=0}^{p-1} \alpha^i \mathbf{e}_i^T && \text{by Corollary 4.2} \\
&= -\sum_{i=0}^{p-1} \left(\sum_{\alpha\in\mathbb{F}_p} (1+\chi(\alpha^2-4))\alpha^i \right) \mathbf{e}_i^T && \text{since } \textstyle\sum_{\mathbb{F}_p} \alpha^i = 0 \\
&= -\sum_{i=0}^{p-1} \left(\sum_{\zeta\in\mathbb{F}_p^\times} (\zeta+\zeta^{-1})^i \right) \mathbf{e}_i^T && \text{by setting } \alpha = \zeta+\zeta^{-1} \\
&= 2\mathbf{e}_{p-1} + \sum_{i=0}^{\frac{p-1}{2}} \binom{2i}{i} \mathbf{e}_{2i}^T && \text{since } \textstyle\sum_{\mathbb{F}_p^\times} \zeta^i = 0 \text{ if } p-1 \nmid i.
\end{aligned} \tag{4.2}$$

Theorem 4.7. *Let p be prime, let $\kappa \in \mathbb{F}_p\backslash\{4\}$, and for $\alpha \in \mathbb{F}_p$ let $\delta_\alpha = 1$ if α is a square and 0 otherwise. Theorem 1.1 (or the Q-Classification Conjecture) holds if and only if $\mathscr{P}^{\perp}(\mathbb{F}_p)$ is the span of*

(1) $\mathbf{y}_{\mathscr{M}}$ and $\delta_\kappa \mathbf{y}_\kappa$ when $\kappa \neq 2, 3, 2+\varphi, 2+\overline{\varphi}$,
(2) $\mathbf{y}_{\mathscr{M}}$, $\delta_\kappa \mathbf{y}_\kappa$, and $\mathbf{y}_1$ when $\kappa = 2$,
(3a) $\mathbf{y}_{\mathscr{M}}$, $\delta_\kappa \mathbf{y}_\kappa$, and $\mathbf{y}_\varphi$ when $\kappa = 2+\varphi$,
(3b) $\mathbf{y}_{\mathscr{M}}$, $\delta_\kappa \mathbf{y}_\kappa$, and $\mathbf{y}_{\overline{\varphi}}$ when $\kappa = 2+\overline{\varphi}$, or

(4) $\mathbf{y}_{\mathscr{M}}$, $\delta_\kappa \mathbf{y}_\kappa$, $\delta_2 \mathbf{y}_2$, *and* $\delta_5 \mathbf{y}_5$ *when* $\kappa = 3$.

Proof. Assume the Q-Classification Conjecture holds (which is slightly weaker than assuming Theorem 1.1 holds, because the group in Theorem 1.1 is generated by Vieta involutions alone). Then every Γ-orbit in $\mathscr{M}(\mathbb{F}_p)$ is either one of the nonessential subsets explicitly listed in cases (1–4b) of Theorem 2.5 or else the complement (in $\mathscr{M}(\mathbb{F}_p)$) of their union. The vectors that Lemma 4.6 associates to these orbits have been listed in cases (1–4) of the present theorem. Note that vectors corresponding to an orbit that only exists for certain p, namely $\mathbf{y}_\kappa$, $\mathbf{y}_2$, and $\mathbf{y}_5$, have been scale by a δ-value accordingly.

Conversely, assume that $\mathscr{P}^\perp(\mathbb{F}_p)$ is the span indicated in one of the cases (1–4), depending on κ. Let $\mathscr{O}$ be a nonempty Γ-orbit in $\mathscr{M}(\mathbb{F}_p)$. Assuming $p \geq 13$, we may fix a primitive root ζ for $\mathbb{F}_p^\times$ such that $\tilde{\alpha} \coloneqq \zeta + \zeta^{-1}$ is neither 0, ± 1, $\pm\sqrt{2}$, $\pm\sqrt{\kappa}$, $\pm\varphi$, nor $\pm\overline{\varphi}$. By Corollary 4.3, $\mathscr{O}$ either contains every triple with first coordinate $\tilde{\alpha}$ or none of them. In other words, either $c_{\mathscr{O}}(\tilde{\alpha}) = c_{\mathscr{M}}(\tilde{\alpha})$ or $c_{\mathscr{O}}(\tilde{\alpha}) = 0$. Suppose the latter occurs. Let us consider how $\sum_{\mathbb{F}_p} c_{\mathscr{O}}(\alpha)\mathbf{x}(\alpha)$, which belongs to $\mathscr{P}^\perp(\mathbb{F}_p)$ by Lemma 4.6, could possibly be expressed as a linear combination of the spanning vectors in any of the cases (1–4). The vectors $\mathbf{x}(\alpha)$ for $\alpha \in \mathbb{F}_p$ form a basis for $\mathbb{F}_p^p$. With respect to this basis, the coefficient of $\mathbf{x}(\tilde{\alpha})$ is 0 in each of the listed $\mathscr{P}^\perp(\mathbb{F}_p)$ spanning vectors except for $\mathbf{y}_{\mathscr{M}}$, because we insisted that $\tilde{\alpha}$ is neither 0, ± 1, $\pm\sqrt{2}$, $\pm\sqrt{\kappa}$, $\pm\varphi$, nor $\pm\overline{\varphi}$. Thus the assumption $c_{\mathscr{O}}(\tilde{\alpha}) = 0$ means $\mathbf{y}_{\mathscr{M}}$ must not appear when $\sum_{\mathbb{F}_p} c_{\mathscr{O}}(\alpha)\mathbf{x}(\alpha)$ is written as a combination of spanning vectors. In particular, $\sum_{\mathbb{F}_p} c_{\mathscr{O}}(\alpha)\mathbf{x}(\alpha)$ is a combination of only $\mathbf{x}(0)$, $\mathbf{x}(\pm 1)$, $\mathbf{x}(\pm\sqrt{2})$, $\mathbf{x}(\pm\sqrt{\kappa})$, $\mathbf{x}(\pm\varphi)$, and $\mathbf{x}(\pm\overline{\varphi})$, meaning $c_{\mathscr{O}}(\alpha) \equiv 0 \bmod p$ for all $\alpha \in \mathbb{F}_p \backslash \{0, \pm 1, \pm\sqrt{2}, \pm\sqrt{\kappa}, \pm\varphi, \pm\overline{\varphi}\}$. Corollary 4.2 tells us that $0 \bmod p$ occurrences implies no occurrences. That is, all triple entries in $\mathscr{O}$ must belong to $\{0, \pm 1, \pm\sqrt{2}, \pm\sqrt{\kappa}, \pm\varphi, \pm\overline{\varphi}\}$. But all such orbits have been listed in Theorem 2.5, and they are nonessential. This proves that any Γ-orbit of essential triples must contain the unique first-coordinate orbit of $\tilde{\alpha}$, implying the uniqueness of such an orbit. This almost shows that Theorem 1.1 (and the slightly weaker Q-Classification Conjecture) holds—it remains only to note that the unique Γ-orbit of essential triples remains unique even if we do not include the double sign change or coordinate permutations as generators in Γ (compare Notation 3.1 to Theorem 1.1). The subgroup of Γ generated by Vieta involutions is normal. Furthermore, the parameterizations in Proposition 4.1 show that if $4 \,|\, \mathrm{ord}(\alpha)$ (so that $\zeta^{2n} = -1$ for some n), then $(\alpha, -\beta, -\gamma)$ can be obtained from (α, β, γ) by way of Vieta involutions alone. Also, for each of τ_x, τ_y, and τ_z, there is some essential triple that the transposition preserves. Thus if there were multiple orbits of essential triples under the group generated by Vieta involutions, they would not collapse into a single Γ-orbit. □

5. Properties of Φ and Φ_x

5.1. **Degree bounds and the canonical form.** Let R be an integral domain with $\mathrm{char}(R) \neq 2$.

Proposition 5.1. *For any integers* $\ell, m, n \geq 0$, *the degree of* $\Phi(x^\ell y^m z^n)$ *is at most* $\max\{\ell, n, m\} + \min\{\ell, m, n\}$, *with equality if* $\ell \equiv m \equiv n \bmod 2$ *and* $\mathrm{char}(R) = 0$. *Furthermore* $\Phi(x^\ell y^m z^n)$ *is even if* $\ell \equiv m \equiv n \bmod 2$ *and odd otherwise.*

Proof. The proof proceeds by induction on the total degree $\ell + m + n$. The claim is clear in the base case, which is total degree 0.

Assume without loss of generality that $\ell \geq m \geq n \geq 0$. If $m = n = 0$, then $\Phi(x^\ell) = x^\ell$, and the proposition follows without any induction hypothesis needed.

If $n = 0$ but $m > 0$, then our first Φ reduction step is

$$\sigma_z(x^\ell y^m) = 2x^{\ell-1}y^{m-1}z. \tag{5.1}$$

Comparing the sum of maximum and minimum exponents from either side above, we have $\ell + 0 \geq (\ell - 1) + \min\{m - 1, 1\}$, with equality if m is even. Furthermore, exponents on the left side above (which includes $n = 0$) are all congruent $\bmod 2$ if and only if exponents on the right are all congruent $\bmod 2$. So the proposition follows by the induction hypothesis.

Finally, if $n > 0$, then our first Φ reduction step is

$$\rho(x^\ell y^m z^n) = x^{\ell-1}y^{m-1}z^{n-1}(x^2 + y^2 + z^2 - \kappa). \tag{5.2}$$

After expanding the right side, the sum of the maximum and minimum exponents in each monomial is at most $\ell + n$, with equality holding for at least the monomial $x^{\ell+1}y^{m-1}z^{n-1}$. And again, congruence of exponents $\bmod 2$ has been preserved. We are done by induction. □

Proposition 5.2. *For any integers $\ell, m, n \geq 0$, the degree in x of $\Phi_x(x^\ell y^m z^n)$ is at most $\ell + \min\{m, n\}$, and the degree in y and z combined is at most $m + n$. Furthermore $\Phi(x^\ell y^m z^n)$ is even if $\ell \equiv m \equiv n \bmod 2$ and odd otherwise.*

Proof. As in the previous proposition, the claim follows from comparing degrees on either side of (5.1) or (5.2) and applying induction. □

It is much easier to find formulas for $\Phi(x^\ell y^m z^n)$ when one of the exponents is 0. We can rewrite polynomials in x and y only by solving the Markoff equation for z:

$$z = \frac{1}{2}\left(xy + \sqrt{x^2y^2 - 4(x^2 + y^2 - \kappa)}\right) \tag{5.3}$$

for some choice of square root. Thus z and $xy - z$ are conjugate with respect to the square root, meaning $f(x, y, z) + f(x, y, xy - z)$ is a polynomial in x and y alone.

Definition 5.3. The *canonical form* of $f \in R[x, y, z]$ is $f^*(x, y) = \frac{1}{2}(f(x, y, z) + f(x, y, xy - z)) \in R[\frac{1}{2}, x, y]$.

The extended coefficient ring $R[\frac{1}{2}]$ for f^* is due to the $\frac{1}{2}$ in (5.3).

Proposition 5.4. *The canonical form of $x^\ell y^m z^n$ has degree $\ell + n$ in x and degree $m + n$ in y. Furthermore, if $f(x)$ denotes the coefficient of y^{m+n} in the canonical form, then $2^n f(x) \equiv x^{\ell+n} \bmod (x^2 - 4)$ in $R[x]$, and the coefficient of $x^{\ell+n}$ in $f(x)$ is 1 if $n = 0$ and $\frac{1}{2}$ if $n \geq 1$.*

Proof. The claim is clear if $n = 0$ since $x^\ell y^m$ is its own canonical form, so assume $n \geq 1$. By expanding (5.3) raised to the power n, the canonical form of $x^\ell y^m z^n$ is

$$\frac{x^\ell y^m}{2^n} \sum_{j=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2j} (xy)^{n-2j}(x^2y^2 - 4(x^2 + y^2 - \kappa))^{2j}.$$

The leading term in the summand with index j is $\binom{n}{2j}x^n y^n$. The sum of every other n^{th} binomial coefficient is 2^{n-1} when $n \geq 1$, so the leading coefficient of $f(x)$ (notation from the proposition statement) is $\frac{2^{n-1}}{2^n} = \frac{1}{2}$ as claimed. Finally, notice in the factor $x^2y^2 - 4(x^2 + y^2 - \kappa)$ that the coefficient of y^2 is $x^2 - 4$. So only the summand with index $i = 0$ picks up y^n with a nonzero coefficient modulo $x^2 - 4$. □

Proposition 5.5. *For any $f \in R[x,y,z]$, $\Phi_x(f^*) = \Phi_x(f)$.*

Proof. Both canonicalization and Φ_x are linear over R, so we need only check the claim when $f = x^\ell y^m z^n$. If $n = 0$ then $f^* = f$, so $\Phi_x(f^*) = \Phi_x(f)$. If $n = 1$ then $f^* = \frac{1}{2}x^{\ell+1}y^{m+1}$, and since $\sigma_z(\frac{1}{2}x^{\ell+1}y^{m+1}) = x^\ell y^m z = f$, we see that $\Phi_x(f^*) = \Phi_x(f)$ in this case as well. If $n \geq 2$, let $g = x^\ell y^m z^{n-2}(xyz + \kappa - x^2 - y^2)$. Then $g - f$ is identically 0 on $\mathscr{M}(R)$ for any R, so $g^* = f^*$. But now observe that the image of g under ρ is $x^\ell y^m z^{n-2}(\rho(xyz) + \kappa - x^2 - y^2) = x^\ell y^m z^n$, so $\Phi_x(g) = \Phi_x(f)$. By induction on the degree of z, we may assume that $\Phi_x(g^*) = \Phi_x(g)$, from which $\Phi_x(f^*) = \Phi_x(f)$ follows. □

5.2. **Partial formulas for $\Phi(f)$.** Given $f \in R[x,y,z]$, our goal is to find a formula for as many coefficients of $\Phi(f)$ as possible. We achieve this for generic f in Theorem 5.11. Another formula for special f is presented in Theorem 5.14.

We start by observing that (3.2) and (3.5), which state that Φ and Φ_x preserve certain sums, are special cases (namely the counting measure) of the following:

Proposition 5.6. *Let $\mathcal{O} \subset \mathscr{M}(R)$ be Γ-invariant, respectively Γ_x-invariant, and let dA be a Γ-invariant, respectively Γ_x-invariant, measure on $\mathcal{O}$. Then*

$$\int_{\mathcal{O}} f dA = \int_{\mathcal{O}} \Phi(f) dA, \text{ respectively } \int_{\mathcal{O}} f dA = \int_{\mathcal{O}} \Phi_x(f) dA,$$

for any $f \in R[x,y,z]$

Proof. The only reduction steps for which it is unclear whether the integral is preserved are σ_x, σ_y, and σ_z. The proof in those cases is identical to (3.1) with integrals in place of sums. □

Notation 5.7. For a fixed $\kappa \in (0,4)$, let $\mathscr{M}^\circ$ denote the compact connected component $\mathscr{M}(\mathbb{R})$ with outward orientation. For $\alpha \in (-\sqrt{\kappa}, \sqrt{\kappa})$, let $\mathcal{O}_\alpha^\circ := \{(x,y,z) \in \mathscr{M}^\circ \mid x = \alpha\}$ with counterclockwise orientation from the perspective of the positive x-axis. We write $\mathcal{O}_x^\circ$ to indicate a generic loop.

The 2-form

$$dA := \frac{dx \wedge dy}{2z - xy} = \frac{dy \wedge dz}{2x - yz} = \frac{dz \wedge dx}{2y - xz}$$

is integrable and nonnegative on $\mathscr{M}^\circ$. Furthermore, the measure defined by integrating dA is Γ-invariant. (The measure is also known to be ergodic for the action of Γ. See [Gol03], [CL09], and especially [Gol97, Section 5].) There is also a Γ_x-invariant line measure on any $\mathcal{O}_\alpha^\circ$ defined by the 1-form

$$dA_\alpha := \frac{dy}{\alpha y - 2z} = \frac{dz}{2y - \alpha z}.$$

As with $\mathcal{O}_x^\circ$, we write dA_x for generic x. Since the 1-form does not appear alongside the 2-form in the literature, we provide a brief proof.

Proposition 5.8. *Each $\mathcal{O}_x^\circ$ is parameterized by*

$$(x,y,z) = \left(2\cos\theta, 2\sqrt{\frac{x^2-\kappa}{x^2-4}}\cos\phi, 2\sqrt{\frac{x^2-\kappa}{x^2-4}}\cos(\theta+\phi)\right)$$

for $\phi \in [0, 2\pi)$. With respect to this parameterization, $\sqrt{4-x^2}dA_x = d\phi$, which induces a Γ_x-invariant measure on $\mathcal{O}_x^\circ$ via integration.

Proof. For the parameterization, note that for any $\alpha \in (-\sqrt{\kappa}, \sqrt{\kappa})$, $\mathcal{O}_\alpha$ is parameterized by case (1) of Proposition 4.1. We have simply rewritten $\zeta + \zeta^{-1}$ and $\zeta^n \vartheta + \zeta^{-n}\vartheta^{-1}$ as $2\cos\theta$ and $2\cos\phi$, respectively.

Now that we have the parameterization, the formula for dA_x can be checked by differentiating. We omit details.

Let us check Γ_x-invariance. The effect of τ_x, σ_z, and $(x, y, z) \mapsto (x, -y, -z)$ on ϕ are $\phi \mapsto \theta + \phi$, $\phi \mapsto \phi$, and $\phi \mapsto \phi + \pi$, respectively. All are shifts, for which $d\phi$ is invariant. Since those three maps generate Γ_x, this shows $d\phi$ (and thus dA_x) is Γ_x-invariant.

Finally, $d\phi$ (and thus dA_x) induces a Γ_x-invariant measure because it is nonvanishing. Our choice of orientation for $\mathcal{O}_x^\circ$ agrees with increasing ϕ. □

The whole point of switching to $\mathbb{R}$ is to utilize the fundamental theorem of calculus.

Corollary 5.9. *For any $m \geq 0$,*

$$\frac{\sqrt{4-x^2}}{2\pi} \int_{\mathcal{O}_x^\circ} y^{2m}\, dA_x = \binom{2m}{m} \left(\frac{x^2-\kappa}{x^2-4}\right)^m.$$

Proof. This is checked by direct computation: replace $\sqrt{4-x^2}dA_x$ with $d\phi$ and y^{2m} with $(\frac{x^2-\kappa}{x^2-4})^m(2\cos\phi)^{2m}$ and antidifferentiate over the interval $[0, 2\pi)$ with respect to ϕ. □

To see why this is useful, let $f \in R[x, y]$, and suppose for the sake of simplicity that $\Phi_x(f)$, which generally lies in $\mathbb{R}[x] + \mathbb{R}[y, z]$, is a polynomial in x only. Then

$$\begin{aligned}
\frac{\sqrt{4-x^2}}{2\pi} \int_{\mathcal{O}_x^\circ} f\, dA_x &= \frac{\sqrt{4-x^2}}{2\pi} \int_{\mathcal{O}_x^\circ} \Phi_x(f)\, dA_x && \text{by Proposition 5.6} \\
&= \frac{\Phi_x(f)\sqrt{4-x^2}}{2\pi} \int_{\mathcal{O}_x^\circ} dA_x && \text{since } \Phi_x(f) \text{ is constant on } \mathcal{O}_x^\circ \\
&= \Phi_x(f) && \text{by Corollary 5.9.}
\end{aligned}$$

But it is no more trouble to instead evaluate the original integral directly with Corollary 5.9, the result being some rational function, say $g(x)$. We can then expand the denominator of $g(x)$ with Taylor series, thereby solving for the coefficients of $\Phi_x(f)$.

It is convenient to expand $g(x)$ with respect to the following basis.

Notation 5.10. For $n \geq 0$, let

$$b_n(x) = \sum_{j=0}^{n} \binom{2j}{j} \frac{x^{n-j}}{1-2j}.$$

The coefficients are those in the McClaurin series for $\sqrt{1-4x}$. In other words,

$$\left(1 - \frac{4}{x}\right)^{\frac{1}{2}} x^n = b_n(x) + \sum_{j=1}^{\infty} \binom{2j}{j} \frac{x^{-j}}{1-2j}. \tag{5.4}$$

The series expansion of $\sqrt{1-4x}$ is just one from a family of expansions that we need. Recall that for any $\alpha \in \mathbb{R}$, the coefficient of x^j in the McClaurin series

expansion of $(1-4x)^\alpha$ is $(-4)^j\alpha(\alpha-1)\cdots(\alpha-j+1)/j!$. When $\alpha = m-\frac{1}{2}$ for some integer m, we may rewrite these coefficients as follows:

$$\prod_{i=1}^{j}\frac{1}{i}(4i-4m-2) = \begin{cases} \binom{-2m}{-m}^{-1}\binom{j-m}{j}\binom{2j-2m}{j-m} & m\le 0, \\ (-1)^m\binom{2m}{m}\binom{j}{m}^{-1}\binom{2j-2m}{j-m} & 0\le m\le j, \\ (-1)^j\binom{2m}{m}\binom{m}{j}\binom{2m-2j}{m-j}^{-1} & m\ge j. \end{cases} \tag{5.5}$$

Theorem 5.11. *Over any integral domain R and for any integers $m,n\ge 0$,*

$$\Phi(x^{2n}y^{2m}) = \sum_{j=0}^{n}\sum_{i=0}^{j}\binom{2m+2i}{m+i}\binom{m+i}{m}\binom{m}{j-i}(-\kappa)^{j-i}b_{n-j}(x^2)+r(x^2)$$

for some $r(x^2)\in R[x]$ of degree at most $2m$.

Proof. As per Proposition 5.2, $\Phi_x(x^{2n}y^{2m})$ is of the form $f(x^2)+g(y^2,z^2)$, where $g(y^2,z^2)$ has total degree at most $2m$. Thus

$$\begin{aligned}\Phi(x^{2n}y^{2m}) &= \Phi(\Phi_x(x^{2n}y^{2m})) \\ &= \Phi(f(x^2)+g(y^2,z^2)) \\ &= f(x^2)+\Phi(g(y^2,z^2)).\end{aligned} \tag{5.6}$$

Proposition 5.4 tells us we may write the canonical form of g as $g^* = g_m(x^2)y^{2m}+g_{m-1}(x^2)y^{2m-2}+\cdots+g_0(x^2)$ with $\deg g_j\le 2m$ for all j. Now we restrict to $R=\mathbb{R}$. Applying Corollary 5.9 to each power of y in g^* gives

$$\begin{aligned} f(x^2)+\sum_{j=0}^{m}\binom{2j}{j}\left(\frac{x^2-\kappa}{x^2-4}\right)^j g_j(x^2) &= \frac{\sqrt{4-x^2}}{2\pi}\int_{\mathcal{O}_x^\circ}(f(x^2)+g^*(x^2,y^2))dA_x \\ &= \frac{\sqrt{4-x^2}}{2\pi}\int_{\mathcal{O}_x^\circ}(f(x^2)+g(y^2,z^2))dA_x && \text{as } \mathcal{O}_x^\circ \text{ and } dA_x \text{ are } \sigma_z\text{-invariant} \\ &= \frac{\sqrt{4-x^2}}{2\pi}\int_{\mathcal{O}_x^\circ}\Phi_x(x^{2n}y^{2m})dA_x \\ &= \frac{\sqrt{4-x^2}}{2\pi}\int_{\mathcal{O}_x^\circ}x^{2n}y^{2m}dA_x && \text{by Proposition 5.6} \\ &= \binom{2m}{m}\frac{x^{2n}(x^2-\kappa)^m}{(x^2-4)^m} && \text{by Corollary 5.9.} \\ &= \binom{2m}{m}\frac{x^{2n}(1-\frac{4}{x^2})^{\frac{1}{2}}(1-\frac{\kappa}{x^2})^m}{(1-\frac{4}{x^2})^{m+\frac{1}{2}}} \\ &= \binom{2m}{m}\left(1-\frac{4}{x^2}\right)^{\frac{1}{2}}\sum_{i=0}^{m}\binom{m}{i}\frac{(-\kappa)^{m-i}x^{2n-2m+2i}}{(1-\frac{4}{x^2})^{m+\frac{1}{2}}}. \end{aligned} \tag{5.7}$$

While the entire chain of equalities above only holds when $x\in(-\sqrt{\kappa},\sqrt{\kappa})\backslash\{0\}$ and $\kappa\in(0,4)$, it implies equality of the two rational functions at the start and end of the

chain. We continue this chain by applying the McClaurin series for $(1-\frac{4}{x^2})^{-m-\frac{1}{2}}$ to obtain the following expression, convergent for $|x|>2$:

$$\binom{2m}{m}\left(1-\frac{4}{x^2}\right)^{\frac{1}{2}}\sum_{i=0}^{m}\binom{m}{i}\frac{(-\kappa)^{m-i}x^{2n-2m+2i}}{(1-\frac{4}{x^2})^{m+\frac{1}{2}}}$$
$$=\left(1-\frac{4}{x^2}\right)^{\frac{1}{2}}\sum_{i=0}^{m}\binom{m}{i}(-\kappa)^{m-i}\sum_{j=m-i}^{\infty}\binom{2i+2j}{i+j}\binom{i+j}{m}x^{2n-2j}$$

After expanding the square root above, (5.4) tells us that the coefficients of non-negative powers of x match those of

$$\sum_{i=0}^{m}\binom{m}{i}(-\kappa)^{m-i}\sum_{j=m-i}^{n}\binom{2i+2j}{i+j}\binom{i+j}{m}b_{n-j}(x^2)$$
$$=\sum_{j=0}^{n}\sum_{i=m-j}^{m}\binom{2i+2j}{i+j}\binom{i+j}{m}\binom{m}{i}(-\kappa)^{m-i}b_{n-j}(x^2)$$
$$=\sum_{j=0}^{n}\sum_{i=0}^{j}\binom{2m+2i}{m+i}\binom{m+i}{m}\binom{m}{j-i}(-\kappa)^{j-i}b_{n-j}(x^2).$$

Now we connect all the way back to the start of (5.7). Each rational function $(\frac{x^2-\kappa}{x^2-4})^j g_j(x^2)$ can be expressed as a Laurent polynomial in $\frac{1}{x^2}$ in which the largest power of x is $\deg g_j$, which we know to be at most $2m$. So the difference between $f(x^2)$ and the final expression above is some combination of powers x^{2j} with $-\infty < j \le m$ that converges when $|x|>2$. Therefore, we have found the first $n-m$ coefficients of $f(x^2)$ (written in terms of $b_{n-j}(x^2)$). According to (5.6), these must also be the first $n-m$ coefficients of $\Phi(x^{2m}y^{2n})$ because $\deg\Phi(g)\le 2m$ by Proposition 5.1.

The argument above applies to $R=\mathbb{R}$. However, only integer coefficients are used throughout the reduction of a monic monomial, and $\mathbb{Z}$ is the initial object in the category of integral domains. Thus the formula holds for general R. □

As a small example to test, consider $n=3$ and $m=1$:

$$\Phi(x^6y^2)=2x^6+(8-2\kappa)x^4+(96-8\kappa)x^2-32\kappa$$
$$=2b_3(x^2)+(12-2\kappa)b_2(x^2)+(124-12\kappa)b_1(x^2)+280-60\kappa.$$

If we ignore the remainder polynomial $r(x^2)$, Theorem 5.11 provides the following formula:

$$\binom{2}{1}b_3(x^2)+\left(\binom{4}{2}\binom{2}{1}-\binom{2}{1}\kappa\right)b_2(x^2)$$
$$+\left(\binom{6}{3}\binom{3}{1}-\binom{4}{2}\binom{2}{1}\kappa\right)b_1(x^2)+\left(\binom{8}{4}\binom{4}{1}-\binom{6}{3}\binom{3}{1}\kappa\right)b_0(x^2)$$

The coefficients of $b_3(x^2)$ and $b_2(x^2)$ above are correct, but the coefficient of $b_1(x^2)$ is not. The polynomial $r(x^2)$ accounts for this error. Note that the coefficient of $b_0(x^2)$ happens to be correct as well. Interestingly, experimentation suggests that Theorem 5.11's formula for the coefficient of $b_0(x^2)$ is always right.

The same basic argument can be used to prove the simpler (though, in our case, less useful) formula

$$\Phi(x^{2m}(y^2-\kappa)^{n-m}(y^2-4)^m) = \binom{2m}{m}(x^2-\kappa)^n + r(x^2) \tag{5.8}$$

for some $r(x^2) \in R[x]$ of degree at most $2m$.

As (5.8) suggests, a Φ input that is divisible by high powers of x^2-4 or y^2-4 lends itself to a clean output formula. Theorem 5.14 below provides such a specialized formula written with respect to the basis $b_0(x^2), b_1(x^2), b_2(x^2), \ldots$. It is possible to prove Theorem 5.14 directly from (5.8), but the proof (at least the one the author found) is far messier and requires many combinatorial identities. The approach taken here only requires the one additional identity in the next lemma.

Notation 5.12. Let n be an integer. For a fixed integral domain R let

$$\Lambda_n = \{\zeta + \zeta^{-1} \,|\, \zeta \in \overline{R},\, \zeta^{2n} = 1\} \quad \text{and} \quad \widehat{\Lambda}_n = \Lambda_n \backslash \{\pm 2\}.$$

Lemma 5.13. *Let ℓ, m, and n be integers with $\ell \geq 0$, $m \geq 1$, and $n > \ell + m$. The coefficient of $x^{\ell+m}$ in the McClaurin series expansion of $(1-4x)^{m-\frac{1}{2}}$ is*

$$\frac{1}{n}\sum_{\alpha \in \widehat{\Lambda}_n} \alpha^{2\ell}(\alpha^2-4)^m.$$

Proof. Let us rewrite the sum over α as a sum over $\zeta^j + \zeta^{-j}$, where ζ is a primitive $2n^{\text{th}}$ root of unity:

$$\frac{1}{n}\sum_{\alpha \in \widehat{\Lambda}_n} \alpha^{2\ell}(\alpha^2-4)^m = \frac{1}{n}\sum_{j=1}^{n-1} \frac{(\zeta^{2j}+1)^{2\ell}(\zeta^{2j}-1)^{2m}}{\zeta^{2j(\ell+m)}}.$$

The right-side is the average of the Laurent polynomial $x^{-\ell-m}(x+1)^{2\ell}(x-1)^{2m}$ as x runs over all n^{th} roots of unity (including $x=1$ dispite the restriction $1 \leq j \leq n-1$; indeed $x^{-\ell-m}(x+1)^{2\ell}(x-1)^{2m}$ vanishes when $x=1$ since $m \geq 1$). But exponents of x in this Laurent polynomial are at most $\ell+m$ in magnitude, which is strictly less than n, so this average picks up only the coefficient of x^0. In other words, the expression above is the coefficient of $x^{\ell+m}$ in the polynomial $(x+1)^{2\ell}(x-1)^{2m}$, which can be evaluated with Kummer's identity for hypergeometric functions:

$$\begin{aligned}
&\sum_{i=0}^{\ell+m}(-1)^i\binom{2\ell}{\ell+m-i}\binom{2m}{i} \\
&\quad = \binom{2m}{\ell+m}\,{}_2F_1(-\ell-m, -2\ell; m-\ell+1; -1) && \text{(assuming } \ell \leq m\text{)} \\
&\quad = \binom{2m}{\ell+m}\frac{(-1)^m(2\ell)!(m-\ell)!}{\ell!\,m!} && \text{by Kummer's identity.}
\end{aligned}$$

If $\ell > m$, the roles of ℓ and m may be reversed to apply Kummer's identity, arriving at the same final expression either way. This matches the second case of (5.5) with i replaced by $\ell+m$. □

Theorem 5.14. *Let $f(y^2) \in R[y]$, and let $m \geq 0$ be such that $(y^2-4)^m \mid f(y^2)$. For any positive integers $\tilde{n} \geq n$ with $\operatorname{char}(R) \nmid \tilde{n}$,*

$$\Phi(x^{2n} f(y^2)) = \frac{1}{\tilde{n}} \sum_{j=0}^{n} \binom{2j}{j} \sum_{\alpha \in \widehat{\Lambda}_{\tilde{n}}} \left(\frac{\alpha^2 - \kappa}{\alpha^2 - 4} \right)^j f(\alpha^2) b_{n-j}(x^2) + r(x^2)$$

for some $r(x^2) \in R[x]$ of degree at most $\max(\deg f(y^2), 2n - 2m)$.

Proof. It suffices to consider polynomials of the form $f(y^2) = y^{2\ell}(y^2-4)^m$.

We start by expanding $x^{2n} y^{2\ell} (y^2-4)^m$ and applying Theorem 5.11 to each of the resulting monomials. This gives the following expression for the coefficient of $b_{n-j}(x^2)$ in $\Phi(x^{2n} y^{2\ell}(y^2-4)^m)$:

$$\begin{aligned}
&\sum_{k=0}^{m} (-4)^{m-k} \binom{m}{k} \sum_{i=0}^{j} \binom{2i+2k+2\ell}{i+k+\ell} \binom{i+k+\ell}{k+\ell} \binom{k+\ell}{j-i} (-\kappa)^{j-i} \\
&= \sum_{k=0}^{m} (-4)^{m-k} \binom{m}{k} \sum_{i=0}^{j} \binom{2i+2k+2\ell}{i+k+\ell} \binom{i+k+\ell}{j} \binom{j}{i} (-\kappa)^{j-i} \\
&= \binom{2j}{j} \sum_{i=0}^{j} \binom{j}{i} (-\kappa)^{j-i} \sum_{k=0}^{m} (-4)^{m-k} \binom{m}{k} \left(\binom{2j}{j}^{-1} \binom{2i+2k+2\ell}{i+k+\ell} \binom{i+k+\ell}{j} \right),
\end{aligned}$$

which holds provided $n - j > \ell + m$ (otherwise Theorem 5.11 tells us nothing about the coefficient of $b_{n-j}(x^2)$).

Now we restrict to $R = \mathbb{R}$. Recall from the first case in (5.5) that the final parenthesized product of binomial coefficients above is the coefficient of $x^{i-j+k+\ell}$ in the McClaurin series of $(1-4x)^{-j-\frac{1}{2}}$. But observe that $\sum_k (-4x)^{m-k} \binom{m}{k} = (1-4x)^m$, so the entire inner sum in the final expression above is the coefficient of $x^{i-j+\ell+m}$ in the McClaurin series of $(1-4x)^{m-j-\frac{1}{2}}$. When $m - j \geq 1$ and $\tilde{n} > i - j + \ell + m$, we have a formula for this coefficient from Lemma 5.13. Picking up where we left off with the final line above, we have shown

$$\begin{aligned}
&\sum_{i=0}^{j} \binom{j}{i} (-\kappa)^{j-i} \sum_{k=0}^{m} (-4)^{m-k} \binom{m}{k} \binom{2i+2k+2\ell}{i+k+\ell} \binom{i+k+\ell}{j} \\
&\qquad = \frac{1}{\tilde{n}} \binom{2j}{j} \sum_{i=0}^{j} \binom{j}{i} (-\kappa)^{j-i} \sum_{\alpha \in \widehat{\Lambda}_{\tilde{n}}} \alpha^{2i+2\ell} (\alpha^2-4)^{m-j} \\
&\qquad = \frac{1}{\tilde{n}} \binom{2j}{j} \sum_{\alpha \in \widehat{\Lambda}_{\tilde{n}}} \alpha^{2\ell} (\alpha^2-4)^{m-j} \sum_{i=0}^{j} \binom{j}{i} \alpha^{2i} (-\kappa)^{j-i} \\
&\qquad = \frac{1}{\tilde{n}} \binom{2j}{j} \sum_{\alpha \in \widehat{\Lambda}_{\tilde{n}}} \alpha^{2\ell} (\alpha^2-4)^{m-j} (\alpha^2-\kappa)^j \\
&\qquad = \frac{1}{\tilde{n}} \binom{2j}{j} \sum_{\alpha \in \widehat{\Lambda}_{\tilde{n}}} \left(\frac{\alpha^2-\kappa}{\alpha^2-4} \right)^j f(\alpha^2).
\end{aligned}$$

This is the desired expression for the coefficient of $b_{n-j}(x^2)$. For this to hold, recall that the necessary inequalities are $n - j > \ell + m$, $m - j > 0$, and $\tilde{n} >$

$i-j+\ell+m$, which (since $\tilde{n} \geq n$) are equivalent to $2n-2j > 2\max(\ell+m, n-m) = \max(\deg y^{2\ell}(y^2-4)^m, 2n-2m)$ as in the theorem statement.

Finally, we remove the restriction to $\mathbb{R}$. Observe that over $\mathbb{Z}$, the only factor in our formula for $\Phi(x^{2n}f(y^2))$ that is not an element of $\overline{\mathbb{Z}}$ is $\frac{1}{\tilde{n}}$ (remember, $(y^2-4)^i$ is assumed to divide $f(y^2)$ when $i \leq m$). Since $\mathrm{char}(R) \nmid \tilde{n}$, this expression is well defined in $\overline{F}$. So because

$$\begin{array}{ccc} \mathbb{Z} & \hookrightarrow & \overline{\mathbb{Q}} \\ \downarrow & & \downarrow \\ R & \hookrightarrow & \overline{F} \end{array}$$

commutes, if arithmetic in $\overline{\mathbb{Q}}$ makes our coefficient of b_{n-j} the correct element of $\mathbb{Z}$, then arithmetic in $\overline{F}$ makes it the correct element of R. □

Consider, for example, the reduction of $x^{10}(y^2-4)^2$, and suppose for simplicity that $\kappa = 1$:

$$\begin{aligned} \Phi(x^{10}(y^2-4)^2) &= 6x^{10} - 12x^8 + 6x^6 + 752x^4 + 6944x^2 - 2560 \\ &= 6b_5(x^2) + 18b_3(x^2) + 812b_2(x^2) + 8664b_1(x^2) + 16632. \end{aligned}$$

If we ignore the remainder polynomial $r(x^2)$, Theorem 5.14 provides the following formulas for the coefficients of $b_5(x^2)$, $b_4(x^2)$, and $b_3(x^2)$:

$$\frac{1}{\tilde{n}}\sum_{\alpha\in\widehat{\Lambda}_{\tilde{n}}}(\alpha^2-4)^2, \quad \frac{2}{\tilde{n}}\sum_{\alpha\in\widehat{\Lambda}_{\tilde{n}}}(\alpha^2-4)(\alpha^2-1), \quad \text{and} \quad \frac{6}{\tilde{n}}\sum_{\alpha\in\widehat{\Lambda}_{\tilde{n}}}(\alpha^2-1)^2$$

for any $\tilde{n} \geq 5$. These equal 6, 0, and $18(1-\frac{3}{\tilde{n}})$, respectively. In particular, the coefficients of $b_5(x^2)$ and $b_4(x^2)$ match, while the coefficient of $b_3(x^2)$ does not. The polynomial $r(x^2)$ accounts for this error because $\max(\deg(y^2-4)^2, 10-4) = 6$.

6. Eigenvectors for $\alpha \neq \pm 2$

As described in Section 3, we aim to build rank in $\mathscr{P}(\mathbb{F}_q)$ by finding polynomials $f \in \overline{\mathbb{Z}}[x,y,z]$ that satisfy $\Phi_x(xf) = \alpha f$ for some $\alpha \in \overline{\mathbb{Z}}$ whose image under a projection $\overline{\mathbb{Z}} \to \overline{\mathbb{F}}_q$ never occurs as an entry in $\mathscr{M}(\mathbb{F}_q)$. An example with $\alpha = 0$ can be found in (3.3).

Although $\overline{\mathbb{Z}}$ is the ring that matters, we continue to work over an arbitrary integral domain R with $\mathrm{char}(R) \neq 2$.

6.1. **Eigenvector existence.** Let $n \geq 1$, and for each $i = 0, ..., n$ define the $(i+1)$-element set

$$\mathscr{B}_{i,n} = \{(x^2-\kappa)^{n-i}y^j z^k \mid j+k = 2i,\ j \geq k\} \subset R[x^2, y, z].$$

Order the elements of $\mathscr{B}_{i,n}$ according to decreasing j/increasing k. Let $\mathscr{B}_n = \cup_i \mathscr{B}_{i,n}$ ordered primarily according to decreasing i, then according to the order on each $\mathscr{B}_{i,n}$. For a linear combination f of elements of $\mathscr{B}_n$, we wish to find another combination from $\mathscr{B}_n$, call it g, satisfying $\Phi_x(xf) = \Phi_x(g)$. From this, the effect of multiplying by x and applying Φ_x can be represented by a matrix whose eigenvectors (with entries corresponding to polynomial coefficients with respect to $\mathscr{B}_n$) are easily computed.

Remark that the sum of degrees in y and z in each monomial is always even. We might also define something like $\widetilde{\mathscr{B}}_{i,n}$ in which y and z degrees sum to $2i+1$, but there would no "interaction" between $\mathscr{B}_n$ and $\widetilde{\mathscr{B}}_n$ (the meaning of this is made

explicit below); we would be doing double the work for nothing—we already know that $\mathscr{P}(R)$ contains all odd degree polynomials anyway due to the inclusion of $(x, y, z) \mapsto (x, -y, -z)$ in Γ. However, the lack of consideration for "$\widetilde{\mathscr{B}}_n$" forces a restricted hypothesis in many of this section's results. Namely, we only prove properties of those $f \in R[x, y, z]$ for which f^* is even as a polynomial in y, as this is true of every monomial in $\mathscr{B}_n$.

Let $i > 0$. Consider what happens when we multiply the first element of $\mathscr{B}_{i,n}$ by x and reduce:

$$x(x^2 - \kappa)^{n-i} y^{2i} \overset{\sigma_z}{\longmapsto} 2(x^2 - \kappa)^{n-i} y^{2i-1} z. \tag{6.1}$$

This is twice the second element of $\mathscr{B}_{i,n}$.

Now consider the $(k+1)^{\text{th}}$ element of $\mathscr{B}_{i,n}$ for $0 < k < 2i$:

$$\begin{aligned} &x(x^2-\kappa)^{n-i} y^j z^k \\ &\qquad \overset{\rho}{\longmapsto} (x^2 - \kappa)^{n-i}(x^2 y^{j-1} z^{k-1} + y^{j+1} z^{k-1} + y^{j-1} z^{k+1} - \kappa y^{j-1} z^{k-1}) \\ &\qquad = (x^2 - \kappa)^{n-i} y^{j+1} z^{k-1} + (x^2 - \kappa)^i y^{j-1} z^{k+1} + (x^2 - \kappa)^{n-i+1} y^{j-1} z^{k-1}. \end{aligned} \tag{6.2}$$

This is the sum of the k^{th} and $(k+2)^{\text{th}}$ elements of $\mathscr{B}_{i,n}$ and the k^{th} element of $\mathscr{B}_{i-1,n}$. Finally, consider the last element of $\mathscr{B}_{i,n}$ (still with $i > 0$):

$$\begin{aligned} x(x^2 - \kappa)^{n-i} y^i z^i &\overset{\rho}{\longmapsto} (x^2 - \kappa)^{n-i}(x^2 y^{i-1} z^{i-1} + y^{i+1} z^{i-1} + y^{i-1} z^{i+1} - \kappa y^{i-1} z^{i-1}) \\ &\overset{\tau_x}{\longmapsto} (x^2 - \kappa)^{n-i}(x^2 y^{i-1} z^{i-1} + 2y^{i+1} z^{i-1} - \kappa y^{i-1} z^{i-1}) \\ &= 2(x^2 - \kappa)^{n-i} y^{i+1} z^{i-1} + (x^2 - \kappa)^{n-i+1} y^{i-1} z^{i-1}. \end{aligned} \tag{6.3}$$

This is twice the penultimate element of $\mathscr{B}_{i,n}$ plus the last element of $\mathscr{B}_{i-1,n}$.

In light of (6.1), (6.2), and (6.3), we define

$$A_0 = [2], \quad A_1 = \begin{bmatrix} 0 & 2 \\ 2 & 0 \end{bmatrix}, \text{ and } A_n = \begin{bmatrix} 2 & 1 & & & & \\ 1 & 1 & \ddots & & & \\ & 1 & \ddots & 1 & & \\ & & \ddots & & 2 & \\ & & & 1 & & \end{bmatrix} \text{ for } n \geq 2, \tag{6.4}$$

where blank entries are 0. These matrices contain the coefficients from those terms in (6.1), (6.2), and (6.3) that come from $\mathscr{B}_{i,n}$, not $\mathscr{B}_{i-1,n}$. To account for the coefficients of terms from $\mathscr{B}_{i-1,n}$, we define the $n \times (n+1)$ matrix

$$B_n = \begin{bmatrix} 0 & 1 & & & \\ 0 & & 1 & & \\ \vdots & & & \ddots & \\ 0 & & & & 1 \end{bmatrix},$$

the $n \times n$ identity matrix with the 0 column appended to its left side. Finally, for $n \geq 0$ let

$$M_n = \begin{bmatrix} A_n & & & & \\ B_n & A_{n-1} & & & \\ & B_{n-1} & \ddots & & \\ & & \ddots & A_1 & \\ & & & B_1 & A_0 \end{bmatrix}. \tag{6.5}$$

This is a square, almost block diagonal matrix over R with $\frac{1}{2}(n^2+3n+2)$ rows and columns.

Note that we have only considered the effect of multiplying by x and applying Φ_x to elements of $\mathscr{B}_{i,n}$ when $i>0$. Regarding $\mathscr{B}_{0,n}=\{(x^2-\kappa)^n\}$, applying Φ_x to $x(x^2-\kappa)^n$ does nothing, and this polynomial does not belong to $\mathscr{B}_n$. In other words, our effort to express $\Phi_x(xf)$ as a linear combination from $\mathscr{B}_n$ fails if the coefficient of $(x^2-\kappa)^n$ in f is nonzero.

Proposition 6.1. *Let $f\in R[x,y,z]$ be a linear combination from $\mathscr{B}_n$ and let $\mathbf{f}$ be the corresponding column vector of coefficients. Then*

$$\Phi_x(xf)=\Phi_x(g)+\omega x(x^2-\kappa)^n,$$

where g is the polynomial corresponding to $M_n\mathbf{f}$ and ω is the last entry of $\mathbf{f}$.

Proof. This is the combination of (6.1), (6.2), and (6.3) and the observation that immediately precedes the proposition. □

In light of Proposition 6.1, the goal is to find eigenvectors $\mathbf{f}$ of M_n with final entry $\omega=0$. This provides polynomials with the following property, which generalizes (3.4) to nonzero α.

Proposition 6.2. *Suppose $f\in R[x,y,z]$ satisfies $\Phi_x(xf)=\alpha\Phi_x(f)$ for some $\alpha\in R$. Then $\sum_{\mathscr{O}_{\tilde{\alpha}}}f(\mathbf{t})=0$ for any finite first-coordinate orbit $\mathscr{O}_{\tilde{\alpha}}$ with $\tilde{\alpha}\neq\alpha$.*

Proof. If $\tilde{\alpha}\neq\alpha$ then

$$\begin{aligned}\sum_{\mathbf{t}\in\mathscr{O}_{\tilde{\alpha}}}f(\mathbf{t})&=\frac{1}{\tilde{\alpha}-\alpha}\sum_{\mathbf{t}\in\mathscr{O}_{\tilde{\alpha}}}(x-\alpha)f(\mathbf{t})\\&=\frac{1}{\tilde{\alpha}-\alpha}\sum_{\mathbf{t}\in\mathscr{O}_{\tilde{\alpha}}}\Phi_x((x-\alpha)f)(\mathbf{t})\\&=\frac{1}{\tilde{\alpha}-\alpha}\sum_{\mathbf{t}\in\mathscr{O}_{\tilde{\alpha}}}(\alpha-\alpha)\Phi_x(f)(\mathbf{t})=0,\end{aligned}$$

as claimed. □

Lemma 6.3. *Suppose* $\mathrm{char}(R)\nmid n$. *Each element of Λ_n is an eigenvalue of A_n. The eigenvector (unique up to scaling) corresponding to $\zeta+\zeta^{-1}$ is*

$$\begin{bmatrix}1\\ \zeta+\zeta^{-1}\\ \zeta^2+\zeta^{-2}\\ \vdots\\ \zeta^{n-1}+\zeta^{1-n}\\ \zeta^n\end{bmatrix}. \tag{6.6}$$

Proof. This claim is a repeated application of

$$(\zeta^{j-1}+\zeta^{1-j})+(\zeta^{j+1}+\zeta^{-j-1})=(\zeta+\zeta^{-1})(\zeta^j+\zeta^{-j})$$

as j ranges over the coordinates of the product of A_n and (6.6). □

Definition 6.4. Define u, v-coordinates on those points $(x, y, z) \in \mathscr{M}(R)$ with $x^2 \neq \kappa, 4$ by

$$(x, y, z) = \left(u + u^{-1}, \sqrt{\frac{\kappa - x^2}{4 - x^2}}(v + v^{-1}), \sqrt{\frac{\kappa - x^2}{4 - x^2}}(uv + u^{-1}v^{-1}) \right).$$

Note that (u, v) and (u^{-1}, v^{-1}) define the same point.

Lemma 6.5. *Let $\alpha \in R$ with $\operatorname{ord}(\alpha) \geq 4$. Suppose $f \in R[x, y, z]$ has canonical form $f^* = f_n(x)y^{2n} + \cdots + f_0(x)$. For $i \geq 0$ define*

$$c_i \coloneqq \begin{cases} 0 & \alpha \notin \Lambda_i, \\ \displaystyle\sum_{j=i}^{n} \binom{2j}{j-i} \left(\frac{\alpha^2 - \kappa}{\alpha^2 - 4} \right)^j f_j(\alpha) & \alpha \in \Lambda_i \backslash \{\pm\sqrt{\kappa}\}, \\ f_i(\alpha) & \alpha = \pm\sqrt{\kappa} \in \Lambda_i. \end{cases} \tag{6.7}$$

Then

$$\frac{1}{|\mathscr{O}_\alpha|} \sum_{\mathbf{t} \in \mathscr{O}_\alpha} f(\mathbf{t}) = \begin{cases} c_0 + \displaystyle\sum_{i=1}^{n} c_i (v^{2i} + v^{-2i}) & \alpha^2 \neq \kappa \\ \displaystyle\sum_{i=0}^{n} c_i y^{2i} & \alpha^2 = \kappa. \end{cases}$$

Remark that the values of y^{2i} and $v^{2i} + v^{-2i}$ are constant on $\mathscr{O}_\alpha$ by Proposition 4.1. The formula above is not ill-defined.

Proof. Consider what happens when $f^* = f_j(x)y^{2j}$ and $\alpha^2 \neq \kappa$. First we switch to u, v-coordinates:

$$\begin{aligned} \frac{1}{|\mathscr{O}_\alpha|} \sum_{\mathbf{t} \in \mathscr{O}_\alpha} f(\mathbf{t}) &= \frac{1}{|\mathscr{O}_\alpha|} \sum_{\mathbf{t} \in \mathscr{O}_\alpha} f_j(\alpha) y^{2j} \\ &= \frac{1}{|\mathscr{O}_\alpha|} \sum_{\mathbf{t} \in \mathscr{O}_\alpha} f_j(\alpha) \left(\frac{\alpha^2 - \kappa}{\alpha^2 - 4} \right)^j (v + v^{-1})^{2j} \\ &= \frac{f_j(\alpha)}{|\mathscr{O}_\alpha|} \left(\frac{\alpha^2 - \kappa}{\alpha^2 - 4} \right)^j \sum_{i=-j}^{j} \binom{2j}{j-i} \sum_{\mathbf{t} \in \mathscr{O}_\alpha} v^{2i}. \end{aligned}$$

By the first case in Proposition 4.1, the v-coordinates in $\mathscr{O}_\alpha$ run over all powers of a $\operatorname{ord}(\alpha)^{\text{th}}$ root of unity (times some constant "ϑ" that depends on exactly which first-coordinate orbit we are in). Thus the inner sum vanishes when $\operatorname{ord}(\alpha) \nmid 2i$. And when $\operatorname{ord}(\alpha) \mid 2i$, the value of v^{2i} is constant on $\mathscr{O}_\alpha$, which cancels the denominator $|\mathscr{O}_\alpha|$. So the lemma holds with the coefficients defined by

$$c_i = \begin{cases} 0 & \alpha \notin \Lambda_i, \\ \displaystyle\binom{2j}{j-i} \left(\frac{\alpha^2 - \kappa}{\alpha^2 - 4} \right)^j f_j(\alpha) & \alpha \notin \Lambda_i \end{cases}$$

for $i \geq 1$. Summing over j for the more general $f^* = f_n(x)y^{2n} + \cdots + f_0(x)$ completes the proof when $\alpha^2 \neq \kappa$.

The argument when $\alpha^2 = \kappa$ is almost identical, just using the second case of Proposition 4.1 rather than the first case. □

Notation 6.6. Given f and α as in Lemma 6.5, let $c_{\alpha,i}(f)$ denote the value of c_i as defined in (6.7).

Note that we are only defining $c_{\alpha,i}(f)$ when f^* is even as a polynomial in y.

Proposition 6.7. *Let $f \in R[x,y,z]$, and suppose f^* is even as a polynomial in y. Then $c_{\alpha,i}(gf) = g(\alpha)c_{\alpha,i}(f)$ for any $g \in R[x]$, $i \geq 0$, and $\alpha \in \overline{R}$.*

Proof. If $f^* = f_n(x)y^{2n} + \cdots + f_0(x)$ then $(gf)^* = g(x)f_n(x)y^{2n} + \cdots + g(x)f_0(x)$. The claim then follows from the formula for $c_{\alpha,i}(gf)$ in (6.7). □

Proposition 6.8. *Suppose* $\mathrm{char}(R) = 0$. *Let $f \in \overline{R}[x,y,z]$ have canonical form $f_n(x)y^{2n} + f_{n-1}(x)y^{2n-2} + \cdots + f_0(x)$. The following are equivalent:*

(1) $f \in \mathscr{P}_x(R,\infty)$ (see Notation 3.6),
(2) $c_{\alpha,i}(f) = 0$ for all but finitely many pairs α, i,
(3) $c_{\alpha,0}(f) = 0$ for all $\alpha \in R$,
(4) $c_{\alpha,0}(f) = 0$ for all but finitely many $\alpha \in R$,
(5) and $\sum_j \binom{2j}{j}(\frac{x^2-\kappa}{x^2-4})^j f_j(x)$ is identically 0.

Proof. First observe that Lemma 6.5 expresses $\sum_{\mathscr{O}_\alpha} f(\mathbf{t})$ in terms of the free variables v and y in an infinite integral domain. So for some fixed α, $\sum_{\mathscr{O}_\alpha} f(\mathbf{t})$ can only vanish for all $\mathscr{O}_\alpha$ if $c_{\alpha,i}(f) = 0$ for all i. In particular, (1) and (2) are equivalent.

Next, (6.7) defines $c_{\alpha,0}(f)$ as the rational expression in (5) evaluated at $x = \alpha$. Any rational expression with infinitely many roots must be identically 0, so (3), (4) and (5) are equivalent, and they and are implied by (1).

To see that (3) implies (2), observe from (6.7) that when $2i > \deg_y f^* = 2n$, $c_{\alpha,i}(f) = 0$ for all $\alpha \in R$. There are only finitely many i with $0 < i \leq n$, and for each one $\widehat{\Lambda}_i$ is finite (crucially using $i > 0$). □

Lemma 6.9. *For any $n \geq 2$ and any $\alpha = \zeta + \zeta^{-1} \in \widehat{\Lambda}_n$,*

$$\prod_{\tilde{\alpha} \in \Lambda_n \setminus \{\alpha\}} (\alpha - \tilde{\alpha}) = 2n\zeta^n.$$

Proof. Let $\tilde{\zeta}$ be a primitive $2n^{\text{th}}$ root of unity, and let $1 \leq i \leq n-1$ satisfy $\tilde{\zeta}^i = \zeta$. We have

$$\begin{aligned}
\prod_{\tilde{\alpha} \in \Lambda_n \setminus \{\alpha\}} (\alpha - \tilde{\alpha}) &= \prod_{\substack{j=0 \\ j \neq i}}^{n} ((\tilde{\zeta}^i + \tilde{\zeta}^{-i}) - (\tilde{\zeta}^j + \tilde{\zeta}^{-j})) \\
&= \prod_{\substack{j=0 \\ j \neq i}}^{n} \zeta^{-1}\big(\tilde{\zeta}^{i+j} - 1\big)\big(\tilde{\zeta}^{i-j} - 1\big) \\
&= \zeta^n(\tilde{\zeta}^i - 1)(\tilde{\zeta}^{i+j} - 1) \prod_{\substack{j=1 \\ j \neq 2i}}^{2n-1} (\tilde{\zeta}^j - 1) \qquad \text{as } \tilde{\zeta}^{i \pm j} \text{ are distinct if } j \neq 0, n \\
&= -\zeta^n(\tilde{\zeta}^{2i} - 1) \prod_{\substack{j=1 \\ j \neq 2i}}^{2n-1} (\tilde{\zeta}^j - 1)
\end{aligned}$$

$$= \zeta^n \prod_{j=1}^{2n-1} (1 - \tilde{\zeta}^j).$$

The final product is $1 + x + \cdots + x^{2n-1}$ evaluated at $x = 1$, which is $2n$. □

Theorem 6.10. *Suppose* $\mathrm{char}(R) \nmid n$. *Let* $\alpha = \zeta + \zeta^{-1} \in \widehat{\Lambda}_n$. *After perhaps scaling (6.6), it extends uniquely to an eigenvector of* M_n *over* $F[\zeta]$ *such that the corresponding (with respect to* $\mathscr{B}_n$*) polynomial* $\not{p}$ *satisfies* $\Phi_x(x\not{p}) = \alpha\Phi_x(\not{p})$ *and*

$$\frac{1}{|\mathscr{O}_\alpha|} \sum_{\mathbf{t} \in \mathscr{O}_\alpha} \not{p}(\mathbf{t}) = \begin{cases} v^{2n} + v^{-2n} & \alpha^2 \neq \kappa \\ y^{2n} & \alpha^2 = \kappa. \end{cases} \tag{6.8}$$

Furthermore, if $\not{p}^* = p_n(x)y^{2n} + \cdots + p_0(x)$, *then*

$$p_n(x) = \begin{cases} \dfrac{\zeta^n}{2n} \left(\dfrac{\alpha^2 - 4}{\alpha^2 - \kappa} \right)^n \displaystyle\prod_{\tilde{\alpha} \in \Lambda_n \setminus \{\alpha\}} (x - \tilde{\alpha}) & \alpha^2 \neq \kappa \\ \dfrac{\zeta^n}{2n} \displaystyle\prod_{\tilde{\alpha} \in \Lambda_n \setminus \{\alpha\}} (x - \tilde{\alpha}) & \alpha^2 = \kappa. \end{cases} \tag{6.9}$$

Proof. We proceed by induction on n. If $n = 2$ (the base case), or more generally if ζ is a *primitive* $2n^{\text{th}}$ root of unity, then Lemma 6.3 tells us A_n is the only matrix along the diagonal of M_n with α as an eigenvalue. In particular, α has algebraic multiplicity one for M_n, so linear algebra provides an eigenvector $\mathbf{p}$ of M_n with the first $n + 1$ entries matching (6.6). (We will scale $\mathbf{p}$ appropriately so that (6.8) and (6.9) hold at the end of the proof.)

Now consider the possibility that ζ is a $2\tilde{n}^{\text{th}}$ root of unity for some positive $\tilde{n} < n$. As an induction hypothesis, assume the present theorem holds in smaller dimensions. Unlike in the base case, linear algebra makes no eigenvector guarantee; we only know that (6.6) extends to a vector $\mathbf{p}$ such that

$$M_n\mathbf{p} = \alpha\mathbf{p} + \tilde{\mathbf{p}} \tag{6.10}$$

for some $\tilde{\mathbf{p}}$ in the α-generalized eigenspace of M_n.

Since (6.6) is an eigenvector of A_n, we see from $\tilde{\mathbf{p}} = M_n\mathbf{p} - \alpha\mathbf{p}$ that the first $n + 1$ coefficients of $\tilde{\mathbf{p}}$ are 0. These initial zeros may be removed to view $\tilde{\mathbf{p}}$ as an element of the α-generalized eigenspace of M_{n-1}, which is a genuine eigenspace by the induction hypothesis. So up to some scalar, say λ, the first nonzero entries of $\tilde{\mathbf{p}}$ must match (6.6) in some dimension $\tilde{n} < n$. Assume by way of contradiction that $\lambda \neq 0$, meaning $\tilde{\mathbf{p}}$ is an eigenvector. Using the induction hypothesis again, $\tilde{\mathbf{p}}$ corresponds to some $\lambda\tilde{\not{p}}$ with respect to $\mathscr{B}_{\tilde{n}}$, where $\tilde{\not{p}}$ satisfies (6.8) with n replaced by $\tilde{n}$. Comparing definitions of $\mathscr{B}_n$ and $\mathscr{B}_{\tilde{n}}$, we see that $\tilde{\mathbf{p}}$ corresponds to $\lambda(x^2 - \kappa)^{n-\tilde{n}}\tilde{\not{p}}$ with respect to $\mathscr{B}_n$.

Now let $\not{p}$ be the polynomial corresponding to $\mathbf{p}$ with respect to $\mathscr{B}_n$ and let $\omega \in \overline{F}$ denote the last entry of $\mathbf{p}$. Then (6.10) combines with Proposition 6.1 to give

$$\Phi_x(x\not{p}) = \alpha\Phi_x(\not{p}) + \omega x(x^2 - \kappa)^n + \lambda\Phi_x((x^2 - \kappa)^{n-\tilde{n}}\tilde{\not{p}}). \tag{6.11}$$

If $\alpha^2 \neq \kappa$ then

$$\frac{\lambda\tilde{n}(\alpha^2 - \kappa)^n}{(\alpha^2 - 4)^{\tilde{n}}}(v^{2\tilde{n}} + v^{-2\tilde{n}}) = \frac{\lambda(\alpha^2 - \kappa)^{n-\tilde{n}}}{|\mathscr{O}_\alpha|} \sum_{\mathbf{t} \in \mathscr{O}_\alpha} \tilde{\not{p}}(\mathbf{t}) \qquad \text{by (6.8) for } \tilde{\not{p}}$$

$$
\begin{aligned}
&= \frac{\lambda}{|\mathscr{O}_\alpha|} \sum_{\mathbf{t}\in\mathscr{O}_\alpha} \Phi_x((x^2-\kappa)^{n-\tilde{n}}\tilde{\rho})(\mathbf{t}) \\
&= \frac{1}{|\mathscr{O}_\alpha|} \sum_{\mathbf{t}\in\mathscr{O}_\alpha} \big(\Phi_x((x-\alpha)\rho)(\mathbf{t}) - \omega x(x^2-\kappa)^n\big) && \text{by (6.11)} \\
&= \omega\alpha(\alpha^2-\kappa)^n && \text{since } x=\alpha \text{ in } \mathscr{O}_\alpha.
\end{aligned}
$$

The final expression is constant in the free variable v while the initial expression is not. This is a contradiction, so λ must be 0 and $\tilde{\rho}$ must be the zero vector. But now note that setting $\lambda = 0$ above proves $\omega\alpha(\alpha^2-\kappa)^n = 0$. So if $\alpha^2 \neq \kappa$ then $\omega = 0$. The definition of M_n is independent of the value of κ, so $\mathbf{p}$ is an eigenvector with final entry $\omega = 0$ even when $\alpha^2 = \kappa$. Thus $\Phi_x(x\rho) = \alpha\Phi_x(\rho)$ as desired.

Next let $\rho^* = p_n(x)y^{2n} + \cdots + p_0(x)$, and consider the expression for $\sum_{\mathscr{O}_\alpha}\rho(\mathbf{t})$ provided by Lemma 6.5. The only powers of y or v that appear are those with exponent divisible by the order of ζ. So by the induction hypothesis, we may adjust ρ by the α-eigenvectors from smaller dimensions in order to cancel all but the top term in Lemma 6.5's formula. That is, we may assume

$$
\frac{1}{|\mathscr{O}_\alpha|}\sum_{\mathbf{t}\in\mathscr{O}_\alpha}\rho(\mathbf{t}) = \begin{cases} p_n(\alpha)\left(\dfrac{\alpha^2-\kappa}{\alpha^2-4}\right)^n (v^{2n}+v^{-2n}) & \alpha^2 \neq \kappa \\ p_n(\alpha)y^{2n} & \alpha^2 = \kappa. \end{cases} \tag{6.12}
$$

It remains only to find a formula for $p_n(x)$ and use it to find the right scalar to make (6.8) and (6.9) true.

By Proposition 5.4, the y-degree of the canonical form of any monomial from $\mathscr{B}_{i,n}$ is $2i$. In particular, $p_n(x)$ is completely determined by the coefficients of monomials from $\mathscr{B}_{n,n}$, which are given in (6.6). From this, and again using Proposition 5.4, we see that $p_n(x)$ has degree n and leading coefficient $\frac{\zeta^n}{2}$ due to the term $\zeta^n y^n z^n$ present in ρ.

Next we determine the roots of $p_n(x)$. Suppose $\tilde{\alpha} \in \widehat{\Lambda}\backslash\{\alpha\}$. On the one hand, Proposition 6.2 says the sum of ρ over any first-coordinate orbit $\mathscr{O}_{\tilde{\alpha}}$ vanishes. On the other hand, Lemma 6.5 expresses such a sum as a Laurent polynomial in the free variable v (if $\tilde{\alpha}^2 \neq \kappa$) or y (if $\tilde{\alpha}^2 = \kappa$). Thus every coefficient $c_{\tilde{\alpha},i}(\rho)$ must be 0. Since $c_{\tilde{\alpha},n}(\rho)$ is a nonzero multiple of $p_n(\tilde{\alpha})$, this forces $p_n(\tilde{\alpha}) = 0$. This accounts for $|\widehat{\Lambda}\backslash\{\alpha\}| = n-2$ roots. We claim that the two remaining roots of $p_n(x)$ are 2 and -2. Proposition 5.4 says we may compute $p_n(x) \bmod (x^2-4)$ by replacing each power of z in $y^{2n} + \alpha y^{2n-2}z^2 + \cdots + \zeta^n y^n z^n$ (the coefficients from (6.6)) with the same power of $\frac{1}{2}xy$. So

$$
p_n(x) \equiv 1 + \sum_{j=1}^{n-1} \frac{(\zeta^j + \zeta^{-j})x^j}{2^j} + \frac{\zeta^n x^n}{2^n} \bmod (x^2-4).
$$

When $x = \pm 2$, the right side above is simply the sum over $-n < j \leq n$ of $(\pm\zeta)^j$, which is 0 since $\zeta \neq \pm 1$. This proves that

$$
p_n(x) = \frac{\zeta^n}{2}\prod_{\tilde{\alpha}\in\Lambda_n\backslash\{\alpha\}}(x-\tilde{\alpha}). \tag{6.13}
$$

By Lemma 6.9, $p_n(\alpha) = n$. In particular, scaling ρ by $\frac{1}{n}(\frac{\alpha^2-4}{\alpha^2-\kappa})^n$ when $\alpha^2 \neq \kappa$ or $\frac{1}{n}$ when $\alpha^2 = \kappa$ turns (6.12) into (6.8) and it turns (6.13) into (6.9). □

Notation 6.11. For $n \geq 2$ with $\mathrm{char}(R) \nmid n$ and $\alpha \in \widehat{\Lambda}_n$, let $\wp_{\alpha,n}$ denote the polynomial $\wp$ in the statement of Theorem 6.10. Also let $\wp^+_{\alpha,n} = \frac{1}{2}(\wp_{\alpha,n} + p_{-\alpha,n})$.

Note that every other entry in (6.6) is negated when α is replaced by $-\alpha$. From the structure of the matrices A_n and B_n, it is not hard to check that this alternating pattern continues along the coefficients of $\wp_{\alpha,n}$ and $\wp_{-\alpha,n}$. In other words, $\wp^+_{\alpha,n}$ is obtained from $\wp_{\alpha,n}$ by deleting every other monomial, only keeping those with even powers of y and z. By Proposition 5.1, we are keeping precisely those monomials that reduce to even polynomials in x.

Corollary 6.12. *For any $n \geq 2$ and $\alpha \in \widehat{\Lambda}_n$, $\wp_{\alpha,n}$ and $\wp^+_{\alpha,n}$ are elements of $\mathscr{P}_x(F, \frac{1}{2}\mathrm{ord}(\alpha))$.*

Proof. This is follows from Proposition 6.2 and the definition of $\mathscr{P}_x(F,d)$. □

Corollary 6.13. *For any $n \geq 2$ and $\alpha \in \widehat{\Lambda}_n$, $\Phi(\wp_{\alpha,n})$ and $\Phi(\wp^+_{\alpha,n})$ are monic of degree $2n$.*

Proof. We know $\wp_{\alpha,n}$ is a linear combination of elements of $\mathscr{B}_n \backslash \mathscr{B}_{0,n}$. By Proposition 5.1, the only element of $\mathscr{B}_n \backslash \mathscr{B}_{0,n}$ that has a Φ-reduction of degree at least $2n$ is y^{2n}, which appears in $\wp_{\alpha,n}$ with coefficient 1 (the first entry in (6.6)). Since $\Phi(y^{2n}) = x^{2n}$, the claim is proved. □

Corollary 6.14. *Suppose $\mathrm{char}(R) = 0$. Let $f \in \overline{R}[x,y,z]$, and suppose f^* is even as a polynomial in y. Then $f \in \mathscr{P}_x(R,\infty)$ if and only if*

$$\Phi_x(f) = \sum_{i=2}^{\infty} \sum_{\alpha \in \widehat{\Lambda}_i} c_{\alpha,i}(f) \Phi_x(\wp_{\alpha,i}),$$

where the $c_{\alpha,i}(f)$ are the unique coefficients for which this equation holds. In this case, $f \in \mathscr{P}_x(R,d)$ for some $d \geq 2$ if and only if $c_{\alpha,i}(f) = 0$ whenever $2d \nmid \mathrm{ord}(\alpha)$.

Proof. First recall that if $2i > \deg_y f^*$ then $c_{\alpha,i}(f) = 0$ by (6.7). This means there are only finitely many pairs α, i with $i \geq 2$ and $\alpha \in \widehat{\Lambda}_i$ for which $c_{\alpha,i}(f)$ could possibly be nonzero. Thus if the summation formula holds, $\Phi_x(f)$ is a finite combination of polynomials $\Phi_x(\wp_{\alpha,i})$, and $\sum_{\mathscr{O}_x} \Phi_x(\wp_{\alpha,i})(\mathbf{t}) = \sum_{\mathscr{O}_x} \wp_{\alpha,i}(\mathbf{t})$ is only nonzero on a first-coordinate orbit $\mathscr{O}_x$ if $x = \alpha$ by Proposition 6.2. Thus $\sum_{\mathscr{O}_x} f(\mathbf{t}) = \sum_{\mathscr{O}_x} \Phi_x(f)(\mathbf{t})$ can only be nonzero for finitely many values of x. That is what it means to belong to $\mathscr{P}_x(R,\infty)$.

Conversely, assume $f \in \mathscr{P}_x(R,\infty)$. Let $f^* = f_n(x)y^{2n} + \cdots + f_0(x)$, and let $p_\alpha(x)$ denote the coefficient of y^{2n} in $\wp^*_{\alpha,n}$ for $\alpha \in \widehat{\Lambda}_n$. From the formula in (6.9), the only common roots among the p_α as α ranges over $\widehat{\Lambda}_n$ are 2 and -2, meaning these polynomials generate the ideal (x^2-4) in $\overline{F}[x]$. But by Proposition 6.8, specifically (1) implies (5), x^2-4 must divide $f_n(x)$. Thus there exist $g_{\alpha,n}(x) \in \overline{F}[x]$ such that $f^* - \sum_{\widehat{\Lambda}_n} g_{\alpha,n}\wp^*_{\alpha,n}$ has degree $2n-2$ in the variable y. And since $\sum_{\widehat{\Lambda}_n} g_{\alpha,n}\wp^*_{\alpha,n}$ belongs to $\mathscr{P}_x(F,\infty)$, we can repeat this process for $n-1$, $n-2$,..., 2. (We must stop after 2 because there is no such thing as "$\wp_{\alpha,1}$".) Thus for the right choice of polynomials $g_{\alpha,i}$, we see that

$$f^* - \sum_{i=2}^{n} \sum_{\alpha \in \widehat{\Lambda}_i} g_{\alpha,i}\wp^*_{\alpha,i}$$

has degree at most 2 in y. Since the sum above still lies in $\mathscr{P}_x(F,\infty)$, Proposition 6.8, specifically (1) implies (5), says it must take the form $\tilde{f}(x)(x^2-4)y^2-2\tilde{f}(x)(x^2-\kappa)$ for some $\tilde{f}\in\overline{F}[x]$. It is quick to check that the image of such a polynomial under Φ_x is the zero polynomial. Thus

$$\begin{aligned}
0 &= \Phi_x(f^*) - \sum_{i=2}^{n}\sum_{\alpha\in\widehat{\Lambda}_i}\Phi_x(g_{\alpha,i}\wp^*_{\alpha,i}) && \text{by linearity of } \Phi\\
&= \Phi_x(f^*) - \sum_{i=2}^{n}\sum_{\alpha\in\widehat{\Lambda}_i}\Phi_x((g_{\alpha,i}\wp_{\alpha,i})^*) && \text{since } g_{\alpha,i}\in\overline{F}[x]\\
&= \Phi_x(f) - \sum_{i=2}^{n}\sum_{\alpha\in\widehat{\Lambda}_i}\Phi_x(g_{\alpha,i}\wp_{\alpha,i}) && \text{by Proposition 5.5}\\
&= \Phi_x(f) - \sum_{i=2}^{n}\sum_{\alpha\in\widehat{\Lambda}_i} g_{\alpha,i}(\alpha)\Phi_x(\wp_{\alpha,i}) && \text{by Proposition 6.7.}
\end{aligned}$$

Now, as a consequence of Proposition 6.2 and (6.8), we know that $\sum_{\mathscr{O}_{\tilde{\alpha}}}\wp_{\alpha,i}(\mathbf{t}) = 0$ for all first-coordinate orbits $\mathscr{O}_{\tilde{\alpha}}$ if and only if $\tilde{\alpha}\neq\alpha$. Combining this with the equation above gives the following for any fixed $\alpha\neq\pm2$ of finite order:

$$\frac{1}{|\mathscr{O}_\alpha|}\sum_{\mathbf{t}\in\mathscr{O}_\alpha}\Phi_x(f)(\mathbf{t}) = \frac{1}{|\mathscr{O}_\alpha|}\sum_{i=2}^{n} g_{\alpha,i}(\alpha)\Phi_x(\wp_{\alpha,i})(\mathbf{t}).$$

Assuming $\alpha^2\neq\kappa$, Lemma 6.5 expresses the left-hand side as

$$\sum_{i=2}^{n} c_{\alpha,i}(f)(v^{2i}+v^{-2i}),$$

where $c_{\alpha,0}(f)=0$ has been omitted since $f\in\mathscr{P}_x(R,\infty)$, as has $c_{\alpha,1}(f)=0$ since $\alpha\notin\Lambda_1=\{\pm2\}$. But then the right-hand side can be evaluated using (6.8). It equals

$$\sum_{i=2}^{n} g_{\alpha,i}(\alpha)(v^{2i}+v^{-2i}).$$

The last two expressions must be equal for any assignment of the free variable v from the infinite domain R. This forces $c_{\alpha,i}(f)=g_{\alpha,i}(\alpha)$, thereby proving our formula.

The corollary's final claim regarding membership in $\mathscr{P}(R,d)$ also follows from the fact that $\sum_{\mathscr{O}_{\tilde{\alpha}}}\wp_{\alpha,i}(\mathbf{t})=0$ for all first-coordinate orbits $\mathscr{O}_{\tilde{\alpha}}$ if and only if $\tilde{\alpha}\neq\alpha$. □

When f^* is also even as a polynomial in x (so $f^*\in R[x^2,y^2]$) we have $c_{\alpha,i}(f)=c_{-\alpha,i}(f)$. Hence this last corollary allows us to express $\Phi_x(f)$ as a linear combination of $\Phi_x(\wp^+_{\alpha,i})$.

6.2. **Another partial formula.** Interestingly, we will compute more coefficients of $\Phi(\wp^+_{\alpha,n})$ than we will of $\wp^+_{\alpha,n}$.

Lemma 6.15. *For any positive integers j and n, $\frac{2n}{n+j}\binom{n+j}{n-j}$ is an integer.*

Proof. Let p be a prime, and let $v_p(j)$ and $v_p(n)$ denote the valuations of j and n at p. Since $\frac{2n}{n+j}\binom{n+j}{n-j}=\frac{n}{j}\binom{n+j-1}{2j-1}$, the task is to show that $v_p(\binom{n+j-1}{2j-1})\geq v_p(j)-v_p(n)$. The inequality is immediate if $v_p(j)\leq v_p(n)$, so assume otherwise. Kummer's

theorem states that $v_p(\binom{n+j-1}{2j-1})$ is the number of carries when $n-j$ and $2j-1$ are added in base p. The coefficients of $p^0, \dots, p^{v_p(j)-1}$ when $2j-1$ is written in base p are all $p-1$, and the coefficient of $p^{v_p(n)}$ when $n-j$ is written in base p is nonzero. Thus a carry occurs at the places $p^{v_p(n)}, \dots, p^{v_p(j)-1}$, for a total of $v_p(j) - v_p(n)$ carries, as needed. □

Lemma 6.16. *Suppose* $\operatorname{char}(R) \nmid n$. *Let* m *and* n *be integers with* $n > m \geq 0$. *Define*

$$f_j(x^2) = \begin{cases} 0 & j < m \\ \dfrac{2n-2m}{n}\binom{n+m}{n-m}(\kappa - x^2)^{n-m} & j = m \\ \dfrac{2n}{n+j}\binom{n+j}{n-j}(x^2-4)^{j-m}(\kappa-x^2)^{n-j} & j > m, \end{cases}$$

and let $f = \sum_j f_j y^{2j}$. *Then* $f \in \mathscr{P}_x(F, \infty)$ *with* $c_{\alpha,i}(f) = 0$ *if* $m < i < n$.

Proof. To show that $f \in \mathscr{P}_x(R, \infty)$ we use the equivalent property (5) from Proposition 6.8, which is

$$\sum_{j=0}^{n} \binom{2j}{j} \left(\frac{x^2-\kappa}{x^2-4}\right)^j f_j(x^2) = 0. \tag{6.14}$$

By substituting in the definition of $f_j(x^2)$ and solving for $f_m(x^2)$, the equation above reduces to the following identity after some straightforward arithmetic:

$$\sum_{j=m+1}^{n} (-1)^j \binom{n}{j}\binom{n+j-1}{j} = (-1)^{m+1}\binom{n-1}{m}\binom{n+m}{m}.$$

This is easily checked by backward induction on m, the base case being $m = n-1$.

Now suppose $m < i < n$ and consider some $\alpha \in \widehat{\Lambda}_i$. By (6.7),

$$\begin{aligned} c_{\alpha,i}(f) &= \sum_{j=i}^{n} \binom{2j}{j-i}\left(\frac{\alpha^2-\kappa}{\alpha^2-4}\right)^j f_j(\alpha^2) \\ &= \frac{(\kappa-\alpha^2)^n}{(\alpha^2-4)^m}\sum_{j=i}^{n} \frac{2n(-1)^j}{n+j}\binom{2j}{j-i}\binom{n+j}{n-j} \\ &= \frac{2n(-1)^i(\kappa-\alpha^2)^n}{(n+i)(\alpha^2-4)^m}\binom{n+i}{n-i}{}_2F_1(i-n, n+i; 2i+1; 1), \end{aligned}$$

which vanishes by Gauss' formula for hypergeometric functions. □

Theorem 6.17. *Suppose* $\operatorname{char}(R) \nmid n$. *For any* $n \geq 2$ *and* $\alpha \in \widehat{\Lambda}_n \backslash \{\pm\sqrt{\kappa}\}$,

$$\Phi(\mathscr{p}^+_{\alpha,n}) = \frac{1}{n}\sum_{j=0}^{n} \binom{2n-j-1}{j}\left(\frac{\alpha^2-4}{\alpha^2-\kappa}\right)^{n-j}(-1)^j b_{n-j}(x^2) + r(x^2)$$

for some $r(x^2) \in \overline{F}[x]$ *of degree at most* $2\lfloor \frac{3}{4}n \rfloor$.

Proof. Define $f_j(x^2)$ as in Lemma 6.16 with $m = \lfloor \frac{3}{4}n \rfloor$, and set

$$f(x^2, y^2) = \sum_{j=0}^{n} f_j(x^2) y^{2j}.$$

For any $\ell \geq 0$ we have $c_{\alpha,i}(x^{2\ell} f) = \alpha^{2\ell} c_{\alpha,i}(f)$, which is 0 when $i > n$ or when $m < i < n$ by Lemma 6.16. If we omit these vanishing coefficients from the expression in Corollary 6.14, the result is

$$\Phi_x(x^{2\ell} f) = \sum_{\alpha \in \widehat{\Lambda}_n} \alpha^{2\ell} c_{\alpha,n}(f) \Phi_x(\wp_{\alpha,n}) + \sum_{i=1}^{m} \sum_{\alpha \in \widehat{\Lambda}_i} \alpha^{2\ell} c_{\alpha,i}(f) \Phi_x(p_{\alpha,i}).$$

By Corollary 6.13, if $i \leq m$ then $\deg \Phi(p_{\alpha,i}) = 2i \leq 2m$. Thus the entire right-side sum above can be absorbed into the remainder polynomial $r(x^2)$ and therefore ignored. Regarding the left-side sum, let us group $\wp_{\alpha,n}$ and $\wp_{-\alpha,n}$ into $2\wp^+_{\alpha,n}$ (which appears as two occurrences of $\wp^+_{\alpha,n}$ in the sum below) using the fact that $c_{\alpha,n}(f) = c_{-\alpha,n}(f)$ because f is even as a polynomial in x. The result is

$$\Phi(x^{2\ell} f) = \sum_{\alpha \in \widehat{\Lambda}_n} \alpha^{2\ell} c_{\alpha,n}(f) \Phi(\wp^+_{\alpha,n}) + r(x^2) \tag{6.15}$$

for some $r(x^2) \in R[x]$ of degree at most $2m = 2\lfloor \frac{3}{4} n \rfloor$.

Now assume $\ell < \lfloor \frac{n}{2} \rfloor$. Recall from the definition of $f_j(x^2)$ in Lemma 6.16 that $(x^2-4)^{j-m} \mid f_j(x^2)$. So for $j > m$, we deduce from Theorem 5.14 that

$$\Phi(x^{2\ell} f_j(x^2) y^{2j}) = \frac{1}{n} \sum_{i=0}^{j} \binom{2i}{i} \sum_{\alpha \in \widehat{\Lambda}_n} \left(\frac{\alpha^2 - \kappa}{\alpha^2 - 4} \right)^i \alpha^{2\ell} f_j(\alpha^2) b_{j-i}(x^2) + r_j(x^2)$$

for some $r_j(x^2) \in R[x]$ of degree at most $\max(\deg x^{2\ell} f_j(x^2), 2j - 2(j-m)) = \max(2(\ell + n - m), 2m)$, which is bounded above by $2m$ because $\ell < \lfloor \frac{n}{2} \rfloor$. When $j \leq m$, we do not care about $\Phi(x^{2\ell} f_j(x^2) y^{2j})$ because it has degree at most $\max(\deg x^{2\ell} f_j(x^2), 2j) \leq 2m$ by Proposition 5.1. Summing the expression above over j and combining all $r_j(x^2)$ polynomials into a single remainder gives

$$\Phi(x^{2\ell} f) = \frac{1}{n} \sum_{j=m+1}^{n} \sum_{i=0}^{j} \binom{2i}{i} \sum_{\alpha \in \widehat{\Lambda}_n} \left(\frac{\alpha^2 - \kappa}{\alpha^2 - 4} \right)^i \alpha^{2\ell} f_j(\alpha^2) b_{j-i}(x^2) + \tilde{r}(x^2)$$

Now substitute the formula in Lemma 6.16 for $f_j(\alpha^2)$. To get the second line below, change variables by replacing i and j with $j - i$ and $n - i$, respectively:

$$\begin{aligned}
&\Phi(x^{2\ell} f) \\
&= \frac{1}{n} \sum_{j=m+1}^{n} \sum_{i=0}^{j} \binom{2i}{i} \sum_{\alpha \in \widehat{\Lambda}_n} \frac{2n(-1)^{n-j} \alpha^{2\ell} (\alpha^2 - \kappa)^{n-j+i}}{(n+j)(\alpha^2-4)^{m-j+i}} \binom{n+j}{n-j} b_{j-i}(x^2) + \tilde{r}(x^2) \\
&= \frac{1}{n} \sum_{j=0}^{n-m} \sum_{\alpha \in \widehat{\Lambda}_n} \frac{(\alpha^2 - \kappa)^j \alpha^{2\ell}}{(\alpha^2-4)^{j+m-n}} \sum_{i=0}^{j} \frac{2n(-1)^i}{2n-i} \binom{2j-2i}{j-i} \binom{2n-i}{i} b_{n-j}(x^2) + \tilde{r}(x^2)
\end{aligned}$$

The sum over i can be evaluated using Saalschütz's theorem for hypergeometric functions:

$$\begin{aligned}
&\sum_{i=0}^{j} \frac{2n(-1)^i}{2n-i} \binom{2j-2i}{j-i} \binom{2n-i}{i} \\
&\qquad = \frac{2n(-1)^j}{2n-j} \binom{2n-j}{j} {}_3F_2(-j, 2n-j, \tfrac{1}{2}; n-j+\tfrac{1}{2}, n-j+1; 1)
\end{aligned}$$

$$= (-1)^j \binom{2n-j-1}{j}.$$

Thus we obtain the formula

$$\Phi(x^{2\ell} f) = \frac{1}{n} \sum_{j=0}^{n-m} \sum_{\alpha \in \widehat{\Lambda}_n} \frac{(\alpha^2-\kappa)^j \alpha^{2\ell}}{(\alpha^2-4)^{j+m-n}} \binom{2n-j-1}{j} (-1)^j b_{n-j}(x^2) + \tilde{r}(x^2).$$

From this we are able to determine the coefficient of some power of x, say x^{2i}, in $c_{\alpha,n}(f)\Phi(\wp^+_{\alpha,n})$ for each $\alpha \in \widehat{\Lambda}_n$. Indeed, combining the equation above with (6.15) determines the sum of these coefficients over $\alpha \in \widehat{\Lambda}_n$, and we have one such equation for each nonnegative $\ell < \lfloor \frac{n}{2} \rfloor$. There are only $\lfloor \frac{n}{2} \rfloor$ values of $\alpha \in \widehat{\Lambda}_n$ up to a change of sign, and the $\lfloor \frac{n}{2} \rfloor \times \lfloor \frac{n}{2} \rfloor$ Vandermonde matrix with each column consisting of powers of some α^2 is invertible. Thus the system of equations we have produced uniquely determines the coefficient of x^{2i} in each $c_{\alpha,n}(f)\Phi(\wp^+_{\alpha,n})$ provided $i > m$. One possibly solution is evident:

$$c_{\alpha,n}(f)\Phi(\wp^+_{\alpha,n}) = \frac{1}{n} \sum_{j=0}^{n} \frac{(\alpha^2-\kappa)^j}{(\alpha^2-4)^{j+m-n}} \binom{2n-j-1}{j} (-1)^j b_{n-j}(x^2) + r_\alpha(x^2),$$

so this must be *the* solution. By (6.7), $c_{\alpha,n}(f) = (\frac{\alpha^2-\kappa}{\alpha^2-4})^n f_n(\alpha^2) = \frac{(\alpha^2-\kappa)^n}{(\alpha^2-4)^m}$. This completes the proof. □

6.3. **The space $\mathscr{P}_x(R,d)$.** Recall that $\mathscr{P}_x(R,d)$ consists of those $f \in \overline{R}[x,y,z]$ such that $\sum_{\mathscr{O}_\alpha} f(\mathbf{t}) = 0$ whenever $2d \nmid \operatorname{ord}(\alpha)$. Proposition 6.2 *almost* implies that $\wp_{\alpha,n}$ (and thus $\wp^+_{\alpha,n}$) belongs to $\mathscr{P}_x(R, \operatorname{ord}(\alpha))$—the problem is that coefficients of $\wp_{\alpha,n}$ are in $\overline{F}$ and generally not in $\overline{R}$ when $n \geq 4$. However, the polynomial "f" from Lemma 6.16 with "m" set to 0 turns out to be a linear combination of the $\wp^+_{\alpha,n}$ (with n fixed), and f has coefficients in R by Lemma 6.15. The exact linear combination is straightforward to compute, so Theorem 6.17 provides a formula for the top coefficients of $\Phi(f)$. Let us first recall the definition of "f":

Notation 6.18. For $n \geq 0$, let

$$f_n(x^2, y^2) = \sum_{j=0}^{n} \frac{2n}{n+j} \binom{n+j}{n-j} (x^2-4)^j (\kappa - x^2)^{n-j} y^{2j}.$$

Corollary 6.19. *For any integers $d, n \geq 2$ and any $g(x^2) \in \overline{R}[x]$, $gf_n \in \mathscr{P}_x(R,d)$. Furthermore,*

$$\Phi(gf_n) = \frac{1}{n} \sum_{j=0}^{n} \sum_{\alpha \in \widehat{\Lambda}_n} \binom{2n-j-1}{j} g(\alpha^2)(\alpha^2-4)^{n-j}(\kappa-\alpha^2)^j b_{n-j}(x^2) + r(x^2)$$

for some $r(x^2) \in \overline{R}[x]$ of degree at most $2\lfloor \frac{3}{4} n \rfloor$.

Proof. Since g is a function of x only, $c_{\alpha,i}(gf_n) = g(\alpha^2)c_{\alpha,i}(f_n)$ by Proposition 6.7, and this equals 0 if $i \neq n$ by Lemma 6.16. So Corollary 6.14 gives

$$\Phi(gf_n) = \sum_{\alpha \in \widehat{\Lambda}_n} c_{\alpha,n}(gf_n)\Phi(\wp^+_{\alpha,n}), \tag{6.16}$$

where we have grouped $\wp_{\alpha,n}$ and $\wp_{-\alpha,n}$ into $2\wp^+_{\alpha,n}$ (which appears as two occurrences of $\wp^+_{\alpha,n}$ in the sum) using the fact that $c_{\alpha,n}(f) = c_{-\alpha,n}(f)$ because gf_n is

even as a polynomial in x. Theorem 6.17 provides a formula for $\Phi(\not{p}^+_{\alpha,n})$. Furthermore, the coefficient of y^{2n} in $(gf_n)^* = gf_n$ is $g(x^2)(x^2-4)^n$, from which Lemma 6.5 provides the formula $c_{\alpha,n} = \frac{1}{n}g(\alpha^2)(\alpha^2-4)^n$. Substituting these into the expression above completes the proof. □

Corollary 6.20. *Let d and n be positive integers with d a prime power, and let $\tilde{n} = d\lceil \frac{n}{d} \rceil$. If $n > 3d$ or if $d \,|\, n$ then $\Phi(\mathscr{P}_x(R,d))$ contains a polynomial of degree at most $2n$ in which the coefficient of x^{2n} is $2\binom{\tilde{n}+n-1}{\tilde{n}-n}(4-\kappa)^{\tilde{n}}\tilde{n}^{\tilde{n}}$.*

Proof. Assume that $\mathrm{char}(R) \nmid n$ since otherwise the claim is immediate. We begin with the simplest case where $d \,|\, n$. Fix any α of rotation order $2n$ and set

$$g(x^2) \coloneqq x^\delta \prod_{\tilde{\alpha} \in \widehat{\Lambda}_n \backslash \{\pm\alpha\}} (x - \tilde{\alpha}),$$

where $\delta = 1$ if $0 \in \widehat{\Lambda}_n \backslash \{\pm\alpha_i\}_i$ and $\delta = 0$ otherwise (to make g an even polynomial).

Observe that $c_{\tilde{\alpha},i}(gf_n) = g(\tilde{\alpha}^2)c_{\tilde{\alpha},i}(f_n)$ by Proposition 6.7, which vanishes unless $i = n$ (by Lemma 6.16) and $\tilde{\alpha} = \pm\alpha$ (by definition of g). Since $2d \,|\, \mathrm{ord}(\alpha)$ by assumption, we have $gf_n \in \mathscr{P}_x(R,d)$ by Corollary 6.14.

Next we apply Corollary 6.19 to conclude that $\Phi(gf_n)$ has degree $2n$ and leading coefficient

$$\frac{1}{n}\sum_{\tilde{\alpha} \in \widehat{\Lambda}_n} g(\tilde{\alpha}^2)(\tilde{\alpha}^2-4)^n = \frac{2}{n}g(\alpha^2)(\alpha^2-4)^n.$$

In $\overline{R}$, $g(\alpha^2)(\alpha^2-4)^n$ divides

$$\prod_{\tilde{\alpha} \in \Lambda_n \backslash \{\alpha\}} (\alpha - \tilde{\alpha})^n,$$

which equals n^n up to a sign by Lemma 6.9. This completes the proof when $d \,|\, n$.

Now suppose $n > 3d$ and let $\tilde{n} = d\lceil \frac{n}{d} \rceil$. We proceed in similar fashion, but with a modified polynomial g. Let p be the prime dividing d. If ζ is a primitive $2\tilde{n}^{\text{th}}$ root of unity and $\alpha = \zeta^i + \zeta^{-i}$ for some i not divisible by p, then $2d \,|\, \mathrm{ord}(\alpha)$. The number of positive integers $i \le \frac{\tilde{n}}{2}$ not divisible by p is $\ell + 1 \coloneqq \lceil \frac{\tilde{n}}{2p} \rceil (p-1)$. Let $\alpha_0, ..., \alpha_\ell$ denote the corresponding α-values in any order, and define

$$g(x^2) \coloneqq x^\delta \prod_{\alpha \in \widehat{\Lambda}_{\tilde{n}} \backslash \{\pm\alpha_i\}_i} (x - \alpha), \tag{6.17}$$

where $\delta = 1$ if $0 \in \widehat{\Lambda}_{\tilde{n}} \backslash \{\pm\alpha_i\}_i$ and $\delta = 0$ otherwise.

Observe that $c_{\alpha,i}(gf_{\tilde{n}}) = g(\alpha^2)c_{\alpha,i}(f_{\tilde{n}})$ by Proposition 6.7, which vanishes unless perhaps $i = \tilde{n}$ (by Lemma 6.16) and $2d \,|\, \mathrm{ord}(\alpha)$ (by definition of g). Hence $x^{2i}gf_{\tilde{n}} \in \mathscr{P}_x(R,d)$ for any $i \ge 0$ by Corollary 6.14.

As before, we apply Corollary 6.17 to conclude that if $\tilde{n} - j > \lfloor \frac{3}{4}\tilde{n} \rfloor$ then the coefficient of $b_{\tilde{n}-j}(x^2)$ in some $\overline{F}$-linear combination $c_0\Phi(x^0gf_{\tilde{n}}) + \cdots + c_\ell\Phi(x^{2\ell}gf_{\tilde{n}})$ is the j^{th} entry (starting at $j = 0$) of the product

$$D_1V_1D_2V_2 \begin{bmatrix} c_0 \\ \vdots \\ c_\ell \end{bmatrix} \tag{6.18}$$

where

$$D_1 = \begin{bmatrix} (-1)^0\binom{2\tilde{n}-0-1}{0} & & \\ & \ddots & \\ & & (-1)^\ell\binom{2\tilde{n}-\ell-1}{\ell} \end{bmatrix}$$

$$V_1 = \begin{bmatrix} \left(\frac{\alpha_0^2-\kappa}{\alpha_0^2-4}\right)^0 & \cdots & \left(\frac{\alpha_\ell^2-\kappa}{\alpha_\ell^2-4}\right)^0 \\ \vdots & & \vdots \\ \left(\frac{\alpha_0^2-\kappa}{\alpha_0^2-4}\right)^\ell & \cdots & \left(\frac{\alpha_\ell^2-\kappa}{\alpha_\ell^2-4}\right)^\ell \end{bmatrix}$$

$$D_2 = \begin{bmatrix} (\alpha_0^2-4)^{\tilde{n}}g(\alpha_0^2) & & \\ & \ddots & \\ & & (\alpha_\ell^2-4)^{\tilde{n}}g(\alpha_\ell^2) \end{bmatrix}$$

$$\text{and } V_2 = \begin{bmatrix} \alpha_0^0 & \cdots & \alpha_0^{2\ell} \\ \vdots & & \vdots \\ \alpha_\ell^0 & \cdots & \alpha_\ell^{2\ell} \end{bmatrix}.$$

The product $V_1D_2V_2$ has entries in $\overline{R}$ since the denominators in V_1 are canceled by entries in D_2. Thus for any $j = 0, ..., \ell$, there exist $c_0, .., c_\ell \in R$ such that the i^{th} entry in the product (6.18) is 0 when $i < j$ and $\binom{2\tilde{n}-j-1}{j}\det(V_1D_2V_2)$ when $i = j$. Remember that these entries are the coefficients of $b_{\tilde{n}}(x^2), \ldots, b_{\tilde{n}-j}(x^2)$ provided $\tilde{n}-j > \lfloor\frac{3}{4}\tilde{n}\rfloor$. We wish to use this with $j = \tilde{n}-n$ for n from the theorem statement, so we have to check that the hypothesis $n > 3d$ is enough to guarantee $\tilde{n}-j > \lfloor\frac{3}{4}\tilde{n}\rfloor$ and $j \le \ell$. The claim will then follow provided $\det(V_1D_2V_2)$ divides $2(4-\kappa)^{\tilde{n}}\tilde{n}^{\tilde{n}}$.

If $n > 3d$ then $\tilde{n}-j = n > \frac{3}{4}(n+d) > \frac{3}{4}d\lceil\frac{n}{d}\rceil \ge \lfloor\frac{3}{4}\tilde{n}\rfloor$ as desired. Next, using $\ell \ge \frac{(p-1)\tilde{n}}{2p} - 1$ followed by $\tilde{n} \le n+d-1$, the desired inequality $j = \tilde{n}-n \le \ell$ can be rewritten as $d \le \frac{p-1}{2p}(n+d-1)$. This holds using $n > 3d$ and $p \ge 2$.

Finally, the determinant of a diagonal or a Vandermonde matrix has a standard product form. The result is

$$\det(V_1D_2V_2) = (4-\kappa)^\ell\left(\prod_{i=0}^{\ell}(\alpha_i^2-4)g(\alpha_i^2)\right)\left(\prod_{0\le i<j\le\ell}(\alpha_i^2-\alpha_j^2)\right). \tag{6.19}$$

Observe that this divides

$$(4-\kappa)^\ell\prod_{i=0}^{\ell}\prod_{\alpha\in\Lambda_{\tilde{n}}\setminus\{\alpha_i\}}(\alpha_i-\alpha)$$

simply by accounting for every factor in (6.19). By Lemme 6.9, this last expression equals $(4-\kappa)^\ell\tilde{n}^{\ell+1}$ up to a sign, which divides $2(4-\kappa)^{\tilde{n}}\tilde{n}^{\tilde{n}}$. □

The leading coefficient $2\binom{n+m-1}{n-m}(4-\kappa)^n n^n$ in the previous corollary is important because we plan to quotient by prime ideals in $\overline{\mathbb{Z}}$ to extract information about $\mathscr{P}(\mathbb{F}_q)$ from $\mathscr{P}_x(\mathbb{Z}, d)$, and we need to know that the degrees of our polynomials are maintained by the quotient.

Proposition 6.21. *Let $\kappa \in \mathbb{F}_q$. Fix a surjection $\pi : \overline{\mathbb{Z}} \to \overline{\mathbb{F}}_q$ and some $\tilde{\kappa} \in \pi^{-1}(\kappa)$. If $2d \in \mathbb{Z}\backslash\{0\}$ does not divide $q \pm 1$, then $\Phi(\pi(\mathscr{P}_x(\overline{\mathbb{Z}}, d)))$ (where $\mathscr{P}_x(\overline{\mathbb{Z}}, d)$*

is determined using $\tilde{\kappa}$) is a subspace of $\mathscr{P}(\mathbb{F}_q)$ that is independent of the choices of π and $\tilde{\kappa}$.

Proof. Consider some $\tilde{f} \in \mathscr{P}_x(\overline{\mathbb{Z}}, d)$, and let $f \in \overline{\mathbb{F}}_q[x, y, z]$ be its image under π. Our goal is to show $\Phi(f) \in \mathscr{P}(\mathbb{F}_q)$.

Each $\alpha \in \mathbb{F}_q$ lifts to some $\pm(\zeta + \zeta^{-1}) \in \overline{\mathbb{Z}}$ with ζ a primitive $\operatorname{ord}(\alpha)^{\text{th}}$ root of unity. Call this lift $\tilde{\alpha}$. Recall that $2d$ does not divide $\operatorname{ord}(\alpha) = \operatorname{ord}(\tilde{\alpha})$ by Corollary 4.2 because $2d$ does not divide $q \pm 1$. Now lift each $\mathcal{O}_\alpha \subset \mathscr{M}(\mathbb{F}_q)$ to some first-coordinate orbit $\mathcal{O}_{\tilde{\alpha}} \subset \mathscr{M}(\overline{\mathbb{Z}})$ of the same size; it does not matter which one of the infinitely many lifts we choose.

Let $\mathcal{O}$ be any Γ-invariant subset of $\mathscr{M}(\mathbb{F}_q)$, and let $\tilde{\mathcal{O}} \subset \mathscr{M}(\overline{\mathbb{Z}})$ be the union of those $\mathcal{O}_{\tilde{\alpha}}$ for which $\mathcal{O}_\alpha \subseteq \mathcal{O}$. The first coordinate of every triple in $\tilde{\mathcal{O}}$ has order not divisible by $2d$, so $\sum_{\tilde{\mathcal{O}}} \tilde{f}(\mathbf{t}) = 0$. But then

$$0 = \pi\left(\sum_{\mathbf{t}\in\tilde{\mathcal{O}}} \tilde{f}(\mathbf{t})\right) = \sum_{\mathbf{t}\in\pi(\tilde{\mathcal{O}})} \pi(\tilde{f})(\mathbf{t}) = \sum_{\mathbf{t}\in\mathcal{O}} f(\mathbf{t}) = \sum_{\mathbf{t}\in\mathcal{O}} \Phi(f)(\mathbf{t}).$$

As $\mathcal{O}$ was arbitrary, this proves $\Phi(f) \in \mathscr{P}(\mathbb{F}_q)$.

We turn to the final claim regarding independence of the choices of π and $\tilde{\kappa}$. Let $\pi_1, \pi_2 : \overline{\mathbb{Z}} \to \overline{\mathbb{F}}_q$ be two surjections, and let $\tilde{\kappa}_1 \in \pi_1^{-1}(\kappa)$ and $\tilde{\kappa}_2 \in \pi_2^{-1}(\kappa)$. Let $\varphi \in \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ satisfy $\pi_1 = \pi_2 \circ \varphi$ (see pages 394–395 in [Was12], for example). Consider some polynomial $\tilde{f}_1$ that belongs to $\mathscr{P}_x(\overline{\mathbb{Z}}, d)$ as determined by $\tilde{\kappa}_1$. Assume that f^* is even as a polynomial in y. This loses no generality because if a monomial with odd degree in y appears in f^*, the Φ reduction of this monomial would be an odd polynomial by Proposition 5.1, and we already know that both $\Phi(\pi_1(\mathscr{P}_x(\overline{\mathbb{Z}}, d)))$ and $\Phi(\pi_2(\mathscr{P}_x(\overline{\mathbb{Z}}, d)))$ contain all odd polynomials (since $\Phi(\pi_i(x^{2n+1})) = x^{2n+1}$). Now, Corollary 6.14 says that $\Phi(\tilde{f}_1) = \sum_\alpha c_{\alpha,i}(\tilde{f}_1)\Phi(\boldsymbol{\rho}_{\alpha,i})$, where $c_{\alpha,i}(\tilde{f}_1)$ can be nonzero only if $2d \,|\, \operatorname{ord}(\alpha)$. So we consider the polynomial $\tilde{f}_2 \coloneqq \sum_\alpha \varphi(c_{\alpha,i}(\tilde{f}_1))\boldsymbol{\rho}_{\alpha,i})$. Since α and $\varphi(\alpha)$ have the same rotation order, $\tilde{f}_2$ belongs to $\mathscr{P}_x(\overline{\mathbb{Z}}, d)$ as determined by $\varphi(\tilde{\kappa}_1)$. Furthermore, by repeatedly using the ring homomorphism property and linearity of Φ,

$$\begin{aligned}
\Phi(\pi_1(\tilde{f}_1)) = \pi_1(\Phi(\tilde{f}_1)) &= (\pi_2 \circ \varphi)(\Phi(\tilde{f}_1)) \\
&= (\pi_2 \circ \varphi)\left(\sum_{\alpha,i} c_{\alpha,i}(\tilde{f}_1)\Phi(\boldsymbol{\rho}_{\alpha,i})\right) \\
&= \pi_2\left(\Phi\left(\sum_{\alpha,i} \varphi(c_{\alpha,i}(\tilde{f}_1)\boldsymbol{\rho}_{\alpha,i})\right)\right) \\
&= \pi_2(\Phi(\tilde{f}_2)) = \Phi(\pi_2(\tilde{f}_2)).
\end{aligned}$$

Finally, recall that each $\varphi(\boldsymbol{\rho}_{\alpha,i})$ that we have used to define $\tilde{f}_2$ is a linear combination of polynomials from $\mathscr{B}_i$. The coefficients in this linear combination are determined by eigenvectors of the matrix M_i, the definition of which does not depend on the value of κ. Thus by replacing $\varphi(\tilde{\kappa}_1)$ with $\tilde{\kappa}_2$ in every element of $\mathscr{B}_i$, each $\varphi(\boldsymbol{\rho}_{\alpha,i})$ with $2d \,|\, \operatorname{ord}(\alpha)$ becomes a polynomial in $\mathscr{P}_x(\overline{\mathbb{Z}}, d)$ as determined by $\tilde{\kappa}_2$ rather than $\varphi(\tilde{\kappa}_1)$. This replacement does not change the image of $\varphi(\boldsymbol{\rho}_{\alpha,i})$ (and thus of $\tilde{f}_2$) under π_2 because $\pi_2(\tilde{\kappa}_2) = \kappa = \pi_1(\tilde{\kappa}_1) = \pi_2(\varphi(\tilde{\kappa}_1))$. Altogether, we

have shown that $\Phi(\pi_1(\tilde{f}_1))$, which is an arbitrary element of $\Phi(\pi_1(\mathscr{P}_x(\overline{\mathbb{Z}}, d)))$ as determined by $\tilde{\kappa}_1$, belongs to $\Phi(\pi_2(\mathscr{P}_x(\overline{\mathbb{Z}}, d)))$ as determined by $\tilde{\kappa}_2$. □

Notation 6.22. If $q \not\equiv \pm 1 \bmod 2d$ let $\mathscr{P}(\mathbb{F}_q, d)$ denote the image of $\Phi(\mathscr{P}_x(\overline{\mathbb{Z}}, d))$ in $\mathscr{P}(\mathbb{F}_q)$ from Proposition 6.21, and if $q \equiv \pm 1 \bmod 2d$ let $\mathscr{P}(\mathbb{F}_q, d) = \{0\}$. Let $\mathscr{P}(\mathbb{F}_q, \infty)$ denote the vector space sum $\sum_d \mathscr{P}(\mathbb{F}_q, d)$ for $d \geq 2$.

By construction, $\mathscr{P}(\mathbb{F}_q, d) \subseteq \mathscr{P}(\mathbb{F}_q, \infty) \subseteq \mathscr{P}(\mathbb{F}_q)$ for any d. In particular $\mathscr{P}^\perp(\mathbb{F}_q) \subseteq \mathscr{P}^\perp(\mathbb{F}_q, \infty) \subseteq \mathscr{P}^\perp(\mathbb{F}_q, d)$, where the orthogonal complement is taken in $\mathbb{F}_q^q$ as in Notation 4.4. This is important in view of Theorem 4.7, which rephrases the Q-Classification Conjecture and Theorem 1.1 in terms of spanning sets for $\mathscr{P}^\perp(\mathbb{F}_q)$.

Notation 6.23. For $n \geq 0$, let $\mathscr{P}_n(\mathbb{F}_q, d)$ and $\mathscr{P}_n(\mathbb{F}_q, \infty)$ denote the set of polynomials in $\mathscr{P}(\mathbb{F}_q, d)$ and $\mathscr{P}(\mathbb{F}_q, \infty)$, respectively, of degree at most n.

7. Generalized eigenvectors for $\alpha = \pm 2$

Given any integer d, the purpose of this section is to reduce the proof of Theorem 1.1 (and the Q-Classification Conjecture) for primes $p \neq \pm 1 \bmod 2d$ to a finite computation with complexity depending on d. This is achieved by the following theorem.

Theorem 7.1. *Let $\kappa \in \mathbb{F}_p \backslash \{4\}$ with $p \geq 7$ a prime. If there exist integers $d \geq 4$ and $n \geq 3d$ such that*

$$\dim(\mathscr{P}_{2n}(\mathbb{F}_p, d)) \geq \begin{cases} 2n-4 & \kappa = 3 \text{ and } d \neq 4, 5 \\ 2n-3 & \kappa = 2, 2+\varphi, 2+\overline{\varphi} \text{ or } \kappa = 3 \text{ and } d = 4, 5 \\ 2n-2 & \text{otherwise,} \end{cases}$$

then Theorem 1.1 (and the Q-Classification Conjecture) holds for κ and p.

We first prove an initial consequence of the rank bound above. Then the proof is paused, and what remains of it is split into several pieces (depending on κ) at the end of this section.

Recall the vectors in (4.1) and (4.2). We also define three new vectors,

$$\begin{aligned} \mathbf{y}_0 &= \mathbf{e}_2^T - 12\mathbf{e}_4^T, \\ \mathbf{y}_p &= (4-\kappa)^{-1}\mathbf{e}_{p-1}^T, \\ \text{and } \mathbf{y}_\mathbb{R} &= -\sum_{i=1}^{\frac{p-1}{2}} \left(\binom{2i}{i} \sum_{j=1}^{i} \binom{2j}{j}^{-1} \frac{\kappa^{j-1}}{j} \right) \mathbf{e}_{2i}^T. \end{aligned}$$

It turns out that even if $\mathscr{P}_n(\mathbb{F}_p, d)$ has the dimension required in the statement of Theorem 7.1, $\mathscr{P}(\mathbb{F}_p, \infty)$ is still not big enough to prove that $\mathscr{P}(\mathbb{F}_q)$ equals what we expect it to. Specifically, $\mathscr{P}(\mathbb{F}_p, \infty)$ can never eliminate the possibility that $\mathbf{y}_0$, $\mathbf{y}_p$, or $\mathbf{y}_\mathbb{R}$ lies in $\mathscr{P}^\perp(\mathbb{F}_p)$, but none of those vectors appear in the spans in Theorem 4.7.

Lemma 7.2. *Let $\kappa \in \mathbb{F}_p \backslash \{4\}$. If the hypothesis of Theorem 7.1 holds, then $\mathscr{P}^\perp(\mathbb{F}_p)$ is contained in the span of*

- *(0)* $\mathbf{y}_\mathscr{M}$, $\mathbf{y}_p$, $\mathbf{y}_\kappa$, *and* $\mathbf{y}_0$ *if* $\kappa = 0$,
- *(1)* $\mathbf{y}_\mathscr{M}$, $\mathbf{y}_\mathbb{R}$, $\mathbf{y}_p$, *and* $\mathbf{y}_\kappa$ *when* $\kappa \neq 0, 2, 3, 2+\varphi, 2+\overline{\varphi}$,
- *(2)* $\mathbf{y}_\mathscr{M}$, $\mathbf{y}_\mathbb{R}$, $\mathbf{y}_p$, $\mathbf{y}_\kappa$, *and* $\mathbf{y}_1$ *when* $\kappa = 2$,
- *(3a)* $\mathbf{y}_\mathscr{M}$, $\mathbf{y}_\mathbb{R}$, $\mathbf{y}_p$, $\mathbf{y}_\kappa$, *and* $\mathbf{y}_\varphi$ *when* $\kappa = 2+\varphi$,

(3b) $\mathbf{y}_{\mathscr{M}}$, $\mathbf{y}_{\mathbb{R}}$, $\mathbf{y}_p$, $\mathbf{y}_\kappa$, *and* $\mathbf{y}_{\overline{\varphi}}$ *when* $\kappa = 2+\overline{\varphi}$, *or*
(4) $\mathbf{y}_{\mathscr{M}}$, $\mathbf{y}_{\mathbb{R}}$, $\mathbf{y}_p$, $\mathbf{y}_\kappa$, $\mathbf{y}_2$, *and* $\mathbf{y}_5$ *when* $\kappa = 3$.

Proof. Our first claim is that if the hypothesis of Theorem 7.1 holds, then

$$\dim(\mathscr{P}_{p-2}(\mathbb{F}_p,\infty)) \geq \begin{cases} p-6 & \kappa = 3 \text{ and } d \neq 4,5 \\ p-5 & \kappa = 2, 2+\varphi, 2+\overline{\varphi} \text{ or } \kappa = 3 \text{ and } d = 4,5 \\ p-4 & \text{otherwise,} \end{cases} \tag{7.1}$$

If $2n > p-2$, this is immediate by linear algebra, so suppose $2n < p-2$. Since $\mathscr{P}(\mathbb{F}_p,\infty)$ automatically contains every odd degree monomial, filling in the gap between $2n$ and $p-2$ amounts to producing a polynomial in $\mathscr{P}(\mathbb{F}_p,\infty)$ of degree $2m$ for all $n < m \leq \frac{p-3}{2}$.

Consider such an m, and let $\tilde{n} = d\lceil \frac{m}{d} \rceil$. By Corollary 6.20, $\Phi(\mathscr{P}_x(\overline{\mathbb{Z}},d))$ contains a polynomial of degree $2m$ with leading coefficient $2\binom{\tilde{n}+m-1}{\tilde{n}-m}(4-\tilde{\kappa})^{\tilde{n}}\tilde{n}^{\tilde{n}}$, where $\tilde{\kappa}$ is any lift of κ with respect to some surjection $\overline{\mathbb{Z}} \to \overline{\mathbb{F}}_p$. The image of this polynomial in $\mathscr{P}(\mathbb{F}_q,d)$ has degree $2m$ provided $\tilde{n}+m \leq p$, because then the leading coefficient does not vanish in $\overline{\mathbb{F}}_p$.

If it happens that $\tilde{n}+m > p$, then $m > p-\tilde{n} \geq p-(m+d-1)$. This rearranges to $2m > p-d+1$. Since $d \leq \frac{1}{3}n$ and $n \leq \frac{p-3}{2}$ by hypothesis, we see that $2m$ is much too large to divide $p+1$ or $p-1$. Thus we may take $d = m$ in Corollary 6.20 to obtain a polynomial in $\Phi(\mathscr{P}_x(\overline{\mathbb{Z}},m))$ of degree $2m$ with leading coefficient $2(4-\tilde{\kappa})^m m^m$. Again, the degree is maintained under the map $\overline{\mathbb{Z}} \to \overline{\mathbb{F}}_p$.

We have shown that $\mathscr{P}_{p-2}(\mathbb{F}_p,\infty)$ contains a polynomial of every degree between $2n$ and $p-2$, thereby proving (7.1). In particular, the orthogonal complement $\mathscr{P}_{p-2}^{\perp}(\mathbb{F}_p,\infty)$ has dimension 6, 5, or 4, depending on κ and d as stated in (7.1). Our final claim is that the 6, 5, or 4 vectors listed in the statement of this lemma span $\mathscr{P}_{p-2}^{\perp}(\mathbb{F}_p,\infty)$ and thus $\mathscr{P}^{\perp}(\mathbb{F}_p)$. This will complete the proof.

The complement $\mathscr{P}_{p-2}^{\perp}(\mathbb{F}_p,\infty)$ evidently contains $\mathbf{y}_p = (4-\kappa)^{-1}\mathbf{e}_{p-1}^T$ because degrees in $\mathscr{P}_{p-2}(\mathbb{F}_p,\infty)$ are bounded by $p-2$.

Now we turn to $\mathbf{y}_\kappa = 2\mathbf{x}(0) + \frac{1}{2}(\mathbf{x}(\sqrt{\kappa}) + \mathbf{x}(-\sqrt{\kappa}))$. Again let $\tilde{\kappa}$ be a lift of κ with respect to some surjection $\overline{\mathbb{Z}} \to \overline{\mathbb{F}}_p$. We will use the case (1) orbit from Theorem 2.5, call it $\tilde{\mathcal{O}} \coloneqq \Gamma \cdot (\sqrt{\tilde{\kappa}},0,0) \subset \mathscr{M}(\overline{\mathbb{Z}})$, to prove that $\mathbf{y}_\kappa$ belongs to $\mathscr{P}_{p-2}^{\perp}(\mathbb{F}_p,\infty)$ for any $\kappa \in \mathbb{F}_p \backslash \{4\}$. By construction of $\mathbf{y}_\kappa$, it suffices to show that $\sum_{\tilde{\mathcal{O}}} f(\mathbf{t}) = 0$ for an any $f \in \mathscr{P}_x(\overline{\mathbb{Z}},d)$ with $d \geq 4$. (Note that when $d = 2$ or 3, there are no primes $p \geq 7$ with $p \not\equiv \pm 1 \bmod 2d$.) To do this, we will show that $\sum_{\tilde{\mathcal{O}}} f^*(\mathbf{t}) = 0$, and we may assume without loss of generality that f^* is even as a polynomial in y because $\tilde{\mathcal{O}}$ is closed under $(x,y,z) \mapsto (x,-y,-z)$. Observe that $\tilde{\mathcal{O}}$ breaks into first coordinate orbits $\tilde{\mathcal{O}}_{\sqrt{\kappa}} \coloneqq \Gamma_x \cdot (\sqrt{\kappa},0,0)$, $\tilde{\mathcal{O}}_{-\sqrt{\kappa}} \coloneqq \Gamma_x \cdot (-\sqrt{\kappa},0,0)$ and $\tilde{\mathcal{O}}_0 \coloneqq \Gamma_x \cdot (0,\sqrt{\kappa},0)$. By Proposition 6.8, specifically (1) implies (5), if $f^* = f_n(x)y^{2n} + \cdots + f_0(x)$ then $(x^2-\kappa) \mid f_0(x)$. Since every y-coordinate in $\tilde{\mathcal{O}}_{\sqrt{\kappa}}$ is 0, we have

$$\sum_{\mathbf{t} \in \tilde{\mathcal{O}}_{\sqrt{\kappa}}} f^*(\mathbf{t}) = \sum_{\mathbf{t} \in \tilde{\mathcal{O}}_{\sqrt{\kappa}}} f_0(x) = |\tilde{\mathcal{O}}_{\sqrt{\kappa}}| f_0(\sqrt{\kappa}) = 0.$$

The sum of f over $\tilde{\mathcal{O}}_{-\sqrt{\kappa}}$ vanishes by the same reasoning. Regarding $\tilde{\mathcal{O}}_0$, since $\operatorname{ord}(0) = 4$ is not divisible by $2d$, we have $\sum_{\tilde{\mathcal{O}}_0} f^*(\mathbf{t}) = 0$ by definition of $\mathscr{P}_x(\overline{\mathbb{Z}},d)$. Summing over all first-coordinate orbits gives $\sum_{\tilde{\mathcal{O}}} f^*(\mathbf{t}) = 0$, as desired.

A similar argument using the case (2) orbit $\Gamma \cdot (1,1,0)$ from Theorem 2.5 proves that $\mathbf{y}_1 = \mathbf{x}(0) + \frac{3}{2}(\mathbf{x}(1) + 3\mathbf{x}(-1))$ belongs to $\mathscr{P}^{\perp}_{p-2}(\mathbb{F}_p, \infty)$ when $\kappa = 2$. Indeed, the orbit entries 0 and ± 1 have rotation order 4 and 6, which are not divisible by $2d$ (assuming there exist primes $p \geq 7$ with $p \not\equiv \pm 1 \bmod 2d$).

In case (3a) and (3b), where $\kappa = 2 + \varphi$ or $2 + \overline{\varphi}$, all orbit entries have order 4, 6, or 10. This appears to create potential trouble for proving that $\mathbf{y}_\varphi$ or $\mathbf{y}_{\overline{\varphi}}$) belongs to $\mathscr{P}^{\perp}(\mathbb{F}_p, d)$ in the special case $d = 5$. However, in order for $\kappa = 2 + \varphi$ or $2 + \overline{\varphi}$ to be possible when $p \geq 7$, we must have $p \equiv \pm 1 \bmod 10$, implying $\mathscr{P}(\mathbb{F}_p, 5) = 0$ by definition. Thus $\mathbf{y}_\varphi \in \mathscr{P}^{\perp}(\mathbb{F}_q, \infty)$ when $\kappa = 2 + \varphi$ and $\mathbf{y}_{\overline{\varphi}} \in \mathscr{P}^{\perp}(\mathbb{F}_q, \infty)$ when $\kappa = 2 + \overline{\varphi}$.

When $\kappa = 3$, the orbits in cases (4a) and (4b) of Theorem 2.5 contain elements of order 4, 6, 8, and 10. There are two possibilities for failure: when $d = 4$ and $p \not\equiv \pm 1 \bmod 8$ the vector

$$\mathbf{y}_2 = 2\mathbf{x}(0) + \tfrac{3}{2}(\mathbf{x}(1) + \mathbf{x}(-1)) + 2(\mathbf{x}(\sqrt{2}) + \mathbf{x}(-\sqrt{2}))$$

may not lie in $\mathscr{P}^{\perp}(\mathbb{F}_p, 4)$ because $\operatorname{ord}(\pm\sqrt{2}) = 8$ is divisible by $2d$; and when $d = 5$ and $p \not\equiv \pm 1 \bmod 10$ the vector

$$\mathbf{y}_5 = 2\mathbf{x}(0) + 3(\mathbf{x}(1) + \mathbf{x}(-1)) + \tfrac{5}{2}(\mathbf{x}(\varphi) + \mathbf{x}(-\varphi)) + \tfrac{5}{2}(\mathbf{x}(\overline{\varphi}) + \mathbf{x}(-\overline{\varphi}))$$

may not lie in $\mathscr{P}^{\perp}(\mathbb{F}_p, 5)$ because $\operatorname{ord}(\pm\varphi) = \operatorname{ord}(\pm\overline{\varphi}) = 10$ is divisible by $2d$. We have accounted for this in the statement Theorem 7.1 and in (7.1) by increasing the rank requirement by one for $\kappa = 3$ when $d = 4$ or 5. This decreases the number of spanning vectors that we must find for $\mathscr{P}^{\perp}_{p-2}(\mathbb{F}_p, \infty)$ by one. (It turns out that $\mathbf{y}_2$ and $\mathbf{y}_5$ do *not* belong to $\mathscr{P}^{\perp}_{p-2}(\mathbb{F}_p, 4)$ or $\mathscr{P}^{\perp}_{p-2}(\mathbb{F}_p, 5)$, respectively. In fact, experimentation suggests that they are not orthogonal to single nonzero even polynomial in $\mathscr{P}_x(\overline{\mathbb{Z}}_p, 4)$ or $\mathscr{P}_x(\overline{\mathbb{Z}}, 5)$.)

From the list of vectors in the lemma statement, it remains to consider $\mathbf{y}_{\mathscr{M}}$ and $\mathbf{y}_{\mathbb{R}}$ for general κ and $\mathbf{y}_0$ for $\kappa = 0$.

Let $f \in \mathscr{P}_x(\overline{\mathbb{Z}}, d)$, and suppose $f^* = f_n(x)y^{2n} + \cdots + f_0(x)$. Choose the lift $\tilde{\kappa}$ of κ to lie in the interval $(0, 4)$ so that we may employ the compact smooth surface $\mathscr{M}^\circ \subset \mathscr{M}(\mathbb{R})$. We have

$$\begin{aligned}
0 &= \int_{-\sqrt{\tilde{\kappa}}}^{\sqrt{\tilde{\kappa}}} \frac{0}{\sqrt{4 - x^2}} dx \\
&= \int_{-\sqrt{\tilde{\kappa}}}^{\sqrt{\tilde{\kappa}}} \frac{\sum_j \binom{2j}{j} (\frac{x^2 - \tilde{\kappa}}{x^2 - 4})^j f_j}{\sqrt{4 - x^2}} dx && \text{by Proposition 6.8} \\
&= \frac{1}{2\pi} \int_{-\sqrt{\tilde{\kappa}}}^{\sqrt{\tilde{\kappa}}} \left(\sum_{j=0}^{n} f_j \int_{\mathscr{O}_x} y^{2j} dA_x \right) dx && \text{by Corollary 5.9} \\
&= \frac{1}{2\pi} \int_{\mathscr{M}^\circ} f^* dA \\
&= \frac{1}{2\pi} \int_{\mathscr{M}^\circ} \Phi(f^*) dA && \text{by } \Gamma\text{-invariance of } dA \text{ and } \mathscr{M}^\circ \\
&= \frac{1}{2\pi} \int_{\mathscr{M}^\circ} \Phi(f) dA && \text{by Proposition 5.5.} \qquad (7.2)
\end{aligned}$$

Only the variable x appears in the argument of the last integral. The integral of any odd-degree monomial term of $\Phi(f)$ vanishes since $\mathscr{M}^\circ$ is closed under $(x, y, z) \mapsto$

$(-x,-y,z)$. Consider what happens when we integrate an even-degree monomial terms of $\Phi(f)$:

$$\frac{1}{2\pi}\int_{\mathscr{M}^\circ} x^{2j}\,dA = \int_{-\sqrt{\tilde\kappa}}^{\sqrt{\tilde\kappa}} \left(\frac{x^{2j}}{2\pi}\int_{\mathscr{O}_x} dA_x\right) dx = \int_{-\sqrt{\tilde\kappa}}^{\sqrt{\tilde\kappa}} \frac{x^{2j}}{\sqrt{4-x^2}}\,dx$$

by Corollary 5.9. This last integral can be computed using integration by parts and induction on j. The result is

$$2\binom{2j}{j}\arcsin\left(\frac{\sqrt{\tilde\kappa}}{2}\right) - \sqrt{4\tilde\kappa-\tilde\kappa^3}\binom{2j}{j}\sum_{i=1}^{j}\binom{2i}{i}^{-1}\frac{\tilde\kappa^{i-1}}{i}.$$

Let $\Phi(f) = c_{\tilde n}x^{2\tilde n} + \cdots + c_0$. By substituting the formula above into (7.2), we see that

$$0 = 2\arcsin\left(\frac{\sqrt{\tilde\kappa}}{2}\right)\sum_{j=0}^{\tilde n}\binom{2j}{j}c_j - \sqrt{4\tilde\kappa-\tilde\kappa^3}\sum_{j=1}^{\tilde n}\binom{2j}{j}c_j\sum_{i=1}^{j}\binom{2i}{i}^{-1}\frac{\tilde\kappa^{i-1}}{i}.$$

By the Hermite–Lindemann theorem, $\arcsin(\frac{1}{2}\sqrt{\tilde\kappa})$ is transcendental because $\frac{1}{2}\sqrt{\tilde\kappa}$ is algebraic and nonzero [Wal00, Chapter 1]. This forces both

$$0 = \sum_{j=0}^{\tilde n}\binom{2j}{j}c_j \quad\text{and}\quad 0 = \sum_{j=1}^{\tilde n}\binom{2j}{j}c_j\sum_{i=1}^{j}\binom{2i}{i}^{-1}\frac{\tilde\kappa^{i-1}}{i}.$$

In particular, the Φ reduction of any linear combination of polynomials in $\mathscr{P}_x(\overline{\mathbb{Z}},d)$, with d allowed to vary, also satisfies the two equations above. If the image in $\mathscr{P}(\mathbb{F}_p,\infty)$ of such a combination has degree at most $p-2$ (or even $p-1$), we see that it is orthogonal to $\mathbf{y}_{\mathscr{M}}$ and $\mathbf{y}_{\mathbb{R}}$. Note that no generality was lost by only considering f for which f^* is even as a polynomial in y—deleting odd powers of y neither affects a polynomial's membership in $\mathscr{P}_x(\overline{\mathbb{Z}},d)$ nor the orthogonality to $\mathbf{y}_{\mathscr{M}}$ or $\mathbf{y}_{\mathbb{R}}$ of its image in $\mathscr{P}_{p-2}(\mathbb{F}_p,\infty)$.

(Remark that $\mathbf{y}_{\mathbb{R}}$ is also in $\mathscr{P}_{p-2}^{\perp}(\mathbb{F}_p,\infty)$ when $\kappa=0$, but it need not be listed in case (0) of the lemma statement because

$$\mathbf{y}_{\mathbb{R}} = -\frac{1}{2}\sum_{i=1}^{\frac{p-1}{2}}\binom{2i}{i}\mathbf{e}_{2i}^T = -\frac{1}{2}\mathbf{y}_{\mathscr{M}} + \frac{1}{6}\mathbf{y}_{\kappa}.$$

This is the one case where $\mathbf{y}_{\mathbb{R}}$ actually belongs in $\mathscr{P}^{\perp}(\mathbb{F}_p)$.)

Finally, consider $\kappa=0$ and $\mathbf{y}_0 = \mathbf{e}_2^T - 12\mathbf{e}_4^T$. We take $\tilde\kappa=0$ as our lift of κ. As usual, let $f\in\mathscr{P}_x(\overline{\mathbb{Z}},d)$ for some $d\geq 4$, and assume without loss of generality that f^* is even as a polynomial in y. By Corollary 6.14, $\Phi(f)$ is a linear combination of the polynomials $\Phi(\wp_{\alpha,i})$ for $i\geq 2$ and $\alpha\in\widehat{\Lambda}_i$ with $2d\,|\,\mathrm{ord}(\alpha)$. To prove that $\Phi(f)$ is orthogonal to $\mathbf{y}_0$ (taking inner products in characteristic 0), we will show that every such $\Phi(\wp_{\alpha,i})$ is orthogonal to $\mathbf{y}_0$. We are only considering those α for which $2d\,|\,\mathrm{ord}(\alpha)$, which excludes $\alpha=0$. Thus $\Phi(\wp_{\alpha,i})$ is orthogonal to $\mathbf{y}_0$ if and only if the same is true of $\alpha^5\Phi(\wp_{\alpha,i}) = \Phi(x^5\wp_{\alpha,i})$. We claim that the Φ reduction of each monomial term in $x^5\wp_{\alpha,i}$ is, by itself, orthogonal to $\mathbf{y}_0$. In fact, this is true of the Φ reduction of any monomial of total degree at least five. Indeed, up to permuting variables, the only monomial $x^\ell y^m z^n$ of total degree five with $\ell\equiv m\equiv n \bmod 2$ is x^3yz. We have $\Phi(x^3yz) = x^4+12x^2$, which is orthogonal to $\mathbf{y}_0$. The reduction of any monomial with odd total degree is also orthogonal to $\mathbf{y}_0$ by Proposition 5.1.

Therefore, by induction on total degree, $\Phi(x^\ell y^m z^n)$ is orthogonal to $\mathbf{y}_0$ whenever $\ell+m+n \geq 5$. $\square$

The last step in the proof of Theorem 7.1 is to whittle the spanning vectors from Lemma 7.2 down to those in the statement of Theorem 4.7. We achieve this using the extra polynomials $\Phi((x^{p+1}-x^2)f) \in \mathscr{P}(\mathbb{F}_p)$, where $f = f(x,y,z)$ is chosen to make the Φ computation as simple as possible (while avoiding those f for which $\Phi((x^{p+1}-x^2)f) \in \mathscr{P}(\mathbb{F}_p,\infty)$). The most convienient polynomials f turn out to come from the as yet unused eigenvalues of A_n in Lemma 6.3, namely ± 2. (Recall that $\mathscr{p}_{\alpha,n}$ has only been defined for $\alpha \in \widehat{\Lambda}_n = \Lambda_n \backslash \{\pm 2\}$.) The eigenvectors of A_n of eigenvalue 2 and -2 extend to generalized eigenvectors of M_n, that we denote $\mathscr{p}_{2,n}$ and $\mathscr{p}_{-2,n}$. It turns out that $\Phi((x^{p+1}-x^2)\mathscr{p}_{2,n})$ and $\Phi((x^{p+1}-x^2)\mathscr{p}_{-2,n})$ are not orthogonal to the extra vectors that appear in Lemma 7.2 but do not appear in Theorem 4.7. Demonstrating this is the only goal for the remained of this section.

The next several pages are devoted to finding a formula for $\Phi((x^{p+1}-x^2)\mathscr{p}^+_{2,n})$ where $\mathscr{p}^+_{2,n} = \frac{1}{2}(\mathscr{p}_{2,n}+\mathscr{p}_{-2,n})$. Similar to Section 6, we achieve this without ever finding the coefficients of $\mathscr{p}^+_{2,n}$. (In particular, our strategy is not to first compute $\mathscr{p}^+_{2,n}$ then apply Theorem 5.11 to $\Phi(x^{p+1}\mathscr{p}^+_{2,n})$ and $\Phi(x^2\mathscr{p}^+_{2,n})$). This formula is essentially Proposition 7.6, which provides the coefficient of x^{2i} in $\Phi((x^{p+1}-x^2)\mathscr{p}^+_{2,n})$ when $i \geq n$. For general κ, we only end up needing a complete formula for $\Phi((x^{p+1}-x^2)\mathscr{p}^+_{2,n})$ for $n \leq 4$, so Proposition 7.6 leaves very little computational work to be done. Then Proposition 7.10 helps computes the dot product of the coefficient vector of $\Phi((x^{p+1}-x^2)\mathscr{p}^+_{2,n})$ with $\mathbf{y}_p$, $\mathbf{y}_{\mathbb{R}}$, and $\mathbf{y}_\kappa$. This allows us to verify that no linear combination of $\mathbf{y}_p$ and $\mathbf{y}_{\mathbb{R}}$ when $\left(\frac{\kappa}{p}\right) = 1$ (the Legendre symbol) or $\mathbf{y}_p$, $\mathbf{y}_{\mathbb{R}}$, and $\mathbf{y}_\kappa$ when $\left(\frac{\kappa}{p}\right) = -1$ is orthogonal to each $\Phi((x^{p+1}-x^2)\mathscr{p}^+_{2,n})$ for $n \leq 4$. Eliminating those two or three (depending on $\left(\frac{\kappa}{p}\right)$) vectors from the span of $\mathscr{P}^\perp(\mathbb{F}_p)$ is all we must do for $\kappa \neq 0,3$. For $\kappa = 0$ we proceed similarly, but with the aim of eliminating $\mathbf{y}_p$ and $\mathbf{y}_0$ from $\mathscr{P}^\perp(\mathbb{F}_p)$; and for $\kappa = 3$ we aim to eliminate $\mathbf{y}_p$, $\mathbf{y}_{\mathbb{R}}$, and potentially $\mathbf{y}_\kappa$, $\mathbf{y}_2$ and $\mathbf{y}_5$ depending on $\left(\frac{\kappa}{p}\right)$, $\left(\frac{2}{p}\right)$, and $\left(\frac{5}{p}\right)$.

Let us now proceed to defining $\mathscr{p}^+_{2,n}$ and computing $\Phi((x^{p+1}-x^2)\mathscr{p}^+_{2,n})$.

Over any integral domain R of characteristic 0, the matrix M_n defined in (6.5) has $n+1$ generalized eigenvectors with eigenvalue 2, denote them $\mathbf{p}_0,\ldots,\mathbf{p}_n$, that satisfy $M_n\mathbf{p}_0 = 2\mathbf{p}_0$ and $M_n\mathbf{p}_i = 2\mathbf{p}_i + \mathbf{p}_{i-1}$. Let us briefly justify this existence claim. Since M_n is nearly a block diagonal matrix with blocks $A_0,\ldots,A_n$, it is convenient to name the corresponding block vectors that concatenate to form $\mathbf{p}_i$. Call them $\mathbf{p}_{i,0},\ldots,\mathbf{p}_{i,n}$, so $\mathbf{p}_{i,j}$ is a $(j+1)$-dimensional column vector over the field of fractions F. Recall from Lemma 6.3 that the algebraic and geometric multiplicities of the eigenvalue 2 for each of the diagonal blocks $A_0,\ldots,A_n$ is exactly one and that the 2-eigenvector of A_i is

$$\mathbf{p}_{i,i} \coloneqq c\begin{bmatrix}1\\2\\\vdots\\2\\1\end{bmatrix} \in R^{i+1}$$

for $c \in F$. Extend this vector upward with zeros by letting $\mathbf{p}_{i,j}$ be the zero vector when $j > i$. Linear algebra then guarantees that there exists a nonzero choice of scalar c and components $\mathbf{p}_{i,j}$ for $j < i$ that make $\mathbf{p}_i$ a generalized eigenvector.

Furthermore, $\mathbf{p}_i$ is not a genuine eigenvector for $i \geq 1$ because there is no solution $\mathbf{p}_{i,i-1}$ to the vector equation

$$B_{i-1}\mathbf{p}_{i,i} + A_{i-1}\mathbf{p}_{i,i-1} = 2\mathbf{p}_{i,i-1}.$$

Indeed, the sum of the entries in $B_{i-1}\mathbf{p}_{i,i}$ is $2i-1 \neq 0$, but the sum of the entries in any one of the columns of $A_{i-1} - 2\mathrm{Id}_i$ is 0. Thus $\mathbf{p}_i$ must satisfy $M_n\mathbf{p}_i = 2\mathbf{p}_i + \mathbf{p}_{i-1}$ (assuming $\mathbf{p}_{i-1}$ was constructed similarly with $\mathbf{p}_{i-1,i-1}$ being the largest nonzero block component).

Note that these vectors are not yet uniquely determined. Since $M_n\mathbf{p}_0 = 2\mathbf{p}_0$, adding any multiple of $\mathbf{p}_0$ to $\mathbf{p}_i$ preserves the equation $M_n\mathbf{p}_i = 2\mathbf{p}_i + \mathbf{p}_{i-1}$. We take the unique choice of $\mathbf{p}_i$ for which

$$\mathbf{p}_{i,0} = [0] \text{ for } i \geq 1. \tag{7.3}$$

Setting $\mathbf{p}_{0,0} = 1$, we have now defined $\mathbf{p}_i$ for $i \geq 1$.

The first three generalized eigenvectors are

$$\mathbf{p}_0 = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{bmatrix}, \quad \mathbf{p}_1 = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}, \quad \text{and } \mathbf{p}_2 = \frac{1}{6}\begin{bmatrix} 0 \\ \vdots \\ 0 \\ 4 \\ 8 \\ 4 \\ 1 \\ 0 \\ 0 \end{bmatrix}. \tag{7.4}$$

Not decorating $\mathbf{p}_i$ with an "n" is an abuse of notation because there is otherwise no indication of what dimension the vector lives in. That is, the number of zero entries above $\mathbf{p}_{i,i}$ in (7.4) is not specified. We eliminate this abuse of notation by switching to polynomials.

Notation 7.3. Let $\mathscr{p}_{2,n} \in F[x,y,z]$ denote the polynomial corresponding $\mathbf{p}_n$ with respect to the basis $\mathscr{B}_n$ defined at the start of Section 6. Also let $\mathscr{p}_{-2,n}(x,y,z) \coloneqq \mathscr{p}_{2,n}(-x,-y,z)$ and $\mathscr{p}^+_{2,n} = \frac{1}{2}(\mathscr{p}_{2,n} + \mathscr{p}_{-2,n})$.

Care must be taken in translating $M_n\mathbf{p}_n = 2\mathbf{p}_n + \mathbf{p}_{n-1}$ into a polynomial equation since $\mathscr{p}_{2,n}$ is defined according to $\mathscr{B}_n$ while $\mathscr{p}_{2,n-1}$ is defined according to $\mathscr{B}_{n-1}$. For $i \leq n-1$, the monomials in $\mathscr{B}_{i,n-1}$ must be scaled by $(x^2-\kappa)$ to match those in $\mathscr{B}_{i,n}$. Thus $M_n\mathbf{p}_n = 2\mathbf{p}_n + \mathbf{p}_{n-1}$ becomes

$$\Phi_x(x\mathscr{p}_{2,n}) = 2\mathscr{p}_{2,n} + (x^2-\kappa)\mathscr{p}_{2,n-1} \tag{7.5}$$

by Proposition 6.1. Let us apply this formula to help compute $\Phi(x^m\mathscr{p}_{2,n})$ for any m. (We need not reference the vectors $\mathbf{p}_i$ again. They are simply a convenient way to prove that the $\mathscr{p}_{2,i}$ exist and to compute their coefficients.)

The lemma below holds for any m and n by regarding empty sums and improper binomial coefficients as 0. Its forthcoming application, however, is to compute $\Phi(x^m\mathscr{p}_n)$ for $n = 1,2,3,4,5$ and large m. So coefficients of the vast majority of powers of x, namely x^i for $i > n$, are fully determined by the next lemma's right-side sum. As we will show, the left-side sum only contributes to coefficients of x^i for $i \leq n$.

Lemma 7.4. *For any $m \geq 0$ and $n \geq 1$,*

$$\Phi(x^m \mathcal{p}_{2,n}) = \sum_{i=0}^{n-1} \binom{m}{i} 2^{m-i} \Phi\big((x^2-\kappa)^i \mathcal{p}_{2,n-i}\big) + 2^{m-n}(x^2-\kappa)^n \sum_{i=0}^{m-n} \binom{m-i-1}{n-1} \frac{x^i}{2^i}.$$

Proof. We will prove the equality above with both occurrences of "Φ" replaced by "Φ_x". That is,

$$\Phi_x(x^m \mathcal{p}_{2,n}) = \sum_{i=0}^{n-1} \binom{m}{i} 2^{m-i} \Phi_x\big((x^2-\kappa)^i \mathcal{p}_{2,n-i}\big) + 2^{m-n}(x^2-\kappa)^n \sum_{i=0}^{m-n} \binom{m-i-1}{n-1} \frac{x^i}{2^i}. \tag{7.6}$$

This would imply the lemma by applying Φ to (7.6) and using $\Phi \circ \Phi_x = \Phi$.

To prove (7.6) we use induction on m. In the base case, $m = 0$, (7.6) becomes the vacuous assertion $\Phi_x(\mathcal{p}_{2,n}) = \Phi_x(\mathcal{p}_{2,n})$. Now assume (7.6) holds for some $m \geq 0$. Observe that

$$\begin{aligned} \Phi_x(x^{m+1}\mathcal{p}_{2,n}) &= \Phi_x(x^m \Phi_x(x\mathcal{p}_{2,n})) \\ &= \Phi_x(x^m \Phi_x(2\mathcal{p}_{2,n} + (x^2-\kappa)\mathcal{p}_{2,n-1})) \\ &= 2\Phi_x(x^m \mathcal{p}_{2,n}) + \Phi_x((x^2-\kappa)\Phi_x(x^m \mathcal{p}_{2,n-1})). \end{aligned} \tag{7.7}$$

Here we consider the case $n = 1$ separately from $n \geq 2$. Recall that $\mathcal{p}_{2,0} = 1$. Applying the equation above when $n = 1$ followed by the induction hypothesis gives

$$\begin{aligned} \Phi_x(x^{m+1}\mathcal{p}_{2,1}) &= 2\Phi_x(x^m \mathcal{p}_{2,1}) + (x^2-\kappa)x^m \\ &= 2\left(2^m \Phi_x(\mathcal{p}_{2,1}) + 2^{m-1}(x^2-\kappa)\sum_{i=0}^{m-1} \frac{x^i}{2^i}\right) + (x^2-\kappa)x^m \\ &= 2^{m+1}\Phi_x(\mathcal{p}_{2,1}) + 2^m(x^2-\kappa)\sum_{i=0}^{m} \frac{x^i}{2^i}, \end{aligned}$$

which is (7.6) with $n = 1$ and m replaced by $m+1$. This completes the induction step when $n = 1$.

For $n \geq 2$, we apply the induction hypothesis to both terms $\Phi_x(x^m \mathcal{p}_{2,n})$ and $\Phi_x(x^m \mathcal{p}_{2,n-1})$ appearing in (7.7). Each application results in an expression of form (7.6), and each of these expressions contains two summations that we call the "left-side sum" and the "right-side sum". We will show that the two left-side sums from $\Phi_x(x^m \mathcal{p}_{2,n})$ and $\Phi_x(x^m \mathcal{p}_{2,n-1})$ combine to give a new left-side sum of the same form with index incremented by one, and that the same thing happens when the two right-side sums are combined.

By applying the induction hypothesis to $\Phi_x(x^m \mathcal{p}_{2,n-1})$, the left-side sum contribution from $\Phi_x((x^2-\kappa)\Phi_x(x^m \mathcal{p}_{2,n-1}))$ is

$$\Phi_x\left((x^2-\kappa)\sum_{i=0}^{n-2} \binom{m}{i} 2^{m-i} \Phi_x\big((x^2-\kappa)^i \mathcal{p}_{2,n-1-i}\big)\right) = \sum_{i=0}^{n-2} \binom{m}{i} 2^{m-i} \Phi_x\big((x^2-\kappa)^{i+1} \mathcal{p}_{2,n-1-i}\big)$$

$$= \sum_{i=1}^{n-1} \binom{m}{i-1} 2^{m+1-i} \Phi_x\big((x^2-\kappa)^i \boldsymbol{p}_{2,n-i}\big). \tag{7.8}$$

By applying the induction hypothesis to $\Phi_x(x^m \boldsymbol{p}_n)$, the left-side sum contribution from $2\Phi_x(x^m \boldsymbol{p}_n)$ is

$$2\sum_{i=0}^{n-1} \binom{m}{i} 2^{m-i} \Phi_x\big((x^2-\kappa)^i \boldsymbol{p}_{2,n-i}\big) = \sum_{i=0}^{n-1} \binom{m}{i} 2^{m+1-i} \Phi_x\big((x^2-\kappa)^i \boldsymbol{p}_{2,n-i}\big).$$

Adding this to (7.8) gives

$$\sum_{i=0}^{n-1} \left(\binom{m}{i} + \binom{m}{i-1}\right) 2^{m+1-i} \Phi_x\big((x^2-\kappa)^i \boldsymbol{p}_{2,n-i}\big) = \sum_{i=0}^{n-1} \binom{m+1}{i} 2^{m+1-i} \Phi_x\big((x^2-\kappa)^i \boldsymbol{p}_{2,n-i}\big),$$

which is the left-side sum in (7.6) with m replaced by $m+1$.

As for the two right-side sums resulting from (7.7), we begin with the contribution from $\Phi_x((x^2-\kappa)\Phi_x(x^m \boldsymbol{p}_{2,n-1}))$ again:

$$\Phi_x\left((x^2-\kappa)\left(2^{m-n+1}(x^2-\kappa)^{n-1} \sum_{i=0}^{m-n+1} \binom{m-i-1}{n-2} \frac{x^i}{2^i}\right)\right) = 2^{m+1-n}(x^2-\kappa)^n \sum_{i=0}^{m+1-n} \binom{m-i-1}{n-2} \frac{x^i}{2^i}.$$

The contribution from $2\Phi_x(x^m \boldsymbol{p}_{2,n})$ is

$$2\left(2^{m-n}(x^2-\kappa)^n \sum_{i=0}^{m-n} \binom{m-i-1}{n-1} \frac{x^i}{2^i}\right) = 2^{m+1-n}(x^2-\kappa)^n \sum_{i=0}^{m+1-n} \binom{m-i-1}{n-1} \frac{x^i}{2^i}.$$

Again we combine the two contributions to get

$$2^{m+1-n}(x^2-\kappa)^n \sum_{i=0}^{m+1-n} \left(\binom{m-i-1}{n-1} + \binom{m-i-1}{n-2}\right) \frac{x^i}{2^i} = 2^{m+1-n}(x^2-\kappa)^n \sum_{i=0}^{m+1-n} \binom{m-i}{n-1} \frac{x^i}{2^i},$$

which is the right-side sum in (7.6) with m replaced by $m+1$. This completes the induction step when $n \geq 2$ and thus the proof. □

This lemma applies equally well to computing coefficients of $\Phi(x^m \boldsymbol{p}_{-2,n})$. Indeed, if m is even then the coefficients of even powers of x in $\Phi(x^m \boldsymbol{p}_{-2,n})$ match those of $\Phi(x^m \boldsymbol{p}_{2,n})$ by Proposition 5.1, while the coefficients of odd powers of x in $\Phi(x^m \boldsymbol{p}_{-2,n})$ are the negations of those of $\Phi(x^m \boldsymbol{p}_{2,n})$. (If m is odd, this gets reversed.) In particular, setting $\boldsymbol{p}^+_{2,n} = \frac{1}{2}(\boldsymbol{p}_{2,n} + \boldsymbol{p}_{-2,n})$ means $\Phi(x^m \boldsymbol{p}^+_{2,n})$ only picks up the even-power coefficients of $\Phi(x^m \boldsymbol{p}_{2,n})$ when m is even.

Notation 7.5. For $n \geq 1$, let $\mathbf{q}_n \in \mathbb{F}_p^p$ be the vector corresponding to $\Phi((x^{p+1} - x^2)\boldsymbol{p}^+_{2,n})$ as described in Notation 4.4.

Proposition 7.6. *Let $1 \leq n \leq \frac{p-1}{2}$. If $i \geq n$, the entry in the $2i^{th}$ coordinate of $\mathbf{q}_n$ is*

$$-2^{2-n-2i} \sum_{j=0}^{n} \binom{n}{j} \binom{2i-2j+n-2}{n-1} (-4)^j \kappa^{n-j}. \tag{7.9}$$

If $1 \leq i < n$ and $n \geq 3$, the entry in the $2i^{th}$ coordinate of $\mathbf{q}_n$ is the sum of (7.9) and

$$c_{2i} + 2^{2-n-2i} \sum_{j=0}^{n} \binom{n}{j} \binom{2j-2i+1}{n-1} 4^j (-\kappa)^{n-j}, \tag{7.10}$$

where c_i is the coefficient of x^i in $-2\Phi((x^2-\kappa)\mathcal{p}_{2,n-1}) - \Phi((x^2-\kappa)^2\mathcal{p}_{2,n-2})$. If $n \geq 2$, the entry in the zeroth coordinate of $\mathbf{q}_n$ is c_0. The entry in the second coordinate of $\mathbf{q}_2$ is $\frac{1}{2}\kappa(4-\kappa)$, and the entry in the zeroth coordinate of $\mathbf{q}_1$ is 0.

Proof. It is a small computation using Lemma 7.4 to verify that the first one or two entries of $\mathbf{q}_1$ and $\mathbf{q}_2$ are as claimed. Let us turn to the $2i^{\text{th}}$ coordinate formula when either $i \geq 3$ and $n \geq 1$ or $i \geq 1$ and $n \geq 3$.

Determining $\mathbf{q}_n$ requires computing $\Phi(x^2\mathcal{p}_{2,n})$ and $\Phi(x^{p+1}\mathcal{p}_{2,n})$. For each of these reductions, Lemma 7.4 provides a formula involving two summations that we again call the left-side sum and the right-side sum. We evaluate the two left-side sums first.

When $n = 1$, the left-side sums from $\Phi(x^{p+1}\mathcal{p}_{2,1})$ and $-\Phi(x^2\mathcal{p}_{2,1})$ cancel and therefore contribute nothing to the coefficient of x^{2i}. When $n = 2$, the difference of the two left-side sums is $-2\Phi((x^2-\kappa)\mathcal{p}_{2,1}) = -2\Phi((x^2-\kappa)(y^2+yz))$, which has degree 2 and thus contributes nothing to the coefficient of x^{2i} again. For $n \geq 3$, we have the following two left-side sums:

$$\begin{aligned}
&\sum_{i=0}^{n-1} \binom{p+1}{i} 2^{p+1-i} \Phi((x^2-\kappa)^i \mathcal{p}_{2,n-i}) - \sum_{i=0}^{n-1} \binom{2}{i} 2^{2-i} \Phi((x^2-\kappa)^i \mathcal{p}_{2,n-i}) \\
&\quad = \sum_{i=0}^{1} \binom{p+1}{i} 2^{2-i} \Phi((x^2-\kappa)^i \mathcal{p}_{2,n-i}) - \sum_{i=0}^{2} \binom{2}{i} 2^{2-i} \Phi((x^2-\kappa)^i \mathcal{p}_{2,n-i}) \\
&\quad = -2\Phi((x^2-\kappa)\mathcal{p}_{2,n-1}) - \Phi((x^2-\kappa)^2 \mathcal{p}_{2,n-2}) \\
&\quad = \sum_{i \geq 0} c_i x^i,
\end{aligned}$$

where the final equality is simply the definition of the c_i. To justify the appearance of c_{2i} in (7.10) but not in (7.9), we must show that $c_{2i} = 0$ when $i \geq n$. In other words, we must show that $-2\Phi((x^2-\kappa)\mathcal{p}_{2,n-1}) - \Phi((x^2-\kappa)^2\mathcal{p}_{2,n-2})$ has degree strictly less than $2n$. Indeed, by definition of the basis $\mathscr{B}_{n-1}$ from Section 6.1, $(x^2-\kappa)\mathcal{p}_{2,n-1}$ is a linear combination of polynomials of the form $(x^2-\kappa)^{i+1}y^j z^k$ with $2i+j+k = 2n-2$ and $j \geq k$. By Proposition 5.1, the Φ reduction of such a polynomial has degree at most $2i+2+k$, which is strictly less than n unless $j = k = 0$ and $i = n-1$. But recall from the construction of $\mathcal{p}_{2,n-1}$ that the coefficient of $(x^2-\kappa)^{2n-2}$ is zero (the last entry in $\mathbf{p}_{n-1}$ as shown in (7.4). Thus $\Phi((x^2-\kappa)\mathcal{p}_{2,n-1})$ has degree at most $2n-2$. The same argument applies to $\Phi((x^2-\kappa)^2\mathcal{p}_{2,n-2})$. Altogether, we have shown that the left-side sums from Lemma 7.4 are fully accounted for by c_{2i} in (7.10).

Regarding the right-side sums, $\Phi(x^2 \not{p}_{2,n})$ contributes nothing when $n \geq 3$ because the summation interval of $i = 0$ to $2 - n$ is empty. When $n = 1$ or $n = 2$ the right-side sum contributes monomials of degree 3 or 4, respectively, which also do not contribute to the coefficient of x^{2i}. The right-side sum from $\Phi(x^{p+1} \not{p}_{2,n})$ is

$$2^{p+1-n}(x^2 - \kappa)^n \sum_{i=0}^{p+1-n} \binom{p-i}{n-1} \frac{x^i}{2^i}.$$

Here we replace 2^{p+1} with 2^2 and expand and distribute $(x^2 - \kappa)^n$. Collecting all terms of degree $2i$ gives

$$\begin{aligned} &2^{2-n} \sum_{j=0}^{\min(i,n)} \left(\binom{n}{j} x^{2j} (-\kappa)^{n-j} \right) \left(\binom{p-2i+2j}{n-1} \frac{x^{2i-2j}}{2^{2i-2j}} \right) \\ &\qquad = 2^{2-n-2i} \sum_{j=0}^{\min(i,n)} \binom{n}{j} \binom{p-2i+2j}{n-1} 4^j (-\kappa)^{n-j} x^{2i} \end{aligned} \tag{7.11}$$

Let us first suppose that the degree $2i$ above exceeds p (making $\min(i,n) = n$). Let $\tilde{i} = i - \frac{p-1}{2}$ so that $x^{2i} \equiv x^{2\tilde{i}} \bmod (x^p - x)$. Substituting $\tilde{i}$ into the expression above, we get the following contribution to the $\tilde{i}^{\text{th}}$ coordinate of $\mathbf{q}_n$:

$$2^{2-n-2\tilde{i}} \sum_{j=0}^{n} \binom{n}{j} \binom{2j - 2\tilde{i} + 1}{n-1} 4^j (-\kappa)^{n-j}.$$

This is precisely the sum in (7.10). Note that this summation neither appears in (7.9) nor in the formula for the zeroth coefficient of $\mathbf{q}_n$. It does not appear in (7.9) because the degree of the right-side sum in Lemma 7.4 (including the factor $(x^2 - \kappa)^n$) is $p + 1 + n$. Thus $2\tilde{i} = 2i - (p-1) \leq (p+1+n) - (p-1) = n + 2$, which is strictly less than $2n$ when $n \geq 3$. It does not appear in the formula for the zeroth coefficient of $\mathbf{q}_n$ because $2\tilde{i} = 2i - (p-1) > p - (p-1) > 0$.

Next let us suppose the degree $2i$ in (7.11) is less than p. In this case we use

$$\binom{p-2i+2j}{n-1} \equiv (-1)^{n-1} \binom{2j-2i+n-2}{n-1} \bmod p$$

(which can fail if $2i - 2j > p$) to rewrite the coefficient of x^{2i} in (7.11) as

$$-2^{2-n-2i} \sum_{j=0}^{n} \binom{n}{j} \binom{2i-2j+n-2}{n-1} (-4)^j \kappa^{n-j}.$$

Remark that replacing the summation bound $\min(i,n)$ in (7.11) with n makes no difference since the binomial coefficient above vanishes when $j \geq i$. The expression above matches (7.9). □

To facilitate forthcoming computations, especially the dot product $\mathbf{q}_n(\mathbf{y}_{\mathbb{R}})$, we express $\mathbf{q}_n$ in terms of the following vectors.

Notation 7.7. For $j = 0, 1, ..., \frac{p-1}{2}$, let

$$\mathbf{f}_j = (4 - \kappa)^{j+1} \sum_{i=j}^{\frac{p-1}{2}} \binom{i}{j} \frac{\mathbf{e}_{2i}}{4^i}.$$

Thanks to Proposition 7.6, a complete formula for $\mathbf{q}_n$ is obtained by computing $2\Phi((x^2-\kappa)\mathcal{p}_{n-1})+\Phi((x^2-\kappa)^2\mathcal{p}_{n-2})$ in order to find the coefficients c_{2i} in (7.10). This can be done by hand for the small values of n we will need (at most 5, though computing $\mathbf{q}_5$ by hand could take a few hours), but it is also easy to code an algorithm to do the work. Either way, once every entry of $\mathbf{q}_n$ has been determined, we may express it as a combination of $\mathbf{f}_0, \mathbf{f}_1, \ldots, \mathbf{f}_{n-1}$ and $\mathbf{e}_0, \mathbf{e}_2, \ldots, \mathbf{e}_{2n-2}$ as follows: First, the binomial coefficients in (7.9) can be viewed as polynomials in the variable i and written in terms of $\binom{i}{0}, \binom{i}{1}, \ldots, \binom{i}{n-1}$, say

$$\binom{2i-2k+n-2}{n-1} = \sum_{j=0}^{n-1} a_{j,k}\binom{i}{j}. \tag{7.12}$$

The correct choice of coefficients makes this equation hold provided $2i-2k+n-2 \geq 0$. (The equation above can fail when $2i-2k+n-2<0$ because in this case the left-side binomial coefficient vanishes while the right side may not. For example, consider which i make

$$\binom{2i-3}{2} = 6\binom{i}{0} - 5\binom{i}{1} + 4\binom{i}{2}$$

true or false. Note that if we were treating the left side as a *generalized* binomial coefficient, which we are not, the equation would hold for all i.) Once the $a_{j,k}$ are computed, we may substitute (7.12) into (7.9) and swap the order of summation. We conclude that all but the first n coordinates of $\mathbf{q}_n$ match those of

$$-\sum_{j=0}^{n-1}\left(\frac{2^{2-n}}{(4-\kappa)^{j+1}}\sum_{k=0}^{n}\binom{n}{k}a_{j,k}(-4)^k\kappa^{n-k}\right)\mathbf{f}_j.$$

Then the first n coordinates of the expression above can be substracted from their correct values to obtain the "adjustment" linear combination of $\mathbf{e}_0, \mathbf{e}_2, \ldots, \mathbf{e}_{2n-2}$ that provides an exact formula for $\mathbf{q}_n$. This is also straightforward to compute by hand or by code. Results for $n \leq 4$ are below. The coefficient matrices have been transposed to save space.

$$\begin{bmatrix}\mathbf{q}_1\\ \mathbf{q}_2\\ \mathbf{q}_3\\ \mathbf{q}_4\end{bmatrix} = \begin{bmatrix}2 & 16 & 120-6\kappa & 896-96\kappa\\ 0 & -2 & -18-\frac{3}{2}\kappa & -144-8\kappa-\kappa^2\\ 0 & 0 & 2 & 20+3\kappa\\ 0 & 0 & 0 & -2\end{bmatrix}^T \begin{bmatrix}\mathbf{f}_0\\ \mathbf{f}_1\\ \mathbf{f}_2\\ \mathbf{f}_3\end{bmatrix}$$

$$-(4-\kappa)\begin{bmatrix}2 & 16-\kappa & 120-\frac{46}{3}\kappa & 896-\frac{7816}{45}\kappa+\frac{166}{45}\kappa^2\\ 0 & 2 & 20-\frac{4}{3}\kappa & \frac{2596}{15}-\frac{967}{45}\kappa+\frac{7}{45}\kappa^2\\ 0 & 0 & \frac{4}{3} & \frac{604}{45}-\frac{11}{9}\kappa\\ 0 & 0 & 0 & \frac{16}{15}\end{bmatrix}^T \begin{bmatrix}\mathbf{e}_0\\ \mathbf{e}_2\\ \mathbf{e}_4\\ \mathbf{e}_6\end{bmatrix} \tag{7.13}$$

To reinforce Notations 7.5 and 7.7, the second line

$$\mathbf{q}_2 = 16\mathbf{f}_0 - 2\mathbf{f}_1 - (4-\kappa)((16-\kappa)\mathbf{e}_0 + 2\mathbf{e}_2)$$

above asserts that

$$\Phi\big((x^{p+1}-x^2)\big(\tfrac{1}{6}(4y^4+4y^2z^2+(x^2-\kappa)y^2)\big)\big)$$

$$\equiv (4-\kappa)\left(\sum_{i=0}^{\frac{p-1}{2}}(16-2(4-\kappa)i)\frac{x^{2i}}{4^i}-16+\kappa-2x^2\right) \bmod (x^p-x).$$

Note that the term $\frac{1}{6}(8y^3z)$, which might be expected to appear based on the "8" in (7.4), is absent because $\mathbf{q}_2$ is defined using $\not{p}^+_{2,2}$ rather than $\not{p}_{2,2}$.

Lemma 7.8. *For any nonnegative integers n and j,*

$$4^n\sum_{i=j}^{n}\binom{2i}{i}\binom{i}{j}\frac{1}{4^i}=\frac{2n+1}{2j+1}\binom{n}{j}\binom{2n}{n}.$$

Proof. Letting $a_j(n)$ and $b_j(n)$ denote the left- and right-side expressions above, we observe that both satisfy the same recursion for $n\geq 1$ and $j\geq 0$:

$$a_j(n)=4a_j(n-1)+\binom{2n}{n}\binom{n}{j}\quad\text{and}\quad b_j(n)=4b_j(n-1)+\binom{2n}{n}\binom{n}{j}.$$

Since $a_0(0)=1=b_0(0)$ and $a_j(0)=0=b_j(0)$ when $j\geq 1$, the claim follows by induction on n. □

Recall the variable vector $\mathbf{x}=\sum_i x^i\mathbf{e}_i$ as well as the vectors $\mathbf{x}(\alpha)=\sum_i \alpha^i\mathbf{e}_i$ for $\alpha\in\mathbb{F}_p$ defined in Notation 4.5.

Lemma 7.9. *For any nonnegative integer j and $x\in\overline{\mathbb{F}}_p\backslash\{4\}$,*

$$\mathbf{f}_j(\mathbf{x})=4x^{2j}\left(\frac{4-\kappa}{4-x^2}\right)^{j+1}\left(1-x^{p-1}\sum_{i=0}^{j}\binom{2i}{i}\left(\frac{1}{4}-\frac{1}{x^2}\right)^i\right)-4x^{p-1}\left(\frac{\kappa}{4}-1\right)^{j+1}\binom{2j}{j}.$$

Proof. Directly from the definition of $\mathbf{f}_j$,

$$\frac{\mathbf{f}_j(\mathbf{x})}{(4-\kappa)^{j+1}}=\sum_{i=j}^{\frac{p-1}{2}}\binom{i}{j}\frac{x^{2i}}{4^i}=4x^{2j}\sum_{i=j}^{\frac{p-3}{2}}\binom{i}{j}4^{\frac{p-3}{2}-i}x^{2(i-j)}+\binom{\frac{p-1}{2}}{j}x^{p-1}. \tag{7.14}$$

The summation in the final expression above (as well as in the middle expression) is the j^{th} derivative with respect to x^2 of a geometric series, which can be evaluated with the product rule:

$$\begin{aligned}4x^{2j}\sum_{i=j}^{\frac{p-3}{2}}\binom{i}{j}4^{\frac{p-3}{2}-i}(x^2)^{i-j}&=\frac{4x^{2j}}{j!}\frac{d^j}{dx^{2j}}\left(\frac{4^{\frac{p-1}{2}}-x^{p-1}}{4-x^2}\right)\\&=\frac{4x^{2j}}{(4-x^2)^{j+1}}\left(1-x^{p-1}\sum_{i=0}^{j}\binom{\frac{p-1}{2}}{i}\left(\frac{4}{x^2}-1\right)^i\right).\end{aligned}$$

Now we substitute

$$\binom{\frac{p-1}{2}}{i}\equiv\frac{(-1)^i}{4^i}\binom{2i}{i}\bmod p \tag{7.15}$$

into the expression above as well as in the final term of (7.14). Scaling both sides of (7.14) by $(4-\kappa)^{j+1}$ completes the proof. □

We make use of the Legendre symbol $\left(\frac{\alpha}{p}\right)=\alpha^{\frac{p-1}{2}}$ for $\alpha\in\mathbb{F}_p$ (including $\alpha=0$).

Proposition 7.10. *If $1 \le j \le \frac{p-3}{2}$ and $\kappa \in \mathbb{F}_p \backslash \{4\}$, then*

$$\mathbf{e}_{2j}(\mathbf{y}_p) = 0, \qquad \mathbf{f}_j(\mathbf{y}_p) = \left(\frac{\kappa}{4} - 1\right)^j \binom{2j}{j},$$

$$\mathbf{e}_{2j}(\mathbf{y}_{\mathbb{R}}) = -\binom{2j}{j} \sum_{i=1}^{j} \binom{2i}{i}^{-1} \frac{\kappa^{i-1}}{i}, \quad \mathbf{f}_j(\mathbf{y}_{\mathbb{R}}) = \frac{2\kappa^j}{2j+1} \left(1 - \left(\frac{\kappa}{p}\right) \sum_{i=0}^{j} \binom{2i}{i} \left(\frac{1}{4} - \frac{1}{\kappa}\right)^i\right),$$

$$\mathbf{e}_{2j}(\mathbf{y}_\kappa) = \kappa^j, \qquad \mathbf{f}_j(\mathbf{y}_\kappa) = (4j+2)\mathbf{f}_j(\mathbf{y}_{\mathbb{R}}) + \left(\frac{\kappa}{p}\right)(4-\kappa)\mathbf{f}_j(\mathbf{y}_p).$$

Furthermore, when $j = 0$ the first four formulas hold, while

$$\mathbf{e}_0(\mathbf{y}_\kappa) = 3 \quad \textit{and} \quad \mathbf{f}_0(\mathbf{y}_\kappa) = 12 - (2 + \left(\frac{\kappa}{p}\right))\kappa.$$

Proof. The formulas involving $\mathbf{e}_{2j}$ are immediate from the definitions of $\mathbf{y}_p$, $\mathbf{y}_{\mathbb{R}}$, and $\mathbf{y}_\kappa$. Also immediate from the definitions of $\mathbf{y}_p$ and $\mathbf{f}_j$ is

$$\mathbf{f}_j(\mathbf{y}_p) = (4-\kappa)^j \binom{\frac{p-1}{2}}{j}.$$

Combining this with (7.15) proves the formula for $\mathbf{f}_j(\mathbf{y}_p)$.

Next we establish the formula for $\mathbf{f}_j(\mathbf{y}_\kappa)$. Observe that

$$\begin{aligned}
\frac{\mathbf{f}_j(\mathbf{y}_{\mathbb{R}})}{(4-\kappa)^{j+1}} &= -\sum_{k=j}^{\frac{p-1}{2}} \binom{k}{j}\binom{2k}{k}\frac{1}{4^k} \sum_{i=1}^{k} \binom{2i}{i}^{-1} \frac{\kappa^{i-1}}{i} \\
&= -\sum_{i=0}^{\frac{p-3}{2}} \binom{2i+2}{i+1}^{-1} \frac{\kappa^i}{i+1} \sum_{k=i+1}^{\frac{p-1}{2}} \binom{k}{j}\binom{2k}{k}\frac{1}{4^k} \\
&= -\sum_{i=0}^{\frac{p-3}{2}} \binom{2i+2}{i+1}^{-1} \frac{\kappa^i}{i+1} \left(\sum_{k=j}^{\frac{p-1}{2}} \binom{k}{j}\binom{2k}{k}\frac{1}{4^k} - \sum_{k=j}^{i} \binom{k}{j}\binom{2k}{k}\frac{1}{4^k}\right) \\
&= -\sum_{i=0}^{\frac{p-3}{2}} \binom{2i+2}{i+1}^{-1} \frac{\kappa^i}{i+1} \left(0 - \frac{2i+1}{2j+1}\binom{i}{j}\binom{2i}{i}\frac{1}{4^i}\right) \qquad \text{by Lemma 7.8} \\
&= \frac{1}{4j+2} \sum_{i=0}^{\frac{p-3}{2}} \binom{i}{j}\frac{\kappa^i}{4^i} \\
&= \frac{1}{4j+2} \left(\sum_{i=0}^{\frac{p-1}{2}} \binom{i}{j}\frac{\kappa^i}{4^i} - \binom{\frac{p-1}{2}}{j}\kappa^{\frac{p-1}{2}}\right) \\
&= \frac{1}{4j+2} \left(\frac{\mathbf{f}_j(\mathbf{x}_\kappa)}{(4-\kappa)^{j+1}} - \left(\frac{\kappa}{p}\right)\frac{\mathbf{f}_j(\mathbf{y}_p)}{(4-\kappa)^j}\right). \qquad (7.16)
\end{aligned}$$

Since $\mathbf{f}_j(\mathbf{x}_\kappa) = \mathbf{f}_j(\mathbf{y}_\kappa)$ when $j \ge 1$, this establishes the claimed linear relation.

It remains only to verify the formula for $\mathbf{f}_j(\mathbf{y}_{\mathbb{R}})$. Letting $x = \sqrt{\kappa}$ in Lemma 7.9 gives

$$\mathbf{f}_j(\mathbf{x}(\sqrt{\kappa})) = 4\kappa^j \left(1 - \left(\frac{\kappa}{p}\right) \sum_{i=0}^{j} \binom{2i}{i} \left(\frac{1}{4} - \frac{1}{\kappa}\right)^i\right) - 4\left(\frac{\kappa}{p}\right)\left(\frac{\kappa}{4} - 1\right)^{j+1} \binom{2j}{j}$$

$$= 4\kappa^j \left(1 - \left(\frac{\kappa}{p}\right) \sum_{i=0}^{j} \binom{2i}{i} \left(\frac{1}{4} - \frac{1}{\kappa}\right)^i\right) + \left(\frac{\kappa}{p}\right)(4-\kappa)\mathbf{f}_j(\mathbf{y}_p).$$

Substituting this into (7.16) completes the proof. □

Proof of Theorem 7.1 when $\kappa \neq 0, 3$. Several of these vectors from the list in Lemma 7.2 must be eliminated to match Theorem 4.7. Specifically, if $\left(\frac{\kappa}{p}\right) = 1$, we must prove that no nonzero linear combination of $\mathbf{y}_\mathbb{R}$ and $\mathbf{y}_p$ lies in $\mathscr{P}^\perp(\mathbb{F}_p)$; all of the other vectors Lemma 7.2 belong when $\kappa \neq 0, 3$. If $\left(\frac{\kappa}{p}\right) = -1$ we must prove that no nonzero linear combination of $\mathbf{y}_\mathbb{R}$, $\mathbf{y}_p$, and $\mathbf{y}_\kappa$ lies in $\mathscr{P}^\perp(\mathbb{F}_p)$; again, all other vectors belong.

Suppose $\kappa \neq 0, 3$ and $\left(\frac{\kappa}{p}\right) = 1$. Proposition 7.10 gives

$$\begin{bmatrix}\mathbf{f}_0\\ \mathbf{f}_1\end{bmatrix}\begin{bmatrix}\mathbf{y}_\mathbb{R} & \mathbf{y}_p\end{bmatrix} = \begin{bmatrix}0 & 1\\ \frac{4}{3} - \frac{1}{3}\kappa & -2 + \frac{1}{2}\kappa\end{bmatrix}$$

and

$$\begin{bmatrix}\mathbf{e}_0\\ \mathbf{e}_2\end{bmatrix}\begin{bmatrix}\mathbf{y}_\mathbb{R} & \mathbf{y}_p\end{bmatrix} = \begin{bmatrix}0 & 0\\ -1 & 0\end{bmatrix}.$$

The top-left 2×2 corner of 7.13 expresses $[\mathbf{q}_1\ \mathbf{q}_2]^T$ as a linear combination (with matrix coefficients) of $[\mathbf{f}_0\ \mathbf{f}_1]^T$ and $[\mathbf{e}_0\ \mathbf{e}_2]^T$. This linear combination combines with the equations above to give

$$\begin{bmatrix}\mathbf{q}_1\\ \mathbf{q}_2\end{bmatrix}\begin{bmatrix}\mathbf{y}_\mathbb{R} & \mathbf{y}_p\end{bmatrix} = \begin{bmatrix}0 & 2\\ \frac{16}{3} - \frac{4}{3}\kappa & 20 - \kappa\end{bmatrix}.$$

The matrix above is nonsingular with determinant $-\frac{8}{3}(4-\kappa) \neq 0$.

Now suppose $\left(\frac{\kappa}{p}\right) = 1$. Since we need only eliminate a 3-dimensional space, namely $\operatorname{span}\{\mathbf{y}_\mathbb{R}, \mathbf{y}_p, \mathbf{y}_\kappa\}$, we might hope that the same strategy used above works with only the three vectors $\mathbf{q}_1$, $\mathbf{q}_2$, and $\mathbf{q}_3$. Unfortunately,

$$\begin{bmatrix}\mathbf{q}_1\\ \mathbf{q}_2\\ \mathbf{q}_3\end{bmatrix}\begin{bmatrix}\mathbf{y}_\mathbb{R} & \mathbf{y}_p & \mathbf{y}_\kappa\end{bmatrix}$$

is singular when $p \equiv 1 \bmod 4$ and $\kappa = \pm 4\sqrt{-1}$ (nonsingular otherwise). But by including $\mathbf{q}_4$, we can obtain a matrix of rank three. Indeed, let

$$\tilde{\mathbf{q}}_3 = 15(272 + 72\kappa - 3\kappa^2)\mathbf{q}_3 - 105(4+\kappa)\mathbf{q}_4.$$

Then (7.13) tells us

$$\begin{bmatrix}\mathbf{q}_1\\ \mathbf{q}_2\\ \tilde{\mathbf{q}}_3\end{bmatrix} = \begin{bmatrix}2 & 16 & 113280 + 51360\kappa - 1800\kappa^2 + 270\kappa^3\\ 0 & -2 & -12960 - 7080\kappa + 450\kappa^2 + \frac{345}{2}\kappa^3\\ 0 & 0 & -240 - 1200\kappa - 405\kappa^2\\ 0 & 0 & 840 + 210\kappa\end{bmatrix}^T \begin{bmatrix}\mathbf{f}_0\\ \mathbf{f}_1\\ \mathbf{f}_2\\ \mathbf{f}_3\end{bmatrix}$$

$$- (4-\kappa)\begin{bmatrix}2 & 16-\kappa & 113280 + \frac{137728}{3}\kappa - 5272x^2 + \frac{908}{3}\kappa^3\\ 0 & 2 & 8912 + \frac{21040}{3}\kappa - 149\kappa^2 + \frac{131}{3}\kappa^3\\ 0 & 0 & -\frac{592}{3} + 544\kappa + \frac{205}{3}\kappa^2\\ 0 & 0 & -448 - 112\kappa\end{bmatrix}^T \begin{bmatrix}\mathbf{e}_0\\ \mathbf{e}_2\\ \mathbf{e}_4\\ \mathbf{e}_6\end{bmatrix}.$$

With another application of Proposition 7.10, we obtain

$$\begin{bmatrix}\mathbf{f}_0\\ \mathbf{f}_1\\ \mathbf{f}_2\\ \mathbf{f}_3\end{bmatrix}\begin{bmatrix}\mathbf{y}_{\mathbb{R}} & \mathbf{y}_p & \mathbf{y}_\kappa\end{bmatrix}$$

$$= \begin{bmatrix} 4 & -\frac{4}{3}+\frac{5}{3}\kappa & \frac{12}{5}-2\kappa+\frac{23}{20}\kappa^2 & -\frac{40}{7}+6\kappa-\frac{5}{2}\kappa^2+\frac{51}{56}\kappa^3 \\ 1 & -2+\frac{1}{2}\kappa & 6-3\kappa+\frac{3}{8}\kappa^2 & -20+15\kappa-\frac{15}{4}\kappa^2+\frac{5}{16}\kappa^3 \\ 12-\kappa & 6\kappa+\frac{1}{2}\kappa^2 & -2\kappa+7\kappa^2+\frac{3}{8}\kappa^3 & 4\kappa-5\kappa^2+\frac{31}{4}\kappa^3+\frac{5}{16}\kappa^4 \end{bmatrix}^T$$

and

$$\begin{bmatrix}\mathbf{e}_0\\ \mathbf{e}_2\\ \mathbf{e}_4\\ \mathbf{e}_6\end{bmatrix}\begin{bmatrix}\mathbf{y}_{\mathbb{R}} & \mathbf{y}_p & \mathbf{y}_\kappa\end{bmatrix} = \begin{bmatrix} 0 & 0 & 3 \\ -1 & 0 & \kappa \\ -3-\frac{1}{2}\kappa & 0 & \kappa^2 \\ -10-\frac{5}{3}\kappa-\frac{1}{3}\kappa^2 & 0 & \kappa^3 \end{bmatrix}$$

The appropriate multiplications and additions with the matrices above gives

$$\begin{bmatrix}\mathbf{q}_1\\ \mathbf{q}_2\\ \tilde{\mathbf{q}}_3\end{bmatrix}\begin{bmatrix}\mathbf{y}_{\mathbb{R}} & \mathbf{y}_p & \mathbf{y}_\kappa\end{bmatrix}$$

$$= \begin{bmatrix} 8 & \frac{224}{3}-\frac{16}{3}\kappa & 480384+217600\kappa-26000\kappa^2+1440\kappa^3-\frac{55}{2}\kappa^4 \\ 2 & 20-\kappa & 120960+60960\kappa-5160\kappa^2+390\kappa^3 \\ 4\kappa & 24\kappa-2\kappa^2 & 182400\kappa+58080\kappa^2-10440\kappa^3+450\kappa^4 \end{bmatrix}^T.$$

This matrix is nonsingular (if $\kappa \neq 0$) with determinant $-2^{19}\kappa$. □

Proof of Theorem 7.1 when $\kappa = 0$. The space that must be eliminated from $\mathscr{P}^\perp(\mathbb{F}_p)$ is only two-dimensional, spanned by $\mathbf{y}_p$ and $\mathbf{y}_0 \coloneqq \mathbf{e}_2^T - 12\mathbf{e}_4^T$. (Recall that $\kappa = 0$ is the unique value for which $\mathbf{y}_{\mathbb{R}}$ actually belongs in $\mathscr{P}^\perp(\mathbb{F}_p)$.) To eliminate it, we need only

$$\mathbf{q}_1 = 2\mathbf{f}_0 - 8\mathbf{e}_0 \quad \text{and} \quad \mathbf{q}_2 = 16\mathbf{f}_0 - 2\mathbf{f}_1 - 64\mathbf{e}_0 - 8\mathbf{e}_2.$$

Applying Proposition 7.10 gives

$$\det\left(\begin{bmatrix}\mathbf{q}_1\\ \mathbf{q}_2\end{bmatrix}\begin{bmatrix}\mathbf{y}_0 & \mathbf{y}_p\end{bmatrix}\right) = \det\begin{bmatrix}-4 & 2\\ 0 & 20\end{bmatrix} = -80,$$

which is nonzero in $\mathbb{F}_p$ for $p \geq 7$. □

Proof of Theorem 7.1 when $\kappa = 3$. We consider $\left(\frac{3}{p}\right) = -1$ and $\left(\frac{3}{p}\right) = 1$ separately.

If $\left(\frac{3}{p}\right) = -1$ then $\mathbf{y}_\kappa$ must be removed from the spanning set for $\mathscr{P}^\perp(\mathbb{F}_p)$ along with $\mathbf{y}_{\mathbb{R}}$ and $\mathbf{y}_p$. If $\left(\frac{2}{p}\right) = -1$ or $\left(\frac{5}{p}\right) = -1$ then $\mathbf{y}_2$ or $\mathbf{y}_5$ must also be removed. This requires at least five vectors, and the natural choice $\mathbf{q}_n$ for $n \leq 5$ turns out to work. The following coefficients have been calculated with computer assistance

using Proposition 7.6:

$$\begin{bmatrix}\mathbf{q}_1\\ \mathbf{q}_2\\ \mathbf{q}_3\\ \mathbf{q}_4\\ \mathbf{q}_5\end{bmatrix} = \begin{bmatrix} 2 & 0 & 0 & 0 & 0\\ 16 & -2 & 0 & 0 & 0\\ 102 & -\frac{45}{2} & 2 & 0 & 0\\ 608 & -177 & 29 & -2 & 0\\ 3540 & -\frac{9695}{8} & \frac{2185}{8} & -\frac{71}{2} & 2\end{bmatrix}\begin{bmatrix}\mathbf{f}_0\\ \mathbf{f}_1\\ \mathbf{f}_2\\ \mathbf{f}_3\\ \mathbf{f}_4\end{bmatrix}$$

$$- \begin{bmatrix} 2 & 0 & 0 & 0 & 0\\ 13 & 2 & 0 & 0 & 0\\ 74 & 16 & \frac{4}{3} & 0 & 0\\ \frac{6122}{15} & 110 & \frac{439}{45} & \frac{16}{15} & 0\\ \frac{706396}{315} & \frac{74516}{105} & \frac{59084}{945} & \frac{2504}{315} & \frac{32}{35}\end{bmatrix}\begin{bmatrix}\mathbf{e}_0\\ \mathbf{e}_2\\ \mathbf{e}_4\\ \mathbf{e}_6\\ \mathbf{e}_8\end{bmatrix}. \tag{7.17}$$

Next, it is straightforward to verify from Proposition 7.10 (for $\mathbf{y}_{\mathbb{R}}$) or directly from the definition of $\mathbf{y}_p$, $\mathbf{y}_\kappa$, $\mathbf{y}_2$ or $\mathbf{y}_5$ that

$$\begin{bmatrix}\mathbf{e}_0\\ \mathbf{e}_2\\ \mathbf{e}_4\\ \mathbf{e}_6\\ \mathbf{e}_8\end{bmatrix}\begin{bmatrix}\mathbf{y}_{\mathbb{R}} & \mathbf{y}_p & \mathbf{y}_\kappa & \mathbf{y}_2 & \mathbf{y}_5\end{bmatrix} = \begin{bmatrix} 0 & 0 & 3 & 9 & 18\\ -1 & 0 & 3 & 11 & 21\\ -\frac{9}{2} & 0 & 9 & 19 & 41\\ -18 & 0 & 27 & 35 & 96\\ -\frac{279}{4} & 0 & 81 & 67 & 241\end{bmatrix}. \tag{7.18}$$

To evaluate $\mathbf{f}_j$ at $\mathbf{y}_2$ or $\mathbf{y}_5$, we first evaluate $\mathbf{f}_j$ at $\mathbf{x}(0)$, $\mathbf{x}(1)$, $\mathbf{x}(\sqrt{2})$ and $\mathbf{x}(\varphi)+\mathbf{x}(\overline{\varphi})$ using Lemma 7.9. Note that x^{p-1} appears in the Lemma 7.9's formula for $\mathbf{f}_j(\mathbf{x})$. We only need to eliminate $\mathbf{y}_2$ when $\left(\frac{2}{p}\right) = -1$, so $\sqrt{2}^{\,p-1}$ takes the value -1 when computing $\mathbf{f}_j(\mathbf{x}(\sqrt{2}))$. Similarly, we need only eliminate $\mathbf{y}_5$ when $\left(\frac{5}{p}\right) = -1$, so φ^{p-1} takes the value

$$\begin{aligned}\left(\frac{1+\sqrt{5}}{2}\right)^{p-1} &= \sum_{i=0}^{p-1}\binom{p-1}{i}\sqrt{5}^i\\ &= \sum_{i=0}^{\frac{p-1}{2}} 5^i - \sqrt{5}\sum_{i=0}^{\frac{p-3}{2}} 5^i \qquad \text{since } \binom{p-1}{i} \equiv (-1)^i \bmod p\\ &= 5^{\frac{p-1}{2}} + (1-\sqrt{5})\sum_{i=0}^{\frac{p-3}{2}} 5^i\\ &= \frac{1-\sqrt{5}}{1+\sqrt{5}} = \frac{\overline{\varphi}}{\varphi} \qquad \text{by telescoping and using } \left(\frac{5}{p}\right) = -1,\end{aligned}$$

and $\overline{\varphi}^{p-1}$ takes the value $\varphi/\overline{\varphi}$. The result from Lemma 7.9 is then

$$\begin{bmatrix}\mathbf{f}_0\\ \mathbf{f}_1\\ \mathbf{f}_2\\ \mathbf{f}_3\\ \mathbf{f}_4\end{bmatrix}\begin{bmatrix}\mathbf{x}(0) & \mathbf{x}(1) & \mathbf{x}(\sqrt{2}) & \mathbf{x}(\varphi)+\mathbf{x}(\overline{\varphi})\end{bmatrix} = \begin{bmatrix} 1 & 1 & 3 & 5\\ 0 & \frac{1}{6} & \frac{7}{2} & \frac{15}{2}\\ 0 & \frac{7}{72} & \frac{27}{8} & \frac{543}{40}\\ 0 & \frac{5}{432} & \frac{55}{16} & \frac{2063}{80}\\ 0 & \frac{175}{10368} & \frac{435}{128} & \frac{156107}{3200}\end{bmatrix}$$

The last three columns are also the values of $\mathbf{f}_j(\mathbf{x}(-1))$, $\mathbf{f}_j(\mathbf{x}(-\sqrt{2}))$, and $\mathbf{f}_j(\mathbf{x}(-\varphi)+\mathbf{x}(-\overline{\varphi}))$ because every odd coordinate in $\mathbf{f}_j$ is 0. Combining this with the definitions of $\mathbf{y}_2$ and $\mathbf{y}_5$ as linear combinations of $\mathbf{x}(\alpha)$ vectors provides the last two columns below. Proposition 7.10 provides the values of $\mathbf{f}_j(\mathbf{y}_\mathbb{R})$, $\mathbf{f}_j(\mathbf{y}_p)$, and $\mathbf{f}_j(\mathbf{y}_\kappa)$ in the first three columns:

$$\begin{bmatrix}\mathbf{f}_0\\ \mathbf{f}_1\\ \mathbf{f}_2\\ \mathbf{f}_3\\ \mathbf{f}_4\end{bmatrix}\begin{bmatrix}\mathbf{y}_\mathbb{R} & \mathbf{y}_p & \mathbf{y}_3 & \mathbf{y}_2 & \mathbf{y}_5\end{bmatrix} = \begin{bmatrix} 4 & 1 & 9 & 17 & 33\\ \frac{11}{3} & -\frac{1}{2} & \frac{45}{2} & \frac{29}{2} & \frac{77}{2}\\ \frac{27}{4} & \frac{3}{8} & \frac{537}{8} & \frac{331}{24} & \frac{1643}{24}\\ \frac{115}{8} & -\frac{5}{16} & \frac{3225}{16} & \frac{1985}{144} & \frac{18577}{144}\\ \frac{19355}{576} & \frac{35}{128} & \frac{77385}{128} & \frac{47155}{3456} & \frac{4216639}{17280}\end{bmatrix} \tag{7.19}$$

Performing the appropriate multiplications and addition with the matrices in (7.17), (7.18), and (7.19) results in

$$\begin{bmatrix}\mathbf{q}_1\\ \mathbf{q}_2\\ \mathbf{q}_3\\ \mathbf{q}_4\\ \mathbf{q}_5\end{bmatrix}\begin{bmatrix}\mathbf{y}_\mathbb{R} & \mathbf{y}_p & \mathbf{y}_\kappa & \mathbf{y}_2 & \mathbf{y}_5\end{bmatrix} = \begin{bmatrix} 8 & 2 & 12 & 16 & 30\\ \frac{176}{3} & 17 & 54 & 104 & 175\\ 361 & 114 & 264 & 568 & 914\\ \frac{21231}{10} & 708 & 1362 & 3036 & 4818\\ \frac{7758343}{630} & 4260 & 7272 & 16396 & \frac{129766}{5}\end{bmatrix},$$

which is nonsingular at all primes $p \geq 29$ with determinant $-\frac{2508193792}{525} = -2^{23} \cdot 3^{-1} \cdot 5^{-2} \cdot 7^{-1} \cdot 13 \cdot 23$. (The McCullough–Wanderley conjectures have already been verified for $p < 29$ [MW13].) Now, if it happens that $\left(\frac{2}{p}\right) = 1$ or $\left(\frac{5}{p}\right) = 1$, then the $\mathbf{y}_2$ or $\mathbf{y}_5$ columns simply become all 0, in which case we are no longer concerned with $\mathbf{y}_2$ or $\mathbf{y}_5$ because they belong in $\mathscr{P}^\perp(\mathbb{F}_p)$ as per Theorem 4.7. The remaining 5×3 or 5×4 matrix must still have full column rank, so we are done. This completes the proof when $\left(\frac{3}{p}\right) = -1$.

When $\left(\frac{3}{p}\right) = 1$, not only does the $\mathbf{y}_\kappa$ column vanish in the matrix above, but the $\mathbf{y}_\mathbb{R}$ column changes due to the appearance of $\left(\frac{\kappa}{p}\right)$ in Proposition 7.10's formula for $\mathbf{f}_j(\mathbf{y}_\mathbb{R})$. Our new version of (7.19) is

$$\begin{bmatrix}\mathbf{f}_0\\ \mathbf{f}_1\\ \mathbf{f}_2\\ \mathbf{f}_3\end{bmatrix}\begin{bmatrix}\mathbf{y}_\mathbb{R} & \mathbf{y}_p & \mathbf{y}_2 & \mathbf{y}_5\end{bmatrix} = \begin{bmatrix} 0 & 1 & 17 & 33\\ \frac{1}{3} & -\frac{1}{2} & \frac{29}{2} & \frac{77}{2}\\ \frac{9}{20} & \frac{3}{8} & \frac{331}{24} & \frac{1643}{24}\\ \frac{59}{56} & -\frac{5}{16} & \frac{1985}{144} & \frac{18577}{144}\end{bmatrix}$$

The only change to (7.17) is the deletion of the last row and column in eqch matrix because we only need to use $\mathbf{q}_n$ for $n \leq 4$ now. Similarly, the only change to (7.19) is the deletion of the middle (corresponding to $\mathbf{y}_\kappa$) column and the last row. Performing the appropriate matrix multiplications and addition gives

$$\begin{bmatrix}\mathbf{q}_1\\ \mathbf{q}_2\\ \mathbf{q}_3\\ \mathbf{q}_4\end{bmatrix}\begin{bmatrix}\mathbf{y}_\mathbb{R} & \mathbf{y}_p & \mathbf{y}_2 & \mathbf{y}_5\end{bmatrix} = \begin{bmatrix} 0 & 2 & 16 & 30\\ \frac{4}{3} & 17 & 104 & 175\\ \frac{77}{5} & 114 & 568 & 914\\ \frac{8753}{70} & 708 & 3036 & 4818\end{bmatrix},$$

which is again nonsingular with determinant $\frac{393216}{35} = 2^{17} \cdot 3 \cdot 5^{-1} \cdot 7^{-1}$. As before, if it happens that $\left(\frac{2}{p}\right) = -1$ or $\left(\frac{5}{p}\right) = -1$, the $\mathbf{y}_2$ column or the $\mathbf{y}_5$ column vanishes,

and no other columns change. This yields either a 4×3 or 4×2 matrix with full column rank, which completes the proof. □

8. Computing $\dim(\mathscr{P}_{2n}(\mathbb{F}_p, d))$

Given positive integers $d \le n$, we provide an algorithm (Algorithm 1) to verify the hypothesis of Theorem 7.1 for all κ and $p \ge 2n$ with $p \not\equiv \pm 1 \bmod 2d$. Executing this Algorithm 1 in Sage for $d = 5$, 7, 9, 11, 13, 16, and 17 proves Theorem 1.1. In particular, the McCullough–Wanderley conjectures hold when $2\,\mathrm{lcm}(1, ..., 17) \nmid p^2 - 1$.

The polynomials we use to build rank in $\mathscr{P}(\overline{\mathbb{Z}}, d)$ take the form gf_n, where f_n is defined in Notation 6.18. As in (6.17), we must choose g to kill those $c_{\alpha,n}(f_n)$ for which $2d \nmid \mathrm{ord}(\alpha)$. Hence we define

$$g_{d,n}(x^2) \coloneqq x^\delta \prod_{\substack{\alpha \in \widehat{\Lambda}_n \\ 2d \nmid \mathrm{ord}(\alpha)}} (x - \alpha), \tag{8.1}$$

where δ is either 0 or 1, whichever makes $g_{d,n}$ an even polynomial (just as in (6.17)). The roots of $g_{d,n}$ are precisely the undesired α-values.

Proposition 8.1. *For any $\ell \ge 0$, $x^{2\ell} g_{d,n} f_n \in \mathscr{P}^n(\mathbb{Z}, d)$.*

Proof. Just as in the proof of Corollary 6.20, this follows from Corollary 6.14 and the fact that $c_{\alpha,n}(x^{2\ell} g_{d,n} f_n) = \alpha^{2\ell} g_{d,n}(\alpha^2)(\alpha^2 - 4)^n$, which vanishes when it needs to by definition of $g_{d,n}$. □

Recall that if $\mathrm{ord}(\alpha) \nmid 2n$ then $c_{\alpha,n}(f) = 0$ for any polynomial f. In particular, the choice of $g_{d,n}$ makes $\Phi(x^{2m} g_{d,n} f_n)$ the zero polynomial when $d \nmid n$; these polynomials are only useful when $d \mid n$.

For computational convenience, we note that $g_{d,n}$ is a product/quotient of (slight variants of) Chebyshev polynomials of the second kind, which can be called directly by a Sage command. Let us demonstrate this when d is a prime power, which is all we ultimately work with. The usual Chebyshev polynomials of the second kind are denoted $U_n(x)$ and defined recursively by $U_0(x) = 1$, $U_1(x) = 2x$, and $U_{n+1}(x) = 2xU_n(x) - U_{n-1}(x)$. The roots of $U_{n-1}(x)$ are $\cos(\frac{m\pi}{n})$ for $m = 1, ..., n-1$. Now define

$$u_n(x^2) \coloneqq \begin{cases} U_{n-1}(\frac{x}{2}) & n \text{ is odd} \\ xU_{n-1}(\frac{x}{2}) & n \text{ is even,} \end{cases}.$$

defined for $n \ge 1$. These are monic, integral polynomials, as can be seen from the recursion $U_0(\frac{x}{2}) = 1$, $U_1(\frac{x}{2}) = x$, and $U_{n+1}(\frac{x}{2}) = xU_n(\frac{x}{2}) - U_{n-1}(\frac{x}{2})$. Furthermore, if $\alpha \in \widehat{\Lambda}_n$, then $\alpha = 2\cos(\frac{m\pi}{n})$ for some $m = 1, ..., n-1$, so $u_n(\alpha^2) = 0$. Therefore, if $d = p^a \ne 2$ and $2n = mp^b$, the equality

$$g_{p^a,n}(x^2) = \begin{cases} u_{mp^{a-1}}(x^2) & p \ne 2 \\ u_{mp^{a-2}}(x^2) & p = 2, \end{cases}$$

can be seen by comparing roots. Similar expressions exist when d is not a prime power, but they involve quotients of Chebyshev polynomials in order to get each desired root exactly once from an inclusion-exclusion argument.

For each n divisible by a given d, we now ask what rank is contributed by the polynomials $\Phi(x^{2m} g_{d,n} f)$ as m ranges over nonnegative integers. This will tell us

when to stop incrementing m in Algorithm 1 for a given n, and it will help us find some n_d for which the polynomials $\Phi(x^{2m} g_{d,n} f)$ for $n \le n_d$ are expected to have the rank Theorem 7.1 requires, namely $2n_d - 2$ for general κ. We know that $\Phi(x^{2m} g_{d,n} f_n)$ lives in the $\overline{\mathbb{Q}}$-span of $\Phi(\not{P}^+_{\alpha,n})$ for $\alpha \in \Lambda_n$ of order divisible by $2d$. This means if $\alpha = \zeta^i + \zeta^{-i}$ for a primitive $2n^{\text{th}}$ root of unity ζ, $2d$ must divide $\frac{2n}{(i,2n)}$. For each divisor $\tilde{d}$ of $\frac{n}{d}$, there are $\phi(\frac{2n}{\tilde{d}})$ values of $i \in \{1, ..., 2n\}$ that make $(i, 2n) = \tilde{d}$. Replacing i with $2n - i$, $n + i$, or $n - i$ produces the same value of α up to a sign, so for any fixed d and n the polynomials $\Phi(x^{2m} g_{d,n} f)$ span a space of dimension at most

$$m_{d,n} \coloneqq \left\lceil \frac{1}{4} \sum_{\tilde{d} \mid \frac{n}{d}} \phi\left(\frac{2n}{\tilde{d}}\right) \right\rceil . \tag{8.2}$$

So a natural choice is to compute $\Phi(x^{2m} g_{d,n} f)$ for all nonnegative $m < m_{d,n}$ in Algorithm 1.

Now we sum $m_{d,n}$ as n ranges over consecutive multiples of d to get the total expected dimension. If n_d denotes the largest multiple of d we use, then we require the sum of $m_{d,n}$ (which is the total number of polynomials to be reduced) to be at least $n_d - 2$; nothing less could satisfy the bound in Theorem 7.1 when combined with the odd-degree monomials $x^1, x^3, \dots x^{2n_d - 1} \in \mathscr{P}_{2n_d}(\mathbb{F}_p, d)$. (Note that the sum of $m_{d,n}$ for $n \le n_d$ must eventually surpass any constant multiple of n_d since $m_{d,n}$ grows roughly linearly in n.) In practice, however, to prove full dimension we typically need at least n_d polynomials, not $n_d - 2$.

When d is a prime power and n is a small multiple of d, $m_{d,n}$ is particularly easy to compute. The reader may verify that for $d = p^a \ge 4$, defining

$$n_d \coloneqq \begin{cases} 4d & p \ne 2, 3 \\ 5d & p = 3 \\ 6d & p = 2 \end{cases} \tag{8.3}$$

makes $\sum_n m_{d,n} \ge n_d$, the sum over $n = d, 2d, \dots n_d$. (Remark that this inequality need not be verified to guarantee correctness of Algorithm 1. Indeed, if $\sum_n m_{d,n} < n_d$, then there will not be enough polynomials to produce the desired rank in $\mathscr{P}_{2n_d}(\mathbb{F}_p, d)$, and the algorithm output will be inconclusive. Or conversely, if a smaller choice of n_d would have made $\sum_n m_{d,n} < n_d$, it means only that the algorithm will work harder than necessary to achieve its output. In similar fashion, the choice of $m_{d,n}$ in (8.2) cannot affect the validity of Algorithm 1. These are simply parameters whose optimal values we hope to have found.)

Finally, let us discuss how to test the dimension hypothesis in Theorem 7.1 for all κ and $p \not\equiv \pm 1 \bmod 2d$ at once. Evidently, we must treat κ as a variable when we compute $\Phi(x^{2m} g_{d,n} f_n)$. Thus all polynomial coefficients lie in $\mathbb{Z}[\kappa]$. For generic κ, we only need coefficient vectors to have rank $n_d - 2$, so we only store the top $n_d - 2$ even-degree coefficients of each polynomial. (All odd-degree coefficients are 0.) That is, for $m < m_{d,n}$ and $n \le n_d$, the coefficients of x^{2i} in $\Phi(x^{2m} g_{d,n} f_n)$ for $i = 3, 4, ..., n_d$ are stored as columns of a matrix. (This procedure can be found in lines 1–8 of Algorithm 1.) Let M_d denote the resulting matrix.

Notation 8.2. For $a, b_1, b_2, b_3, b_4 \in \mathbb{Z}$ with each $b_j \ge 0$, let

$$h(\kappa; a, b_1, b_2, b_3, b_4) = a(\kappa - 4)^{b_1} (\kappa - 3)^{b_2} (\kappa - 2)^{b_3} (\kappa^2 - 5\kappa + 5)^{b_4} \in \mathbb{Z}[\kappa].$$

Proposition 8.3. *Given d, let n_d and M_d be as defined above. Let $p > 2n_d$ be a prime with $p \not\equiv \pm 1 \bmod 2d$. If the ideal in $\mathbb{Z}[\kappa]$ generated by the $(n_d-2)\times(n_d-2)$ minor determinants of M_d contains $h(\kappa; a, b, 2, 1, 1)$ for some a and $b \geq 0$, then the hypothesis of Theorem 7.1 holds for all $\kappa \in \mathbb{F}_p \backslash \{4\}$ provided $p \nmid a$.*

Proof. Reduce M_d modulo p so that the entries lie in $\mathbb{F}_p[\kappa]$. The columns of $M_d \bmod p$ generate a free $\mathbb{F}_p[\kappa]$-module because $\mathbb{F}_p[\kappa]$ is a PID. Furthermore, if $p \nmid a$ as in the proposition statement, this free module must have full rank $n_d - 2$ because the ideal in $\mathbb{F}_p[\kappa]$ generated by the $(n_d-2)\times(n_d-2)$ minor determinants of $M_d \bmod p$ contains the nonzero element $h(\kappa; a, b, 2, 1, 1)$. So fix a basis for our free module and use it to form the columns of a new $(n_d-2)\times(n_2-d)$ matrix M. Without loss of generality, assume M is upper triangular (again, $\mathbb{F}_p[x]$ is a PID, so column operations put M in Hermite normal form) so that $\det M$ is a product of its diagonal entries. Since $\det M$ divides every $(n_d-2)\times(n_d-2)$ minor determinant of $M_d \bmod p$, it must also divide $h(\kappa; a, b, 2, 1, 1)$ in $\mathbb{F}_p[\kappa]$. So up to scaling by a unit, every diagonal entry of M is $\kappa - 4$, $\kappa - 3$, $\kappa - 2$, $\kappa - 2 - \varphi$, $\kappa - 2 - \overline{\varphi}$, or some (perhaps empty) product of them. Furthermore, at most one diagonal entry can be divisible by $\kappa - 2$, $\kappa - 2 - \varphi$, or $\kappa - 2 - \overline{\varphi}$, and at most two can be divisible by $\kappa - 3$. Thus substituting a specific element of $\mathbb{F}_p \backslash \{4\}$ in for κ in the entries of M produces a matrix of rank at least $n_d - 4$ if $\kappa = 3$, $n_d - 3$ if $\kappa \in \{2, 2+\varphi, 2+\overline{\varphi}\}$, and $n_d - 2$ otherwise. The same rank bound must hold for such a κ substitution into $M_d \bmod p$ because the columns of $M_d \bmod p$ generate those of M. Extending $M_d \bmod p$ by three rows—the coefficients $\bmod p$ of 1, x^2, and x^4 in each $\Phi(x^{2m} g_{d,n} f_n)$—cannot decrease the column rank. But now each extended column corresponds to an element of $\mathscr{P}_{2n_d}(\mathbb{F}_p, d)$, which therefore has the desired dimension. □

The goal of Algorithm 1 is to find such an ideal element $a(\kappa-4)^b(\kappa-3)^2(\kappa-2)(\kappa^2-5\kappa+5)$, but with a only divisible by primes to which Theorem 7.1 would not apply anyway: $p < 2n$ or $p \equiv \pm 1 \bmod 2d$. There are several natural ways to accomplish this in Sage, and the fastest appears to be with resultants. Specifically, for a given $(n_d-2)\times(n_d-2)$ minor of M_d, we compute its determinant in $\mathbb{Z}[\kappa]$ and divide out all acceptable factors: up to one factor of $\kappa - 2$ and $\kappa^2 - 5\kappa + 5$, up to two factors of $\kappa - 3$, and as many as possible factors of $\kappa - 4$ or rational primes less than $2d$. (It would also be permissible to divide out primes $p \equiv \pm 1 \bmod 2d$, but we do not bother.) We keep this reduced determinant, and compute its resultant with each of the previously computed reduced minor determinants. The resultant of two polynomials in $\mathbb{Z}[\kappa]$ is an integer that lies in the ideal they generate, so if the greatest common divisor of all our resultants is ever equal to 1, we are done! This procedure can be found in lines 9–17 of Algorithm 1.

Sage code for Algorithm 1 is available on the author's website: `dem6.people.clemson.edu`. Note that in order to execute line 7, the Sage implementation precomputes $\Phi(x^{2m}y^{2n})$ for sufficiently large m and n. Then each $\Phi(x^{2m} g_{d,n} f_n)$ is a linear combination of the precomputed reductions. This is faster than computing each $\Phi(x^{2m} g_{d,n} f_n)$ directly because it avoids repeated work. (Though line 7 is not the bottleneck of the algorithm either way; line 14 is.)

The author has executed this algorithm for all prime powers $d \leq 17$ with an output of $\Delta = 1$ in each case. This proves Theorems 1.1 and 1.2.

Algorithm 1: Verify the McCullough–Wanderley conjectures over $\mathbb{F}_p$ for congruence classes of primes p.

Input: A prime power $d \geq 5$
Output: $\Delta \in \mathbb{Z}$; conjectures hold if $p \nmid \Delta$, $p \not\equiv \pm 1 \bmod 2d$, and $p > 2n_d$.

$M_d \leftarrow$ empty matrix over $\mathbb{Z}[\kappa]$
$n_d \leftarrow$ integer from (8.3)
for $0 < n \leq n_d$ such that $d \mid 2n$ **do**
  $f_n, g_{d,n} \leftarrow$ polynomials from (6.18), (8.1)
  $m_{d,n} \leftarrow$ integer from (8.2)
  for $0 \leq m < m_{d,n}$ **do**
    $a_0 + \cdots + a_{n_d} x^{2n_d} \leftarrow \Phi(x^{2m} g_{d,n} f_n)$ ▷ reduce with κ a variable
    append column $[a_3 \cdots a_{n_d}]^T$ to M_d ▷ each a_i is in $\mathbb{Z}[\kappa]$
$\Delta \leftarrow 0$ ▷ gcd of resultants
$\mathscr{D} \leftarrow \emptyset$ ▷ set of minor determinants
for maximal minors $\hat{M}$ of M_d **do**
  $D \leftarrow \det \hat{M} / h(\kappa; a, b_1, b_2, b_3, b_4)$ with a and each b_j maximal such that a is $2n_d$-smooth, $b_2 \leq 2$, $b_3, b_4 \leq 1$, and $D \in \mathbb{Z}[\kappa]$ ▷ see Notation 8.2
  for $\tilde{D}$ in $\mathscr{D}$ **do**
    $\Delta \leftarrow \gcd(\Delta, \text{resultant}(D, \tilde{D}))$
    if $\Delta = 1$ **then** ▷ typically occurs at $|\mathscr{D}| = 2$
      return 1
  $\mathscr{D} \leftarrow \mathscr{D} \cup \{D\}$
return Δ

References

[Bar91] Arthur Baragar. The Markoff equation and equations of Hurwitz. PhD thesis. Brown University, 1991.

[Bar96] Arthur Baragar. Rational points on K3 surfaces in $\mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1$. *Mathematische Annalen* 305.1 (1996), pp. 541–558.

[Bar98] Arthur Baragar. The exponent for the Markoff–Hurwitz equations. *pacific journal of mathematics* 182.1 (1998), pp. 1–21.

[BGS16a] Jean Bourgain, Alexander Gamburd, and Peter Sarnak. Markoff surfaces and strong approximation, 1. arXiv:1607.01530. 2016.

[BGS16b] Jean Bourgain, Alexander Gamburd, and Peter Sarnak. Markoff triples and strong approximation. *Comptes Rendus Mathématique* 354.2 (2016), pp. 131–135.

[BGS25] Jean Bourgain, Alexander Gamburd, and Peter Sarnak. Strong approximation and Diophantine properties of Markoff triples. *Journal of the American Mathematical Society* (2025).

[BGS26] Jean Bourgain, Alexander Gamburd, and Peter Sarnak. Strong approximation for varieties of Markoff type (2026). In preparation.

[Boa05] Philip Boalch. From Klein to Painlevé via Fourier, Laplace and Jimbo. *Proceedings of the London Mathematical Society* 90.1 (2005), pp. 167–208.

[Cam25] João Campos-Vargas. Markoff triples and generating pairs of $\mathrm{SL}_2(\mathbb{F}_p)$. arXiv:2508.21671. 2025.

[CF12] Richard H. Crowell and Ralph Hartzler Fox. Introduction to knot theory. Vol. 57. Springer Science & Business Media, 2012.

[Che+23] Yu-Fang Chen, Vojtěch Havlena, Ondřej Lengàl, and Andrea Turrini. A symbolic algorithm for the case-split rule in solving word constraints with extensions. *Journal of Systems and Software* 201, e111673 (2023).

[Che24] William Y. Chen. Nonabelian level structures, Nielsen equivalence, and Markoff triples. *Annals of Mathematics* 199.1 (2024), pp. 301–443.

[CL09] Serge Cantat and Frank Loray. Dynamics on character varieties and Malgrange irreducibility of Painlevé VI equation. *Annales de l'institut Fourier* 59.7 (2009), pp. 2927–2978.

[CLM25] Matthew de Courcy-Ireland, Matthew Litman, and Yuma Mizuno. Divisibility by p for Markoff-like Surfaces. arXiv:2509.02187. 2025.

[DG99] Persi Diaconis and Ronald Graham. The graph of generating sets of an abelian group. *Colloquium Mathematicae* 80.1 (1999), pp. 31–38.

[DM00] Boris Dubrovin and Marta Mazzocco. Monodromy of certain Painlevé VI transcendents and reflection groups. *Inventiones mathematicae* 141.1 (2000), pp. 55–147.

[DM24] Joel D. Day and Florin Manea. On the structure of solution-sets to regular word equations. *Theory of Computing Systems* 68.4 (2024), pp. 662–739.

[Edd+25] Jillian Eddy, Elena Fuchs, Matthew Litman, Daniel E. Martin, and Nico Tripeny. Connectivity of Markoff mod p graphs and maximal divisors. *Proceedings of the London Mathematical Society* 130.2 (2025), e70027.

[FRS95] Benjamin Fine, Gerhard Rosenberger, and Michael Stille. Nielsen transformations and applications: A survey. *Groups – Korea 94*. Vol. 94. Berlin, Germany: De Gruyter, 1995, pp. 69–105.

[Fuc+24] Elena Fuchs, Matthew Litman, Joseph H Silverman, and Austin Tran. Orbits on K3 surfaces of Markoff type. *Experimental Mathematics* 33.4 (2024), pp. 663–700.

[Gol03] William M. Goldman. The modular group action on real SL(2)–characters of a one-holed torus. *Geometry & Topology* 7.1 (2003), pp. 443–486.

[Gol97] William M. Goldman. Ergodic theory on moduli spaces. *Annals of Mathematics* 146.3 (1997), pp. 475–507.

[IK21] Henryk Iwaniec and Emmanuel Kowalski. Analytic Number Theory. Vol. 53. American Mathematical Soc., 2021.

[Lou10] Larsen Louder. Nielsen equivalence in closed surface groups. arXiv:1009.0454. 2010.

[LT14] Oleg Lisovyy and Yuriy Tykhyy. Algebraic solutions of the sixth Painlevé equation. *Journal of Geometry and Physics* 85 (2014), pp. 124–163.

[Lus91] Martin Lustig. Nielsen equivalence and simple-homotopy type. *Proceedings of the London Mathematical Society* 3.3 (1991), pp. 537–562.

[Mac69] Alexander M. Macbeath. Generators of the linear fractional groups. *Proceedings of Symposia in Pure Mathematics*. American Mathematical Society. Providence, Rhode Island, 1969, pp. 14–32.

[Mar25] Daniel E. Martin. A new proof of Chen's theorem for Markoff graphs. *Inventiones Mathematicae* 241 (2025), pp. 623–626.

[Mar79] Andrey Markoff. Sur les formes quadratiques binaires indéfinies. *Mathematische Annalen* 15.3 (1879), pp. 381–406.

[McC05] Darryl McCullough. Exceptional subgroups of SL(2,F). math.ou.edu/~dmccullough/research/manuscripts.html. 2005.

[MW13] Darryl McCullough and Marcus Wanderley. Nielsen equivalence of generating pairs of SL$(2, q)$. *Glasgow Mathematical Journal* 55.3 (2013), pp. 481–509.

[Oan11] Daniel Oancea. A note on Nielsen equivalence in finitely generated abelian groups. *Bulletin of the Australian Mathematical Society* 84.1 (2011), pp. 127–136.

[Pak01] Igor Pak. What do we know about the product replacement algorithm? *Groups and computation* 3 (2001), pp. 301–347.

[PCI24] Michel Planat, David Chester, and Klee Irwin. Dynamics of Fricke–Painlevé VI Surfaces. *Dynamics* 4.1 (2024), pp. 1–13.

[Wal00] Michel Waldschmidt. Diophantine Approximation on Linear Algebraic Groups. Vol. 326. Grundlehren der Mathematischen Wissenschaften. Berlin: Springer, 2000.

[Was12] Lawrence C. Washington. Introduction to cyclotomic fields. Vol. 83. Springer Science & Business Media, 2012.

[Zie70] Heiner Zieschang. Über die Nielsensche Kürzungsmethode in freien Produkten mit Amalgam. *Inventiones Mathematicae* 10.1 (1970), pp. 4–37.

Clemson University, O-110 Martin Hall, 220 Parkway Drive, Clemson, SC
Email address: dem6@clemson.edu