hexagon:2611.00916v2

# XIA'S EQUATIONS FOR THE HIGMAN–MCLAUGHLIN (1961) CONJECTURE: EXACT SOLUTION COUNTS WHEN THE NORM EQUATION IS REPLACED BY ITS SUM, AND OTHER MISCELLANEA

DAVE GOEL

Abstract. Every known finite flag-transitive projective plane is Desarguesian, and it is an old conjecture, first mentioned by Higman and McLaughlin in 1961, that there are no others. By theorems of Kantor and of Thas and Zagier, a counterexample of order $n$ would force $p = n^2+n+1$ to be prime and make the subgroup of order $n+1$ of $\mathbb{F}_p^\times$ a planar difference set. Then $n \equiv 8 \pmod{24}$, and from the difference set Xia derived a further necessary condition: a system of polynomial equations over a field of characteristic 3 has a solution. The system consists of a Frobenius relation, a norm equation, an autocorrelation equation and a doubling equation, and Xia conjectured that it has no solution for $n > 8$. We completely solve the norm-free system, obtained by replacing the norm equation by its sum over all indices: for every $n \equiv 8 \pmod{24}$ and every even divisor $\sigma$ of $n$ (the shift in the Frobenius relation), the resulting system has exactly $4\prod_i(3^{L_i} - 1)$ solutions, where the $L_i$ are the lengths of explicit Frobenius orbits on roots of unity. So any proof of Xia's conjecture must use the norm equation itself. For $\sigma = 2$ we show that, once the Fourier transform of the unknowns is fixed on the $(n/2)$-th roots of unity, the norm equation becomes two conditions, each involving only one eigenspace of an involution of the remaining parameters. For $n = 2^e$ with $e \geq 5$ odd the two conditions are not independent: the remaining parameters lie on a conic. Xia's system with $\sigma = 2$ has at most $16\,(4/3)^b\,3^{n/8}$ solutions ($b \geq 0$ is an explicit integer, $b = 0$ when $16 \mid n$), and at most $16(3^{n/8} - 1)$ when $n = 2^e$ with $e \geq 5$ odd. For $8 \mid n$, the analogous exact count, $4\prod_i(r^{L_i} - 1)$, holds for the norm-free versions of Xia's systems in every characteristic $r$ with $r \nmid pn$ and $r \not\equiv -1$ modulo the 2-part of $n$. We show that solutions of a special form force every odd prime factor of $n$ to be a base-2 Wieferich prime, and verify by computation that at $\sigma = 2$ the system has no solution for $n = 32$, 56 and 80, and that at $n = 128$ it has none for any even $\sigma$ dividing 128. For $n = 2^e$ and the system without its Frobenius relation, which Xia conjectures has no solution, a group of $n^2/4$ affine substitutions of the indices acts on the solutions; we show that for odd $e$ a solution fixed by a non-trivial substitution lies on one explicit locus or its shift, that for $e \geq 5$ no solution of Xia's system with $\sigma = 2$ lies there, and that the group acts freely for $n = 32$ and $n = 128$. Extending a search of Thas and Zagier, we report a computer search (one program over the whole range, with an independent partial check) showing that a non-Desarguesian flag-transitive plane has order $n \geq 10^{14}$, and we discuss open questions, among them the orders $n = 2^e$, which appear to be open in the literature. The conjectures of Xia and of Higman and McLaughlin remain open.

*This is the expanded version of the paper "Xia's equations for the Higman–McLaughlin (1961) conjecture: exact solution counts when the norm equation is replaced by its sum"* [5].

## 1. Introduction

We study the Higman–McLaughlin (1961) conjecture, that every finite flag-transitive projective plane is Desarguesian, through the polynomial systems of Xia [19].

A projective plane is *flag-transitive* if its collineation group acts transitively on the incident point–line pairs. The Desarguesian planes $\mathrm{PG}(2, q)$ are flag-transitive, and it is an old conjecture, first mentioned by Higman and McLaughlin [9] in 1961 (see [17, p. 174]), that among the finite

*Date*: First version: November 4, 2026. This version: November 23, 2026.

2020 *Mathematics Subject Classification.* Primary 51E15; Secondary 05B10, 11T22, 11T24.

*Key words and phrases.* flag-transitive projective plane, planar difference set, finite fields, Gauss sums, Xia's equations.

planes there are no others. We call this the Higman–McLaughlin (1961) conjecture. It is still open. A *counterexample* would be a non-Desarguesian finite flag-transitive plane. Kantor [12, Theorem A] showed, using the classification of finite simple groups, that a finite flag-transitive plane of order $n$ is either Desarguesian, or its collineation group is a Frobenius group of odd order $(n^2+n+1)(n+1)$ and $p = n^2+n+1$ is prime. In the second case the plane is the development of the subgroup $H$ of order $n+1$ of $\mathbb{F}_p^\times$: the points and lines are the elements of $\mathbb{F}_p$, and $x$ lies on $y$ if and only if $x-y \in H$ (Thas and Zagier [17, Proposition 2.1, Theorem 2.4]; they describe their Proposition 2.1 as essentially a restatement of a result of Fink). So the conjecture is equivalent to the following arithmetic statement.

**Question 1.1** (Kantor)**.** Let $n > 8$ be even and let $p = n^2+n+1$ be prime. Can the subgroup $H$ of order $n+1$ of $\mathbb{F}_p^\times$ be a planar difference set, that is, can every non-zero element of $\mathbb{F}_p$ be a difference $h - h'$ of two elements of $H$ in exactly one way?

For $n = 2$ ($H = \{1, 2, 4\}$ in $\mathbb{F}_7$) and $n = 8$ the answer is yes, and the planes are $\mathrm{PG}(2,2)$ and $\mathrm{PG}(2,8)$ [17, Section 2]. A counterexample must have $8 \mid n$ (Jungnickel and Vedder [11]; also Feit [3], as stated in [17, p. 189]), $n \equiv 2 \pmod 3$ [17, p. 189], [19, Lemma 4.1], every divisor of $n$ in $H$ (Feit [3]; an elementary proof is in K. Thas [16]; see [17, p. 175]), and $n \geq 2 \cdot 10^{11}$ (Thas and Zagier [17, Appendix]). We continue their search and obtain $n \geq 10^{14}$ (Proposition 8.4). Thas and Zagier also gave several equivalent forms of planarity, through Gauss periods and the points of Fermat curves [17, Theorem 3.1].

Two published arguments would together settle the question completely, and Thas and Zagier explain why neither is complete [17, Remark 1.2]: as they point out, Feit's claim that $n$ is not a power of 2 uses a lemma of Gordon, Mills and Welch [6] beyond the hypotheses under which it is proved, and Ott's claim that the order is a prime power has a gap in one derivation. Ho and Pott [10] also deduce that $n$ is not a power of 2. For $n = 2^e$ their argument (in the proof of their Lemma 3.1(2)) uses [10, Theorem 2.2]: the multiplier group of a cyclic plane of order $p_0^k$ ($p_0$ prime) consists of the powers of $p_0$. They attribute this to Gordon, Mills and Welch. As stated in [6], that result concerns the difference sets constructed there, a class that includes the Singer difference sets of $\mathrm{PG}(2,q)$ [6, Theorem 5]. So the case of orders $n = 2^e$ appears to be open in the literature. Since $p = 4^e + 2^e + 1$ must be prime, $e$ is a power of 3 (Section 8.5), say $e = 3^j$. Here $j = 1$ gives $n = 8$; for $j = 2$ ($n = 512$) Thas and Zagier checked directly that $H$ is not planar; and for $3 \leq j \leq 14$ the number $p$ is composite (Section 8.5; for $j \geq 10$ the prime factors are taken from Alpern's table [1] and checked here). So an open power-of-two order satisfies $n \geq 2^{3^{15}} = 2^{14348907}$.

Xia [19, Theorem 1.3] translated Question 1.1 into polynomial systems over finite fields of characteristic 3, using the Gauss periods of $H$. For a counterexample of order $n > 8$ we have $n \equiv 8 \pmod{24}$, and there is an even divisor $\sigma$ of $n$ such that the following system, in $n$ unknowns $y_0, \ldots, y_{n-1}$ from $\mathbb{F}_{3^{n/\sigma}}$ (subscripts modulo $n$), has a solution: the reductions of $n$ times these periods (Remark 2.5). Its four lines are a Frobenius relation (L1) with shift $\sigma$, a *norm equation* (L2), an autocorrelation equation (L3) and a doubling equation (L4):

$$
\begin{aligned}
&\text{(L1)} \quad y_{s+\sigma} = y_s^3, && s = 0, 1, \ldots, n-1,\\
&\text{(L2)} \quad y_s\, y_{s+n/2} = -1, && s = 0, 1, \ldots, n/2-1,\\
&\text{(L3)} \quad \textstyle\sum_{t=0}^{n-1} y_t\, y_{s+t} = 0, && s = 0, 1, \ldots, n/2-1,\\
&\text{(L4)} \quad \textstyle\sum_{t=0}^{n-1} (-1)^t y_t\, y_{2s-t} = \big(y_s + y_{s+n/2}\big) \sum_{t=0}^{n-1} (-1)^t y_t, && s = 0, 1, \ldots, n/2-1.
\end{aligned}
\tag{1}
$$

This is the system (12) of [19]; we call it *Xia's system*. Xia conjectured that for $n > 8$ with $n \equiv 8 \pmod{24}$ it has no solution for any even $\sigma \mid n$ [19, Conjecture 5.2] and reported no solution for $n = 32$; we call this conjecture Xia's conjecture (it is stated already in the first arXiv version of [19], 2017). The norm equation says $y_s\, y_{s+n/2} = -1$ for each $s$; summing it over all $s \in \mathbb{Z}/n$ gives $R(n/2) = -n$, where $R(s) := \sum_t y_t\, y_{t+s}$ is the periodic autocorrelation of $y$, and $-n = 1$ in $\mathbb{F}_3$ as

$n \equiv 2 \pmod 3$. For $\sigma = 2$, (L1) ties every $y_t$ to $y_0$ or $y_1$, and the norm equation becomes two norm conditions, $\mathrm{N}(y_0) = \mathrm{N}(y_1) = -1$, where $\mathrm{N}(x) = x^{1+3^{n/4}}$ is the norm from $\mathbb{F}_{3^{n/2}}$ to $\mathbb{F}_{3^{n/4}}$ (Section 2). For $\sigma = 2$, fix the values of the Fourier transform of $y$ on the $(n/2)$-th roots of unity (the *lower layers*). The solutions of the norm-free system (Xia's system with the norm equation replaced by its sum $R(n/2) = 1$) with these values form a *fibre*, and Theorem 5.1 places it in an $\mathbb{F}_3$-vector space $V$ with an involution $T$ whose eigenspaces are $V_+$ and $V_-$. We do not decide whether Xia's system has a solution for any $n > 8$. Figure 1 shows the chain of reductions from a counterexample to Xia's system, and where the results of this paper sit in it.

This paper is the expanded version of [5]: Sections 2–5 and 7 contain the results of [5], with the same proofs, and the other sections contain further results. The table and Figure 2 compare our main results with the best results known before this paper; in the table, $2^a$ is the 2-part of $n$, the $L_i$ are lengths of explicit Frobenius orbits on roots of unity, and $\sigma_r$ is Xia's shift in characteristic $r$.

| Best result before this paper | New result |
|---|---|
| $n \geq 2 \cdot 10^{11}$ (Thas and Zagier [17, Appendix]) | A non-Desarguesian flag-transitive plane has order $n \geq 10^{14}$ (Proposition 8.4; one program, with an independent partial check) |
| No count; Xia's heuristic compares $n$ unknowns with $5n/2$ equations [19, Section 5] | Xia's system with the norm equation replaced by its sum (the norm-free system), for every $n$ with $8 \mid n$ and $3 \nmid n$ (in particular every $n \equiv 8 \pmod{24}$) and every even divisor $\sigma$ of $n$: exactly $4\prod_i(3^{L_i}-1)$ solutions, always at least one (Theorem 4.1 and Proposition 4.3) |
| Xia's computation at $n = 32$ [19, Section 5]; no published bound for larger $n$ | Xia's system, $\sigma = 2$: at most $16(3^{n/8}-1)$ solutions for $n = 2^e$, $e \geq 5$ odd (Corollary 3.6), and at most $16\,(4/3)^b\,3^{n/8}$ for every $n \equiv 8 \pmod{24}$, where $b$ is the number of case-B blocks (defined in the list of results below; Corollary 5.2) |
| No count; the systems exist [19, Theorem 3.4], and Xia's shift satisfies the sign condition [19, Lemma 3.5] | For $8 \mid n$, the norm-free systems in characteristic $r \nmid pn$, $r \not\equiv -1 \pmod{2^a}$: exactly $4\prod_i(r^{L_i}-1)$ solutions for Xia's shift $\sigma_r$, none for a shift of the other parity (Theorem 7.5) |
| verified at $n = 32$ [19, Section 5] | Xia's conjecture: verified at $n = 128$ for every even $\sigma$, and at $\sigma = 2$ for $n = 56$ and $n = 80$ (Proposition 9.23, Section 8) |
| stated without computations [19, Section 5] | Toward the strong form of [19, Conjecture 5.4], for (1) with (L1) deleted: the group of $n^2/4$ substitutions acts freely on its solutions for $n = 32$ and $n = 128$ (Section 9) |

**Results.** Our main results describe Xia's system after the norm equation is replaced by its sum over all indices, which is a consequence of it when $n \equiv 2 \pmod 3$; we call the result the *norm-free system* (Definition 2.3).

- **Every** $n$ (Theorem 4.1 and Proposition 4.3). For every $n \equiv 8 \pmod{24}$ and every even divisor $\sigma$ of $n$, the norm-free system has exactly $4\prod_i(3^{L_i}-1)$ solutions, where $L_i$ is the common length of the two orbits in the $i$-th pair of orbits of $\xi \mapsto \xi^3$ on the $\xi \in \mu_n$ whose order is divisible by the 2-part of $n$ (the *top layer*; $\mu_n$ is the group of $n$-th roots of unity in an algebraic closure of $\mathbb{F}_3$); for odd $\sigma$ it has none. The proof constructs every solution layer by layer (a *layer* is the set of elements of $\mu_n$ whose order has a given 2-part; Figure 3 shows the layers for $n = 80$). Hence any obstruction lies in the norm equation, and not

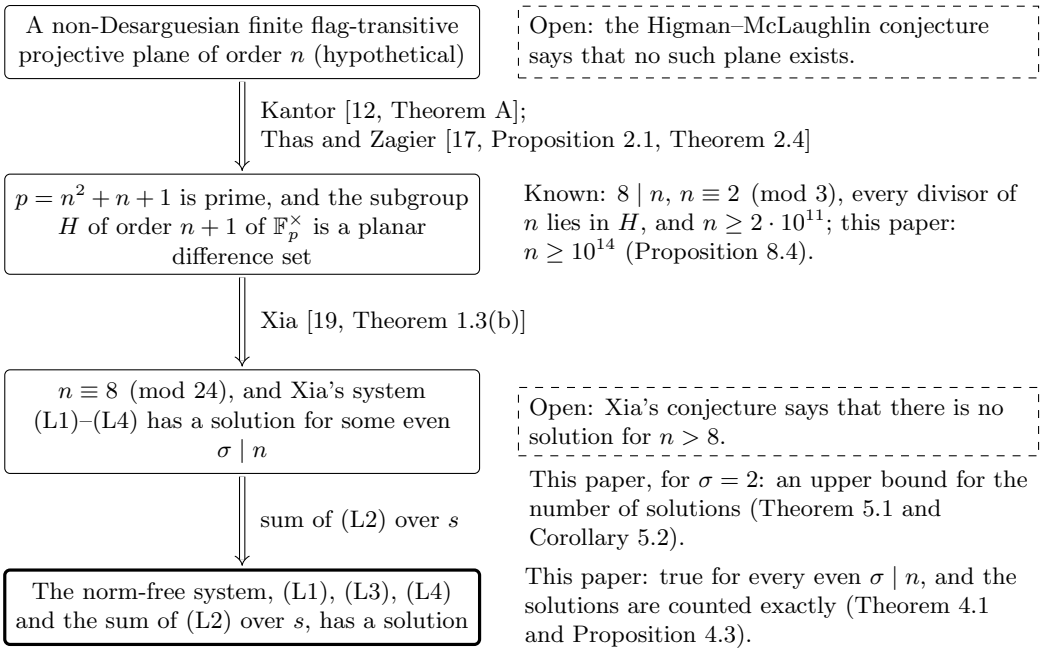


FIGURE 1. The known chain of reductions, and where the results of this paper sit. The first three boxes concern a hypothetical plane of order $n$; the last holds for every $n \equiv 8 \pmod{24}$ (Theorem 4.1 and Proposition 4.3). Each double arrow is an implication for such a plane: the first two are proved in the cited works, and the last one sums (L2) over $s$. Dashed frames mark the two open conjectures, and the thick frame the condition that this paper proves.

in the count of equations against unknowns with which Xia supports Xia's conjecture [19, Section 5].

- **Powers of two** (Theorems 3.1 and 3.5, Corollary 3.6). These are the orders whose exclusion in [3] and [10] is incomplete (see above). For $n = 2^e$ and $\sigma = 2$ the solutions of the norm-free system are given by one parameter $\theta$ and two signs; there are $4(3^{n/4} - 1)$ of them. For odd $e \geq 5$ an involution of the parameter space splits the norm equation into two conditions, one on each of its two eigenspaces; they stay coupled through a conic relating the components $\theta_+$, $\theta_-$ of the parameter. Xia's system has at most $16(3^{n/8} - 1)$ solutions.
- **The two norm conditions for general** $n$ (Theorem 5.1 and Corollary 5.2). This extends the previous item from powers of two to the residue class to which every counterexample belongs ([17, p. 189], [19, Lemma 4.1]). For every $n \equiv 8 \pmod{24}$ the substitution $t \mapsto (1 + n/2)t$ of the indices is a symmetry of the norm-free system; it splits the top data (the values of the Fourier transform of $y$ on the top layer) into the two eigenspaces $V_+$, $V_-$ of the involution $T$ it induces. On each fibre (the lower layers fixed), $y_0$ depends only on $V_+$ and $y_1$ only on $V_-$. The map $\xi \mapsto -\xi$ permutes the orbits of $\xi \mapsto \xi^3$ on the top layer, and we group these orbits into *blocks* (Figure 3): a pair $\{O, O^{-1}\}$ is a block of *case A* if $-O = O$ and of *case B* if $-O = O^{-1}$, and every other orbit lies in a block $\{O, O^{-1}, -O, -O^{-1}\}$ of *case C*. Theorem 5.1(c) describes the points of a fibre block by block (Table 4 lists the blocks for the five smallest $n \equiv 8 \pmod{24}$). Thus, for $n \equiv 8 \pmod{24}$ and $\sigma = 2$, Xia's system has a solution if and only if, in some fibre, a $V_+$-component allowed by $\mathrm{N}(y_0) = -1$ and a $V_-$-component allowed by $\mathrm{N}(y_1) = -1$ add up to a point of the fibre. This is the open question drawn in Figure 2. Xia's system (1) with $\sigma = 2$ has at most $16\,(4/3)^b\,3^{n/8}$ solutions, where $b$ is the number of case-B blocks. Xia's proof fixes $\sigma$ for each $n$, and we

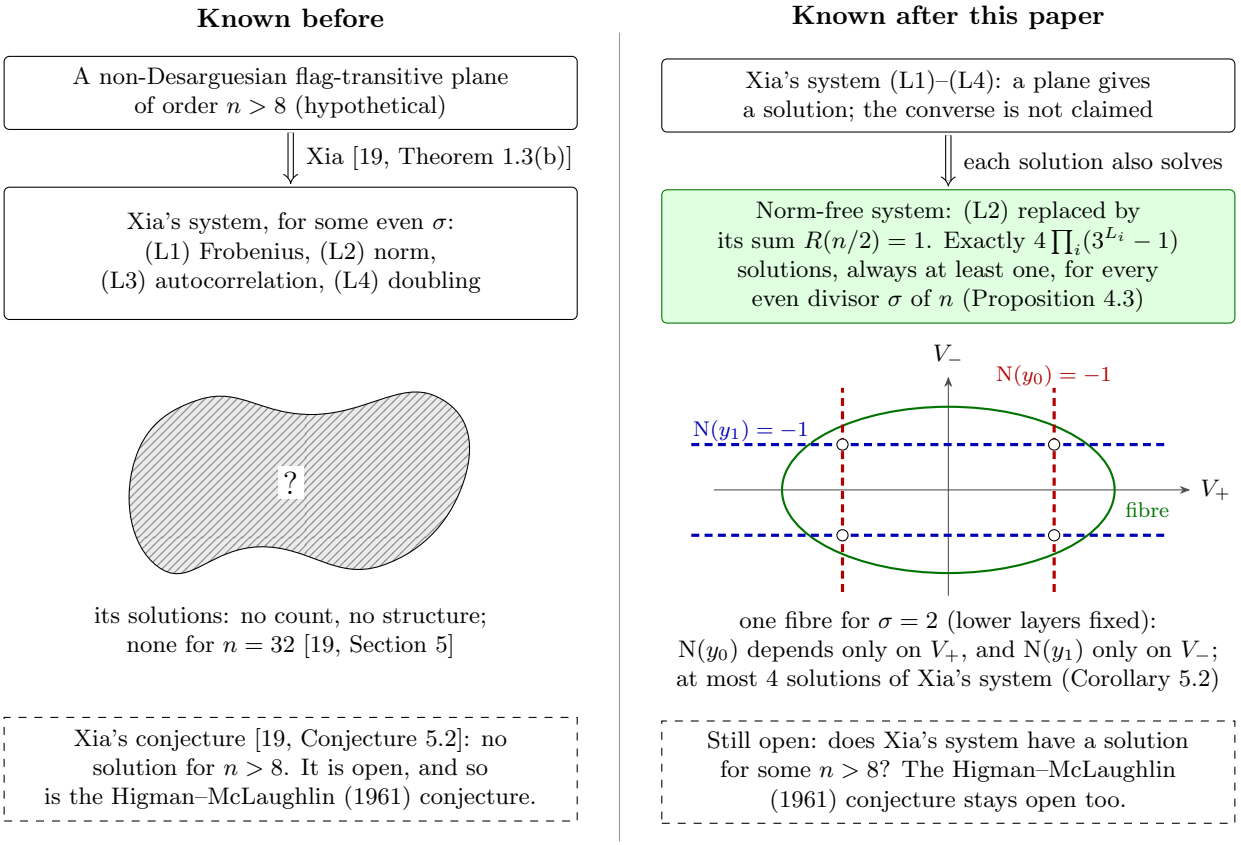


FIGURE 2. Xia's system before and after this paper. Left: a plane gives a solution of Xia's system (one-way arrow); the solutions were not classified. Right: with the norm equation replaced by its sum $R(n/2) = 1$, the solutions are counted exactly (Proposition 4.3); for $\sigma = 2$ each of the two norm conditions depends on one eigenspace of an involution $T$, and each fibre contains at most 4 solutions of Xia's system (Theorem 5.1 and Corollary 5.2). The right picture is a schematic of one fibre (the closed curve) inside $V = V_+ \oplus V_-$. The dashed vertical lines mark where $\mathrm{N}(y_0) = -1$ (at most two values of the $V_+$-component), and the dashed horizontal lines where $\mathrm{N}(y_1) = -1$ (at most two values of the $V_-$-component). A solution of Xia's system would be a crossing on the curve. Whether one exists for some $n > 8$ is open, so the crossings (circles) are drawn off the curve. The involution $T$ fixes $V_+$ and negates $V_-$; the crossings on the curve, if there are any, form one orbit of the group generated by $T$ and $v \mapsto -v$.

call this value the $\sigma$ *of* $n$ (Section 2): $n/\sigma$ is the order of 3 in $\mathbb{F}_p^\times/H$. The bound bears on a counterexample of order $n$ only when the $\sigma$ of $n$ is 2, which is the case for every $n = 2^e \geq 8$ with $p$ prime but not for $n = 80$.

- **The slice** $y_1 = \pm i$ (Theorem 6.2). Here $i \in \mathbb{F}_9$ and $i^2 = -1$. Any solution of (1) at $\sigma = 2$, and more generally any solution of the norm-free system, with $y_0 = \pm i$ or $y_1 = \pm i$ forces $8 \nmid n/2$ and, for every odd prime $q \mid n/2$, that $\mathrm{ord}_q(3)$ is even and $q$ is a base-2 Wieferich prime. Of the two known base-2 Wieferich primes, 1093 and 3511, only 3511 has $\mathrm{ord}_q(3)$ even ($\mathrm{ord}_{1093}(3) = 7$), and Dorais and Klyve found no other Wieferich prime below $6.7 \times 10^{15}$ [2].

- **Other primes** (Theorems 7.2 and 7.5). Xia's system has an analogue in characteristic $r$ for every prime $r \nmid pn$; Xia derives these systems [19, Theorem 3.4] and illustrates them with $r = 3$ only. For $n = 2^e$ with $e$ odd and $r = 5$, Xia's shift can be taken to be 1 whenever $p$ is prime. With this shift the norm-free system in characteristic 5 has exactly $4(5^{n/4} - 1)$ solutions, and the norm equation becomes a single condition on $y_0$. More generally, write $n = 2^a n_{\text{odd}}$ with $a \geq 3$ and $n_{\text{odd}}$ odd, and let $r \not\equiv -1 \pmod{2^a}$. For any integer shift $\sigma_r$, the norm-free system in characteristic $r$ has no solution if $(-1)^{\sigma_r} \neq \left(\frac{p}{r}\right)$, and exactly $4\prod_i (r^{L_i} - 1)$ solutions otherwise, $L_i$ now being the common length of the two orbits in the $i$-th pair of orbits of $\xi \mapsto \xi^r$. When $p$ is prime, Xia's own shift is defined by $\chi_r(r) = \varpi_r^{\sigma_r}$ for an $r$-adic multiplicative character $\chi_r$ of order $n$ on $\mathbb{F}_p$ (values in $\mathbb{C}_r$, as for $r = 3$ in Section 2) and a primitive $n$-th root of unity $\varpi_r$. For $r = 3$, with $\varpi_3$ chosen so that $\sigma_3 \mid n$ (as in Section 2), it is the $\sigma$ of $n$. Since $\chi_r^{n/2}$ is the quadratic character of $\mathbb{F}_p$, $(-1)^{\sigma_r} = \chi_r(r)^{n/2} = \left(\frac{r}{p}\right)$, and $\left(\frac{r}{p}\right) = \left(\frac{p}{r}\right)$ by quadratic reciprocity, as $p \equiv 1 \pmod 4$ and $r$ is odd. This is [19, Lemma 3.5] in our setting, and it needs no plane. So, for $r \not\equiv -1 \pmod{2^a}$ (and for every $r$ when $n = 2^a$, by Proposition 7.7), no argument that uses the norm-free system for one prime $r$ can exclude a counterexample.
- **Beyond** $2 \cdot 10^{11}$ (Proposition 8.4). No $n \equiv 8 \pmod{24}$ with $2 \cdot 10^{11} \leq n < 10^{14}$ and $p$ prime satisfies $2^{n+1} \equiv 1 \pmod p$ (one program over the whole range; an independent program checked the coverage and the counts and recomputed 176 of the 41588 blocks). So a non-Desarguesian flag-transitive projective plane has order $n \geq 10^{14}$, which improves the bound $n \geq 2 \cdot 10^{11}$ of Thas and Zagier [17, Appendix] by a factor of 500.
- **The geometric relaxation** (Section 9). Deleting the Frobenius relation (L1) from (1) leaves a system that does not involve $\sigma$; let $W(n)$ be its set of solutions over $\overline{\mathbb{F}}_3$. A plane of order $n$ gives a point of $W(n)$, and Xia conjectures that $W(n)$ is empty (the strong form of [19, Conjecture 5.4]), but gives no computation for it. For $n = 2^e$ with $e$ odd, the group $G$ of the $n^2/4$ substitutions $t \mapsto ct + s$ ($c$ odd, $s$ even) acts on $W(n)$. We show by hand that no point of $W(2^e)$ is fixed by a reflection or by $t \mapsto (n/2 - 1)t + s$ (Lemmas 9.10 and 9.13). So a point with a non-trivial stabiliser lies on one explicit locus or on its shift. Of the shapes a point on this locus can take, two are impossible for every odd $e \geq 7$ (Lemmas 9.35 and 9.37), and a third is impossible unless a certain function $\Theta$ is a square at every root (Lemmas 9.42 and 9.32(c)). For a fourth shape, Theorem 9.65 (with one computer-algebra step, Lemma 9.54) shows for every odd $e \geq 11$ that such a point either gives a point, with coordinates of prescribed degrees, of one of finitely many sets over $\mathbb{F}_{3^8}$ (of two kinds), or falls in one remaining case. These sets are given by polynomial equations and one inequation and do not depend on $e$. The remaining case gives a point of one of the fixed sets of Theorem 9.67, at a level that may grow with $e$ (Question 9.68). The locus is empty for $n = 32$, by hand (Corollary 9.43), and for $n = 128$, by hand and computation (Proposition 9.44); so $G$ acts freely on $W(32)$ and on $W(128)$. For planes the locus plays no role: for every odd $e \geq 5$ no solution of (1) with $\sigma = 2$ lies on it or on its shift (Corollary 9.20), so a plane of order $2^e$ gives a point of $W(2^e)$ with trivial stabiliser, on which the map $F^{n/4}$, where $F(y) = (y_t^3)_t$, acts as the shift by $n/2$. For $\sigma = n/2$ the system (1) reduces to $\mathbb{F}_3$-sequences with no zero that satisfy three relations. We classify them by hand for length 16 (Corollary 9.29: the only ones are $\pm(J + \delta_{r_0})$, where $J$ is the all-one sequence and $\delta_{r_0}$ is 1 at $r_0$ and 0 elsewhere, which Lemma 9.21 excludes), and this settles $n = 32$, $\sigma = 16$ without computation. For length 64 two independent programs classify them. Together with two independent programs for $\sigma = 4, 8, 16, 32$, this shows that at $n = 128$ the system (1) has no solution for any even $\sigma \geq 4$ dividing 128 (Proposition 9.23).
- **Computations** (Section 8). At $\sigma = 2$ the system (1) has no solution for $n = 32$, 56 and 80; Xia reports no solution for $n = 32$ [19, Section 5]; 56 and 80 are new. These are statements

about Xia's system, which depends only on $n$ and $\sigma$; they are not new results on planes (for $n = 32$ and 56 the number $p$ is not prime, and for $n = 80$, where $p = 6481$ is prime, a plane would have $\sigma = 10$). For $n = 128$ two independent programs give the same answer (Section 8.1), and for $n = 104$ one program does (Remark 8.1). Two further independent programs find no solution for $\sigma = 14, 28$ at $n = 56$, for $\sigma = 10, 20, 40$ at $n = 80$ and for $\sigma = 26, 52$ at $n = 104$ (Remark 9.24); at $n = 80$ this includes $\sigma = 10$, the value a plane of order 80 would have.

The paper is organised as follows. Section 2 recalls Xia's system and puts it in Fourier form. Section 3 treats powers of two. Section 4 solves the norm-free system for every $n$, and Section 5 extends the eigenspace split of Section 3.2 to every $n$. Section 6 treats the slice, Section 7 the prime 5 and the other primes, and Section 8 the computations. Section 9 studies the system without its Frobenius relation. Section 10 explains why the standard routes stop, and Section 11 lists open questions.

## 2. Xia's system and its Fourier form

We recall Xia's theorem, reduce the system for $\sigma = 2$ to the norm-free system and two norm conditions, and put the equations in the Fourier form that the later sections use.

2.1. **Xia's theorem.** Let $n \geq 2$ and $p := n^2 + n + 1$. We write $H$ for the subgroup of order $n + 1$ of $\mathbb{F}_p^\times$ when $p$ is prime.

**Theorem 2.1** (Xia [19, Theorem 1.3(b)])**.** *If there exists a finite non-Desarguesian flag-transitive projective plane of order $n$, then $p = n^2 + n + 1$ is prime, $n \equiv 8 \pmod{24}$, $n > 8$, and there exist a positive even integer $\sigma$ dividing $n$ and $y_0, \dots, y_{n-1} \in \mathbb{F}_{3^{n/\sigma}}$ such that* (1) *of the introduction holds.*

In (L4) the factor $y_s + y_{s+n/2}$ multiplies the whole alternating sum. The integer $\sigma$ comes from the proof of Theorem 1.3 in [19]: if $\chi$ is a 3-adic multiplicative character of order $n$ on $\mathbb{F}_p$, then $\chi(3) = \varpi^\sigma$ for a primitive $n$-th root of unity $\varpi$ in $\mathbb{C}_3$ and a positive divisor $\sigma$ of $n$. Here $\mathbb{C}_3$ is the completion of an algebraic closure of $\mathbb{Q}_3$. This $\sigma$ is determined by $n$ (see the proof of Lemma 2.2), and we call it the *$\sigma$ of $n$*. By Theorem 2.1 and its proof in [19], to exclude the planes of order $n$ it suffices to prove that (1) has no solution for this $n$ and the $\sigma$ of $n$.

**Lemma 2.2.** *Let $8 \mid n$ and let $p = n^2 + n + 1$ be prime. Then 3 is a fourth power modulo $p$ if and only if $3 \mid n$. Consequently, if $n \equiv 8 \pmod{24}$, then the $\sigma$ of $n$ satisfies $\sigma \equiv 2 \pmod 4$, and $\sigma = 2$ when $n$ is a power of 2.*

*Proof.* Since $8 \mid n$, $p \equiv 1 \pmod 8$, so $-1$ is a fourth power modulo $p$, and 3 is a fourth power if and only if $-3$ is. Since $4p = (2n+1)^2 + 3$, we have $-3 \equiv (2n+1)^2 \pmod p$; as $-1$ is a square (and $x^2 = z^4$ means $x = \pm z^2$), $-3$ is a fourth power if and only if $2n + 1$ is a square modulo $p$. Here $p$ is a prime larger than $2n + 1$, so $\gcd(2n + 1, p) = 1$, and $3 \nmid 2n + 1$ (else $3 \mid 4p$, so $p = 3$). Applying Jacobi reciprocity twice ($p \equiv 2n + 1 \equiv 1 \pmod 4$) and using $\left(\frac{4}{2n+1}\right) = 1$ and $4p \equiv 3 \pmod{2n+1}$, we get

$$\left(\frac{2n+1}{p}\right) = \left(\frac{p}{2n+1}\right) = \left(\frac{4p}{2n+1}\right) = \left(\frac{3}{2n+1}\right) = \left(\frac{2n+1}{3}\right),$$

which is 1 if and only if $2n + 1 \equiv 1 \pmod 3$, that is, $3 \mid n$.

For the consequence, write $3 = g^c$ for a generator $g$ of $\mathbb{F}_p^\times$. Since $\chi(g)$ is a primitive $n$-th root of unity, $\chi(3)$ has order $n/\gcd(c, n)$. Xia takes $\varpi$ primitive and $\sigma \mid n$ with $\chi(3) = \varpi^\sigma$ [19, proof of Theorem 1.3], so $\varpi^\sigma$ has order $n/\sigma$, and $\sigma = \gcd(c, n)$. As $H = \ker \chi$, $n/\sigma$ is also the order of 3 in $\mathbb{F}_p^\times / H$. This does not depend on $g$: another generator is $g^u$ with $\gcd(u, p - 1) = 1$, and $3 = (g^u)^{c'}$ gives $uc' \equiv c \pmod{p-1}$, so $\gcd(c', n) = \gcd(c, n)$ as $n \mid p - 1$. Since $n \equiv 8 \pmod{24}$, $n \equiv 2 \pmod 3$, so $p \equiv 4 + 2 + 1 \equiv 1 \pmod 3$; also $p \equiv 1 \pmod 4$. Quadratic reciprocity then shows that 3 is a square modulo $p$, so $c$ is even. Since $3 \nmid n$, by the first part 3 is not a fourth

power, so $c \equiv 2 \pmod 4$. With $8 \mid n$ this gives $\sigma = 2\gcd(c, n_{\mathrm{odd}})$, where $n_{\mathrm{odd}}$ is the odd part of $n$. Since $\gcd(c, n_{\mathrm{odd}})$ is odd, $\sigma \equiv 2 \pmod 4$, and $\sigma = 2$ when $n$ is a power of 2. (A power $n = 2^e$ with $8 \mid n$ and $p$ prime has $e$ odd: for $e$ even, $n \equiv 1 \pmod 3$ and $3 \mid p$. So it lies in the range $n \equiv 8 \pmod{24}$.) □

We call the residue class $n \equiv 8 \pmod{24}$ *Xia's range*. If a non-Desarguesian flag-transitive plane of order $n = 2^e$ exists, then $n$ is in Xia's range (Theorem 2.1) and the $\sigma$ of $n$ is 2 (Lemma 2.2). For $n_{\mathrm{odd}} > 1$ the $\sigma$ of $n$ may exceed 2. For $n = 80$ it is 10 by the proof of Lemma 2.2, as $3^{1296} \equiv 1 \pmod{6481}$ makes 3 a fifth power modulo $p$. Proposition 4.3 counts the solutions of the norm-free system with shift $\sigma$ for every even divisor $\sigma$ of $n$. In the next subsection, apart from Definition 2.3, $\sigma = 2$ and $n$ is in Xia's range. Then $m := n/2 \equiv 4 \pmod{12}$, so $m/2$ is even and $m \equiv 1 \pmod 3$.

2.2. **The norm-free system and the two norm conditions.** With $\sigma = 2$, (L1) ties every $y_t$ to $y_0$ or $y_1$, and (L2) reduces to two conditions. Put $F := \mathbb{F}_{3^m}$, $\phi(x) := x^3$, $Q := 3^{m/2}$, $k_0 := \mathbb{F}_Q \subset F$, $\bar{x} := \phi^{m/2}(x) = x^Q$ (the involution of $F$ over $k_0$), and $\mathrm{N} := \mathrm{N}_{F/k_0}$, so $\mathrm{N}(x) = x\bar{x}$. By (L1) with $\sigma = 2$,

$$y_{2k} = \phi^k(y_0), \qquad y_{2k+1} = \phi^k(y_1) \qquad (k \in \mathbb{Z}/m),$$

and $y_{t+m} = \overline{y_t}$. Hence (L2) holds if and only if $\mathrm{N}(y_0) = \mathrm{N}(y_1) = -1$.

Let $R(s) := \sum_t y_t\, y_{t+s}$ for $s \in \mathbb{Z}/n$; then $R(-s) = R(s)$, so (L3) gives $R(s) = 0$ for every $s \not\equiv m$, and (L2) gives $R(m) = \sum_t(-1) = -n$, which is 1 in $\mathbb{F}_3$ as $n \equiv 2 \pmod 3$. Let

$$S := \sum_{t=0}^{n-1} (-1)^t y_t.$$

**Definition 2.3.** Let $\sigma$ be a divisor of $n$. The *norm-free system with shift* $\sigma$ is the system (L1), (L3), $R(m) = 1$, (L4) for $y \in \mathbb{F}_{3^{n/\sigma}}^n$. For $\sigma = 2$ we call it the *norm-free system*; then $y \in F^n$.

Hence the solutions of (1) with $\sigma = 2$ are exactly the solutions of the norm-free system with $\mathrm{N}(y_0) = \mathrm{N}(y_1) = -1$.

2.3. **Fourier form.** In this subsection $n$ is any even integer with $3 \nmid n$, $m = n/2$, $F = \mathbb{F}_{3^m}$, and the norm-free system is defined as in Definition 2.3. Let $\mu_n$ be the group of $n$-th roots of unity in an algebraic closure $\overline{\mathbb{F}}_3$ of $F$. For $y \in F^n$ put

$$\widehat{y}(\xi) := \sum_{t \in \mathbb{Z}/n} y_t\, \xi^t \qquad (\xi \in \mu_n), \qquad \text{so} \qquad y_t = n^{-1} \sum_{\xi \in \mu_n} \widehat{y}(\xi)\, \xi^{-t}.$$

Then $S = \widehat{y}(-1)$.

**Proposition 2.4.** *Let $n$ be even with $3 \nmid n$. The map $y \mapsto \widehat{y}$ is a bijection from the solutions of the norm-free system onto the functions $\widehat{y}\colon \mu_n \to \overline{\mathbb{F}}_3$ with*

$$\begin{aligned} &\textit{(F1)} \quad \widehat{y}(\xi^3) = \xi^6\, \widehat{y}(\xi)^3, \\ &\textit{(F3)} \quad \widehat{y}(\xi)\, \widehat{y}(\xi^{-1}) = \xi^m, \\ &\textit{(F4)} \quad \widehat{y}(\xi)\, \widehat{y}(-\xi) = \widehat{y}(-1)\, \widehat{y}(\xi^2) \end{aligned}$$

*for all $\xi \in \mu_n$ (the labels follow (L1), (L3), (L4); there is no (F2), as (L2) has been replaced by $R(m) = 1$). Here (F1) is equivalent to (L1), (F3) to (L3) together with $R(m) = 1$, and (F4) to (L4). Moreover, $\widehat{y}$ has no zero on $\mu_n$, $\widehat{y}(\xi^{3^k}) = \xi^{2k3^k}\widehat{y}(\xi)^{3^k}$ for every $k \geq 0$, and $S^2 = (-1)^m$; so $S^2 = 1$ when $m$ is even, in particular in Xia's range.*

*Proof.* (F1). We have $\widehat{y}(\xi)^3 = \sum_t y_t^3 \xi^{3t}$. If (L1) holds, this is $\sum_t y_{t+2}\xi^{3t} = \xi^{-6}\widehat{y}(\xi^3)$. Conversely, if (F1) holds on $\mu_n$, then cubing the inversion formula and using that $\xi \mapsto \xi^3$ permutes $\mu_n$ (and

$n^{-1} \in \mathbb{F}_3$) gives $y_t^3 = y_{t+2}$; then $y_t^{3^m} = y_{t+n} = y_t$, so $y_t \in F$. Iterating (F1) gives $\widehat{y}(\xi^{3^k}) = \xi^{c_k}\widehat{y}(\xi)^{3^k}$ with $c_0 = 0$ and $c_{k+1} = 6 \cdot 3^k + 3c_k$, so $c_k = 2k\,3^k$.

(F3). We have $\widehat{y}(\xi)\widehat{y}(\xi^{-1}) = \sum_s R(s)\xi^s$. Write $[P]$ for 1 if $P$ holds and 0 otherwise; the condition $R(s) = [s = m]$ for all $s \in \mathbb{Z}/n$ is exactly (L3) together with $R(m) = 1$. By the inversion formula over $s$, this is equivalent to (F3) on all of $\mu_n$.

(F4). Let $c(w) := \sum_t (-1)^t y_t\, y_{w-t}$; then $\sum_w c(w)\xi^w = \widehat{y}(-\xi)\widehat{y}(\xi)$. For odd $w$ the substitution $t \mapsto w - t$ changes the sign of every term, so $c(w) = 0$. (L4) says $c(2s) = S\,(y_s + y_{s+m})$ for $0 \le s < m$; for $s \ge m$ both sides are unchanged by $s \mapsto s - m$, as $2s \equiv 2(s-m) \pmod n$. Since $\sum_{s\in\mathbb{Z}/m}(y_s + y_{s+m})\xi^{2s} = \sum_{s\in\mathbb{Z}/n} y_s\xi^{2s} = \widehat{y}(\xi^2)$, (L4) is equivalent to (F4) on $\mu_n$, with $S = \widehat{y}(-1)$.

Finally, (F3) shows that $\widehat{y}$ has no zero, and (F3) at $\xi = -1$ gives $S^2 = \widehat{y}(-1)^2 = (-1)^m$. □

*Remark* 2.5. The identities (F1), (F3), (F4) have the shape of the Frobenius law, the reflection law and the Hasse–Davenport product law for Gauss sums (for the last two see [19, Lemma 2.1]). This is expected: in Xia's proof the $y_s$ are reductions of the sums $g_s$ of [19, (1)], which are $n$ times Gauss periods [19, §2.3 and proof of Theorem 3.4].

*Remark* 2.6 (the two halves). Let $m$ be even. By (L1), $y_{t+m} = \overline{y_t}$. Write $y = y^+ + y^-$ with $y^+ := (y + \bar{y})/2 \in k_0^n$ (of period $m$) and $y^- := (y - \bar{y})/2$, so $\overline{y_t^-} = -y_t^-$ and $y_{t+m}^- = -y_t^-$. In (L3) and (L4) the cross terms $\sum_t y_t^+ y_{t+s}^-$ and $\sum_t (-1)^t y_t^+ y_{2s-t}^-$ change sign under $t \mapsto t + m$, so they vanish. Hence (L3) splits: $y^+$ has perfect periodic and $y^-$ perfect negaperiodic autocorrelation. (L4) does not split: its right side is $S(y_s + y_{s+m}) = 2Sy_s^+$. As $y^+$ has period $m$ and $y_{t+m}^- = -y_t^-$, $\widehat{y^+}$ vanishes where $\xi^m = -1$ and $\widehat{y^-}$ where $\xi^m = 1$. Thus $\widehat{y} = \widehat{y^+}$ on $\mu_m$ and $\widehat{y} = \widehat{y^-}$ on $\mu_n \setminus \mu_m$, and in the Fourier domain (L4) reads

$$\widehat{y^+}(\xi)\,\widehat{y^+}(-\xi) = S\,\widehat{y^+}(\xi^2) \quad (\xi \in \mu_m), \qquad \widehat{y^-}(\xi)\,\widehat{y^-}(-\xi) = S\,\widehat{y^+}(\xi^2) \quad (\xi \in \mu_n \setminus \mu_m).$$

So (L4) couples the halves, and the norm equation, $(y_t^+)^2 - (y_t^-)^2 = -1$ for every $t$, couples them index by index. Since $\mu_m$ is the union of the lower layers and $\mu_n \setminus \mu_m$ is the top layer, $y^+$ is the lower-layer part of $y$ and $y^-$ its top-layer part. Section 5 fixes the first and studies the second.

2.4. **Notation.** Table 1 lists every symbol of Sections 2–7 once (local proof variables excepted).

TABLE 1. Notation.

| symbol | meaning | where |
|---|---|---|
| $n$, $p$ | order of the plane; $p = n^2 + n + 1$ | §2 |
| $H$ | subgroup of order $n+1$ of $\mathbb{F}_p^\times$ | §2 |
| $\sigma$ | Xia's parameter, $\chi(3) = \varpi^\sigma$ | Thm. 2.1 |
| (L1)–(L4) | the four lines of Xia's system (1) | Thm. 2.1 |
| $m$ | $n/2$ | §2 |
| $F$, $\phi$ | $\mathbb{F}_{3^m}$; $\phi(x) = x^3$ | §2.2 |
| $Q$, $k_0$, $\bar{x}$, N | $3^{m/2}$; $\mathbb{F}_Q$; $x^Q$; $\mathrm{N}(x) = x\bar{x}$ | §2.2 |
| $R(s)$, $S$ | $\sum_t y_t y_{t+s}$; $\sum_t (-1)^t y_t$ | §2.2 |
| $\mu_n$, $\widehat{y}$ | $n$-th roots of unity; $\widehat{y}(\xi) = \sum_t y_t\xi^t$ | §2.3 |
| (F1), (F3), (F4) | Fourier form of (L1), (L3)+$R(m) = 1$, (L4) | Prop. 2.4 |
| $y^\pm$ | the halves $(y \pm \bar{y})/2$ | Rem. 2.6 |
| $\xi_0$, $\theta$ | a fixed element of order $n$; the parameter $\widehat{y}(\xi_0)$, $\theta^{Q-1} = -1$ | §3.1 |
| $O$, $O^{-1}$ | the two Frobenius orbits of elements of order $n = 2^e$ | §3.1 |
| $q$, $\iota$ | $3^{m/4} = 3^{n/8}$; $\xi_0^{n/4}$ (of order 4) | §3.2 |
| $\nu$ | $\theta^{1+q}$ ($\nu^{q-1} = -1$) | §3.2 |
| $V$, $V_\pm$ | $\{x \in F : x^Q = -x\}$ (the parameters and 0); the $\pm1$ eigenspaces of $T$; in §5 the sum of the block parameter spaces | Thm. 3.5, 5.1 |
| $T$ | the involution $x \mapsto \iota x^q$ of $V$; in §5 the block involutions | Thm. 3.5, 5.1 |

| symbol | meaning | where |
|---|---|---|
| $\Lambda_\nu$, $\Lambda'_\nu$ | the $\mathbb{F}_3$-linear maps of Section 3.2 | §3.2 |
| $a$, $n_{\mathrm{odd}}$ | $n = 2^a n_{\mathrm{odd}}$, $n_{\mathrm{odd}}$ odd (for $n = 2^e$: $a = e$) | Lem. 2.2, §4 |
| $j(\xi)$, $\mathcal{L}_a$, $\Xi_a$ | index of the layer that contains $\xi$; top layer ($j = a$); elements of order $2^a$ of $\mu_{2^a}$ | §4 |
| $I$, $L_i$ | index set of the pairs of top orbits $\{O, O^{-1}\}$; their lengths ($i \in I$) | Thm. 4.1 |
| $\mathrm{NF}(n)$, $K_n$ | solutions of the norm-free system; group of solutions of (h1), (h3), (h4) | §4 |
| $\mathcal{D}$, $\mathcal{D}^0$ | top data; their homogeneous version | §4 |
| $f$, $P(\alpha)$ | $\widehat{y}$ on $\mu_{n_{\mathrm{odd}}}$; the layer-1 product in (E1) | §4 |
| $G$, $G'$, $G''$, $G''_0$ | the module of Step 5; the torsors of $f$ and of $P$; the coset $(\tau f_0/f_0)(\tau-1)G$ | §4 |
| $\tau$, $\Pi$ | squaring automorphism $g \mapsto g(\alpha^2)$ of $G$; the map $\lambda \mapsto P_\lambda$ on homogeneous top data | §4 |
| $\beta$, $\ell$, $h$, $s$ | $\alpha^{2^{-(a-1)}}$; orbit length (not the $\ell$ of §6); half length of a self-inverse orbit; product over a fibre | §4 |
| $u$, $y^{(u)}$ | $1+m$; $y^{(u)}_t = y_{ut}$ (not the $u_k$ of §6) | §5 |
| $\rho_O$, $c_O$, $V_O$ | a fixed element of the top orbit $O$; $\rho_O^{-2L}$; $\{t : t^{3^L} = c_O t\}$ | §5 |
| $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$, $b$ | the sets of blocks of case A ($-O = O$), B ($-O = O^{-1}$), C (otherwise); $b = \lvert\mathcal{B}\rvert$ | §5 |
| $q_O$, $\iota_O$, $\nu_O$ | $3^{L/2}$ (cases A, B); $\rho_O^{Lq_O}$; the $\nu$-datum $(\widehat{y}(\rho_O)\widehat{y}(-\rho_O)$ in case A, $tt'$ in case C) | §5 |
| $\delta_O$ | the case-B constant $-\rho_O^{-Lq_O} t_0^{-1-q_O}$ (not the $\delta$ of Theorem 6.2) | §5 |
| $\Phi$, $\mathcal{Y}_0$, $\mathcal{Y}_1$ | the size of a fibre; the $\mathbb{F}_3$-linear maps with $y_0^- = \mathcal{Y}_0(v_+)$, $y_1^- = \mathcal{Y}_1(v_-)$ | Thm. 5.1 |
| $i$ | a square root of $-1$ in $\mathbb{F}_9 \subset F$ | §6 |
| $U$ | $\ker \mathrm{N}$, the norm-one torus of $F$ (order $Q+1$) | §6 |
| Tr | $\mathrm{Tr}_{F/\mathbb{F}_3}$ | §6 |
| $\omega$, $u_k$, $\widehat{u}$ | $y_0 = i\omega$; $u_k = \phi^k(\omega)$; $\widehat{u}(x) = \sum_k u_k x^k$ on $\mu_m$ | §6 |
| $J_j$, $B_Z(c)$ | $\sum_k u_k u_{j-k}$; $\sum_k \phi^k(Z)\phi^{c-k}(Z)$ | §6 |
| $\varepsilon$, $\varepsilon'$ | signs in $\{\pm 1\}$ ($y_1 = \varepsilon i$; order-8 step) | §6 |
| $\gamma$, $\psi$, $W$ | $Si$ (resp. $-Si$); $\widehat{u}(x)/\widehat{u}(-x)$; $\gamma\widehat{u}(-x)$ | §6 |
| $\ell$, $w$ | an odd prime dividing $m$ (not the orbit length $\ell$ of §4); $m/4 = n/8$ (odd part of $m$ only if $8 \nmid m$) | §6 |
| $\delta$, $g$, $b$ | an odd prime power $\ell^a$ dividing $m$; $\mathrm{ord}_\delta(2)$; $\mathrm{ord}_\delta(3)$ (not $\delta_O$ or $b = \lvert\mathcal{B}\rvert$ of §5; this $a$ is not the $a$ of $n = 2^a n_{\mathrm{odd}}$) | Thm. 6.2 |
| $r$ | an auxiliary prime, $r \nmid pn$ ($r = 5$ until §7.4) | §7 |
| $\chi_5$, $\varpi_5$, $\sigma_5$ | 5-adic character of order $n$; $\varpi_5 \in \mathbb{C}_5$; $\chi_5(5) = \varpi_5^{\sigma_5}$ | Prop. 7.1 |
| $\chi_r$, $\varpi_r$, $\sigma_r$ | the same for the prime $r$: $\chi_r(r) = \varpi_r^{\sigma_r}$ | §7.4 |
| (L1$_r$)–(L4$_r$) | Xia's system for the prime $r$ (for $r = 5$: (11)) | §7.4 |
| $Q_5$, $\kappa$ | $5^{n/4}$; $n^2 p$ in $\mathbb{F}_5$ (in §7.4: in $\mathbb{F}_r$) | §7 |
| $\iota_5$, $\theta'$ | $\xi_0^{n/4}$ in $\mathbb{F}_{5^n}$; the parameter $\widehat{y}(\xi_0)$, $\theta'^{\,Q_5-1} = -\iota_5$ | Thm. 7.2 |
| $I_r$ | index set of the pairs of top orbits of $\xi \mapsto \xi^r$ | Thm. 7.5 |
| $\mathrm{N}_5$, $\vartheta$ | $x \mapsto x^{1+5^{n/2}}$; $\vartheta^2 = n^3$ in $\mathbb{F}_{25}$ (Remark 7.4) | §7 |

## 3. The case $n = 2^e$

We treat $n = 2^e$ first because every map is explicit here, and because for a possible counterexample of such an order the $\sigma$ of $n$ is 2 (Lemma 2.2), so that Theorem 5.1 bears on it. In this section $n = 2^e$ with $e \geq 3$, $m = n/2$, $Q = 3^{m/2}$, $F = \mathbb{F}_{3^m}$ and $k_0 = \mathbb{F}_Q$, as in Section 2. Such an $n$ is in

Xia's range ($n \equiv 8 \pmod{24}$) exactly when $e$ is odd. We solve the norm-free system completely: its solutions are given by one parameter $\theta$ and two signs.

### 3.1. **One parameter and two signs.**

**Theorem 3.1.** *Let $n = 2^e$ with $e \geq 3$, and fix $\xi_0 \in F$ of order $n$. The norm-free system has exactly $4(Q-1)$ solutions $y \in F^n$. The map $y \mapsto (\widehat{y}(\xi_0), S, \widehat{y}(1))$ is a bijection onto*

$$\{\theta \in F :\ \theta^{Q-1} = -1\} \times \{1,-1\} \times \{1,-1\}.$$

The first set has $Q-1$ elements: $2(Q-1)$ divides $3^m - 1 = (Q-1)(Q+1)$, and the set is $\mu_{2(Q-1)} \setminus \mu_{Q-1}$.

*Proof of Theorem 3.1. Step 1 (the group $\mu_n$).* By the lifting-the-exponent lemma ($v_2$ is the 2-adic valuation), $v_2(3^m-1) = v_2(m)+2 = e+1$ and $v_2(Q-1) = v_2(m/2)+2 = e$ (as $m/2 = 2^{e-2}$ is even), so $\mu_n \subset k_0 \subset F$. Further $(\mathbb{Z}/2^e)^\times = \{\pm 1\} \times \langle 3\rangle$ with $\operatorname{ord}(3) = 2^{e-2} = m/2$. Hence the elements of order $n$ form two Frobenius orbits $O = \{\xi_0^{3^k}\}$ and $O^{-1} = \{\xi_0^{-3^k}\}$ ($k \bmod m/2$), exchanged by $\xi \mapsto \xi^{-1}$. Every element of order $2^j$, $1 \leq j \leq e-1$, has exactly two square roots $\pm\xi$ in $\mu_n$, both of order $2^{j+1}$.

*Step 2 (top layer).* Given a solution, put $\theta := \widehat{y}(\xi_0)$; it is non-zero by Proposition 2.4. The iterate of (F1) with $k = m/2$ (so $3^k = Q \equiv 1 \pmod{n}$) gives

$$\theta = \xi_0^{2kQ}\theta^Q = \xi_0^{mQ}\theta^Q = -\theta^Q,$$

as $\xi_0^m = -1$ and $Q$ is odd; that is, $\theta^{Q-1} = -1$. Conversely, for such $\theta$ define $\widehat{y}(\xi_0^{3^k}) := \xi_0^{2k3^k}\theta^{3^k}$ for $k = 0, \ldots, m/2-1$. Then (F1) holds along $O$; at the wrap $k = m/2-1 \to 0$ (where (F1) closes up after going once around the orbit) it is the identity $\theta = -\theta^Q$. Define $\widehat{y}$ on $O^{-1}$ by (F3): $\widehat{y}(\xi^{-1}) := \xi^m/\widehat{y}(\xi) = -1/\widehat{y}(\xi)$. The orbits $O$ and $O^{-1}$ are disjoint, as $-1 \notin \langle 3\rangle$ modulo $2^e$ ($\langle 3\rangle = \{1,3\}$ modulo 8), so this does not clash with the definition on $O$. (F1) on $O^{-1}$: $\widehat{y}(\xi^{-3}) = -1/\widehat{y}(\xi^3) = -1/(\xi^6\widehat{y}(\xi)^3) = (\xi^{-1})^6\big(-1/\widehat{y}(\xi)\big)^3 = (\xi^{-1})^6\widehat{y}(\xi^{-1})^3$.

*Step 3 (descent, $j = e-1, \ldots, 1$).* Fix a sign $S \in \{1,-1\}$ (for a given solution, $S = \widehat{y}(-1)$; see Step 4). For $\eta$ of order $2^j$ write $\eta = \xi^2$ with $\xi$ of order $2^{j+1}$ and define

$$\widehat{y}(\eta) := S\,\widehat{y}(\xi)\,\widehat{y}(-\xi)$$

(by (F4); the two roots $\pm\xi$ give the same product). If (F1) and (F3) hold on the layer of order $2^{j+1}$, they hold at $\eta$: since $\eta^3 = (\xi^3)^2$ and $-(\xi^3) = (-\xi)^3$,

$$\widehat{y}(\eta^3) = S\,\widehat{y}(\xi^3)\widehat{y}(-\xi^3) = S\,\xi^{12}\big(\widehat{y}(\xi)\widehat{y}(-\xi)\big)^3 = S\,\xi^{12}\big(S\widehat{y}(\eta)\big)^3 = \eta^6\,\widehat{y}(\eta)^3$$

(using $S^4 = 1$), and

$$\widehat{y}(\eta)\widehat{y}(\eta^{-1}) = S^2\big[\widehat{y}(\xi)\widehat{y}(\xi^{-1})\big]\big[\widehat{y}(-\xi)\widehat{y}(-\xi^{-1})\big] = \xi^m(-\xi)^m = \xi^{2m} = \eta^m$$

($m$ even). (F4) holds at every $\xi$ of order at least 4: it is the definition of $\widehat{y}(\xi^2)$. This descent is the classical Hasse–Davenport computation for Gauss sums of 2-power order (compare [19, Lemma 2.1(b)]).

*Step 4 (bottom).* The elements of order 4 of $\mu_n$ are $\pm\iota$, where $\iota := \xi_0^{n/4}$. The step $j = 1$ gives $\widehat{y}(-1) = S\,\widehat{y}(\iota)\widehat{y}(-\iota) = S\,\iota^m = S$ by (F3) at $\iota$, as $4 \mid m$. So (F4) at $\xi = \pm 1$, which reads $\widehat{y}(-1)\widehat{y}(1) = S\,\widehat{y}(1)$, holds for every value of $\widehat{y}(1)$; (F3) at 1 forces $\widehat{y}(1)^2 = 1$, and then (F1) at 1 holds. (F3) at $-1$ gives $S^2 = 1$. Finally $S = \widehat{y}(-1) = \sum_t (-1)^t y_t$, so the $S$ used in (F4) is the $S$ of $y$, as (L4) requires.

*Step 5 (count).* By Proposition 2.4, the $y$ built from $(\theta, S, \widehat{y}(1))$ solves the norm-free system. Conversely, every value of $\widehat{y}$ of a solution is forced by $(\theta, S, \widehat{y}(1))$ through Steps 2–4, and $y \leftrightarrow \widehat{y}$ is a bijection ($n$ is invertible modulo 3). Hence the map of the theorem is a bijection, and the count is $(Q-1)\cdot 2 \cdot 2$. □

**Corollary 3.2.** *Let $n = 2^e$ with $e \geq 3$ odd. Then (1) with $\sigma = 2$ has a solution if and only if some $\theta$ with $\theta^{Q-1} = -1$, together with some signs $S$ and $\widehat{y}(1)$, gives $\mathrm{N}(y_0) = \mathrm{N}(y_1) = -1$, where $y_0$ and $y_1$ are computed from $(\theta, S, \widehat{y}(1))$ by the construction in the proof of Theorem 3.1.*

*Proof.* For $e$ odd, $n \equiv 8 \pmod{24}$, and by Section 2 the solutions of (1) with $\sigma = 2$ are the solutions of the norm-free system with $\mathrm{N}(y_0) = \mathrm{N}(y_1) = -1$. Apply Theorem 3.1. □

*Remark* 3.3 (translation). The translation $y_t \mapsto y_{t+1}$ maps the solution set of the norm-free system to itself: (L1), (L3) and $R(m)$ are translation invariant, and in (L4) $\sum_t (-1)^t y_{t+1} y_{2s+1-t} = -c(2s+2) = -S\,(y_{s+1} + y_{s+1+m})$, while $S$ becomes $-S$. In the parameters of Theorem 3.1 it acts by $(\theta, S, \widehat{y}(1)) \mapsto (\xi_0^{-1}\theta, -S, \widehat{y}(1))$, and it maps $y_0$ to $y_1$. So the two norm conditions of Corollary 3.2 are exchanged by a symmetry of the system.

*Remark* 3.4 (a lift to characteristic 0). Every value of $\widehat{y}$ is a root of unity of order dividing $2(Q-1)$ (a product of values $\theta^{3^k}$, $\xi_0^j$ and $\pm 1$). The Teichmüller lift $\tilde{\widehat{y}}$ of $\widehat{y}$ therefore satisfies (F1), (F3), (F4) exactly in characteristic 0, with values of modulus 1, so the lifted sequence $\tilde{y}_t = n^{-1} \sum_\xi \tilde{\widehat{y}}(\xi) \xi^{-t}$ is a perfect sequence in the ordinary sense: its periodic autocorrelation $\sum_t \tilde{y}_t \overline{\tilde{y}_{t+u}}$ is $[u = 0]$. With (F3), $\overline{\tilde{\widehat{y}}(\xi)} = 1/\tilde{\widehat{y}}(\xi) = \xi^{-m} \tilde{\widehat{y}}(\xi^{-1})$, hence $\tilde{y}_{t+m} = \overline{\tilde{y}_t}$; so the norm equation $y_t y_{t+m} = -1$ lifts to the congruence $|\tilde{y}_t|^2 \equiv -1$ modulo the prime above 3 that gives $y$.

3.2. **The two norm conditions on the eigenspaces of $T$.** In this subsection $n = 2^e$ with $e \geq 4$. This is the one-block case of Section 5. In this case the two components $\theta_+, \theta_-$ of the parameter (Theorem 3.5(c)) are tied to each other by a conic. Put

$$q := 3^{m/4} = 3^{n/8}, \qquad \iota := \xi_0^{n/4}, \qquad V := \{x \in F :\ x^Q = -x\},$$

so $Q = q^2$, $\iota$ has order 4 and lies in $\mathbb{F}_9 \subset k_0$, and $V$ is an $\mathbb{F}_3$-subspace of $F$ of dimension $m/2$ whose non-zero elements are exactly the parameters $\theta$ of Theorem 3.1. Since $m/4 = 2^{e-3}$ is even, $q \equiv 1 \pmod 4$, so $\iota^q = \iota$; and by the lifting-the-exponent lemma, $v_2(q-1) = e-1$, that is,

$$q \equiv 1 + n/2 \pmod n. \tag{2}$$

For a parameter $\theta$ put $\nu := \theta^{1+q}$. Then $\nu^{q-1} = \theta^{Q-1} = -1$, so $\nu^q = -\nu$ and $\nu \in k_0$. For a solution we write $y_j = y_j^+ + y_j^-$ $(j = 0, 1)$ with $y_j^\pm = (y_j \pm \overline{y_j})/2$, as in Remark 2.6; then $\mathrm{N}(y_j) = (y_j^+)^2 - (y_j^-)^2$. The signs in $y_j^\pm$ refer to the conjugation $x \mapsto \overline{x}$, not to the eigenspaces $V_\pm$ of Theorem 3.5. For $\nu \in k_0$ with $\nu^{q-1} = -1$ define the $\mathbb{F}_3$-linear maps $F \to F$ below; by Theorem 3.5(b) they give the top-layer parts $y_0^-$, $y_1^-$ of $y_0$, $y_1$ in terms of the parameter $\theta$:

$$\Lambda_\nu(x) := \sum_{k=0}^{m/4-1} \Big( \xi_0^{2k3^k} - \xi_0^{-2k3^k} (\iota\nu)^{-3^k} \Big) x^{3^k},$$

$$\Lambda'_\nu(x) := \sum_{k=0}^{m/4-1} \Big( \xi_0^{(2k-1)3^k} + \xi_0^{-(2k-1)3^k} (\iota\nu)^{-3^k} \Big) x^{3^k}.$$

**Theorem 3.5.** *Let $n = 2^e$ with $e \geq 4$.*

(a) *$T(x) := \iota x^q$ is an $\mathbb{F}_3$-linear involution of $V$. Hence $V = V_+ \oplus V_-$ with $V_\pm := \{x \in V : Tx = \pm x\}$, and each of $V_+$, $V_-$ is a line over $\mathbb{F}_q$.*

(b) *For every solution $(\theta, S, \widehat{y}(1))$ of the norm-free system, with $\nu = \theta^{1+q}$,*

$$y_0^- = n^{-1} \Lambda_\nu(\theta + T\theta), \qquad y_1^- = n^{-1} \Lambda'_\nu(\theta - T\theta).$$

(c) *$\nu = -\iota\, \theta\, T(\theta)$. With $\theta = \theta_+ + \theta_-$, where $\theta_\pm \in V_\pm$, this reads $\theta_+^2 - \theta_-^2 = \iota\nu$. The values $y_0^+$ and $y_1^+$ depend only on $(\nu, S, \widehat{y}(1))$; hence $y_0$ depends only on $(\nu, S, \widehat{y}(1), \theta_+)$ and $y_1$ only on $(\nu, S, \widehat{y}(1), \theta_-)$. The map $T$ sends parameters to parameters, preserves $\nu$, and satisfies $y_0(T\theta) = y_0(\theta)$ and $y_1(T\theta) = \overline{y_1(\theta)}$ (with the same $S$ and $\widehat{y}(1)$).*

(d) *For every $\nu \in k_0$ with $\nu^{q-1} = -1$, $\Lambda_\nu$ is injective on $V_+$ and $\Lambda'_\nu$ is injective on $V_-$. Hence the $\mathbb{F}_3$-linear map $x \mapsto n^{-1}\Lambda_\nu(x + Tx)$ on $V$ has kernel exactly $V_-$.*

By (a), $\theta + T\theta = 2\theta_+ = -\theta_+$ and $\theta - T\theta = -\theta_-$. So, with Corollary 3.2, each of the two norm conditions involves only one of the two components $\theta_+$, $\theta_-$ of the parameter:

**Corollary 3.6.** *Let $n = 2^e$ with $e \geq 5$ odd, so that $q = 3^{n/8}$.*

(i) *System (1) with $\sigma = 2$ has a solution if and only if there exist $\nu$ with $\nu^{q-1} = -1$, signs $S$, $\widehat{y}(1)$, and $(\theta_+, \theta_-) \in V_+ \times V_-$ on the conic $\theta_+^2 - \theta_-^2 = \iota\nu$ with*

$$\mathrm{N}\big(y_0^+ + n^{-1}\Lambda_\nu(-\theta_+)\big) = -1 \quad \textit{and} \quad \mathrm{N}\big(y_1^+ + n^{-1}\Lambda'_\nu(-\theta_-)\big) = -1,$$

*where $y_0^+$, $y_1^+$ are the values determined by $(\nu, S, \widehat{y}(1))$. The first condition involves only $\theta_+$, the second only $\theta_-$.*

(ii) *Above each triple $(\nu, S, \widehat{y}(1))$, that is, in each fibre of Theorem 5.1, system (1) with $\sigma = 2$ has at most 4 solutions; if there are any, they form the orbit $\{\pm\theta_+ \pm \theta_-\}$ of the group generated by $T$ and $\theta \mapsto -\theta$, so there are 0, 2 or 4 of them. Hence (1) with $\sigma = 2$ has at most $16(q-1) = 16(3^{n/8} - 1)$ solutions.*

For comparison, the norm-free system has $4(Q-1) = 4(q^2-1)$ solutions (Theorem 3.1); for $n = 32$ the bound is 1 280, compared with 26 240, and for $n = 128$ the two numbers are 688 747 520 and 7 412 080 755 407 360.

*Proof of Theorem 3.5.* (a) For $x \in V$, $(\iota x^q)^Q = \iota(x^Q)^q = -\iota x^q$, as $\iota \in k_0$; so $T(V) \subseteq V$. Further $T^2x = \iota^{1+q}x^{q^2} = \iota^2 x^Q = -\iota^2 x = x$. As 2 is invertible modulo 3, $V = V_+ \oplus V_-$. For every constant $c$ the map $x \mapsto x^q - cx$ is $\mathbb{F}_q$-linear, so $V_\pm = \{x \in V : \ x^q = \pm\iota^{-1}x\}$ are $\mathbb{F}_q$-subspaces; each has at most $q$ elements (roots of $x^q = \pm\iota^{-1}x$), and $|V| = q^2$, so each is a line.

(b) By Step 2 of the proof of Theorem 3.1 and (F3),

$$\widehat{y}(\xi_0^{3^k}) = \xi_0^{2k3^k}\theta^{3^k}, \qquad \widehat{y}(\xi_0^{-3^k}) = -\xi_0^{-2k3^k}\theta^{-3^k} \qquad (k \geq 0),$$

where for $k \geq m/2$ the formulas follow from (F1), the step from $k$ to $k+m/2$ being the wrap $\theta^Q = -\theta$ (as $\xi_0^{mQ} = -1$). By Remark 2.6, $\widehat{y} = \widehat{y^-}$ on $O \cup O^{-1} = \mu_n \setminus \mu_m$, so $y_0^- = n^{-1}\sum_{\xi \in O\cup O^{-1}} \widehat{y}(\xi)$ and $y_1^- = n^{-1}\sum_{\xi \in O\cup O^{-1}} \widehat{y}(\xi)\xi^{-1}$. Pair the index $k$ with $k + m/4$ for $0 \leq k < m/4$. By (2), $2(k+m/4)3^{k+m/4} \equiv 2k3^k + (n/4)3^k \pmod n$, so

$$\xi_0^{2(k+m/4)3^{k+m/4}} = \xi_0^{2k3^k}\iota^{3^k}.$$

On $O$, since $3^{k+m/4} = q3^k$, the pair contributes $\xi_0^{2k3^k}\big(\theta^{3^k} + \iota^{3^k}\theta^{q3^k}\big) = \xi_0^{2k3^k}(\theta + \iota\theta^q)^{3^k}$. On $O^{-1}$ use $\theta^{-1} = \theta^q/\nu$: then $\theta^{-3^k} = \nu^{-3^k}\theta^{q3^k}$, and $\theta^{-q3^k} = (\theta^{q^2}\nu^{-q})^{3^k} = \big((-\theta)(-\nu^{-1})\big)^{3^k} = \nu^{-3^k}\theta^{3^k}$, so the pair contributes

$$-\xi_0^{-2k3^k}\nu^{-3^k}\big(\theta^{q3^k} + \iota^{-3^k}\theta^{3^k}\big) = -\xi_0^{-2k3^k}(\iota\nu)^{-3^k}(\theta + \iota\theta^q)^{3^k}.$$

Summing over $k < m/4$ gives $y_0^- = n^{-1}\Lambda_\nu(\theta + T\theta)$. For $y_1^-$ the extra factor $\xi^{-1}$ is $\xi_0^{-3^k}$ on $O$ and $\xi_0^{3^k}$ on $O^{-1}$, and at the paired index the extra factor is multiplied by $\xi_0^{-(n/2)3^k} = -1$; the same steps give $y_1^- = n^{-1}\Lambda'_\nu(\theta - T\theta)$.

These computations use only $\theta^Q = -\theta$ and $\nu^q = -\nu$. Fix $\nu$ with $\nu^{q-1} = -1$, and for $x \in V$ define the function $h_x$ on $O \cup O^{-1}$ by $h_x(\xi_0^{3^k}) := \xi_0^{2k3^k}x^{3^k}$ and $h_x(\xi_0^{-3^k}) := -\xi_0^{-2k3^k}\nu^{-3^k}x^{q3^k}$. Then

$$n^{-1}\sum_{\xi \in O\cup O^{-1}} h_x(\xi) = n^{-1}\Lambda_\nu(x + Tx), \qquad n^{-1}\sum_{\xi \in O\cup O^{-1}} h_x(\xi)\xi^{-1} = n^{-1}\Lambda'_\nu(x - Tx) \tag{3}$$

for every $x \in V$; for a parameter $x = \theta$ with $\theta^{1+q} = \nu$, $h_\theta = \widehat{y}$ on $O \cup O^{-1}$.

(c) $\theta^q = \iota^{-1}T\theta = -\iota\,T\theta$, so $\nu = \theta\theta^q = -\iota\,\theta\,T(\theta) = -\iota(\theta_+ + \theta_-)(\theta_+ - \theta_-)$, and $\theta_+^2 - \theta_-^2 = -\iota^{-1}\nu = \iota\nu$. Moreover, $T\theta$ is a non-zero element of $V$, hence a parameter, and $(T\theta)^{1+q} = \iota^{1+q}\theta^q\theta^{q^2} = -\theta^q(-\theta) = \nu$.

The values $y_0^+$, $y_1^+$ are determined by $\widehat{y}$ on $\mu_m$ (Remark 2.6). Every element $\eta$ of order $m$ is $\rho^2$ with $\rho = \xi_0^{\pm 3^k}$, and by (2) $-\rho = \rho^{1+n/2} = \rho^q$ lies in the same orbit as $\rho$. So Step 3 of the proof of Theorem 3.1 gives $\widehat{y}(\eta) = S\,\widehat{y}(\rho)\widehat{y}(\rho^q) = S\,\xi_0^{2k3^k}\xi_0^{2(k+m/4)3^{k+m/4}}\,\nu^{3^k}$ for $\rho \in O$, and $S\,\xi_0^{-2k3^k}\xi_0^{-2(k+m/4)3^{k+m/4}}\,\nu^{-3^k}$ for $\rho \in O^{-1}$. The values at the elements of order $2^{e-2}, \dots, 2$ are products of these values and $S$, and $\widehat{y}(1)$ is the remaining value (Steps 3–4). Thus $\widehat{y}$ on $\mu_m$, and with it $y_0^+$ and $y_1^+$, depends only on $(\nu, S, \widehat{y}(1))$. Finally $T\theta + T(T\theta) = \theta + T\theta$ and $T\theta - T(T\theta) = -(\theta - T\theta)$, so by (b) $y_0(T\theta) = y_0(\theta)$ and $y_1(T\theta) = y_1^+ - y_1^- = \overline{y_1(\theta)}$.

(d) Fix $\nu$. For $x \in V$ let $h_x$ be as in (b), and put $y_t^-(x) := n^{-1}\sum_{\xi \in O \cup O^{-1}} h_x(\xi)\xi^{-t}$ for $t \in \mathbb{Z}/n$. (i) $x \mapsto h_x$ is injective, as $h_x(\xi_0) = x$. (ii) $h_x \mapsto (y_t^-(x))_t$ is injective: it is the inverse Fourier transform of a function supported on $O \cup O^{-1}$. (iii) $h_x$ satisfies (F1) on $O \cup O^{-1}$ for every $x \in V$: along $O$, $\xi_0^{6\cdot 3^k}\big(\xi_0^{2k3^k}x^{3^k}\big)^3 = \xi_0^{2(k+1)3^{k+1}}x^{3^{k+1}}$, along $O^{-1}$ likewise, and the two wraps at $k = m/2$ use only $x^Q = -x$ and $\nu^Q = \nu$. As $n^{-1} \in \mathbb{F}_3$ and $\xi \mapsto \xi^3$ permutes $O \cup O^{-1}$,

$$\phi\big(y_t^-(x)\big) = n^{-1}\sum_{\xi} h_x(\xi)^3\xi^{-3t} = n^{-1}\sum_{\xi}\xi^{-6}h_x(\xi^3)\xi^{-3t} = y_{t+2}^-(x),$$

so $(y_0^-(x), y_1^-(x))$ determines every $y_t^-(x)$. (iv) By (3), $y_0^-(x) = n^{-1}\Lambda_\nu(x + Tx)$ and $y_1^-(x) = n^{-1}\Lambda'_\nu(x - Tx)$. By (i)–(iv), $x \mapsto \big(\Lambda_\nu(x + Tx), \Lambda'_\nu(x - Tx)\big)$ is injective on $V$. For $x \in V_+$ this is $(\Lambda_\nu(-x), 0)$, so $\Lambda_\nu$ is injective on $V_+$; for $x \in V_-$ it is $(0, \Lambda'_\nu(-x))$, so $\Lambda'_\nu$ is injective on $V_-$. Since $x + Tx = -x_+$ for the $V_+$-component $x_+$ of $x$, the map $x \mapsto n^{-1}\Lambda_\nu(x + Tx)$ vanishes exactly when $x_+ = 0$, that is, on $V_-$. □

*Proof of Corollary 3.6.* (i) For $e$ odd the solutions of (1) with $\sigma = 2$ are the solutions of the norm-free system with $\mathrm{N}(y_0) = \mathrm{N}(y_1) = -1$ (Corollary 3.2). By Theorem 3.1 and Theorem 3.5(b), (c), these are the parameters $\theta = \theta_+ + \theta_-$ on the conic of (c) that, together with signs $S$ and $\widehat{y}(1)$, satisfy the two displayed conditions; conversely, since $\theta^{1+q} = -\iota\,\theta\,T(\theta)$ for every $\theta \in V$, every $\theta = \theta_+ + \theta_-$ on the conic is non-zero and has $\theta^{1+q} = \nu$.

(ii) Let $(\theta, S, \widehat{y}(1))$ be a solution and $\nu = \theta^{1+q}$. From $\mathrm{N}(y_0) = (y_0^+)^2 - (y_0^-)^2 = -1$ and Theorem 3.5(c), $y_0^-$ is one of the two square roots of $(y_0^+)^2 + 1$, where $y_0^+$ is fixed by $(\nu, S, \widehat{y}(1))$. As $y_0^- = n^{-1}\Lambda_\nu(-\theta_+)$ and $\Lambda_\nu$ is injective and $\mathbb{F}_3$-linear on $V_+$ (Theorem 3.5(d)), $\theta_+$ is one of two values $\pm x_0$. Likewise $\mathrm{N}(y_1) = -1$ fixes $\theta_-$ up to sign. Hence at most 4 solutions lie above $(\nu, S, \widehat{y}(1))$. The two norm conditions and the conic are invariant under $T$ ($\theta_+ + \theta_- \mapsto \theta_+ - \theta_-$) and under $\theta \mapsto -\theta$ (which preserves $\nu$, as $1 + q$ is even), so the solutions above $(\nu, S, \widehat{y}(1))$, if there are any, form one orbit of the group of order 4 generated by these two maps, of size 2 (when $\theta_+ = 0$ or $\theta_- = 0$) or 4. There are $q - 1$ values of $\nu$ (the set $\mu_{2(q-1)} \setminus \mu_{q-1}$, as after Theorem 3.1 with $q$ for $Q$) and 4 choices of the signs, so there are at most $16(q - 1)$ solutions. □

*Remark* 3.7. (a) The translation of Remark 3.3, $(\theta, S, \widehat{y}(1)) \mapsto (\xi_0^{-1}\theta, -S, \widehat{y}(1))$, exchanges the two components: by (2), $T(\xi_0^{-1}\theta) = \xi_0^{-q}T\theta = -\xi_0^{-1}T\theta$, so $\theta \mapsto \xi_0^{-1}\theta$ maps $V_-$ onto $V_+$. This matches the fact that the translation maps $y_0$ to $y_1$. In particular Question 11.1 concerns only the pairs $(\nu, \theta_+)$. (b) The hypothesis $e \geq 4$, that is, $m/4$ even, is used for $\iota^q = \iota$ and for (2), which fails at $e = 3$ since $q = 3 \not\equiv 5 \pmod 8$. For $n = 8$ (the order of $\mathrm{PG}(2, 8)$), $m/4 = 1$ is odd and $T^2 = -1$, so the theorem does not apply there. (c) In Theorem 3.5 the two components remain coupled through $\nu$, which enters $y_0^+$, $y_1^+$, $\Lambda_\nu$, $\Lambda'_\nu$ and the conic.

*Remark* 3.8. An exact computation (Section 8) confirms Theorem 3.5 at $n = 16, 32, 64, 128$: $T^2 = \mathrm{id}$, $T$ preserves $\nu$, $y_0(T\theta) = y_0(\theta)$ and $y_1(T\theta) = \overline{y_1(\theta)}$ (with $y_0$, $y_1$ computed from the full construction of Theorem 3.1 and the inverse Fourier transform), and the kernel of $x \mapsto n^{-1}\Lambda_\nu(x + Tx)$

is $V_-$ in every fibre tested. It also confirms the consequence of (d) that $y_0 \in k_0$ exactly when $\theta \in V_-$ and $y_1 \in k_0$ exactly when $\theta \in V_+$ (Section 8.2 gives the counts at $n = 16$ and 32).

## 4. The norm-free system for general $n$

This section proves Theorem 4.1 and Proposition 4.3. Here $n = 2^a n_{\mathrm{odd}}$ with $a \geq 3$, $n_{\mathrm{odd}}$ odd and $3 \nmid n$, and $m = n/2$; we use Proposition 2.4, which holds for every even $n$ with $3 \nmid n$. With $F = \mathbb{F}_{3^m}$, we write $\mathrm{NF}(n) \subset F^n$ for the set of solutions of the norm-free system (Definition 2.3); as in Section 2, $\mu_n$ lies in an algebraic closure $\overline{\mathbb{F}}_3$ of $F$. Every $\xi \in \mu_n$ can be written uniquely as $\xi = \zeta\alpha$ with $\zeta \in \mu_{2^a}$ and $\alpha \in \mu_{n_{\mathrm{odd}}}$; $\xi$ lies in layer $j(\xi) := \log_2 \mathrm{ord}(\zeta)$. As in the introduction, the top layer is $\mathcal{L}_a := \{\xi : j(\xi) = a\}$, of size $m$, and layer 0 (the bottom layer) is $\mu_{n_{\mathrm{odd}}}$. Let $\Xi_a$ be the set of the $2^{a-1}$ elements of order $2^a$ of $\mu_{2^a}$.

**Theorem 4.1.** *Let $n = 2^a n_{\mathrm{odd}}$ as above. The orbits of $\xi \mapsto \xi^3$ on $\mathcal{L}_a$ come in pairs $\{O, O^{-1}\}$ with $O \neq O^{-1}$; for each pair $i \in I$ ($I$ indexes the pairs) let $L_i$ be the common length of $O$ and $O^{-1}$, so that $\sum_{i\in I} L_i = n/4$. Then the number of solutions $y \in F^n$ of the norm-free system is*

$$|\mathrm{NF}(n)| = 4 \prod_{i\in I} \bigl(3^{L_i} - 1\bigr).$$

*In particular* $\mathrm{NF}(n)$ *is not empty, and* $|\mathrm{NF}(n)| = 4\,Q \prod_{i\in I}(1 - 3^{-L_i})$ *with* $Q = 3^{n/4}$.

For $n = 2^e$ there is one pair, of length $n/4$, and the count is the $4(Q-1)$ of Theorem 3.1.

**Corollary 4.2.** *Let $n \equiv 8 \pmod{24}$. Then* (1) *with $\sigma = 2$ has a solution if and only if some point of* $\mathrm{NF}(n)$ *has* $\mathrm{N}(y_0) = \mathrm{N}(y_1) = -1$. *In particular, any proof that* (1) *with $\sigma = 2$ has no solution must use the norm equation (L2) beyond its consequence $R(m) = 1$.*

*Proof.* By Section 2, the solutions of (1) with $\sigma = 2$ are the points of $\mathrm{NF}(n)$ with $\mathrm{N}(y_0) = \mathrm{N}(y_1) = -1$, and by Theorem 4.1 $\mathrm{NF}(n)$ is not empty. □

Xia also conjectured that such systems have no solution "even after deleting some equations" [19, Section 1]. Without the norm equation, the system has the trivial solution $y = 0$. Theorem 4.1 and Proposition 4.3 say more: replacing the norm equation by its consequence $R(m) = 1$, which excludes $y = 0$, still leaves solutions, for every $n \equiv 8 \pmod{24}$ and every even divisor $\sigma$ of $n$. Hence Xia's statement about deleting equations cannot extend to deleting the norm equation, even when the trivial solution is excluded. Xia's numbered conjectures are not affected: Conjecture 5.2 keeps all four lines of (1), and Conjecture 5.4 deletes the Frobenius relation (L1), not the norm equation (L2). Xia's heuristic [19, Section 5], which compares the number of equations with the number of unknowns, cannot tell (1) from the norm-free system: both have more equations than their $n$ unknowns ($5n/2$ and $2n+1$, respectively), yet by Theorem 4.1 the norm-free system has solutions.

4.1. **Homogeneous laws.** If $\widehat{y}, \widehat{y}'$ satisfy (F1), (F3), (F4), then $\lambda := \widehat{y}'/\widehat{y}$ satisfies the homogeneous laws

$$\text{(h1) } \lambda(\xi^3) = \lambda(\xi)^3, \qquad \text{(h3) } \lambda(\xi)\,\lambda(\xi^{-1}) = 1, \qquad \text{(h4) } \lambda(\xi)\,\lambda(-\xi) = \lambda(-1)\,\lambda(\xi^2),$$

and conversely, if $\widehat{y}$ satisfies (F1), (F3), (F4) and $\lambda$ satisfies (h1), (h3), (h4), then $\lambda\widehat{y}$ satisfies (F1), (F3), (F4). Hence $\mathrm{NF}(n)$, identified with the set of the $\widehat{y}$, is empty or a torsor under the group $K_n$ of solutions of (h1), (h3), (h4): $K_n$ acts on it by multiplication, freely and transitively. The group $K_n$ is finite, since (h1) iterated $\mathrm{ord}_n(3)$ times gives $\lambda(\xi)^{3^{\mathrm{ord}_n(3)}-1} = 1$.

TABLE 2. The layers of $\mu_n$ in the proof of Theorem 4.1. The choices multiply to $|\mathrm{NF}(n)| = 4\prod_{i\in I}(3^{L_i}-1)$. Layer 0 uses $f$ and $P$ of Step 4 and $G$, $G^\tau$, $G_0''$ of Step 5.

| Layer | Elements | What fixes $\widehat{y}$ there | Choices |
|---|---|---|---|
| $a$ (top) | $\mathcal{L}_a = \mu_n \setminus \mu_m$ | (F1) along each orbit of $\xi \mapsto \xi^3$, with its wrap, and (F3) from $O$ to $O^{-1}$ (Step 2) | $\prod_{i\in I}(3^{L_i}-1)$ |
| $a-1,\dots,1$ | $\mu_m \setminus \mu_{n_{\mathrm{odd}}}$ | a sign $S$, then (F4): $\widehat{y}(\eta^2) = S\,\widehat{y}(\eta)\widehat{y}(-\eta)$ (Step 3) | 2 (the sign $S$) |
| 0 | $\mu_{n_{\mathrm{odd}}}$ | $f(1) = \pm 1$, and (E1)–(E3) on $\mu_{n_{\mathrm{odd}}} \setminus \{1\}$, whose solutions form a $G^\tau$-torsor if $P \in G_0''$ and do not exist otherwise (Steps 4–7) | $2\,\lvert G^\tau\rvert$ for a fraction $1/\lvert G^\tau\rvert$ of the top data, none for the rest |

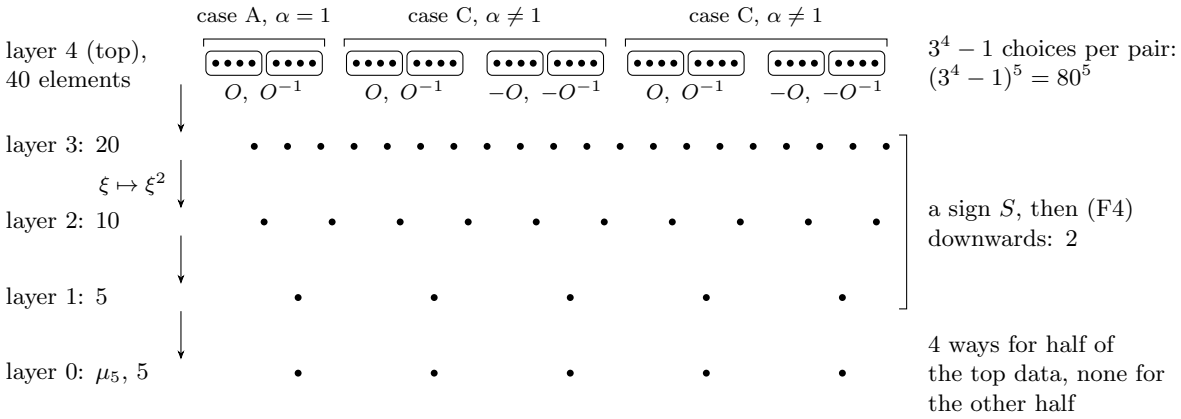


FIGURE 3. The layers of $\mu_n$ for $n = 80$ (Remark 4.4: $a = 4$, $n_{\mathrm{odd}} = 5$). An element $\xi = \zeta\alpha$ lies in layer $j$ when $\zeta$ has order $2^j$. The top layer has 40 elements and splits into ten orbits of $\xi \mapsto \xi^3$, each of length 4, in five inverse pairs $\{O, O^{-1}\}$. The pair with $\alpha = 1$ is a block of case A ($-O = O$), and the four pairs with $\alpha \neq 1$ form two blocks $\{O, O^{-1}, -O, -O^{-1}\}$ of case C (Table 4). Squaring maps each layer above layer 0 onto the layer below. The proof of Theorem 4.1 fixes $\widehat{y}$ from the top layer down; the right column gives the choices of Table 2, which multiply to $4 \cdot 80^5$.

4.2. **Proof of Theorem 4.1.** The proof fixes $\widehat{y}$ layer by layer, from the top layer down to layer 0. Table 2 lists the steps and the choices at each layer. For $n = 80$, Figure 3 draws the layers and Remark 4.4 follows the proof.

*Step 1 (top orbits).* If $\xi \in \mathcal{L}_a$ and $\xi^{-1} = \xi^{3^k}$, the 2-parts give $\zeta^{3^k+1} = 1$ with $\mathrm{ord}(\zeta) = 2^a$, so $3^k \equiv -1 \pmod{2^a}$, which is impossible for $a \geq 3$ since $\langle 3\rangle = \{1, 3\}$ modulo 8. Thus no orbit on $\mathcal{L}_a$ is self-inverse.

*Step 2 (top data).* On an orbit $O = \{\rho^{3^k}\}$ of length $L$, (F1) gives $\widehat{y}(\rho^{3^k}) = \rho^{2k3^k}\widehat{y}(\rho)^{3^k}$, and the wrap gives $\widehat{y}(\rho)^{3^L-1} = \rho^{-2L3^L}$: there are $3^L - 1$ choices of $t = \widehat{y}(\rho)$ (the polynomial $X^{3^L-1} - c$ with $c \neq 0$ has distinct roots, as $3 \nmid 3^L - 1$). Then (F3) defines $\widehat{y}$ on $O^{-1}$ by $\widehat{y}(\xi^{-1}) = \xi^m/\widehat{y}(\xi)$, and (F1) holds there, by the computation in Step 2 of the proof of Theorem 3.1. Let $\mathcal{D}$ be the set of such top data; $|\mathcal{D}| = \prod_{i\in I}(3^{L_i}-1)$. Its homogeneous version $\mathcal{D}^0$, the set of $\lambda\colon \mathcal{L}_a \to \overline{\mathbb{F}}_3^{\times}$ with (h1) and (h3) on $\mathcal{L}_a$, is a group of the same order.

*Step 3 (descent, layers $a-1,\dots,1$).* Fix a sign $S \in \{1, -1\}$ (for a given solution, $S = \widehat{y}(-1)$). For $1 \leq j(\xi) \leq a-1$ both square roots $\pm\eta$ of $\xi$ lie in layer $j+1$, and (F4) at $\eta$ defines $\widehat{y}(\xi) := S\,\widehat{y}(\eta)\widehat{y}(-\eta)$.

By induction,

$$\widehat{y}(\xi) = S^{2^{a-j}-1} \prod_{\rho\in\mathcal{L}_a,\ \rho^{2^{a-j}}=\xi} \widehat{y}(\rho) \qquad (j = j(\xi) \geq 1), \tag{4}$$

the $2^{a-j}$ roots all lying in $\mathcal{L}_a$. (F1) and (F3) pass from layer $j+1$ to layer $j$ exactly as in Theorem 3.1, Step 3 (the odd part plays no role: $(\eta^3)^2 = (\eta^2)^3$, $(-\eta)^3 = -\eta^3$, $S^4 = 1$, $\eta^{2m} = (\eta^2)^m$). At $-1$ (layer 1, odd part 1), (4) gives $\widehat{y}(-1) = S\prod_{\zeta\in\Xi_a}\widehat{y}(\zeta)$, and, pairing $\zeta$ with $\zeta^{-1}$, we get from (F3) $\prod_{\zeta\in\Xi_a}\widehat{y}(\zeta) = \prod_{\{\zeta,\zeta^{-1}\}}\zeta^m = (-1)^{2^{a-2}} = 1$ ($\zeta^m = (-1)^{n_{\mathrm{odd}}} = -1$; $a \geq 3$). So $\widehat{y}(-1) = S$ for both signs of $S$.

*Step 4 (layer 0).* For $\alpha \in \mu_{n_{\mathrm{odd}}}$ the remaining equations are (F1) and (F3) on $\mu_{n_{\mathrm{odd}}}$, and (F4) at $\alpha$ and at $-\alpha$; these two instances of (F4) both read

$$\text{(E1)}\quad f(\alpha^2) = P(\alpha)\, f(\alpha), \qquad f := \widehat{y}|_{\mu_{n_{\mathrm{odd}}}}, \quad P(\alpha) := S\,\widehat{y}(-\alpha) = \prod_{\rho\in\mathcal{L}_a,\ \rho^{2^{a-1}}=-\alpha} \widehat{y}(\rho)$$

(by (4) with $j = 1$ and $S^{2^{a-1}} = 1$); $P$ does not depend on $S$. At $\alpha = 1$: $P(1) = 1$ (Step 3), (F3) gives $f(1) = \pm 1$, and (F1), (F4) hold, so there are 2 choices. On $\mu_{n_{\mathrm{odd}}} \setminus \{1\}$ the equations are (E1) and

$$\text{(E2)}\quad f(\alpha^3) = \alpha^6 f(\alpha)^3, \qquad \text{(E3)}\quad f(\alpha)\, f(\alpha^{-1}) = \alpha^m,$$

and $P$ inherits from layer 1 the laws $P(\alpha^3) = \alpha^6 P(\alpha)^3$ and $P(\alpha)P(\alpha^{-1}) = \alpha^m$.

*Step 5 (the group $G$).* Let $G$ be the group of maps $g\colon \mu_{n_{\mathrm{odd}}} \setminus \{1\} \to \overline{\mathbb{F}}_3^{\times}$ with $g(\alpha^3) = g(\alpha)^3$ and $g(\alpha^{-1}) = g(\alpha)^{-1}$; it is finite, and the map $\tau$ given by $(\tau g)(\alpha) := g(\alpha^2)$ is an automorphism of $G$ (squaring permutes $\mu_{n_{\mathrm{odd}}}$ and commutes with cubing and inversion). Let $G'$ be the set of $f$ with (E2), (E3), and $G''$ the set of $P$ with $P(\alpha^3) = \alpha^6 P(\alpha)^3$, $P(\alpha)P(\alpha^{-1}) = \alpha^m$; when non-empty, both are torsors under $G$, and $f \mapsto \tau f/f$ maps $G'$ into $G''$. We write $G$ multiplicatively and put $(\tau-1)G := \{\tau g/g :\ g \in G\}$ and $G^\tau := \{g \in G :\ \tau g = g\}$. Given $P \in G''$ and $f_0 \in G'$, write $f = f_0 g$ with $g \in G$. Then (E1) reads $\tau g/g = P\, f_0/\tau f_0$. Hence the $f \in G'$ with (E1) form a $G^\tau$-torsor if $P \in G_0'' := (\tau f_0/f_0)\,(\tau-1)G$, a coset independent of $f_0$, and there is none otherwise. The set $G'$ is non-empty: on an orbit of $\langle 3\rangle$ of length $\ell$ choose $f(\alpha)$ with $f(\alpha)^{3^\ell-1} = \alpha^{-2\ell 3^\ell}$ and extend along the orbit by (E2); pair the orbits that are not self-inverse by (E3); on a self-inverse orbit ($\alpha^{-1} = \alpha^{3^h}$, $\ell = 2h$) take a root of $f(\alpha)^{3^h+1} = \alpha^{m-2h3^h}$ ((E3) at $\alpha$; $3 \nmid 3^h + 1$). This choice also satisfies the wrap condition: after raising to the power $3^h - 1$ and using $3^h \equiv -1$ modulo $\mathrm{ord}(\alpha)$, the exponents are $(m - 2h3^h)(3^h - 1) \equiv -2m - 4h$ and $-2\ell\, 3^\ell \equiv -4h$, which agree as $\mathrm{ord}(\alpha) \mid n_{\mathrm{odd}} \mid m$; and (E3) on the whole orbit then follows from (E2). Hence $G''$ is non-empty too: it contains $\tau f_0/f_0$.

*Step 6 (surjectivity).* For $\lambda \in \mathcal{D}^0$ put $P_\lambda(\alpha) := \prod_{\rho\in\mathcal{L}_a,\ \rho^{2^{a-1}}=-\alpha} \lambda(\rho)$, the homogeneous version of $P$; it lies in $G$ by (h1) and (h3). The homomorphism $\Pi\colon \mathcal{D}^0 \to G$, $\lambda \mapsto P_\lambda$, is onto. Indeed $P_\lambda(\alpha) = \widetilde{P}_\lambda(\beta)$ with $\beta := \alpha^{2^{-(a-1)}} \in \mu_{n_{\mathrm{odd}}}$ and $\widetilde{P}_\lambda(\beta) := \prod_{\zeta\in\Xi_a}\lambda(\zeta\beta)$, and $\beta \leftrightarrow \alpha$ commutes with cubing and inversion. Fix $\beta_0 \in \mu_{n_{\mathrm{odd}}} \setminus \{1\}$, let $\ell$ be the length of its $\langle 3\rangle$-orbit, and let $O$ be the top orbit of $\rho_0 := \zeta_0\beta_0$ with $\zeta_0 \in \Xi_a$ (length $L$, $\ell \mid L$). Put $\lambda = 1$ on every top orbit except $O$ and $O^{-1}$, and $\lambda(\rho_0) = t$ with $t \in \mu_{3^L-1}$. The elements of $O$ over $\beta_0$ (that is, with odd part $\beta_0$) are $\rho_0^{3^{j\ell}}$, $j < L/\ell$, so their product is $s := t^{(3^L-1)/(3^\ell-1)}$, which runs over all of $\mu_{3^\ell-1}$. (i) If the orbit of $\beta_0$ is not self-inverse, $O^{-1}$ lies over the inverse orbit, and $\widetilde{P}_\lambda(\beta_0) = s$ runs over $\mu_{3^\ell-1}$, the set of values of the $g \in G$ at $\beta_0$. (ii) If it is self-inverse, say $\beta_0^{-1} = \beta_0^{3^h}$ with $\ell = 2h$, then $O^{-1}$ also contains elements over $\beta_0$, namely the inverses of the $\rho_0^{3^{h+j\ell}}$. They contribute $s^{-3^h}$, and they lie in an orbit other than $O$, since $O^{-1} \neq O$ by Step 1. So $\widetilde{P}_\lambda(\beta_0) = s^{1-3^h}$, which runs over $\mu_{3^h+1}$. This is again the set of values at $\beta_0$ of the $g \in G$, since every $g \in G$ satisfies $g(\beta_0)^{-1} = g(\beta_0)^{3^h}$. For such $\lambda$, $\widetilde{P}_\lambda$ is 1 off the orbit of $\beta_0$ and its inverse, and $g \in G$ is determined by its values at one $\beta_0$ in each $\langle 3, -1\rangle$-orbit; as $\Pi$ is a homomorphism, its image contains a generating set of $G$, so $\Pi$ is onto.

*Step 7 (count).* Consider first the homogeneous laws; here $S$ stands for $\lambda(-1) = \pm 1$. Then $\lambda \in \mathcal{D}^0$ and $S$ determine layers $a-1, \dots, 1$ (Step 3). In the homogeneous case we may take $f_0 = 1$, so $G_0'' = (\tau - 1)G$; thus $\lambda$ extends if and only if $P_\lambda \in (\tau-1)G$, and then in exactly $|G^\tau|$ ways on $\mu_{n_{\mathrm{odd}}} \setminus \{1\}$, times 2 at $\alpha = 1$, times 2 for $S$. As $\Pi$ is onto, the number of $\lambda$ with $P_\lambda \in (\tau-1)G$ is $|\mathcal{D}^0|\,|(\tau-1)G|/|G| = |\mathcal{D}^0|/|G^\tau|$ (as $|(\tau-1)G|\,|G^\tau| = |G|$). Hence $|K_n| = 4\,|G^\tau|\,|\mathcal{D}^0|/|G^\tau| = 4\prod_{i\in I}(3^{L_i}-1)$. To see that $\mathrm{NF}(n)$ is not empty, fix $S$; as the top data vary, the inhomogeneous $P$ runs through a coset of $\Pi(\mathcal{D}^0) = G$ in $G''$, which is all of $G''$ (non-empty by Step 5); so some top data give $P \in G_0''$, and then $f$ exists (Step 5). Hence $|\mathrm{NF}(n)| = |K_n|$. □

**Proposition 4.3** (arbitrary shift $\sigma$)**.** *Let $\sigma$ be a divisor of $n$. If $\sigma$ is even, the norm-free system with shift $\sigma$ (Definition 2.3) has exactly $4\prod_{i\in I}(3^{L_i}-1)$ solutions. If $\sigma$ is odd, it has none.*

*Proof.* As in Proposition 2.4, $y \mapsto \widehat{y}$ identifies the solutions with the functions satisfying (F3), (F4) and (F1$_\sigma$) $\widehat{y}(\xi^3) = \xi^{3\sigma}\widehat{y}(\xi)^3$; in the converse, $y_t^{3^{n/\sigma}} = y_{t+n} = y_t$. The homogeneous laws (h1), (h3), (h4) do not involve $\sigma$, so $K_n$ and Steps 1, 6 and 7 are unchanged; we check that the other steps still close for even $\sigma$. Step 2: the iterate is $\widehat{y}(\rho^{3^k}) = \rho^{\sigma k 3^k}\widehat{y}(\rho)^{3^k}$, and the wrap $\widehat{y}(\rho)^{3^L-1} = \rho^{-\sigma L 3^L}$ again has $3^L - 1$ roots. Step 3: one layer down, (F1$_\sigma$) becomes $\widehat{y}(\xi^3) = (-1)^\sigma S^4 \xi^{3\sigma}\widehat{y}(\xi)^3$, which is (F1$_\sigma$) since $\sigma$ is even and $S^2 = 1$. Step 4: (E2) and the law of $P$ become $f(\alpha^3) = \alpha^{3\sigma} f(\alpha)^3$ and $P(\alpha^3) = \alpha^{3\sigma}P(\alpha)^3$, as $(-\alpha)^{3\sigma} = \alpha^{3\sigma}$, and $f \mapsto \tau f/f$ still maps $G'$ into $G''$. Step 5: on a self-inverse orbit take a root of $f(\alpha)^{3^h+1} = \alpha^{m-\sigma h 3^h}$; after raising it to the power $3^h - 1$, the exponents are $-2m - 2\sigma h$ and $-2\sigma h$, which agree as $\mathrm{ord}(\alpha) \mid m$. For odd $\sigma$, (L1) gives $S^3 = \sum_t (-1)^t y_{t+\sigma} = -S$, while (F3) at $-1$ gives $S^2 = (-1)^m = 1$; so $S = S^3 = -S$, hence $S = 0$, a contradiction. □

*Remark* 4.4 ($n = 80$). Here $a = 4$ and $n_{\mathrm{odd}} = 5$; $n = 80$ is the smallest $n > 8$ in Xia's range with $p$ prime ($p = 6481$). Over $\alpha = 1$ there are two top orbits of length 4 (one pair), and over $\alpha \neq 1$ eight (four pairs), so $|\mathcal{D}| = (3^4-1)^5 = 80^5$. On layer 0, $\mu_5 \setminus \{1\}$ is one orbit of $\langle 2\rangle = \langle 3\rangle = (\mathbb{Z}/5)^\times$; $G$ consists of the $g$ with $g(\beta) \in \mu_{80}$, $g(\beta)^{-1} = g(\beta)^9$, so $|G| = 10$, and $G^\tau = \{\pm 1\}$. The extendable top data satisfy $P(\alpha)^5 = \alpha^2$, which holds for half of the 10 possible values of $P(\alpha)$. (For $f_0 \in G'$, (E2) and (E3) give $f_0(\alpha)^{10} = \alpha^{-1}$ and $\tau f_0/f_0 = f_0^6$, and $(\tau-1)G = \{g :\ g^5 = 1\}$.) Each such top datum extends in 2 ways at $\alpha \neq 1$, so the count is $80^5 \cdot \frac{1}{2} \cdot 2 \cdot 4 = 4 \cdot 80^5$, as the theorem says.

The computational checks of Theorem 4.1 are listed in Section 8.3.

## 5. The two norm conditions for general $n$

This section proves Theorem 5.1 and Corollary 5.2. A fibre is not a linear space, so we place it in an $\mathbb{F}_3$-vector space $V$ with one summand for each block. On $V$ the substitution $y \mapsto y^{(u)}$ becomes an $\mathbb{F}_3$-linear involution $T$, and we extend the top data linearly to all of $V$ (the formal top function in the proof of Theorem 5.1(d)). Throughout, $n = 2^a n_{\mathrm{odd}}$ with $a \geq 3$, $n_{\mathrm{odd}}$ odd and $3 \nmid n$, as in Theorem 4.1, and $u := 1 + m$. The lower layers make up $\mu_m = \{\xi : \xi^m = 1\}$ and the top layer is $\mathcal{L}_a = \{\xi : \xi^m = -1\}$; so, as in Remark 2.6, $y_j^+ = n^{-1}\sum_{\xi\in\mu_m}\widehat{y}(\xi)\xi^{-j}$ and $y_j^- = n^{-1}\sum_{\xi\in\mathcal{L}_a}\widehat{y}(\xi)\xi^{-j}$. For a sequence $y$ put $y_t^{(u)} := y_{ut}$.

5.1. **Blocks and fibres.** For each orbit $O$ of $\xi \mapsto \xi^3$ on $\mathcal{L}_a$ fix $\rho_O \in O$, let $L = |O|$, and put

$$c_O := \rho_O^{-2L}, \qquad V_O := \{t \in \overline{\mathbb{F}}_3 :\ t^{3^L} = c_O\, t\},$$

an $\mathbb{F}_3$-space of dimension $L$. By Step 2 of the proof of Theorem 4.1, the top data of a solution on $O$ are $\widehat{y}(\rho_O^{3^k}) = \rho_O^{2k3^k} t^{3^k}$ with $t = \widehat{y}(\rho_O) \in V_O \setminus \{0\}$ (as $\rho_O^{3^L} = \rho_O$), and (F3) gives $\widehat{y}(\xi^{-1}) = -1/\widehat{y}(\xi)$ on $\mathcal{L}_a$. Since $-\xi = \xi^u$, the map $\xi \mapsto -\xi$ permutes the orbits. As in the introduction, an orbit $O$ is of *case A* if $-O = O$, of *case B* if $-O = O^{-1}$, and of *case C* otherwise. Its *block* is $\{O, O^{-1}\}$ in cases A and B, and $\{O, O^{-1}, -O, -O^{-1}\}$ in case C; let $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$ be the sets of blocks of each case, and $b := |\mathcal{B}|$. In cases A and B, $L$ is even (see the proof of Theorem 5.1(c)) and we put $q_O := 3^{L/2}$.

- Case A: $-\rho_O = \rho_O^{q_O}$; put $\iota_O := \rho_O^{Lq_O}$. The block parameter is $t \in V_O$, its *$\nu$-datum* is $\nu_O := \widehat{y}(\rho_O)\widehat{y}(-\rho_O) = \iota_O t^{1+q_O}$, and $T(t) := \iota_O t^{q_O}$.
- Case B: $-\rho_O = \rho_O^{-q_O}$. Here $\widehat{y}(\rho_O)\widehat{y}(-\rho_O) = -\rho_O^{-Lq_O} t^{1-q_O}$, and the $\nu$-datum is the coset $t\,\mathbb{F}_{q_O}^{\times}$. On a coset $t_0\mathbb{F}_{q_O}^{\times}$ write $t = t_0 x$ and $\widehat{y}(\rho_O^{-1}) = -t_0^{-1}x'$, so that (F3) reads $xx' = 1$; the block parameter is $(x, x') \in \mathbb{F}_{q_O}^2$, the actual top data lie on the hyperbola $xx' = 1$, and $T(x, x') := (\delta_O x',\, x/\delta_O)$ with $\delta_O := -\rho_O^{-Lq_O} t_0^{-1-q_O}$. The substitution $y \mapsto y^{(u)}$ acts on $x$ by $x \mapsto \delta_O/x$ (proof of Theorem 5.1(c)), which is not linear. With the second coordinate $x' = 1/x$, it is the restriction of the linear map $T$ to the hyperbola.
- Case C: put $\rho_{-O} := -\rho_O$, so $V_{-O} = V_O$. The block parameter is $(t, t') = (\widehat{y}(\rho_O), \widehat{y}(-\rho_O)) \in V_O^2$, its $\nu$-datum is $\nu_O := tt'$, and $T(t, t') := (t', t)$.

Let $V$ be the direct sum of the block parameter spaces (for case B, with $t_0$ fixed). For $n = 2^e$ with $e \geq 4$ there is one block, of case A, with $q_O = q$, $\iota_O = \iota$ and $c_O = -1$, so $V_O$ and $T$ are the $V$ and $T$ of Theorem 3.5, and $\nu_O = \iota\nu$. Table 3 summarizes the three cases.

TABLE 3. The three cases of blocks. The last two columns give the factor that a block contributes to the size $\Phi$ of a non-empty fibre (Theorem 5.1(c)) and to the number of non-empty fibres. The number of non-empty fibres is 4 times the product of the last column, and the bound of Corollary 5.2 is 16 times that product.

| Case | Condition | Occurs only if | Parameter | $\nu$-datum | $T$ | Factor in $\Phi$ | Factor in fibre count |
|---|---|---|---|---|---|---|---|
| A | $-O = O$ | $a \geq 4$ | $t \in V_O$ | $\iota_O t^{1+q_O}$ | $t \mapsto \iota_O t^{q_O}$ | $q_O + 1$ | $q_O - 1$ |
| B | $-O = O^{-1}$ | $a = 3$ | $(x, x') \in \mathbb{F}_{q_O}^2$ | $t\,\mathbb{F}_{q_O}^{\times}$ | $(x, x') \mapsto (\delta_O x', x/\delta_O)$ | $q_O - 1$ | $q_O + 1$ |
| C | otherwise | $n_{\mathrm{odd}} > 1$ | $(t, t') \in V_O^2$ | $tt'$ | $(t, t') \mapsto (t', t)$ | $3^L - 1$ | $3^L - 1$ |

**Theorem 5.1.** *Let $n = 2^a n_{\mathrm{odd}}$ with $a \geq 3$, $n_{\mathrm{odd}}$ odd and $3 \nmid n$.*

(a) *The map $y \mapsto y^{(u)}$ is an involution of* $\mathrm{NF}(n)$ *and of the solution set of* (1) *with $\sigma = 2$. It preserves $S$ and $\widehat{y}$ on $\mu_m$, satisfies $\widehat{y^{(u)}}(\xi) = \widehat{y}(-\xi)$ on $\mathcal{L}_a$, preserves $y_0$, and sends $y_1$ to $\overline{y_1}$.*

(b) *For $a \geq 4$ only cases A and C occur; for $a = 3$ only cases B and C.*

(c) *In each case $T$ is an $\mathbb{F}_3$-linear involution of the block parameter space, preserves the $\nu$-datum (in case B, preserves $xx'$), and is the action of $y \mapsto y^{(u)}$. The values of $\widehat{y}$ on $\mu_m$ depend only on the $\nu$-data, on $S$ and on $f := \widehat{y}|_{\mu_{n_{\mathrm{odd}}}}$, and the equations for $f$ depend on the top data only through the $\nu$-data. Call the set of solutions of the norm-free system with given $\nu$-data, $S$ and $f$ a* fibre. *A non-empty fibre is in bijection, through its top data, with the set of all top data with these $\nu$-data. Every non-empty fibre has*

$$\Phi := \prod_{\mathcal{A}} (q_O + 1) \prod_{\mathcal{B}} (q_O - 1) \prod_{\mathcal{C}} (3^L - 1)$$

*elements, and there are $|\mathrm{NF}(n)|/\Phi = 4 \prod_{\mathcal{A}}(q_O - 1) \prod_{\mathcal{B}}(q_O + 1) \prod_{\mathcal{C}}(3^L - 1)$ non-empty fibres.*

(d) *Fix a fibre, and let $V_+$ and $V_-$ be the eigenspaces of $T$, so that $V = V_+ \oplus V_-$. There are $\mathbb{F}_3$-linear maps $\mathcal{Y}_0, \mathcal{Y}_1 \colon V \to F$, with $\mathcal{Y}_0$ injective on $V_+$ and $\mathcal{Y}_1$ injective on $V_-$, such that every point $v = v_+ + v_-$ of the fibre has $y_0^- = \mathcal{Y}_0(v_+)$ and $y_1^- = \mathcal{Y}_1(v_-)$.*

Equivalently, a fibre is the set of solutions with given values of $\widehat{y}$ on $\mu_m$, since by (c) these values are fixed by the $\nu$-data, $S$ and $f$; conversely they give $S = \widehat{y}(-1)$, $f$, and the $\nu$-data, as $\widehat{y}(\rho_O)\widehat{y}(-\rho_O) = S\,\widehat{y}(\rho_O^2)$ (in case B this product fixes $t^{1-q_O}$, hence the coset $t\mathbb{F}_{q_O}^{\times}$).

**Corollary 5.2.** *Let $n \equiv 8 \pmod{24}$. Each fibre contains at most 4 solutions of* (1) *with $\sigma = 2$; if it contains any, they form one orbit of the group generated by $T$ and $v \mapsto -v$, so there are 0, 2 or*

4 *of them. Hence* (1) *with* $\sigma = 2$ *has at most*

$$16 \prod_{\mathcal{A}} (q_O - 1) \prod_{\mathcal{B}} (q_O + 1) \prod_{\mathcal{C}} (3^L - 1) \;\le\; 16\,(4/3)^b\, 3^{n/8}$$

*solutions.*

For $16 \mid n$ there is no case-B block, and the bound is less than $16 \cdot 3^{n/8}$, compared with $|\mathrm{NF}(n)| < 4 \cdot 3^{n/4}$ (Theorem 4.1). For $n = 2^e$ with $e \ge 5$ odd it is the bound $16(q-1)$ of Corollary 3.6. For $n = 8$ (one case-B block, $L = 2$) the bound 64 exceeds $|\mathrm{NF}(8)| = 32$. Table 4 shows the blocks, $|\mathrm{NF}(n)|$ and the bound for the five smallest $n$ in Xia's range.

TABLE 4. Blocks (case: orbit length $L$), $|\mathrm{NF}(n)|$ (Theorem 4.1) and the bound of Corollary 5.2. Of these five values, only $n = 8$ and $n = 80$ make $p = n^2 + n + 1$ prime, and a counterexample needs $n \ge 2 \cdot 10^{11}$. For $n = 80$ the $\sigma$ of $n$ (Section 2) is 10, not 2, so the bound does not apply to a plane of order 80.

| $n$ | $a$ | blocks | $\lvert\mathrm{NF}(n)\rvert$ | bound |
|---|---|---|---|---|
| 8 | 3 | B: 2 | 32 | 64 |
| 32 | 5 | A: 8 | 26 240 | 1 280 |
| 56 | 3 | B: 2, 6, 6 | 16 959 488 | 50 176 |
| 80 | 4 | A: 4; C: 4, 4 | 13 107 200 000 | 819 200 |
| 104 | 3 | B: 2; C: 6, 6 | 8 988 257 288 192 | 33 918 976 |

5.2. **Proofs.**

*Proof of Theorem 5.1.* (a) $u^2 = 1 + 2m + m^2 \equiv 1 \pmod n$, as $2m = n$ and $m^2 = n \cdot n/4$; so $u$ is a unit and $y \mapsto y^{(u)}$ is an involution. As $um \equiv m$, $y_t^{(u)} y_{t+m}^{(u)} = y_{ut} y_{ut+m}$, so (L2) is preserved; (L1) is preserved as $2u \equiv 2$. In Fourier form $\widehat{y^{(u)}}(\xi) = \widehat{y}(\xi^u)$, and (F1), (F3), (F4) are preserved: $\xi^{6u} = \xi^6$, $\xi^{um} = \xi^m$, $(-\xi)^u = -\xi^u$ ($u$ odd), and $\widehat{y}((-1)^u) = S$. By Proposition 2.4, $\mathrm{NF}(n)$ is preserved. Now $\xi^u = \xi \cdot \xi^m$ is $-\xi$ on $\mathcal{L}_a$ and $\xi$ on $\mu_m$. The value $y_0 = n^{-1} \sum_\xi \widehat{y}(\xi)$ is preserved, as $\xi \mapsto -\xi$ permutes $\mathcal{L}_a$, and $y_1^{(u)} = y_{1+m} = \overline{y_1}$.

(b) $-O = O^{-1}$ means $-\rho_O = \rho_O^{-3^k}$ for some $k$, that is, $u \equiv -3^k$ modulo $\mathrm{ord}(\rho_O)$, a multiple of $2^a$. As $m \equiv 2^{a-1} \pmod{2^a}$, this gives $3^k \equiv -1 - 2^{a-1} \pmod{2^a}$, hence $3^k \equiv 7 \pmod 8$ when $a \ge 4$, which is impossible since $\langle 3 \rangle = \{1, 3\}$ modulo 8. For $a = 3$, case A needs $3^k \equiv 1 + m \equiv 5 \pmod 8$, which is impossible too.

(c) We treat case B last. *Case A.* Let $-\rho_O = \rho_O^{3^h}$ with $0 < h < L$. Then $\rho_O^{3^{2h}} = (-\rho_O)^{3^h} = -\rho_O^{3^h} = \rho_O$, so $L \mid 2h$, and $2h = L$. Hence

$$\rho_O^{q_O - 1} = -1. \tag{5}$$

Then $\widehat{y}(-\rho_O) = \widehat{y}(\rho_O^{3^h}) = \rho_O^{Lq_O} t^{q_O} = T(t)$, so $T$ is the action of $y \mapsto y^{(u)}$ on $t$. As $\rho_O^{3^L} = \rho_O$, we have $\iota_O^{3^L} = \iota_O$, and $c_O^{q_O - 1} = (\rho_O^{q_O - 1})^{-2L} = 1$ by (5); so $(Tt)^{3^L} = \iota_O (c_O t)^{q_O} = c_O\, Tt$, and $T$ maps $V_O$ into $V_O$. Next $\iota_O^{1+q_O} c_O = \rho_O^{L(q_O + q_O^2 - 2)} = \rho_O^{L(q_O - 1)} = 1$ ($q_O^2 = 3^L \equiv 1$ modulo $\mathrm{ord}(\rho_O)$, and $L$ is even), so $T^2 t = \iota_O^{1+q_O} t^{3^L} = t$, and $\nu_O(Tt) = \iota_O^{1+q_O} c_O \cdot \iota_O t^{1+q_O} = \nu_O(t)$.

*Case C.* $V_{-O} = V_O$, as $(-\rho_O)^{-2L} = c_O$; the swap is the action of $y \mapsto y^{(u)}$, since $\widehat{y^{(u)}}(\rho_O) = \widehat{y}(-\rho_O)$, and it preserves $tt'$.

*Case B.* Let $-\rho_O = \rho_O^{-3^g}$ with $0 < g < L$. Raising to the power $-3^g$ gives $\rho_O^{3^{2g}} = \rho_O$, so $L \mid 2g$; and $L \nmid g$, since otherwise $-\rho_O = \rho_O^{-1}$ and $\rho_O$ would have order 4, while its order is a multiple of $2^a \ge 8$. Hence $2g = L$, and

$$\rho_O^{1+q_O} = -1. \tag{6}$$

By (F3), $\widehat{y}(-\rho_O) = \widehat{y}(\rho_O^{-q_O}) = -1/\widehat{y}(\rho_O^{q_O}) = -\rho_O^{-Lq_O} t^{-q_O}$, which gives the formula for $\widehat{y}(\rho_O)\widehat{y}(-\rho_O)$. The level sets of $t \mapsto \widehat{y}(\rho_O)\widehat{y}(-\rho_O)$ on $V_O \setminus \{0\}$ are the cosets $t_0\mathbb{F}_{q_O}^\times$, and there are $(3^L-1)/(q_O-1) = q_O+1$ of them. With $t = t_0 x$, the map $y \mapsto y^{(u)}$ sends $x$ to $\widehat{y}(-\rho_O)/t_0 = \delta_O/x$, that is, $(x, x') \mapsto (\delta_O x', x/\delta_O)$ on the hyperbola. Moreover $\delta_O \in \mathbb{F}_{q_O}$ for every $t_0 \in V_O \setminus \{0\}$: by $t_0^{3^L-1} = c_O$, $\delta_O^{q_O-1} = \rho_O^{-Lq_O(q_O-1)} c_O^{-1} = \rho_O^{L(q_O+1)} = 1$, using $q_O^2 \equiv 1$ modulo $\mathrm{ord}(\rho_O)$, (6) and $L$ even. The formula for $T$ gives $T^2 = \mathrm{id}$, and $T$ preserves $xx'$.

*Lower layers.* Every $\xi$ in layer $a-1$ is $\rho^2$ for exactly one pair $\pm\rho$ in $\mathcal{L}_a$, and $\pm\rho$ lie in one block. (F4) gives $\widehat{y}(\rho^2) = S\,\widehat{y}(\rho)\widehat{y}(-\rho)$, and for $\rho = \rho_O^{3^k}$,

$$\widehat{y}(\rho)\widehat{y}(-\rho) = \begin{cases} \rho_O^{2k3^k(1+q_O)}\,\nu_O^{3^k} & \text{(case A)},\\ \rho_O^{4k3^k}\,\nu_O^{3^k} & \text{(case C)},\\ -\rho_O^{2k3^k-2(k+g)3^{k+g}}\left(t^{1-q_O}\right)^{3^k} & \text{(case B)}, \end{cases}$$

the last one constant on a coset $t_0\mathbb{F}_{q_O}^\times$. On $O^{-1}$ the products are the inverses of these, as $\widehat{y}(\rho^{-1})\widehat{y}(-\rho^{-1}) = 1/(\widehat{y}(\rho)\widehat{y}(-\rho))$. Hence the values of $\widehat{y}$ on layer $a-1$ are functions of the $\nu$-data and $S$, and so are those on layers $a-2, \dots, 1$, by (4). On layer 0, the equations are (E1)–(E3) of Step 4 of the proof of Theorem 4.1; (E2) and (E3) do not involve the top data, and in (E1), $P(\alpha)$ is the product of $\widehat{y}(\rho)$ over the $\rho \in \mathcal{L}_a$ with $\rho^{2^{a-1}} = -\alpha$; this set contains $-\rho$ with $\rho$, so $P$ is a product of values $\widehat{y}(\rho)\widehat{y}(-\rho)$, a function of the $\nu$-data. Hence, for $\nu$-data, $S$ and $f$ that occur, all top data with these $\nu$-data give solutions, and the top data determine them: the fibre is the set of $v$ with $\nu_O(v) = \nu_O$ for every block of case A or C and $xx' = 1$ for every block of case B. Its size is a product over the blocks. In case A, $V_O \setminus \{0\} = t_1\mathbb{F}_{3^L}^\times$ for any non-zero $t_1 \in V_O$, and $t \mapsto \iota_O t^{1+q_O}$ is $\iota_O t_1^{1+q_O}$ times the norm from $\mathbb{F}_{3^L}$ to $\mathbb{F}_{q_O}$, whose level sets on $\mathbb{F}_{3^L}^\times$ have $q_O+1$ elements. In case C, $t$ is free in $V_O \setminus \{0\}$ and $t' = \nu_O/t$: $3^L-1$ elements. In case B, the coset has $q_O-1$ elements. As $\mathrm{NF}(n)$ is the disjoint union of the fibres, Theorem 4.1 gives their number.

(d) Fix a fibre. For $v \in V$ define the *formal top function* $\mathrm{top}_v$ on $\mathcal{L}_a$: on $O$ by $\mathrm{top}_v(\rho_O^{3^k}) := \rho_O^{2k3^k} t^{3^k}$ (with $t'$ on $-O$ in case C, and $t = t_0 x$ in case B), and on $O^{-1}$ by $\mathrm{top}_v(\rho_O^{-3^k}) := -\rho_O^{-2k3^k}(t^*)^{3^k}$, with the *linear* formal inverse

$$t^* := \iota_O t^{q_O}/\nu_O \ \text{ (case A)}, \qquad t^* := t'/\nu_O, \ \ t'^* := t/\nu_O \ \text{ (case C)}, \qquad t^* := t_0^{-1}x' \ \text{ (case B)}.$$

On the fibre, $t^* = t^{-1}$ and $\mathrm{top}_v = \widehat{y}$ on $\mathcal{L}_a$. The map $v \mapsto \mathrm{top}_v$ is $\mathbb{F}_3$-linear. Put $y_s^-(v) := n^{-1}\sum_{\xi\in\mathcal{L}_a} \mathrm{top}_v(\xi)\xi^{-s}$, $\mathcal{Y}_0(v) := y_0^-(v)$ and $\mathcal{Y}_1(v) := y_1^-(v)$.

(P1) $\mathrm{top}_v$ *satisfies (F1) on* $\mathcal{L}_a$ *for every* $v \in V$. Along each orbit this holds by construction; the wraps need $t^{3^L} = c_O t$ on $O$ and $(t^*)^{3^L} = c_O^{-1} t^*$ on $O^{-1}$. In case A, $\nu_O^{q_O} = \iota_O^{q_O} c_O t^{1+q_O} = \iota_O^{q_O-1} c_O \nu_O$ gives $(t^*)^{q_O} = \iota_O t/\nu_O$, and then $(t^*)^{3^L} = \iota_O^{q_O} t^{q_O}/(\iota_O^{q_O-1} c_O \nu_O) = c_O^{-1} t^*$. In case C, $(t'/\nu_O)^{3^L} = c_O t'/(c_O^2 \nu_O)$. In case B, $x, x' \in \mathbb{F}_{q_O} \subseteq \mathbb{F}_{3^L}$. Consequently, as $n^{-1} \in \mathbb{F}_3$ and $\xi \mapsto \xi^3$ permutes $\mathcal{L}_a$, $\phi(y_s^-(v)) = y_{s+2}^-(v)$ for all $s$; and $y_{s+m}^-(v) = -y_s^-(v)$, as $\xi^{-m} = -1$ on $\mathcal{L}_a$. So $\phi^m$ fixes $y_s^-(v)$: the values $\mathcal{Y}_0(v)$, $\mathcal{Y}_1(v)$ lie in $F$ for every $v \in V$, not only on the fibre.

(P2) $\mathrm{top}_{Tv}(\xi) = \mathrm{top}_v(-\xi)$ *for all* $\xi \in \mathcal{L}_a$ *and* $v \in V$. By the wraps of (P1), both formulas defining $\mathrm{top}_v$ are $L$-periodic in $k$ (for instance $\rho_O^{2(k+L)3^{k+L}}(c_O t)^{3^k} = \rho_O^{2k3^k} t^{3^k}$), so they may be used at indices $k+h$, $k+g \geq L$. In case C, (P2) is the definition of the swap. In case A, on $O$: $\mathrm{top}_{Tv}(\rho_O^{3^k}) = \rho_O^{2k3^k} \iota_O^{3^k} t^{3^{k+h}}$ and $\mathrm{top}_v(-\rho_O^{3^k}) = \mathrm{top}_v(\rho_O^{3^{k+h}}) = \rho_O^{2(k+h)3^{k+h}} t^{3^{k+h}}$; with $\iota_O = \rho_O^{2h3^h}$ the exponents differ by $2k3^k(q_O-1)$, and $\rho_O^{2k3^k(q_O-1)} = 1$ by (5). On $O^{-1}$: $\iota_O^{1+q_O} c_O = 1$ gives $(Tt)^* = t/\nu_O$, and $(t^*)^{q_O} = \iota_O t/\nu_O$; so $\mathrm{top}_{Tv}(\rho_O^{-3^k}) = -\rho_O^{-2k3^k}(t/\nu_O)^{3^k}$ and $\mathrm{top}_v(-\rho_O^{-3^k}) = \mathrm{top}_v(\rho_O^{-3^{k+h}}) = -\rho_O^{-2(k+h)3^{k+h}} \iota_O^{3^k} (t/\nu_O)^{3^k}$, and

$$-2(k+h)3^{k+h} + 2h3^h 3^k = -2k3^k q_O = -2k3^k - 2k3^k(q_O-1)$$

shows that the two values agree. In case B, on $O$: $\mathrm{top}_{Tv}(\rho_O^{3^k}) = \rho_O^{2k3^k}(t_0\delta_O x')^{3^k}$, while $-\rho_O^{3^k} = \rho_O^{-3^{g+k}} \in O^{-1}$ gives $\mathrm{top}_v(-\rho_O^{3^k}) = -\rho_O^{-2(g+k)3^{g+k}} t_0^{-3^{g+k}} x'^{3^k}$. With $\delta_O^{3^k} = -\rho_O^{-Lq_O 3^k} t_0^{-3^k-3^{g+k}}$ both have the form $-\rho_O^{\varepsilon} t_0^{-3^{g+k}} x'^{3^k}$, with exponents $\varepsilon$ that differ by $2k3^k(1+q_O)$; so the two values agree by (6). On $O^{-1}$: $\mathrm{top}_{Tv}(\rho_O^{-3^k}) = -\rho_O^{-2k3^k}(t_0^{-1}x/\delta_O)^{3^k}$, while $-\rho_O^{-3^k} = \rho_O^{3^{g+k}} \in O$ gives $\mathrm{top}_v(-\rho_O^{-3^k}) = \rho_O^{2(g+k)3^{g+k}} t_0^{3^{g+k}} x^{3^k}$ (as $x \in \mathbb{F}_{q_O}$); with $\delta_O^{-3^k} = -\rho_O^{Lq_O 3^k} t_0^{3^k+3^{g+k}}$ both are $\rho_O^{\varepsilon'} t_0^{3^{g+k}} x^{3^k}$, and again the exponents $\varepsilon'$ differ by $2k3^k(1+q_O)$, so the two values agree.

(P3) $v \mapsto \mathrm{top}_v$ *is injective*: $\mathrm{top}_v(\rho_O) = t$, $\mathrm{top}_v(-\rho_O) = t'$ in case C, and in case B $\mathrm{top}_v(\rho_O) = t_0 x$ and $\mathrm{top}_v(\rho_O^{-1}) = -t_0^{-1}x'$.

*Separation.* By (P2), $\mathcal{Y}_0(Tv) = \mathcal{Y}_0(v)$ and $\mathcal{Y}_1(Tv) = n^{-1}\sum_\xi \mathrm{top}_v(-\xi)\xi^{-1} = -\mathcal{Y}_1(v)$. For $v \in V_-$ this gives $\mathcal{Y}_0(v) = \mathcal{Y}_0(Tv) = -\mathcal{Y}_0(v)$, so $\mathcal{Y}_0(V_-) = 0$ (characteristic 3); likewise $\mathcal{Y}_1(V_+) = 0$. Hence $y_0^- = \mathcal{Y}_0(v_+)$ and $y_1^- = \mathcal{Y}_1(v_-)$ for every point $v$ of the fibre.

*Injectivity.* If $\mathcal{Y}_0(v) = \mathcal{Y}_1(v) = 0$, then $y_s^-(v) = 0$ for every $s$ by (P1), so $\mathrm{top}_v = 0$ (inverse Fourier transform of a function supported on $\mathcal{L}_a$), so $v = 0$ by (P3). For $v \in V_+$, $\mathcal{Y}_1(v) = 0$ already, so $\mathcal{Y}_0(v) = 0$ forces $v = 0$. Likewise $\mathcal{Y}_1$ is injective on $V_-$. □

*Proof of Corollary 5.2.* For $n \equiv 8 \pmod{24}$ the solutions of (1) with $\sigma = 2$ are the points of $\mathrm{NF}(n)$ with $\mathrm{N}(y_0) = \mathrm{N}(y_1) = -1$ (Corollary 4.2). In a fibre $y_0^+$ is fixed (it depends only on $\widehat{y}$ on $\mu_m$), so $\mathrm{N}(y_0) = (y_0^+)^2 - (y_0^-)^2 = -1$ leaves two values $\pm w_0$ for $y_0^-$, and by Theorem 5.1(d) $v_+$ is one of two values $\pm x_0$; likewise $v_-$. Hence a fibre contains at most 4 solutions. Both norms are invariant under $T$ ($y_0$ is preserved, $y_1 \mapsto \overline{y_1}$ and $\mathrm{N}(\overline{y_1}) = \mathrm{N}(y_1)$) and under $v \mapsto -v$ ($y_j^- \mapsto -y_j^-$, $y_j^+$ preserved), and both maps preserve the fibre (case A: $(-1)^{1+q_O} = 1$; case C: $(-t)(-t') = tt'$; case B: $(-x)(-x') = xx'$). So the solutions in a fibre, if any, form one orbit. Multiplying the bound 4 by the number of non-empty fibres (Theorem 5.1(c)) gives the bound. For the inequality, $n/4 = \sum_{\mathcal{A}} L + \sum_{\mathcal{B}} L + 2\sum_{\mathcal{C}} L$, and $q_O + 1 \le \frac{4}{3} q_O$ as $L \ge 2$. □

*Remark* 5.3. Two independent computations (Section 8) confirm Theorem 5.1: in exact arithmetic, every block space has dimension $L$, $\delta_O \in \mathbb{F}_{q_O}$, $T$ is an involution preserving the $\nu$-data, (P1) and (P2) hold, and $\ker \mathcal{Y}_0 = V_-$, $\ker \mathcal{Y}_1 = V_+$ exactly, at $n = 8$, 32, 40, 56, 80 (all three cases occur). Every fibre of $\mathrm{NF}(n)$ for $n = 8$, 16, 32, 40, 56 (at $n = 56$ all 16959488 points in all 12544 fibres), and 20 sampled fibres at $n = 80$, has exactly $\Phi$ points, with $y_0^-$ an injective function of $v_+$ and $y_1^-$ of $v_-$.

## 6. The slice $y_1 = \pm i$

In this section $\sigma = 2$, $n \equiv 8 \pmod{24}$, and we use the notation of Section 2. Since $m$ is even, $F$ contains $\mathbb{F}_9$; fix $i \in \mathbb{F}_9$ with $i^2 = -1$. Since $m/2$ is even, $Q \equiv 1 \pmod 4$, so $\mathrm{N}(i) = i^{1+Q} = -1$ and $i^{3^r} = (-1)^r i$. Let $U := \ker \mathrm{N}$, the subgroup of order $Q+1$ of $F^\times$, and $\mathrm{Tr} := \mathrm{Tr}_{F/\mathbb{F}_3}$.

The *slice* is the set of solutions of the norm-free system (Definition 2.3) with $y_1 = \pm i$ or $y_0 = \pm i$; it contains the solutions of (1) with this property. We show that the slice is empty unless $m/4$ is odd and built from base-2 Wieferich primes.

**Definition 6.1.** We say that *Claim C holds at $n$* if every $y \in F^n$ satisfying (L1)–(L3) of (1) with $\sigma = 2$ has $y_0 = \pm i$ or $y_1 = \pm i$.

**Theorem 6.2.** *Let $n \equiv 8 \pmod{24}$ and suppose that the norm-free system (Definition 2.3, $\sigma = 2$) has a solution with $y_1 = \varepsilon i$ or $y_0 = \varepsilon i$, $\varepsilon \in \{\pm 1\}$. Then*

(a) *$8 \nmid m$;*
(b) *$\mathrm{ord}_\ell(3)$ is even for every odd prime $\ell \mid m$;*
(c) *$v_\ell(2^g - 1) > v_\ell(3^b - 1) \ge 1$ for every odd prime $\ell \mid m$, where $g = \mathrm{ord}_\ell(2)$ and $b = \mathrm{ord}_\ell(3)$; in particular $\ell^2 \mid 2^{\ell-1} - 1$.*

*More generally, for an odd prime power $\delta = \ell^a$ dividing $m$, with $g = \mathrm{ord}_\delta(2)$ and $b = \mathrm{ord}_\delta(3)$, $v_\ell(2^g-1) \geq v_\ell(3^b-1) + a - v_\ell(b)$.*

By Section 2, every solution of (1) with $\sigma = 2$ is a solution of the norm-free system, so the theorem applies to the solutions of (1) in the slice. For $n = 2^e$ with odd $e \geq 5$, 8 divides $m = 2^{e-1}$, so by (a) no solution of the norm-free system has $y_0 = \pm i$ or $y_1 = \pm i$. By Corollary 9.20 this means that no solution of (1) lies on the two loci of Section 9.

6.1. **Reduction of (L4).** Applying $\phi$ to (L4) at $s$ gives (L4) at $s+2$ (as $S \in \mathbb{F}_3$ by Proposition 2.4), so (L4) reduces to $s = 0, 1$. For $Z \in F$ and $c \in \mathbb{Z}/m$ put $B_Z(c) := \sum_{k\in\mathbb{Z}/m} \phi^k(Z)\,\phi^{c-k}(Z)$. Splitting $t = 2k$ and $t = 2k+1$ in (L4), and using $y_{s+m} = \overline{y_s}$ (by (L1)), we get

$$(7) \qquad (\mathrm{L4}_0)\quad B_{y_0}(0) - B_{y_1}(-1) = S\,(y_0 + \overline{y_0}), \qquad (\mathrm{L4}_1)\quad B_{y_0}(1) - B_{y_1}(0) = S\,(y_1 + \overline{y_1}).$$

6.2. **Proof of Theorem 6.2.** *Set-up (case $y_1 = \varepsilon i$).* Write $y_0 = i\omega$ with $\omega \in F$; we do not assume $\omega \in U$ (equivalently, $\mathrm{N}(y_0) = -1$). Put $u_k := \phi^k(\omega)$ for $k \in \mathbb{Z}/m$; then $u_{k+m/2} = \phi^k(\overline{\omega})$. Let $J_j := \sum_k u_k u_{j-k}$, and on $\mu_m$ (note $3 \nmid m$) let $\widehat{u}(x) := \sum_k u_k x^k$, so $\sum_j J_j x^j = \widehat{u}(x)^2$. For a condition $\mathcal{C}$ we write $[\mathcal{C}]$ for 1 if $\mathcal{C}$ holds and 0 otherwise.

*Step 1 (L3).* The shift $2r$ in (L3) reads $\mathrm{Tr}(y_0^{1+3^r}) + \mathrm{Tr}(y_1^{1+3^r}) = 0$. Here $(\varepsilon i)^{1+3^r} = -(-1)^r$ has trace $-(-1)^r m = -(-1)^r$, and $(i\omega)^{1+3^r} = -(-1)^r\omega^{1+3^r}$. So $R_u(r) := \sum_k u_k u_{k+r} = \mathrm{Tr}(\omega^{1+3^r}) = -1$ for $0 \leq r < m/2$; as $R_u(-r) = R_u(r)$, $R_u(r) = -1$ for all $r \not\equiv m/2$. Next, $R_u(m/2) = \sum_k \phi^k(\omega\overline{\omega}) = \mathrm{Tr}(\mathrm{N}(\omega))$, and by (L1), $R(m) = \sum_t \mathrm{N}(y_t) = \mathrm{Tr}(\mathrm{N}(y_0)) + \mathrm{Tr}(\mathrm{N}(y_1))$ with $\mathrm{N}(y_0) = \mathrm{N}(i)\,\mathrm{N}(\omega) = -\mathrm{N}(\omega)$ and $\mathrm{N}(y_1) = -1$; so $R(m) = 1$ reads $-R_u(m/2) - m = 1$, that is, $R_u(m/2) = 1$. (The odd shifts hold automatically: $\mathrm{Tr}(y_0\phi^r(y_1)) = -\varepsilon(-1)^r\,\mathrm{Tr}(\omega) = -\mathrm{Tr}(y_1\phi^{r+1}(y_0))$.) Taking transforms, $\widehat{u}(x)\widehat{u}(x^{-1}) = \sum_r R_u(r)x^r = -m[x=1] - x^{m/2}$, that is,

$$(8) \qquad \widehat{u}(x)\,\widehat{u}(x^{-1}) = -x^{m/2} \quad (x \in \mu_m,\ x \neq 1), \qquad \widehat{u}(1)^2 = 1.$$

Note that $\widehat{u}(1) = \mathrm{Tr}(\omega) \in \{\pm 1\}$. In particular $\widehat{u}$ has no zero.

*Step 2 (L1).* Since $u_k^3 = u_{k+1}$, $\widehat{u}(x)^3 = x^{-3}\widehat{u}(x^3)$, so

$$(9) \qquad \widehat{u}(x^3) = x^3\,\widehat{u}(x)^3, \qquad \text{and by induction} \qquad \widehat{u}(x^{3^b}) = x^{b3^b}\,\widehat{u}(x)^{3^b}.$$

*Step 3 (L4).* One computes $B_{i\omega}(0) = -J_0$, $B_{\varepsilon i}(-1) = m = 1$, $B_{i\omega}(1) = J_1$, $B_{\varepsilon i}(0) = -m = -1$, $y_0 + \overline{y_0} = i(u_0 + u_{m/2})$ (as $\overline{i} = i$) and $y_1 + \overline{y_1} = 2\varepsilon i = -\varepsilon i$. So (7) becomes $J_0 = -1 - S\,i\,(u_0 + u_{m/2})$ and $J_1 = -1 - S\varepsilon i$. Applying $\phi^r$ (with $J_c^3 = J_{c+2}$, $S \in \mathbb{F}_3$) and using that $m/2$ is even, so that $(-1)^r$ is defined for $r \in \mathbb{Z}/(m/2)$,

$$J_{2r} = -1 - S(-1)^r i\,(u_r + u_{r+m/2}), \qquad J_{2r+1} = -1 - S\varepsilon(-1)^r i.$$

Now $\sum_{r \bmod m/2} x^{2r} = (m/2)[x^2 = 1] = -[x^2 = 1]$ (as $m/2 \equiv 2 \pmod 3$) and $\sum_{r \bmod m/2}(-1)^r(u_r + u_{r+m/2})x^{2r} = \sum_{k \bmod m}(-1)^k u_k x^{2k} = \widehat{u}(-x^2)$. Hence

$$(10) \qquad \widehat{u}(x)^2 = (x+1)[x^2 = 1] + S\varepsilon i\,x\,[x^2 = -1] - S\,i\,\widehat{u}(-x^2) \qquad (x \in \mu_m).$$

For $x^2 \neq \pm 1$ this says $\widehat{u}(-x^2) = \gamma\,\widehat{u}(x)^2$ with $\gamma := Si$; note $\gamma^2 = -1$.

*Step 4 (proof of (b)).* Let $x \in \mu_m$ with $x^2 \neq \pm 1$. By (10) at $x$ and at $-x$, $\widehat{u}(x)^2 = \widehat{u}(-x)^2$, so $\psi(x) := \widehat{u}(x)/\widehat{u}(-x) \in \{\pm 1\}$. By (9) at $x$ and at $-x$, $\psi(x^3) = x^3\widehat{u}(x)^3/((-x)^3\widehat{u}(-x)^3) = -\psi(x)$. (The point $x^3$ is again admissible: $(x^3)^2 = \pm 1$ would give $x^{12} = 1$, hence $x^4 = 1$ as $3 \nmid \mathrm{ord}\,x$.) If $x$ has order $\delta$ and $b := \mathrm{ord}_\delta(3)$, then $x^{3^b} = x$ and $\psi(x) = (-1)^b\psi(x)$, so $b$ is even. With $\delta = \ell$ this is (b).

*Step 5 (proof of (c)).* Let $x$ have odd prime order $\ell \mid m$, and put $W(x) := \gamma\,\widehat{u}(-x) \neq 0$. By (10) at the point $-x$, $\widehat{u}(-x^2) = \gamma\,\widehat{u}(-x)^2$, i.e. $W(x^2) = W(x)^2$; iterating $g = \mathrm{ord}_\ell(2)$ times gives $W(x)^{2^g-1} = 1$. By (9) at $-x$, $\widehat{u}(-x^3) = -x^3\widehat{u}(-x)^3$, so $W(x^3) = x^3W(x)^3$; iterating $b = \mathrm{ord}_\ell(3)$ times as in Step 2 gives $W(x) = x^{b3^b}W(x)^{3^b} = x^bW(x)^{3^b}$, so $W(x)^{3^b-1} = x^{-b}$, which has order $\ell$

as $0 < b < \ell$. Let $o := \operatorname{ord} W(x)$; then $o \mid 2^g - 1$, and $\operatorname{ord}(W(x)^{3^b-1}) = o/\gcd(o, 3^b - 1) = \ell$ with $\ell \mid 3^b - 1$ forces $v_\ell(o) = v_\ell(3^b - 1) + 1$. Hence $v_\ell(2^g - 1) \geq v_\ell(3^b - 1) + 1$. For $x$ of order $\ell^a$ the element $x^{-b}$ has order $\ell^{a-v_\ell(b)}$, which gives the general form.

*Step 6 (proof of (a)).* Suppose $8 \mid m$. Then $i^{m/2} = 1$, and $\mu_m$ contains elements of order 8.

*Order* 4. (10) at $x = i$ gives $\widehat{u}(i)^2 = -S(\varepsilon + i \operatorname{Tr}(\omega))$. (9) at $i$ gives $\widehat{u}(-i) = -i\,\widehat{u}(i)^3$, and (8) at $i$ gives $\widehat{u}(i)\widehat{u}(-i) = -1$. So $\widehat{u}(i)^4 = -i$. In $\mathbb{F}_9$, $(\varepsilon + i \operatorname{Tr}(\omega))^2 = -\varepsilon \operatorname{Tr}(\omega) i$, hence $\varepsilon \operatorname{Tr}(\omega) = 1$.

*Order* 8. Let $y_*$ have order 8 and $y_*^2 = -\varepsilon' i$ with $\varepsilon' \in \{\pm 1\}$, so $-y_*^2 = \varepsilon' i$. By (10) at $y_*$, $\widehat{u}(\varepsilon' i) = \gamma\,\widehat{u}(y_*)^2$, and by (10) at $\varepsilon' i$, $\widehat{u}(\varepsilon' i)^2 = -S(\varepsilon'\varepsilon + i \operatorname{Tr}(\omega))$. So $\widehat{u}(y_*)^4 = \widehat{u}(\varepsilon' i)^2/\gamma^2 = S(\varepsilon'\varepsilon + i \operatorname{Tr}(\omega))$ and $\widehat{u}(y_*)^8 = -\varepsilon'\varepsilon \operatorname{Tr}(\omega) i$. On the other hand $3^2 \equiv 1 \pmod 8$ and (9) give $\widehat{u}(y_*) = y_*^{18}\widehat{u}(y_*)^9 = y_*^2\widehat{u}(y_*)^9$, so $\widehat{u}(y_*)^8 = y_*^{-2} = \varepsilon' i$. Hence $\varepsilon \operatorname{Tr}(\omega) = -1$, a contradiction.

*The case $y_0 = \varepsilon i$, $y_1 = i\omega$ ($\omega \in F$).* The even shifts of (L3) and the relation $R(m) = 1$ are symmetric in $y_0, y_1$ and the odd shifts cancel as before, so (8) holds for $\widehat{u}(x) = \sum_k \phi^k(\omega) x^k$. Now $B_{\varepsilon i}(0) = -1$, $B_{i\omega}(-1) = J_{-1}$, $y_0 + \overline{y_0} = -\varepsilon i$, $B_{\varepsilon i}(1) = 1$, $B_{i\omega}(0) = -J_0$, $y_1 + \overline{y_1} = i(u_0 + u_{m/2})$, so $J_{-1} = -1 + S\varepsilon i$ and $J_0 = -1 + S\,i\,(u_0 + u_{m/2})$. As in Step 3,

$$\widehat{u}(x)^2 = (x + 1)[x^2 = 1] + S\varepsilon i\, x\,[x^2 = -1] + S\,i\,\widehat{u}(-x^2),$$

so $\widehat{u}(-x^2) = \gamma\,\widehat{u}(x)^2$ with $\gamma := -Si$, again $\gamma^2 = -1$. Steps 4 and 5 use only $\gamma^2 = -1$. In Step 6, $\widehat{u}(i)^2 = S(-\varepsilon + i \operatorname{Tr}(\omega))$ and $\widehat{u}(i)^4 = \varepsilon \operatorname{Tr}(\omega) i = -i$, so $\varepsilon \operatorname{Tr}(\omega) = -1$; at order 8, $\widehat{u}(y_*)^4 = S(\varepsilon'\varepsilon - i \operatorname{Tr}(\omega))$ and $\widehat{u}(y_*)^8 = \varepsilon'\varepsilon \operatorname{Tr}(\omega) i = \varepsilon' i$, so $\varepsilon \operatorname{Tr}(\omega) = 1$. A contradiction again. □

*Remark* 6.3. The proof uses that $m/2$ is even and $m \equiv 1 \pmod 3$ (so $\operatorname{Tr}(1) = m = 1$ and $m/2 = -1$ in $\mathbb{F}_3$), the relations (L1), (L3), $R(m) = 1$ and (L4) of the norm-free system, and $S^2 = 1$ from Proposition 2.4; it does not use the norm equation (L2). With $S$ fixed, (L4) in the slice expresses the convolution values $J_j$ as affine-linear functions of the Frobenius orbit $(u_k)$, and its Fourier form (10) is a squaring law. Outside the slice, (L4) is the product law (F4) and this argument does not apply.

6.3. **Consequences.** A prime $\ell$ is a base-2 Wieferich prime if $\ell^2 \mid 2^{\ell-1} - 1$. By Theorem 6.2(c), if the slice is not empty, every odd prime factor of $m$ is one. Only 1093 and 3511 are known, and Dorais and Klyve report "that there are no other Wieferich primes $p < 6.7 \times 10^{15}$" [2, Abstract] (there a Wieferich prime is a prime $p$ with $2^{p-1} \equiv 1 \pmod{p^2}$). A direct computation gives: $\operatorname{ord}_{1093}(3) = 7$ (indeed $3^7 - 1 = 2 \cdot 1093$), so 1093 fails (b); $\operatorname{ord}_{3511}(3) = 270$, $\operatorname{ord}_{3511}(2) = 1755$, $v_{3511}(2^{1755} - 1) = 2 > 1 = v_{3511}(3^{270} - 1)$, so 3511 passes (b) and (c); and $\operatorname{ord}_{3511^2}(3) = 947970$, $\operatorname{ord}_{3511^2}(2) = 1755$, $v_{3511}(3^{947970} - 1) = 2$ and $v_{3511}(947970) = 1$, so the prime-power form of (c) with $\delta = 3511^2$ fails ($2 < 2 + 2 - 1$), and $3511^2 \nmid m$.

**Corollary 6.4.** *Let $n \equiv 8 \pmod{24}$, $n > 8$, put $w := n/8 = m/4$, and suppose that Claim C holds at $n$. (This $w$ is the odd part of $m$ only when $8 \nmid m$.)*

(i) *If (1) with $\sigma = 2$ has a solution, then $w$ is odd, $w > 1$, and every prime factor $\ell$ of $w$ is a base-2 Wieferich prime with $\operatorname{ord}_\ell(3)$ even and $v_\ell(2^{\operatorname{ord}_\ell(2)} - 1) > v_\ell(3^{\operatorname{ord}_\ell(3)} - 1)$. Hence $w = 3511$ (that is, $n = 28088$) or $w$ has a prime factor larger than $6.7 \times 10^{15}$.*

(ii) *If there is a non-Desarguesian flag-transitive projective plane of order $n$ with $\sigma = 2$, then $w$ has a prime factor $\ell > 6.7 \times 10^{15}$ as in (i).*

*Proof.* (i) Claim C puts the solution in the slice. By Theorem 6.2(a), $m = 4w$ with $w$ odd, and $w > 1$ as $n > 8$. Every prime factor of $w$ satisfies (b) and (c), hence is a base-2 Wieferich prime. By [2] a prime factor below $6.7 \times 10^{15}$ is 1093 or 3511; 1093 fails (b), and $3511^2 \nmid m$ by the computation above. So if no prime factor of $w$ exceeds $6.7 \times 10^{15}$, then $w = 3511$. (ii) By Theorem 2.1 the plane gives a solution of (1). Thas and Zagier verified that no non-Desarguesian flag-transitive plane has order $n < 2 \cdot 10^{11}$ [17, Appendix], so $w > 3511$, and (i) applies. □

*Remark* 6.5. Theorem 2.1 goes from planes to solutions of (1), and the search in [17] excludes planes, not solutions. This is why (i) and (ii) are stated separately: at $n = 28088$ Theorem 6.2 says

nothing about (1). For $n = 8$ ($m = 4$) the theorem is vacuous; the solutions of (1) at $n = 8$ lie in the slice. Claim C holds at $n = 8$, 32, 56 and 80 by computation (Section 8.1).

## 7. Other characteristics

Xia's system (1) is the case $r = 3$ of a family: for every prime $r \nmid pn$ Xia's Theorem 3.4(b) gives a system over a finite field of characteristic $r$. We first treat $r = 5$ for $n$ a power of 2. A non-Desarguesian flag-transitive plane of order $2^e$ also gives a solution of the system (11) below (Proposition 7.1), so the solvability of (11) is another necessary condition for such a plane. The solutions of the norm-free system in characteristic 5 are again given by one parameter and two binary choices, and the norm equation becomes a *single* condition, on $y_0$ alone (Corollary 7.3). The Fourier form for $r = 5$ carries over to every prime $r$. For $8 \mid n$, Section 7.4 counts the solutions of the norm-free system in characteristic $r$ exactly for every prime $r \nmid pn$ with $r \not\equiv -1 \pmod{2^a}$, where $2^a$ is the 2-part of $n$, and, when $n = 2^a$, for every prime $r \nmid pn$.

7.1. **The system for $r = 5$.** Let $n = 2^e$ with $e$ odd, $e \geq 3$, and $p = n^2 + n + 1$. Then $n \equiv 2$ or 3 (mod 5), $n^2 \equiv -1$, $n^4 \equiv 1$ and $p \equiv n \pmod 5$, so $p \equiv 2$ or 3 (mod 5); in particular $5 \nmid pn$.

**Proposition 7.1.** *Let $n = 2^e$ with $e \geq 3$ odd, and suppose there is a non-Desarguesian flag-transitive projective plane of order $n$. Then there are $y_0, \dots, y_{n-1} \in \mathbb{F}_{5^n}$ such that, with subscripts modulo $n$ and $t$ running over $\mathbb{Z}/n$, (L1$_5$) holds for every $s \in \mathbb{Z}/n$ and (L2$_5$)–(L4$_5$) hold for $s = 0, \dots, n/2 - 1$:*

$$\begin{aligned} &(L1_5)\quad y_{s+1} = y_s^5, \qquad (L2_5)\quad y_s\, y_{s+n/2} = n^3, \qquad (L3_5)\quad \textstyle\sum_t y_t\, y_{s+t} = n(1-p), \\ &(L4_5)\quad \textstyle\sum_t (-1)^t y_t\, y_{2s-t} = \big(y_s + y_{s+n/2}\big) S, \qquad S := \textstyle\sum_t (-1)^t y_t. \end{aligned} \tag{11}$$

*Proof.* By [19, Proposition 1.2], $p$ is prime and $H$ is a $(p, n+1, 1)$ difference set, that is, an $n$th-cyclotomic difference set in the sense of [19]. Here $H$, written $H_{v,n}$ by Xia (there $v$ is our $p$), is the group of non-zero $n$-th powers in $\mathbb{F}_p$, that is, the subgroup of order $n+1$ of $\mathbb{F}_p^\times$. Let $\chi_5$ be a 5-adic multiplicative character of order $n$ on $\mathbb{F}_p$. For a primitive $n$-th root of unity $\varpi_5 \in \mathbb{C}_5$ (defined as $\mathbb{C}_3$ is) write $\chi_5(5) = \varpi_5^{\sigma_5}$. By [19, Lemma 3.5], $(-1)^{\sigma_5} = \big((-1)^{n/2} p/5\big) = (p/5) = -1$, as the squares modulo 5 are 1 and 4. Hence $\sigma_5$ is odd for every choice of $\varpi_5$ ([19, Lemma 3.5] holds for every primitive $\varpi_5$); so $\chi_5(5)$ has order $n = 2^e$, and with $\varpi_5 := \chi_5(5)$ we get $\sigma_5 = 1$. Since $H = \ker \chi_5$ and $2 \in H$ [19, Lemma 4.1], we have $\chi_5(2) = 1 = \varpi_5^0$; the condition $2 \in H$ is the case $d = 2$ of Feit's condition that every divisor $d$ of $n$ satisfies $d^{n+1} \equiv 1 \pmod p$ (see [17, p. 175]). Apply [19, Theorem 3.4(b)] with Xia's $q$ equal to $p$, character order $n$, $r = 5$, exponent 1 for $\chi_5(5)$ and 0 for $\chi_5(2)$. With $1 + (n-1)p = n^3$ the resulting system is (11), over $\mathbb{F}_{5^{n/\gcd(1,n)}} = \mathbb{F}_{5^n}$. □

As for $r = 3$, we replace the norm equation by its sum. With $m := n/2$ and $R(s) := \sum_t y_t y_{t+s}$, we have $R(-s) = R(s)$, (L3$_5$) gives $R(s) = n(1-p)$ for $s \not\equiv m$, and (L2$_5$) gives $R(m) = n \cdot n^3 = n^4$. The *norm-free system in characteristic* 5 is (L1$_5$), (L3$_5$), $R(m) = n^4$, (L4$_5$) for $y \in \mathbb{F}_{5^n}^n$. Put

$$\kappa := n^2 p \in \mathbb{F}_5.$$

Then $\kappa = -p$ is a non-square of $\mathbb{F}_5$ and $\kappa^2 = p^2 = -1$.

7.2. **Fourier form for $r = 5$.** With $\widehat{y}(\xi) := \sum_t y_t \xi^t$ for $\xi \in \mu_n \subset \overline{\mathbb{F}}_5$, exactly as in Proposition 2.4 (now $5 \nmid n$), the norm-free system in characteristic 5 is equivalent to

$$\begin{aligned} &(\mathrm{F1}_5)\quad \widehat{y}(\xi^5) = \xi^5\, \widehat{y}(\xi)^5, \\ &(\mathrm{F3}_5)\quad \widehat{y}(\xi)\, \widehat{y}(\xi^{-1}) = \kappa\, \xi^m \quad (\xi \neq 1), \qquad \widehat{y}(1)^2 = n^2, \\ &(\mathrm{F4}_5)\quad \widehat{y}(\xi)\, \widehat{y}(-\xi) = \widehat{y}(-1)\, \widehat{y}(\xi^2). \end{aligned}$$

Indeed, (F1$_5$) is equivalent to (L1$_5$) as in Proposition 2.4, with the iterate $\widehat{y}(\xi^{5^k}) = \xi^{k5^k} \widehat{y}(\xi)^{5^k}$; for (F3$_5$), $\widehat{y}(\xi)\widehat{y}(\xi^{-1}) = \sum_s R(s)\xi^s = n(1-p)\big(n[\xi = 1] - \xi^m\big) + n^4 \xi^m$, which is $n(n^3 - 1 + p)\xi^m = \kappa \xi^m$

for $\xi \neq 1$ (as $n^3-1=(n-1)p$) and $n(1-p)(n-1)+n^4=n^2$ at $\xi=1$. Finally, ($\mathrm{F4}_5$) is equivalent to ($\mathrm{L4}_5$) by the proof for (F4), word for word, since 2 is a unit modulo 5. Also $S=\widehat{y}(-1)$.

7.3. **The norm-free system in characteristic 5.**

**Theorem 7.2.** *Let $n=2^e$ with $e$ odd, $e\geq 3$, $p=n^2+n+1$, $Q_5:=5^{n/4}$, $\xi_0\in\mathbb{F}_{5^n}$ of order $n$, and $\iota_5:=\xi_0^{n/4}$. The norm-free system in characteristic 5 has exactly $4(Q_5-1)$ solutions $y\in\mathbb{F}_{5^n}^n$, and $y\mapsto(\widehat{y}(\xi_0),S,\widehat{y}(1))$ is a bijection onto*

$$\{\theta'\in\mathbb{F}_{5^n}:\ {\theta'}^{Q_5-1}=-\iota_5\}\times\{S:\ S^2=\kappa\}\times\{n,-n\}.$$

The first set is a coset of $\mu_{Q_5-1}$ in $\mu_{4(Q_5-1)}$; it lies in $\mathbb{F}_{5^n}$, as $4(Q_5-1)$ divides $5^n-1=(Q_5-1)(Q_5+1)(Q_5^2+1)$, and it has $Q_5-1$ elements, as $x\mapsto x^{Q_5-1}$ maps $\mu_{4(Q_5-1)}$ onto $\mu_4\ni-\iota_5$. The second set lies in $\mathbb{F}_{25}$.

*Proof. Step 1 (the group $\mu_n$).* By the lifting-the-exponent lemma, $v_2(5^{n/4}-1)=v_2(4)+v_2(n/4)=e$, so $\mu_n\subset\mathbb{F}_{Q_5}$. As $(\mathbb{Z}/2^e)^\times=\{\pm1\}\times\langle 5\rangle$ with $\mathrm{ord}(5)=m/2$ and $-1\notin\langle 5\rangle$, the elements of order $n$ form two disjoint Frobenius orbits $O=\{\xi_0^{5^k}\}$ and $O^{-1}=\{\xi_0^{-5^k}\}$ ($k \bmod m/2$), exchanged by $\xi\mapsto\xi^{-1}$. Every element of order $2^j$, $1\leq j\leq e-1$, has exactly two square roots $\pm\xi$ in $\mu_n$.

*Step 2 (top layer).* Put $\theta':=\widehat{y}(\xi_0)$. It is non-zero by ($\mathrm{F3}_5$). The iterate of ($\mathrm{F1}_5$) with $k=m/2$ (so $5^k=Q_5\equiv 1 \pmod n$) gives $\theta'=\xi_0^{(n/4)Q_5}{\theta'}^{Q_5}=\iota_5\,{\theta'}^{Q_5}$, as $Q_5\equiv 1 \pmod 4$; so ${\theta'}^{Q_5-1}=-\iota_5$. Conversely, for such $\theta'$ put $\widehat{y}(\xi_0^{5^k}):=\xi_0^{k5^k}{\theta'}^{5^k}$ for $0\leq k<m/2$; ($\mathrm{F1}_5$) holds along $O$, the wrap being $\theta'=\iota_5{\theta'}^{Q_5}$. On $O^{-1}$ put $\widehat{y}(\xi^{-1}):=\kappa\xi^m/\widehat{y}(\xi)=-\kappa/\widehat{y}(\xi)$; there is no clash as $O\cap O^{-1}=\emptyset$, ($\mathrm{F3}_5$) between $O$ and $O^{-1}$ holds by definition, and ($\mathrm{F1}_5$) on $O^{-1}$ reads $-\kappa/(\xi^5\widehat{y}(\xi)^5)=\xi^{-5}(-\kappa)^5/\widehat{y}(\xi)^5$, true as $\kappa^4=1$.

*Step 3 (descent, $j=e-1,\dots,1$).* Fix $S$ with $S^2=\kappa$. For $\eta=\xi^2$ of order $2^j$ put $\widehat{y}(\eta):=\widehat{y}(\xi)\widehat{y}(-\xi)/S$ (the same for $\pm\xi$). If ($\mathrm{F1}_5$) and ($\mathrm{F3}_5$) hold on the layer above, then $\widehat{y}(\eta^5)=\widehat{y}(\xi^5)\widehat{y}(-\xi^5)/S=-\xi^{10}S^4\widehat{y}(\eta)^5$, which equals $\eta^5\widehat{y}(\eta)^5=\xi^{10}\widehat{y}(\eta)^5$ because $S^4=\kappa^2=-1$; and for $\eta\neq 1$, $\widehat{y}(\eta)\widehat{y}(\eta^{-1})=[\widehat{y}(\xi)\widehat{y}(\xi^{-1})][\widehat{y}(-\xi)\widehat{y}(-\xi^{-1})]/S^2=\kappa\xi^m\cdot\kappa(-\xi)^m/\kappa=\kappa\eta^m$. ($\mathrm{F4}_5$) at every $\xi$ of order at least 4 is the definition.

*Step 4 (bottom).* $\widehat{y}(-1)=\widehat{y}(\iota_5)\widehat{y}(-\iota_5)/S=\kappa\iota_5^m/S=\kappa/S=S$, so the $S$ of the construction is $\sum_t(-1)^t y_t$, as ($\mathrm{L4}_5$) requires. ($\mathrm{F4}_5$) at $\pm1$ is an identity; ($\mathrm{F3}_5$) at 1 gives $\widehat{y}(1)=\pm n$, and at $-1$ it gives $S^2=\kappa$; ($\mathrm{F1}_5$) holds at 1 and at $-1$, as $n^4=1$ and $S^4=-1$.

*Step 5 (count).* Every value of $\widehat{y}$ of a solution is forced by $(\theta',S,\widehat{y}(1))$: the top layer by ($\mathrm{F1}_5$) and ($\mathrm{F3}_5$), each layer of Step 3 by ($\mathrm{F4}_5$), the bottom by $S$ and $\widehat{y}(1)$. Every triple gives a solution, and $y\leftrightarrow\widehat{y}$ is a bijection. The count is $(Q_5-1)\cdot 2\cdot 2$. □

The prime 5 enters only in Step 1 (the orbits of $\langle 5\rangle$), Step 2 (the wrap constant $\iota_5$) and Step 3, where $S^4=-1$ is equivalent to $p^2\equiv -1 \pmod 5$, the same fact that makes $\sigma_5$ odd in Proposition 7.1. The proof uses only that $p\equiv\pm2 \pmod 5$ and $n=2^e\geq 8$.

**Corollary 7.3.** *A sequence $y\in\mathbb{F}_{5^n}^n$ satisfies (11) if and only if it solves the norm-free system in characteristic 5 and $\mathrm{N}_5(y_0)=n^3$, where $\mathrm{N}_5(x):=x^{1+5^{n/2}}$.*

*Proof.* ($\mathrm{L1}_5$) gives $y_{n/2}=y_0^{5^{n/2}}$, so ($\mathrm{L2}_5$) at $s=0$ is $\mathrm{N}_5(y_0)=n^3$. If (11) holds, ($\mathrm{L2}_5$) gives $R(m)=n^4$, so $y$ solves the norm-free system in characteristic 5, and $\mathrm{N}_5(y_0)=n^3$. Conversely, if $y$ solves the norm-free system in characteristic 5 and $\mathrm{N}_5(y_0)=n^3$, then ($\mathrm{L2}_5$) holds at $s=0$, and applying ($\mathrm{L1}_5$) gives it for every $s$, as $n^3\in\mathbb{F}_5$. □

So for $r=5$, deciding whether (11) has a solution comes down to one norm condition on $y_0$, compared with two conditions for $r=3$ (Section 2).

*Remark* 7.4 (one-element form). Write $y_0=\vartheta\omega$ with $\vartheta\in\mathbb{F}_{25}$, $\vartheta^2=n^3$, and $\omega$ in the norm-one torus $\mu_{5^{n/2}+1}$. Then ($\mathrm{L1}_5$)–($\mathrm{L3}_5$) say $\mathrm{Tr}_{\mathbb{F}_{5^n}/\mathbb{F}_5}(\omega^{1+5^j})=(-1)^j(p-1)$ for all $j\in\mathbb{Z}/n$, $j\neq n/2$.

7.4. **The norm-free system in characteristic $r$.** Let $n = 2^a n_{\mathrm{odd}}$ with $a \geq 3$ and $n_{\mathrm{odd}}$ odd ($3 \mid n$ is allowed when $r \neq 3$), $m = n/2$, $p := n^2 + n + 1$, and let $r$ be a prime with $r \nmid pn$; the layers and $\mathcal{L}_a$ are as in Section 4, now in an algebraic closure of $\mathbb{F}_r$. In Theorem 7.5 below, $n$, $p$ and the integer $\sigma_r$ are parameters: no plane is assumed. If a non-Desarguesian flag-transitive plane of order $n$ exists, let $\chi_r$ be an $r$-adic character of order $n$ on $\mathbb{F}_p$ and write $\chi_r(r) = \varpi_r^{\sigma_r}$ for a primitive $n$-th root of unity $\varpi_r$. Then [19, Theorem 3.4(b)] with $\chi_r(2) = 1$ gives, exactly as in the proof of Proposition 7.1, elements $y_0, \dots, y_{n-1}$ of $\mathbb{F}_{r^{n/g}}$, $g = \gcd(\sigma_r, n)$, with

$$(\mathrm{L1}_r)\ y_{s+\sigma_r} = y_s^r, \quad (\mathrm{L2}_r)\ y_s y_{s+m} = n^3, \quad (\mathrm{L3}_r)\ \textstyle\sum_t y_t y_{s+t} = n(1-p), \quad (\mathrm{L4}_r)\ \text{as } (\mathrm{L4}_5).$$

For $r = 3$ this is (1); for $r = 5$ and $n = 2^e$ it is (11). As for $r = 5$, $(\mathrm{L2}_r)$ gives $R(m) = n^4$. For any integer $\sigma_r$ and $g = \gcd(\sigma_r, n)$, the *norm-free system in characteristic* $r$ is $(\mathrm{L1}_r)$, $(\mathrm{L3}_r)$, $R(m) = n^4$, $(\mathrm{L4}_r)$ for $y \in \mathbb{F}_{r^{n/g}}^n$. With $\kappa := n^2 p \in \mathbb{F}_r$, this system is equivalent to $(\mathrm{F1}_r)$ $\widehat{y}(\xi^r) = \xi^{r\sigma_r}\widehat{y}(\xi)^r$, $(\mathrm{F3}_r)$ $\widehat{y}(\xi)\widehat{y}(\xi^{-1}) = \kappa\xi^m$ ($\xi \neq 1$), $\widehat{y}(1)^2 = n^2$, and $(\mathrm{F4}_r)$ $\widehat{y}(\xi)\widehat{y}(-\xi) = \widehat{y}(-1)\widehat{y}(\xi^2)$, by the computation of the Fourier form for $r = 5$ above with 5 replaced by $r$ (and $\sigma_5 = 1$ by $\sigma_r$). $(\mathrm{F3}_r)$ at $-1$ gives $S^2 = \kappa$.

**Theorem 7.5.** *Let $n = 2^a n_{\mathrm{odd}}$ with $a \geq 3$, let $r$ be a prime with $r \nmid pn$ and $r \not\equiv -1 \pmod{2^a}$, and let $\sigma_r$ be any integer. The orbits of $\xi \mapsto \xi^r$ on $\mathcal{L}_a$ come in pairs $\{O, O^{-1}\}$ with $O \neq O^{-1}$; for each pair $i \in I_r$ let $L_i$ be the common length of $O$ and $O^{-1}$, so that $\sum_i L_i = n/4$.*

(i) *If $(-1)^{\sigma_r} \neq (p/r)$, the norm-free system in characteristic $r$ has no solution.*
(ii) *If $(-1)^{\sigma_r} = (p/r)$, it has exactly $4\prod_{i\in I_r}(r^{L_i} - 1)$ solutions.*

For $r = 3$ and $\sigma_r$ a divisor of $n$, this is Theorem 4.1 with Proposition 4.3 ($\kappa = 1$ and $(p/3) = 1$ when $n \equiv 2 \pmod 3$, so case (ii) is the case of even $\sigma$); for $r = 5$ and $n = 2^e$, $e$ odd, there is one pair, of length $n/4$, and the count is the $4(Q_5 - 1)$ of Theorem 7.2.

**Corollary 7.6.** *Let $p$ be prime, as it is when a non-Desarguesian flag-transitive plane of order $n$ exists. For every prime $r \nmid pn$, Xia's shift $\sigma_r$ satisfies $(-1)^{\sigma_r} = \big((-1)^{n/2}p/r\big) = (p/r)$ by* [19, Lemma 3.5]*. The argument for other primes in the introduction shows that this needs only that $p$ is prime. Thus the sign condition of Theorem 7.5(ii) and of Proposition 7.7 holds. Hence the norm-free system in characteristic $r$ is solvable for every $r \not\equiv -1 \pmod{2^a}$, and, by Proposition 7.7, for every $r$ when $n = 2^a$. As this system is $(L1_r)$–$(L4_r)$ with its norm equation $(L2_r)$ replaced by the single consequence $R(m) = n^4$, no argument built on one such system without its norm equation can exclude a plane.*

*Proof of Theorem 7.5.* We follow the proof of Theorem 4.1 with 3 replaced by $r$, and list the changes.

*Step 1.* For $a \geq 3$, $-1 \in \langle r\rangle \bmod 2^a$ only if $r \equiv -1 \pmod{2^a}$: write $r = \varepsilon 5^c$ in $(\mathbb{Z}/2^a)^\times = \{\pm 1\} \times \langle 5\rangle$; $r^k = -1$ forces $k$ odd and $2^{a-2} \mid ck$, so $2^{a-2} \mid c$ and $r = \varepsilon = -1$. Hence no top orbit is self-inverse.

*Step 2.* On an orbit of length $L$, $(\mathrm{F1}_r)$ gives $\widehat{y}(\rho^{r^k}) = \rho^{\sigma_r k r^k}\widehat{y}(\rho)^{r^k}$ and the wrap $\widehat{y}(\rho)^{r^L-1} = \rho^{-\sigma_r L r^L}$: $r^L - 1$ choices; $(\mathrm{F3}_r)$ defines $\widehat{y}$ on $O^{-1}$, and $(\mathrm{F1}_r)$ holds there as $\kappa^r = \kappa$.

*Step 3.* For $\xi$ in layer $j$, $1 \leq j \leq a-1$, put $\widehat{y}(\xi) := S^{-1}\widehat{y}(\eta)\widehat{y}(-\eta)$ ($\eta^2 = \xi$). On the layer below, $(\mathrm{F1}_r)$ becomes $\widehat{y}(\xi^r) = (-1)^{\sigma_r} S^{r-1}\xi^{r\sigma_r}\widehat{y}(\xi)^r$, and $S^{r-1} = \kappa^{(r-1)/2} = (\kappa/r) = (p/r)$ by Euler's criterion, for both roots $S$. So the descent closes if and only if $(-1)^{\sigma_r} = (p/r)$; otherwise the forced values give $\widehat{y}(\xi^r) = -\widehat{y}(\xi^r)$ at layer $a-1$, so $\widehat{y}(\xi^r) = 0$, contradicting $(\mathrm{F3}_r)$. This proves (i). $(\mathrm{F3}_r)$ passes down as $S^{-2}\kappa\eta^m \cdot \kappa(-\eta)^m = \kappa\xi^m$, and $\widehat{y}(-1) = S$ is consistent, as in Step 3 of the proof of Theorem 4.1: now $\prod_{\zeta\in\Xi_a}\widehat{y}(\zeta) = (-\kappa)^{2^{a-2}} = S^{2^{a-1}}$; $(\mathrm{F1}_r)$ at $-1$ is again $(-1)^{\sigma_r}S^{r-1} = 1$, which is, in Fourier form, the argument by which Xia proves [19, Lemma 3.5].

*Step 4.* (E1) reads $f(\alpha^2) = P(\alpha)f(\alpha)$ with $P(\alpha) := S^{-1}\widehat{y}(-\alpha) = \kappa^{-2^{a-2}}\prod\widehat{y}(\rho)$, the product over $\rho \in \mathcal{L}_a$ with $\rho^{2^{a-1}} = -\alpha$; it does not depend on $S$. Further $f(1) = \pm n$, (E2) $f(\alpha^r) = \alpha^{r\sigma_r}f(\alpha)^r$, (E3) $f(\alpha)f(\alpha^{-1}) = \kappa\alpha^m$, and $P(\alpha^r) = \alpha^{r\sigma_r}P(\alpha)^r$, $P(\alpha)P(\alpha^{-1}) = \alpha^m$.

*Step 5.* The group $G$ is defined with $r$ in place of 3; $\kappa$ cancels in $\tau f/f$, and on a self-inverse orbit one takes a root of $f(\alpha)^{1+r^h} = \kappa\alpha^{m-\sigma_r h r^h}$.

*Steps 6 and 7* involve no constant and no $\sigma_r$ and go through word for word; in the homogeneous descent $\lambda(\xi^r) = s_0^{r-1}\lambda(\xi)^r = \lambda(\xi)^r$ for both $s_0 = \lambda(-1) = \pm 1$, as $r-1$ is even. □

**Proposition 7.7** ($r \equiv -1 \pmod{2^a}$)**.** *Let $n = 2^a$ with $a \geq 3$, let $r$ be a prime with $r \nmid p$ and $r \equiv -1 \pmod{2^a}$, and let $\sigma_r$ be any integer. If $(-1)^{\sigma_r} \neq (p/r)$, the norm-free system in characteristic $r$ has no solution; if $(-1)^{\sigma_r} = (p/r)$, it has exactly $4(r+1)^{n/4}$ solutions.*

*Proof.* Every top orbit is $\{\rho, \rho^{-1}\}$, as $\rho^r = \rho^{-1}$; (F1$_r$) at $\rho$ and (F3$_r$) give $\widehat{y}(\rho)^{1+r} = \kappa\rho^{m-r\sigma_r}$, with $r+1$ roots, and (F1$_r$) at $\rho^{-1}$ (the wrap) follows as $\rho^{m(r-1)} = 1$. Step 3 of the proof of Theorem 7.5 does not use Step 1, so the first claim follows as in that proof. In the second case layers $a-1, \dots, 1$ are determined by the $n/4$ top orbits and by $S$, with $S^2 = \kappa$, and layer 0 is $\{1\}$, where $\widehat{y}(1) = \pm n$. So there are $(r+1)^{n/4} \cdot 2 \cdot 2$ solutions. □

For $r \equiv -1 \pmod{2^a}$ and $n_{\mathrm{odd}} > 1$ we make no claim.

*Remark* 7.8. The computations for Theorems 7.2 and 7.5 are in Section 8.4. For Theorem 7.2, at $n = 8$ two programs find the $96 = 4(5^2-1)$ norm-free points and the 16 with (L2$_5$); at $n = 32$ none of the $4(5^8-1)$ points satisfies (L2$_5$).

## 8. Computations

All computations below are exact. Each program implements its own finite-field arithmetic or uses a library (PARI/GP, python-flint, Singular or msolve), runs on one thread, and checks itself on known cases before the main run. A computational result is used in a proof only when two independently written programs agree; a result from one program is reported as such, mostly in remarks, and no proof uses it. Table 8 lists the programs and logs with the MD5 checksums of the original files. They are in the archive of programs that accompanies this paper, from which header lines and machine-specific paths were removed; its README gives the checksum of each published copy.

8.1. **Xia's system at $\sigma = 2$.** *The fibre solver (S).* By Proposition 2.4 and Theorem 5.1(c), every point of NF($n$) lies in the fibre of its $\nu$-data, $S$ and $f$. The solver takes one choice of top data for each $\nu$-datum, both signs $S$, and every solution $f$ of (E1)–(E3) on layer 0 (found from the cycle relations of $\langle 2, 3, -1\rangle$ on $\mu_{n_{\mathrm{odd}}}$, then re-checked); the lower layers give $y_0^+$ and $y_1^+$. By (L2), $(y_j^-)^2 = (y_j^+)^2 + 1$ with $\overline{y_j^-} = -y_j^-$, which leaves at most two values of each $y_j^-$, so at most four candidates $(y_0, y_1)$ per fibre. As (L1) gives $y_{2j} = \phi^j(y_0)$ and $y_{2j+1} = \phi^j(y_1)$, each candidate determines $y$, and it is tested on all of (1) in the time domain. So every solution is found, in the fibre of its own data, and everything reported is a solution. Exhaustiveness uses Proposition 2.4, (L2) and the part of Theorem 5.1(c) which says that the values of $\widehat{y}$ on $\mu_m$ depend only on the $\nu$-data, $S$ and $f$. The counts of Theorems 4.1 and 5.1 only predict the number of fibres, which serves as a check. For $n = 104$ the run is reduced by the shift $y_t \mapsto y_{t+1}$ and by $y \mapsto -y$: both preserve (1), and every orbit of fibres under them meets the fibres enumerated.

*The other programs.* (B) enumerates all $y$ in the time domain ($n = 8$). (E) enumerates all solutions of (L1)–(L3) at $\sigma = 2$ exhaustively and then tests (L4) ($n = 32$, 56). (F) enumerates every point of every fibre of NF($n$) and tests (L2) ($n = 8$, 32, 56). (X) and (X′) are two exhaustive searches for the solutions of (L1)–(L3) in the form $y_j = i\omega_j$ with $\mathrm{N}(\omega_j) = 1$, over classes under the Frobenius and $-1$ ($n = 80$; (X′) also at $n = 8$, 32, 56). (Q) is the program of Section 8.2. (Q′), written independently, makes the same reduction as (Q) at $n = 128$ (one $\nu$ in each orbit, $S = 1$, both values of $\widehat{y}(1)$: 2690420 fibres) and decides in each fibre whether it contains a point of the norm-free system with $\mathrm{N}(y_0) = -1$.

TABLE 5. Xia's system (1) at $\sigma = 2$. Blocks as in Section 5. "Fibres" and "candidates" are those of (S); the number of fibres equals $|\mathrm{NF}(n)|/\Phi$ (for $n = 104$, divided by the orbit size 104).

| $n$ | blocks | fibres | candidates | solutions | programs |
|---|---|---|---|---|---|
| 8 | B | 16 | 32 | 16 | (S), (B), (F) |
| 32 | A | 320 | 256 | 0 | (S), (E), (F); Xia [19, Section 5] |
| 56 | B, B, B | 12544 | 12992 | 0 | (S), (E), (F) |
| 80 | C, A, C | 204800 | 189440 | 0 | (S), (X), (X′) |
| 104 | B, C, C | 81536 | 81240 | 0 | (S) |
| 128 | A | – | – | 0 | (Q), (Q′) |

At $n = 8$ the 16 solutions are the 8 that Xia's construction gives for $\mathrm{PG}(2, 8)$ and their negatives (a direct check, Table 8), two in each of 8 fibres; this is a positive control for (S), (B) and (F). At $n = 32$ and 56, (E) finds 128 and 224 solutions of (L1)–(L3), all with $y_0 = \pm i$ or $y_1 = \pm i$, and none passes (L4); at $n = 56$, (F) runs through all 16959488 points of NF(56) in all 12544 fibres and none has $\mathrm{N}(y_0) = \mathrm{N}(y_1) = -1$. At $n = 80$, (X) and (X′) both find that (L1)–(L3) alone have no solution. In particular Claim C (Definition 6.1) holds at $n = 8$, 32, 56 and 80: (X′) finds 32, 128 and 224 solutions of (L1)–(L3) at $n = 8$, 32, 56, and (E) finds the same 128 and 224 at $n = 32$ and 56, all with $y_0 = \pm i$ or $y_1 = \pm i$ (at $n = 8$ by a direct check of all 32, Table 8), and at $n = 80$ there are none. So (1) with $\sigma = 2$ has no solution for $n = 32$, 56 and 80, by at least three programs each, and for $n = 128$ by two: (Q) finds no point of the norm-free system with $\mathrm{N}(y_0) \in \mu_{128}$ and (Q′) none with $\mathrm{N}(y_0) = -1$, while a solution would be a point of both kinds, since $-1 \in \mu_{128}$. As noted in the introduction, these are statements about Xia's system, not new results on planes. Other even $\sigma$: (B) gives no solution at $n = 8$ for $\sigma = 4$, 8; for $n = 56$, 80 and 104, two other independent programs treat $\sigma = 14, 28$, $\sigma = 10, 20, 40$ and $\sigma = 26, 52$, respectively (Remark 9.24), and $\sigma = 4$, 8 (and $\sigma = 16$ for $n = 80$) were not computed.

*Remark* 8.1. By one program: at $n = 104$, the reduced run of (S) finds no solution of (1) with $\sigma = 2$ (Table 5).

8.2. **Question P.** Question 11.1 asks whether $\mathrm{N}(y_0) \notin \mu_n$ for every solution of the norm-free system when $n = 2^e$ with $e \geq 5$ odd. *The program (Q).* Let $n = 2^e$. By Theorem 3.5(c), $y_0$ depends only on $(\nu, S, \widehat{y}(1), \theta_+)$. The shift $y_t \mapsto y_{t+2}$ is the Frobenius by (L1), so it preserves the event $\mathrm{N}(y_0) \in \mu_n$; on $\nu$ it acts as $\nu \mapsto \xi_0^{-4}\nu$ (by Remark 3.7 and (2)), with orbits of size $n/4$. So (Q) takes one $\nu$ in each orbit, that is $(q-1)/32 = 1345210$ values at $n = 128$ ($q = 3^{16}$), with $S = 1$ (by $y \mapsto -y$) and both values of $\widehat{y}(1)$. In a fibre $y_0^+$ is fixed and $y_0^- = n^{-1}\Lambda_\nu(-\theta_+)$ is $\mathbb{F}_3$-linear in $\theta_+ \in V_+$, a line over $\mathbb{F}_q$; (Q) decides whether some $\theta_+$ on the conic gives $\mathrm{N}(y_0) \in \mu_n$, and re-checks every hit with the full construction of Theorem 3.1 and the inverse Fourier transform. The run at $n = 128$ was made in two parts with the same program. The first run was stopped after the representative $\nu$ number 1029999 (its last progress line), and the second covered $1030000, \ldots, 1345209$. There are no hits.

*Exact counts at* $n = 16$ *and* 32. The norm-free system has 320 solutions at $n = 16$ and 26240 at $n = 32$. Among them, $y_0 \in k_0$ exactly when $\theta \in V_-$ and $y_1 \in k_0$ exactly when $\theta \in V_+$ (32 solutions each at $n = 16$, 320 each at $n = 32$), and never both (Theorem 3.5(d)). At $n = 32$ no solution has $\mathrm{N}(y_0)$ or $\mathrm{N}(y_1)$ in $\mu_{32}$. The relation $\mathrm{Tr}_{k_0/\mathbb{F}_3}\mathrm{N}(y_0) + \mathrm{Tr}_{k_0/\mathbb{F}_3}\mathrm{N}(y_1) = -1$, which follows from $R(m) = 1$, holds for every solution.

*Sampling.* We sample uniform random points of the norm-free system ($\theta = \theta_0\,\mathrm{N}(z)$ with $\theta_0$ one fixed parameter and $z$ uniform) and record the components of $\mathrm{N}(y_0)$ in the factors $d_j = (3^{2^j} + 1)/2$ of the odd part of $|k_0^\times|$ (Table 6; "trivial" means that the component is 1). At $n = 32$ the sample reproduces the exact census, a control. At $n = 64$ and 128 every level is trivial at the rate of a

uniform element of $k_0^\times$, and so is every pair of levels within sampling error (the largest deviation is the pair $(41, 3281)$ at $n = 128$: 54 against 74.3 in $10^7$ samples, $z = (54 - 74.3)/\sqrt{74.3} = -2.4$). The top level $d = 21523361$ at $n = 128$ is trivial with probability $1/21523361$, so sampling cannot test it (0 against 0.5 expected in $10^7$ samples).

TABLE 6. Sampling of $\mathrm{N}(y_0)$: number of samples with the component at level $d$ trivial, against the expected number (for $n = 32$: the exact census rate; otherwise a uniform element of $k_0^\times$).

| $n$ | samples | $d = 5$ | $d = 41$ | $d = 3281$ | $\mathrm{N}(y_0) \in \mu_n$ |
|---|---|---|---|---|---|
| 32 | $10^5$ | 20344 / 20366 | 3014 / 2927 | – | 0 / 0 |
| 64 | $10^6$ | 200133 / 200000 | 24134 / 24390.2 | 318 / 304.8 | 3 / 1.49 |
| 128 | $10^5$ | 19804 / 20000 | 2383 / 2439.0 | 27 / 30.5 | 0 / 0.00 |
| 128 | $10^7$ | 2000129 / 2000000 | 244081 / 243902.4 | 3055 / 3047.9 | 0 / 0.00 |

*Joint law of* $\mathrm{N}(y_0)$ *and* $\mathrm{N}(y_1)$. For small $n$ the two norm tests are not independent. Below, $z$ is the signed square root of Pearson's $\chi^2$ statistic of the $2 \times 2$ table of the samples (level trivial for both norms, for $y_0$ only, for $y_1$ only, for neither). At $n = 32$ (exact) the level 41 is trivial for both norms in 128 solutions, against 22.5 if the two were independent with the observed marginals, and the level 5 in 768 against 1088.4. At $n = 64$ ($10^6$ samples) the level 41 is trivial for both in 700 samples against 585.2 ($z = 4.9$), while the level 5 is at chance (40321 against 40081.8). At $n = 128$ ($10^6$ samples) both are within sampling error: the level 41 in 628 samples against 595.1 ($z = 1.4$), the level 5 in 40209 against 39973.1 ($z = 1.5$). So the dependence fades as $n$ grows (for the level 41 the ratio to independence is 5.7, 1.20 and 1.06 at $n = 32$, 64, 128). The relation of the traces held in every sample.

8.3. **Checks of the theorems.** *Theorem 4.1.* A PARI/GP program that uses none of the proof (discrete logarithms, congruences solved by Hermite normal form) gives the count of Theorem 4.1 for all 34 values $n \le 400$ with $8 \mid n$, $3 \nmid n$ at $\sigma = 2$, and for every even $\sigma$ at the 18 values $n \le 208$; for odd $\sigma$ it gives 0 at $n = 40$. Two further programs evaluate the formula, one independently and one by a Smith normal form ($n = 40$, 56, 80, 88). A count of every solution by (F) agrees at $n = 32$ for $\sigma = 4$, 8, 16, 32 and at $n = 40$, every solution checked in the time domain, and at $n = 56$ (the run of (F) above; every 8000th solution checked in the time domain).

*Theorem 3.5.* (Q) in test mode checks at $n = 16$, 32, 64, 128 that $T^2 = \mathrm{id}$, that $T$ preserves $\nu$, that $y_0(T\theta) = y_0(\theta)$ and $y_1(T\theta) = \overline{y_1(\theta)}$ (with $y_0$, $y_1$ from the full construction), and that the kernel of $x \mapsto n^{-1}\Lambda_\nu(x + Tx)$ is $V_-$ in every fibre tested.

*Theorem 5.1.* Two programs. A spot check verifies at $n = 8$, 32, 40, 56, 80 (all three cases; at $n = 56$ in $\mathbb{F}_{3^{84}}$) that each $V_O$ has dimension $L$, that $\delta_O \in \mathbb{F}_{q_O}$, that $T$ is an involution preserving the $\nu$-data, that (P1) and (P2) hold, and that $\ker \mathcal{Y}_0 = V_-$ and $\ker \mathcal{Y}_1 = V_+$ exactly, with a negative control for each block type. The program (F) checks at $n = 8$, 16, 32, 40, 56 (every fibre) and at 20 sampled fibres at $n = 80$ that every fibre has $\Phi$ points and that $y_0^-$ is an injective function of $v_+$ and $y_1^-$ of $v_-$.

8.4. **Other primes.** *Theorem 7.2 at* $n = 8$. Two programs. (R) builds the norm-free $r = 5$ solutions from the parameters of Theorem 7.2 and checks every one of them in the time domain: there are $96 = 4(5^2 - 1)$, and exactly 16 of them satisfy ($\mathrm{L2}_5$). (R′) enumerates all $5^8 = 390625$ elements $y_0$ of $\mathbb{F}_{5^8}$ with its own field arithmetic: exactly 96 give a solution of the norm-free system, exactly the 96 points of the construction, which (R′) builds again and compares, and 16 satisfy ($\mathrm{L2}_5$); a negative control (the wrong root of the parameter equation) fails on all 96. A third check, a brute force over the norm coset $\{y_0 : \mathrm{N}_5(y_0) = n^3\}$ (626 elements) in the form of Remark 7.4 (which uses ($\mathrm{L1}_5$)–($\mathrm{L3}_5$) only), also finds exactly 16 elements.

*Remark* 8.2. One program each. At $n = 16$ (outside the scope of Theorem 7.2, as $e$ is even) (R′) builds $2496 = 4(5^4 - 1)$ norm-free solutions by the construction of Theorem 7.2 and checks each in the time domain; none satisfies (L2$_5$). At $n = 32$ (formal: $p = 1057 = 7 \cdot 151$ is not prime) (R) builds all $4(5^8 - 1) = 1562496$ points, checks 120 of them in the time domain, and finds none with (L2$_5$), as expected for about $4 \cdot 5^8$ points against one norm condition in $\mathbb{F}_{5^{16}}$.

*Theorem 7.5.* An exact congruence count (r-count) writes every value as a power of a generator of $\mu_N$, $N = (r^L - 1)n$ with $L = \mathrm{ord}_n(r)$, so that (F1$_r$), (F3$_r$) and (F4$_r$) become linear congruences modulo $N$, and counts their solutions; it uses none of the proof. For $n \in \{8, 16, 32, 40, 56, 64, 80, 88, 104\}$, the primes $r \le 23$ with $r \nmid pn$ (58 pairs) and every divisor $\sigma_r$ of $n$ (411 cases), it gives the count of Theorem 7.5 in the 211 cases with $(-1)^{\sigma_r} = (p/r)$ (for the 8 pairs with $r \equiv -1 \pmod{2^a}$, the count of Remark 8.3) and 0 in the other 200. Program (F), with its own field arithmetic and every point checked in the time domain, gives the same exact counts at $n = 8$ for $r = 5, 7, 11, 13, 19, 37$ and every $\sigma_r \mid 8$, and at $n = 16$ for $r = 5$ and 11; a search over all of $\mathbb{F}_{5^8}$ and of $\mathbb{F}_{7^8}$ without any Fourier step finds 96 and 256 solutions, the lists of Theorem 7.2 and of Proposition 7.7. For $n_{\mathrm{odd}} > 1$, (F) takes 20000 random top data at $n = 40$ ($r = 11$, 13) and 5000 at $n = 56$ ($r = 5$) and extends each in every way: the mean numbers of extensions are 3.987, 4.001 and 4.051, against 4, and in two runs of 2000 top data with the wrong parity none extends. A Smith-form computation of the homogeneous group (the analogue of $K_n$), for 82 of the 91 pairs $(n, r)$ with $8 \mid n \le 88$, $r \le 31$, $r \nmid pn$ (all but $r \in \{19, 29\}$ with $n \ge 56$), gives $4\prod(r^{L_i} - 1)$ in the 64 pairs with $r \not\equiv -1 \pmod{2^a}$ and the formula of Remark 8.3 in the other 18.

*Remark* 8.3. For $r \equiv -1 \pmod{2^a}$ the congruence count equals $4\prod(r^{L_i} - 1)\prod(r^{L_j/2} + 1)$, over the pairs and the self-inverse top orbits, in all 8 pairs $(n, r)$ of the survey, also for $n_{\mathrm{odd}} > 1$, where Proposition 7.7 makes no claim; a direct time-domain search at $n = 8$, $r = 7$ finds $256 = 4 \cdot 8^2$ solutions for $\sigma_7 = 1$ and for $\sigma_7 = 3$.

8.5. **The orders $2^{3^j}$.** Let $n = 2^e$ and $p = 4^e + 2^e + 1$ as in the introduction. If $p$ is prime, then $e$ is a power of 3: $p = (2^{3e} - 1)/(2^e - 1)$ is the product of the $\Phi_d(2)$ over the $d \mid 3e$ with $d \nmid e$, every factor exceeds 1, and if $e = 3^j r$ with $r > 1$ and $3 \nmid r$, both $d = 3^{j+1}$ and $d = 3^{j+1}r$ occur. Conversely, for $e = 3^j$ we have $3^{j+1} \parallel 2^e + 1$ (lifting the exponent), so $3e \mid n + 1$, and $2^{n+1} \equiv 1 \pmod{p}$ because $p \mid 2^{3e} - 1$. For $e = 3^j$ the number $p$ is $\Phi_{3^{j+1}}(2)$, and it is prime for $j = 0$, 1, 2 ($p = 7$, 73, 262657). Every prime factor $q$ of $\Phi_{3^{j+1}}(2)$ has $\mathrm{ord}_q(2) = 3^{j+1}$, so $q \equiv 1 \pmod{2 \cdot 3^{j+1}}$, and each factor is a certificate that one can check by hand: $q \mid p$ if and only if $2^{3^{j+1}} \equiv 1$ and $2^{3^j} \not\equiv 1 \pmod{q}$.

For $3 \le j \le 9$ two programs show that $p$ is composite. Program (D) divides $p$ by the primes $q \le 10^8$ of this form and tests $3^{p-1}$ and $5^{p-1}$ modulo $p$; program (D′) tests $3^{p-1}$ modulo $p$. For $j = 8$ there is no factor $q \le 10^8$; there $3^{p-1} \not\equiv 1 \pmod{p}$ (both programs) and $5^{p-1} \not\equiv 1 \pmod{p}$ ((D)), and either one proves that $p$ is composite.

For larger $j$ we use the table of Alpern [1], which lists prime factors of $4^{3^j} + 2^{3^j} + 1$ (it writes $n$ for our $j$) from several contributors, for 96 exponents $j \le 8757$. It agrees with (D) for $3 \le j \le 9$. We do not rely on the table: program (D″) recomputes each of its 122 factors $q$ and checks that $a = 2^{3^j} \bmod q$ satisfies $a^2 + a + 1 \equiv 0 \pmod{q}$, and for $j \le 16$ also that $q$ divides $p$ computed in full; all 122 pass. Program (P) searches, for $10 \le j \le 16$, the primes $q = 2 \cdot 3^{j+1}h + 1$ with $h \le 10^8$ in increasing order; it finds exactly the factors of Table 7 for $j = 11$, 12, 14, 16, which are therefore the smallest prime factors of $p$, and none for $j = 10$, 13, 15. Table 7 gives one prime factor for each $j$ with $3 \le j \le 16$, $j \ne 15$. So $p$ is composite for $3 \le j \le 14$, for $j = 16$, and for many larger $j$. The smallest open case is $j = 15$: there $p$ has 8638903 digits, [1] reports no factor $c \cdot 3^{16} + 1$ with $c \le 2 \cdot 10^{11}$ ((P): none with $c \le 2 \cdot 10^8$), and a Fermat test is beyond our means (one squaring modulo $p$ takes about one second, and $2.9 \cdot 10^7$ of them are needed). This gives the

bound $n \geq 2^{3^{15}} = 2^{14348907}$ stated in the introduction. The open exponents do not form an interval: among $j \leq 40$ they are $j = 15$, 18, 20, 22, 24, 25, 27, 28, 31, 32, 35, 36, 37, 38, 40.

TABLE 7. $p = 4^e + 2^e + 1 = \Phi_{3^{j+1}}(2)$ for $e = 3^j$. For $j \leq 9$, $q$ is the smallest prime factor of $p$ ((D); for $j = 8$, (D″) checks that no $q \equiv 1 \pmod{2 \cdot 3^9}$ below 141560137 divides $p$). For $j \geq 10$, $q$ is the smallest factor listed in [1]; (D″) re-checks it and proves it prime, and (P) shows that it is the smallest prime factor of $p$ for $j = 11$, 12, 14, 16.

| $j$ | $e$ | digits of $p$ | prime factor $q$ |
|---|---|---|---|
| 3 | 27 | 17 | 2593 ($p = 2593 \cdot 71119 \cdot 97685839$ [17]) |
| 4 | 81 | 49 | 487 |
| 5 | 243 | 147 | 80191 |
| 6 | 729 | 439 | 39367 |
| 7 | 2187 | 1317 | 209953 |
| 8 | 6561 | 3951 | 141560137 [1] (none $\leq 10^8$ by (D)) |
| 9 | 19683 | 11851 | 472393 |
| 10 | 59049 | 35552 | 10939874335459407703 |
| 11 | 177147 | 106654 | 88219207 |
| 12 | 531441 | 319960 | 4361981634559 |
| 13 | 1594323 | 959879 | 168354963224856703 |
| 14 | 4782969 | 2879635 | 258280327 |
| 15 | 14348907 | 8638903 | none known (open) |
| 16 | 43046721 | 25916709 | 3357644239 |

8.6. **Beyond the search of Thas and Zagier.** Thas and Zagier searched all even $n < 5 \cdot 10^9$, and then all $n \equiv 8 \pmod{24}$ with $n < 2 \cdot 10^{11}$, for $2^{n+1} \equiv 1 \pmod{n^2 + n + 1}$. In the class 8 (mod 24) they found only $n = 8$, 512 and 134217728 [17, Appendix]. We continued the search.

**Proposition 8.4** (one program, with an independent partial check)**.** *Let $n \equiv 8 \pmod{24}$ with $2 \cdot 10^{11} \leq n < 10^{14}$, and suppose that $p = n^2 + n + 1$ has no prime factor $\ell \leq 2^{22}$. Then $2^{n+1} \not\equiv 1 \pmod{p}$. Hence a non-Desarguesian flag-transitive projective plane has order $n \geq 10^{14}$.*

The second sentence follows from the first: for such a plane, $p$ is prime, $2^{n+1} \equiv 1 \pmod{p}$, $n \equiv 8 \pmod{24}$ and $n \geq 2 \cdot 10^{11}$ (Section 1), and $p > 4 \cdot 10^{22}$ has no prime factor $\ell \leq 2^{22}$.

*Method.* A prime $\ell \neq 3$ divides some $n^2 + n + 1$ only if $\ell \equiv 1 \pmod 3$, and $3 \nmid p$ because $n \equiv 2 \pmod 3$. For each of the 147867 primes $\ell \equiv 1 \pmod 3$ with $\ell < 2^{22}$, a segmented sieve removes the $n$ with $n^2 + n + 1 \equiv 0 \pmod{\ell}$. For every remaining $n$ the program (T) computes $2^{n+1} \bmod p$ by left-to-right binary exponentiation in two-word Montgomery arithmetic ($p < 2^{94}$). The range contains 4158333333334 values $n \equiv 8 \pmod{24}$; 514761666018 of them survive the sieve, and none of these satisfies $2^{n+1} \equiv 1 \pmod p$. The logs have one line per block of at most $10^8$ consecutive values $n \equiv 8 \pmod{24}$, with the number of values, of survivors and of solutions, and as a checksum the sum modulo $2^{64}$ of the residues $2^{n+1} \bmod p$ over the survivors.

*Checks.* (i) Without the sieve, on $8 \leq n < 5 \cdot 10^9$, program (T) finds exactly $n = 8$, 512, 134217728 among 208333333 values: the hits of the first stage of Thas and Zagier that lie in the class 8 mod 24. (ii) With the sieve, on $70000 \leq n < 5 \cdot 10^9$ (so that $p$ exceeds every sieve prime), it finds none among 208330416 values; in particular $n = 134217728$ is removed, as $2593 \mid p$. (iii) An independent program (T′) checked that the blocks of the logs cover the range exactly once, that the counts add up and that no solution is reported, and recomputed 176 blocks in full with its own sieve and exact arithmetic (the first, the last and 20 random blocks of each of the eight log files), with the same counts and checksums.

TABLE 8. Programs and logs (MD5 of the original files).

| program | file (MD5) | logs (MD5) |
|---|---|---|
| (S) PARI/GP | `xia12_solver.gp` (6104a6fd), driver (57f89079) | $n = 8$: 2be9a561; 32: 587e704f; 56: 9b4178bc; 80: 0d6ea21d, aea77d44 (reduced); 104: 3d1a9d7f (reduced) |
| (Q) C | `questionP.c` v0.10 (15d3b0f0) same, v0.30–v0.60 (final 80f51060; each version keeps the earlier modes) | $n = 128$: 90dc1157, 074aba09 census b54c9f42; joint 4af66f26, 80b55cd5, 9fdbb9c8; samples d884ee6f, 959df6e5, f2776185, 4d9ab36b |
| (Q′) C | `xia_fibre_independent.c` v0.20 (56125e27) | $n = 128$: c3400e59; controls 092284bc |
| (B) Python | `xia12_bruteforce.py` v0.11 (9626acae) | fb3665b0 |
| $n = 8$, direct check, Python | `n8_direct.py` v0.10 (72931237) | 7e2beac2 |
| (E) Python | `xia12_sigma2_count.py` v0.11 (3ccd7c19) | $n = 32$: ee21b6b6 |
| | `xia12_sigma2_big.py` v0.11 (8921db0e) | $n = 56$: 7a7cdb5f |
| (F) C | `fibre_count` v0.71 (binary 51dff7ee), v0.91 (binary b8c754dc) | $n = 8$, 16: a8868a10; 32: 78730199; 40: 0971d375; 56: 4b659b79; 80 (sample): a1f7cbaa |
| (X) C | `omega_search_a.c` v0.10 (c68c0f9e), v0.20 (46e0ae0e) | 359ffcea, 49366c7a |
| (X′) C | `omega_search_b.c` v0.20 (f53c9bee) | $n = 80$: b2f91e16; $n = 8$, 32, 56: 24eb5def |
| count, PARI/GP | `normfree_count.gp` v0.30 (d723fa83) | 086d262d, 6bfe8d45 |
| formula, Python | `normfree_formula.py` (7ea89dff) | 92aeed16 |
| Smith form, Python | `normfree_smith.py` (ba5efc10) | 68fe5e26 |
| time domain, C | `fibre_count` v0.71 | 4bb17000, bc064974 |
| spot check, Python | `decoupling_spot.py` v0.40 (64f3257e) | 787b1e6e |
| (R) Python | `r5_torsor.py` (3835d02c); `r5_shadow.py` (0ea5a43b) | $n = 8$: db193532, 6f8c30c4; 32: 9ff62472 |
| (R′) C | `r5_normfree.c` v0.11 (020057b5) | $n = 8$: 5680a6d3; 16: 240dae55 |
| $r$-count, Python | `rsystem_count.py` (04c5206a) | ba4eb4b4 |
| time domain $r = 7$, Python | `r7_n8_timedomain.py` (c1886f82) | 1ef1fb9c |
| (F), for Theorem 7.5 | `fibre_count` v0.61 (binary 669b2784), v0.71 (binary 51dff7ee) | 3584ef6d (v0.61), 2354f47f (v0.71) |
| Smith form $r$, Python | `rsystem_smith.py` (98e3c7d7) | 18d3a138 |
| even shifts, Python | `evenshift_L4.py` v0.20 (d532d996) | $n = 8$: f4435a26; 32: cf984c3c; 56: 68c41c12 |
| (D) Python | `phi3j_composite.py` v0.31 (f00735e2) | $j = 3$–9: c4bff3d5 |
| (D′) Python | `phi3j_prp.py` (36a8ef5f) | $j \le 8$: 59b8a197; $j = 9$: 6a216f50 |
| (D″) Python | `alpern_factor_check.py` v0.21 (c43af0f2) | 122 factors of [1]: e5bd325b |
| (P) Python | `phi3j_factor.py` v0.10 (e33dee16) | $j = 10$–16: 9b585d41 |
| (T) C | `tz_extend.c` v0.40 (bebecc36), v0.50 (2317d4db) | 8809fe39, 08144a09, fd89c9d2, defc708c, b0e17878, 544c80e6, e602ffd0, a0a1d123; controls 337f9171, c753b4e1 |
| (T′) Python | `tz_check.py` v0.30 (4a08a6de) | 460ed524, 5a650803, f40a299b, 25cf1553 |
| Cor. 6.4, valuations, Python | `sec5_wieferich_facts.py` v0.20 (b4b8fd8d) | 8a68b8a6 |
| *Section 9.* Two rows for one statement are two independent programs, except the two Singular rows of Proposition 9.16(b) and the two rows of Proposition 9.72: two encodings solved by one engine. "Check" = a program that checks a statement that is proved by hand. | | |
| Lemma 9.10, check, Python | `fixrefl.py` (61f4f808) | $n = 8$: e2fc1466; 16: 7aa040ed; 32: 5bf7d442; 64: b01c1f51 |
| Lemma 9.10, check, C | `refl_time.c` v0.11 (0a0ace10; binary ec4c12a7) | $n \le 32$: 82a28d68; 64: 8213c822 |
| Lemma 9.13, check, Python | `twin_forced_zero.py` (40f7af0f) | feb83f06 |
| Prop. 9.16(a), (d), C | `mu4_scan.c` (25a8bb11) | $n = 64$: d4950713, 0319a7dd, 363c2a35, f157b19a; 16: 779d44d5 |
| Prop. 9.16(a), (d), PARI/GP | `mu4_scan.gp` v0.20 (1d2dadd7) | $n = 64$: d967ed31 |
| Prop. 9.16(b), encoding 1, Singular | `signpiece_a.py` v0.50 (a0399b0c), driver (0657491b) | 5b4bb76d; 377e59b6, 1fadd604, 23217307, e94fdd5f, 983977d4, 5e8322d6, 4a449f08 |
| Prop. 9.16(b), msolve | runners (1e3ccbe6, e12c65ea), 6 patterns | 5fc7e926, 4eb57567 |

| program | file (MD5) | logs (MD5) |
|---|---|---|
| Prop. 9.16(b), PARI/GP | `fourier_tree.gp` v0.10 (46aa1445), run (f2c7ad4d), 6 patterns | 2e2e924f |
| Prop. 9.16(b), encoding 2, Singular | `signpiece_b.py` v0.10 (97828feb), drivers (7f82bdfa, a2694ea6) | 5f23b031 |
| Remark 9.17, $n = 16$, Singular | `w16_fglm.sing` (c02ae4bf) | 0d9d5f3f |
| Remark 9.17, $n = 16$, msolve | `geomW_msolve.py` v0.10 (aac8d73a), `geomW_gen.py` (62e3643a) | bases 15d88401, d91f6a5c; count 3411b7cb |
| Remark 9.17, $n = 16$, orbit, Python | `w16_orbit.py` v0.10 (962123eb) | 6fe91aa4 |
| Remark 9.18, Python | `twin_odd.py` v0.10 (c2a69933) | f41f475f |
| Remark 9.18, C | `conj_scan.c` (50a97388) | f51b2ed3 |
| (H) C | `linear_fibre_a.c` (05688fac) | $\sigma = 32$: 26b8cfb4; 16: e17f3be8; 8: 6368ef2a; 4: a456d9fa; controls e9cb76db, 8364f9ac |
| (H′) C | `linear_fibre_b.c` v0.11 (23f456b6; binary 408ac3b8) | 5b04f2e6; test db0afa7e |
| (H) control, search over $\beta$, C | `half_twist.c` v0.20 (eaabefb7) | 6b0acae4 |
| (Z) C, PARI/GP | `f3base_scan.c` v0.10 (66f1da7a), `f3base_vals.gp` (1ae3dbc8) | a66a4501; control 5b4fb37c |
| (Z′) C | `f3base_nz.c` v0.21 (b439e339; binary 63716b82) | d9cca6f8; test da2a73b6 |
| (G) C, PARI/GP | `even_shift_a.c` v0.40 (4d3de760; binary b7fbf180), field table (e252a259) | a005e550, b6f86a99, b86cda15, 26b9d5aa, b13cea6b, 071bb7c8, 072ff4c8; controls eff775f3 |
| (G′) C | `even_shift_b.c` v0.11 (f8475e85; binary 24d69691); v0.31 (06537224; binary c8e993be) | v0.11: 92aac33b, test 85702561; v0.31 ($n = 80$, $\sigma = 40$): 1636daae; ($n = 104$, $\sigma = 52$, class $(1, 1)$): c2ece396; test b0632110 |
| Remark 9.33, $n = 32$, Python | `caseI_omega.py` v0.20 (572a28bb) | ba17e7c8 |
| Remark 9.33, $n = 32$, PARI/GP | `omega_check.gp` v0.10 (cabd65f2) | a02775c9 |
| Remark 9.33, $n = 128$, Python | `omega_sweep.py` (0ef76090), `forced_positions.py` (2a8cf116), `forced_full.py` (87177d9a), `omega_survivors.py` v0.20 (7fc5ea39) | a3993714, 08026b33, c0febe8a, 0fef3a71 |
| Remark 9.33, $n = 128$, C | `chain_fibre_b.c` v0.31 (d02bbf0c; binary a76fcfb1) | e7236b99; test 8ff56ef5 |
| Lemma 9.38, check, Python | `block_lemma_check.py` v0.10 (add5892f) | e284452d |
| Question 9.39, $M = 32$, Python | `D1_full.py` v0.10 (19751da6) | 6efb656e |
| Question 9.39, $M = 32$, C | `chain_fibre_b.c` v0.51 (447e91e3; binary a683b374) | 7f41f098; test a363a56d |
| Question 9.39, $M = 32$, PARI/GP | `d1_chi.gp` v0.20 (41c6110e) | 4e3a25cc |
| Remark 9.41, Python | `q2_J.py` (23bc4817), `q2_Jverify.py` (76821c88), `q2_K2check.py` (ba1d61b1) | dd744ccb; 7197272f |
| Remark 9.41, PARI/GP | `j128.gp` v0.10 (7db71fb1) | 1fcc0af3 |
| Remark 9.41, C | `chain_direct_512.c` v0.21 (92b12689; binary 7f4cc4ce) | 76163e31; test 3a990f2d |
| Lemma 9.42, checks, PARI/GP | `nsgen_units.gp` (b384b88f), `nsgen_census.gp` (ffe244ef) | df305db8, a1baf4c0 |
| Prop. 9.44(a) | the two programs of Remark 9.33, $n = 128$ | |
| Prop. 9.44(b), PARI/GP | `chain_fibre_a.gp` v0.10 (4ebda46c) | a28c36bb; controls 2fe1b0f9 |
| Prop. 9.44(b), C | `chain_fibre_b.c` v0.41 (5fb908d0; binary 267f5864) | 905c60fc; test 7007fa62 |
| Prop. 9.44(c), Python | `chain_fibre_c.py` v0.20 (855bc1a1) | f1f74fa2 |
| Prop. 9.44(c), C | `chain_fibre_b.c` v0.21 (561b5adc) | 586b7819; test cdfc9123 |
| Remark 9.47, PARI/GP | `modes8.gp` v0.30 (276ffe3f), `chainlib.gp` v0.30 (b58f7978) | 64226da3 |
| Remark 9.50, pairs, bases, Python | `m32_stage.py` v0.60 (787e4b5e) | controls 46f0a04f, b2d3fcb7 |
| Remark 9.50, descent, Python | `descent32.py` (9cffd5c0), `lambda_probe2.py` (461d06b5) | 98ca9b5e |
| Remark 9.50, signs, Python | `c_sign_check.py` (7fa97f26), `psi_order.py` (6cff7fd0) | 8cc03f29 |
| Remark 9.50, classes, rank, Python | `r4_omega_class.py` (8ab6d2f1), `r2_classes.py` v0.30 (30cdeb97) | 2eba219c, e7535789 |
| Remark 9.50, S2 census, Python | `m32_stage.py` v0.60 (787e4b5e) | b0bac079 |

| program | file (MD5) | logs (MD5) |
|---|---|---|
| Remark 9.50, modes, Python | `s3low.py` (fa65f94a), `s3low2.py` (7f787445) | ba232dea, 8233a9a9 |
| Remark 9.51, S3 sample, Python | `m32_stage.py` v0.60 (787e4b5e) | 41347580 |
| Lemma 9.54, Singular | `s2inv6.sing` v0.30 (edef5415) | 57217c48 |
| Lemma 9.54, msolve, FLINT | `s2inv6_elimA.ms` (de5898c0), `s2inv_check.py` v0.10 (e4a74747) | 7da0dbee; factors 0c7524e4 |
| Lemma 9.54, check, Singular | `invcheck.sing` (94196604) | a314fca4 |
| Table 9, $n = 8, 16$, Singular | `geom_W.py` (a9d9dae6), driver v0.30 (8d29f3bc) | b973aaef |
| Table 9, $n = 8$, orbit, Python | `w8_orbit.py` v0.10 (961258df) | a857277a |
| twist systems (§9.9), Singular | `twist_groebner.py` v0.20 (c4397949); `twist_brute.py` v0.10 (deb5a980) | fe21b119, f9e2e56d, 7495220e, 429fa475; 827d2dcd, e47a5000 |
| twist systems (§9.9), C | `twist_time.c` v0.11 (81943c00; binary 6306218e) | 23b88ac2; test b9d3b142 |
| Prop. 9.71, C | `f81_bases_a.c` v0.10 (8eba93f4) | 7a0e617f; controls 1cf7b692 |
| Prop. 9.71, C | `f81_bases_b.c` v0.20 (39ecf7f1) | 30b6aa94; controls 4c1d0d15 |
| Prop. 9.72, encoding 1, Singular | `quotient_a.py` v1.20 (279b74d3) | b1312840, b36fa540; $n = 16$ control 8970dc28 |
| Prop. 9.72, encoding 2, Singular | `quotient_b.py` v0.60 (a1cb707c), v1.20 (dbd964dc) | 8ba8ae0d, ce10cb58 |

## 9. The geometric relaxation

Line (L1) of (1) is the only line that contains $\sigma$. Deleting it leaves a system with coefficients in $\mathbb{F}_3$. Xia conjectures that this system has no solution in $\mathbb{F}_{3^{n/2}}$, and adds that the field may be replaced by any field of characteristic 3 [19, Conjecture 5.4]. We call the second statement the strong form. Xia reports that systems (11) and (12) of that paper, each with a Frobenius relation ((L1) in (12)), have no solution for $n = 32$ [19, Section 5]. We know of no check of Xia's Conjecture 5.4, in either form, for any $n$. Proposition 9.72 below checks a part of the strong form at $n = 32$. A proof of the strong form for one $n$ would exclude order $n$ for every $\sigma$ at once. In this section $n = 2^e$ with $e \geq 3$, $m = n/2$, and indices are modulo $n$.

Subsections 9.1–9.4 study the variety $W(n)$ of solutions of (L2)–(L4) and a group $G$ acting on it, and state Conjecture 9.7, which for odd $e \geq 5$ is equivalent to the strong form for $n = 2^e$ (Remark 9.8); by Corollary 9.20, for odd $e \geq 5$ every point that comes from a plane has trivial stabiliser in $G$. Subsections 9.5 and 9.6 treat Xia's system for $\sigma > 2$ (Proposition 9.23: no solution at $n = 128$). Subsections 9.7 and 9.8 treat, for odd $e$, the two loci on which every point with a non-trivial stabiliser lies; this concerns only the strong form. They show that $G$ acts freely on $W(32)$ and $W(128)$ (Corollary 9.43, Proposition 9.44); for larger $n$ some cases remain open, among them Questions 9.39 and 9.68. Subsection 9.9 treats $n = 32$, and Table 9 sums up $n = 8$, 16, 32 and 64.

### 9.1. The varieties $W(n)$ and $W'(n)$.

**Definition 9.1.** $W(n)$ is the set of $y \in \overline{\mathbb{F}}_3^n$ that satisfy (L2), (L3) and (L4) of (1). $W'(n)$ is defined in the same way with the norm equation (L2) replaced by $y_s\, y_{s+m} = 1/n$ for all $s$; we call this relation the *line* of $W'(n)$, or just the line.

For $e$ odd, $1/n = -1$ in $\mathbb{F}_3$, so $W'(n) = W(n)$; this is the case $n \equiv 8 \pmod{24}$ of (1). For $e$ even, $1/n = 1$, and $y \mapsto iy$ ($i^2 = -1$) maps $W(n)$ onto $W'(n)$; so $W'(n)$ is $W(n)$ up to this scalar, and it is non-empty for $n = 16$ (Table 9). On $W(n)$ itself, for even $e$, $(\sum_t y_t)^2 = \sum_s R(s) = R(m) = -n = -1$, so $\sum_t y_t \notin \mathbb{F}_3$, while (L1) forces $(\sum_t y_t)^3 = \sum_t y_t$; hence (1) has no solution for even $e$, in line with the condition $n \equiv 2 \pmod 3$ of [19, Lemma 4.1]. The strong form of Xia's Conjecture 5.4 for $n = 2^e$ is the statement $W(2^e) = \emptyset$ for odd $e \geq 5$.

Let $\xi$ be a primitive $n$-th root of unity in $\overline{\mathbb{F}}_3$. For $y \in \overline{\mathbb{F}}_3^n$ put $Y(x) := \sum_t y_t x^t \in \overline{\mathbb{F}}_3[x]/(x^n - 1)$ and $Y_k := Y(\xi^k) = \widehat{y}(\xi^k)$ for $k \in \mathbb{Z}/n$. On $W'(n)$ put $S(y) = \sum_t (-1)^t y_t = Y(-1)$ and $f_0(y) = \sum_t y_t = Y(1)$. Both lie in $\{\pm 1\}$: the line of $W'(n)$ gives $R(m) = n \cdot (1/n) = 1$, and (F3), whose

proof in Proposition 2.4 uses only (L3) and $R(m) = 1$, gives $Y_0^2 = 1$ and $Y_m^2 = (-1)^m = 1$. So $W'(n)$ is the disjoint union of four classes $W'_{S,f_0}(n)$.

**Lemma 9.2.** *Let $S, f_0 \in \{\pm 1\}$ and $y \in \overline{\mathbb{F}}_3^{\,n}$.*

(a) *$y \in W'_{S,f_0}(n)$ if and only if, in $\overline{\mathbb{F}}_3[x]/(x^n - 1)$,*

$$Y(x)\,Y(x^{-1}) = x^m, \qquad Y(x)\,Y(-x) = S\,Y(x^2), \qquad Y(1) = f_0,$$

*and $y_t\, y_{t+m} = 1/n$ for all $t$.*

(b) *If $Y(x)Y(x^{-1}) = x^m$, then $y_t\, y_{t+m} = 1/n$ for all $t$ if and only if*

$$\sum_{k \in \mathbb{Z}/n} (-1)^k\, Y_k\, Y_{2j-k} = 0 \qquad \text{for } 0 < j < m.$$

*Proof.* (a) The coefficient of $x^s$ in $Y(x)Y(x^{-1})$ is $R(s) = \sum_t y_t y_{t+s}$. Under the line, $R(m) = 1$, and $R(n-s) = R(s)$; so the first identity is equivalent to (L3). The coefficient of $x^r$ in $Y(x)Y(-x)$ is $\sum_t (-1)^{r-t} y_t y_{r-t}$. For odd $r$ it is 0, since the terms $t$ and $r-t$ cancel; for $r = 2s$ it is the left side of (L4). The polynomial $Y(x^2)$ has only even powers, and its coefficient of $x^{2s}$ is $y_s + y_{s+m}$. Hence the second identity is (L4) with the constant $S$ in place of $\sum_t (-1)^t y_t$. At $x = 1$ it gives $Y(1)Y(-1) = S\,Y(1)$, and $Y(1) = f_0 \neq 0$, so $S = Y(-1) = \sum_t (-1)^t y_t$.

(b) Put $p_t := y_t y_{t+m}$, so that $p_{t+m} = p_t$. Since $(-1)^k = \xi^{km}$, summing over $k$ first gives $\sum_k (-1)^k Y_k Y_{u-k} = n \sum_t p_t\, \xi^{u(t+m)}$ for every $u$. The right side is 0 for odd $u$, because $p_{t+m} = p_t$, and it is $n \sum_t p_t\, \xi^{ut}$ for even $u$. So $p$ is constant if and only if the left side vanishes for $u = 2j$ with $0 < j < m$. The constant is then $1/n$, because $\sum_t p_t = R(m) = 1$. □

The first three conditions in (a) define a coset of a group. A $Y$ that satisfies them is a unit, because $Y(x)Y(x^{-1}) = x^m$. If $Y$ and $Y'$ both satisfy them, then $U = Y'Y^{-1}$ satisfies $U(x)U(x^{-1}) = 1$, $U(x)U(-x) = U(x^2)$ and $U(1) = 1$; these $U$ form a subgroup of the unit group of $\overline{\mathbb{F}}_3[x]/(x^n - 1)$, and conversely $YU$ satisfies the three conditions for every such $U$. The line is the only condition that is not of this kind.

**Proposition 9.3.** *The four classes $W'_{S,f_0}(n)$ are isomorphic. The shift $y \mapsto (y_{t+1})_t$ maps $W'_{S,f_0}$ onto $W'_{-S,f_0}$, and $y \mapsto -y$ maps $W'_{S,f_0}$ onto $W'_{-S,-f_0}$.*

*Proof.* (L2) and (L3) are invariant under every shift and under $y \mapsto -y$. For $y'_t = y_{t+1}$ the left side of (L4) at $s$ is $\sum_t (-1)^t y_{t+1} y_{2s-t+1} = -\sum_u (-1)^u y_u y_{2(s+1)-u} = -(y'_s + y'_{s+m})\, S(y)$, and $S(y') = -S(y)$, so (L4) holds for $y'$; clearly $f_0(y') = f_0(y)$. Under $y \mapsto -y$ both sides of (L4) keep their value, and $S$ and $f_0$ change sign. □

**Proposition 9.4.** *For $c$ odd and $s$ even, $y \mapsto (y_{ct+s})_t$ maps each class $W'_{S,f_0}(n)$ onto itself. These maps form a group $G$ of order $n^2/4$. The map $F\colon y \mapsto (y_t^3)_t$ also maps each class onto itself and commutes with $G$, and a point $y \in W(n)$ satisfies (L1) with $\sigma$ if and only if $F(y) = (y_{t+\sigma})_t$.*

*Proof.* For (L2) use $cm \equiv m \pmod n$. The autocorrelation of $(y_{ct+s})_t$ at lag $u$ is that of $y$ at lag $cu$, and $cu \equiv m$ only if $u \equiv m$, so (L3) holds. In (L4) substitute $u = ct + s$: then $(-1)^t = (-1)^u$ because $c$ is odd and $s$ is even, and $c(2s' - t) + s = 2v - u$ with $v = cs' + s$; so the left side at $s'$ is the left side for $y$ at $v$, and $S$, $f_0$ are unchanged. The equations have coefficients in $\mathbb{F}_3$, so $F$ preserves them, and $F$ commutes with every permutation of the indices. The last statement is (L1) read as an identity of sequences. □

| $n$ | points per class | structure |
|---|---|---|
| 8 | 8 (each of multiplicity 2) | one $G$-orbit, stabilisers of order 2; each point satisfies $F(y) = (y_{t+2})_t$ or $F(y) = (y_{t-2})_t$ |
| 16 ($W'$) | 32 (reduced) | one $G$-orbit, stabilisers of order 2; values in $\mu_4$; base $w$ a delta; (L1) with $\sigma = 8$ |
| 32 | open | no point with $u_1 v_1 = 0$ (Proposition 9.72; $u_1, v_1$ are defined just before (22)); no point fixed by an involution of $G$; (1) empty for every even $\sigma$ ($\sigma = 2$: Section 8.1; $\sigma = 4, 8, 16$: the controls in Subsection 9.5, and Corollary 9.29 for $\sigma = 16$; $\sigma = 32$: Remark 9.24); no base over $\mathbb{F}_{81}$ |
| 64 ($W'$) | 1024 with a delta base | these have values in $\mu_4$ and satisfy (L1) with $\sigma = 32$; every other point, if any, lies in a free $G$-orbit (Proposition 9.16) |

TABLE 9. The varieties $W(n)$ and $W'(n)$ for $n = 8, 16, 32, 64$. The counts for $n = 8$ and 16 are, in each class, the dimensions of the quotient by a Gröbner basis of the system and by that of its radical (Table 8); the two programs of Proposition 9.71 find the same points.

9.2. **Base and fibre.** For $y \in W'(n)$ put $w_r = y_r + y_{r+m}$ and $d_r = y_r - y_{r+m}$. Then $w$ is $m$-periodic and $d$ is $m$-antiperiodic, and the line $y_s y_{s+m} = 1/n$ becomes the pointwise relation $d_r^2 = w_r^2 - 1/n$. We call $w$ the *base* of $y$. It is determined by the values $Y_k$ at even $k$, and over a fixed base the values $d_r$ are fixed up to sign. Under (L1) with $\sigma = 2$, $w_r$ and $d_r$ are, up to the factor 2, the parts $y^+$ and $y^-$ of Remark 2.6.

**Lemma 9.5.** *Let $e$ be odd. No point of $W(2^e)$ has $w = \pm(\delta_{r,r_0})_r$ for some $r_0 \in \mathbb{Z}/m$.*

*Proof.* By Proposition 9.3 we may take $w_r = \delta_{r,r_0}$. Then $d_r^2 = w_r^2 + 1$ gives $d_r = \pm 1$ for $r \neq r_0$ and $d_{r_0} = \pm i$ with $i^2 = -1$. In (L4) at $s = r$ write $y_t = -(w_t + d_t)$; the products $w_u d_{2r-u}$ cancel in pairs under $u \mapsto u + m$, so the left side is $\sum_u (-1)^u (w_u w_{2r-u} + d_u d_{2r-u})$, the sum over $u$ modulo $n$. Take $r \not\equiv r_0 \pmod{m/2}$. Then $w_r = 0$, the products $w_u w_{2r-u}$ vanish, and $d_u d_{2r-u}$ is imaginary for exactly four $u$, namely $u \equiv r_0$ or $2r - u \equiv r_0 \pmod m$. These four terms are equal, so, as $4 = 1$ in $\mathbb{F}_3$, they add up to $(-1)^{r_0} d_{r_0} d_{2r-r_0} = \pm i$, while all other terms are in $\mathbb{F}_3$. Hence the left side of (L4) is not in $\mathbb{F}_3$, but the right side is 0. □

9.3. **Delta bases and Conjecture DB.** Let $e \geq 3$, $n = 2^e$, $m = n/2$, with $\xi$ and $Y_k$ as in Subsection 9.1, and put $\zeta := \xi^2$. Let $y \in W'_{S,f_0}(n)$. Evaluating the identities of Lemma 9.2(a) at $x = \xi^k$ gives

$$Y_k\, Y_{-k} = (-1)^k \qquad (k \in \mathbb{Z}/n), \tag{12}$$

$$Y_k\, Y_{k+m} = S\, Y_{2k} \qquad (k \in \mathbb{Z}/n), \tag{13}$$

and $Y_0 = f_0$, $Y_m = S$; in particular no $Y_k$ is zero. Since $w_r = y_r + y_{r+m}$ and $\xi^{2j(r+m)} = \xi^{2jr}$,

$$Y_{2j} = \sum_{r \in \mathbb{Z}/m} w_r\, \zeta^{jr} =: \widehat{w}(j) \qquad (j \in \mathbb{Z}/m),$$

and we say that $y$ has a *delta base* if $w = \pm\delta_{r_0}$ for some $r_0 \in \mathbb{Z}/m$, where $\delta_{r_0} = (\delta_{r,r_0})_{r \in \mathbb{Z}/m}$; equivalently, $\widehat{w}(j) = \pm\zeta^{jr_0}$ for all $j$. Lemma 9.5 says that for odd $e$ no point of $W(2^e)$ has a delta base. The next lemma describes delta bases through the values $Y_k$ at odd $k$.

**Lemma 9.6.** *Let $e \geq 3$ and $y \in W'_{S,f_0}(2^e)$.*

(a) *$Y_{m-k} = -S\, Y_{-2k}\, Y_k$ for every odd $k$.*

(b) *Let $r_0 \in \mathbb{Z}/m$. Then $w = \pm\delta_{r_0}$ if and only if $f_0 = S(-1)^{r_0}$ and*

$$Y_{m-k} = -S f_0\, \xi^{-2kr_0}\, Y_k \qquad \text{for every odd } k \text{ with } 0 < k < m/2. \tag{14}$$

*In that case* $w = f_0\delta_{r_0}$.

*Proof.* (a) By (13) at $-k$, $Y_{-k}Y_{m-k} = S\,Y_{-2k}$, and by (12), $Y_{-k} = -Y_k^{-1}$ for odd $k$.

(b) Let $w = \varepsilon\delta_{r_0}$ with $\varepsilon = \pm 1$, so that $\widehat{w}(j) = \varepsilon\zeta^{jr_0}$ for all $j$. At $j = 0$ this gives $\varepsilon = Y_0 = f_0$, and at $j = m/2$ it gives $S = Y_m = f_0(-1)^{r_0}$. For odd $k$ it gives $Y_{-2k} = f_0\xi^{-2kr_0}$, and (a) becomes (14).

Conversely, let $f_0 = S(-1)^{r_0}$ and let (14) hold. We show that $Y_l = f_0\xi^{lr_0}$ for every non-zero $l \in \mathbb{Z}/n$ with $l$ even. For such $l$ let $v(l)$ be its 2-adic valuation, $1 \le v(l) \le e-1$. First let $v(l) = 1$. Then $l = \pm 2k$ for one odd $k$ with $0 < k < m/2$ and one sign. Comparing (14) with (a) gives $Y_{-2k} = f_0\xi^{-2kr_0}$, since $Y_k \neq 0$; and (12) at the even index $2k$ gives $Y_{2k} = Y_{-2k}^{-1} = f_0\xi^{2kr_0}$. Next let the claim hold for all $l$ with $v(l) = v$, where $1 \le v \le e-2$. If $v(l) = v$, then $v(l+m) = v$ because $v(m) = e-1 > v$, and (13) gives

$$Y_{2l} = S\,Y_l\,Y_{l+m} = Sf_0^2\,\xi^{(2l+m)r_0} = S(-1)^{r_0}\xi^{2lr_0} = f_0\,\xi^{2lr_0}.$$

Every $l'$ with $v(l') = v+1$ has the form $2l$ with $v(l) = v$, so the claim holds for $v+1$. Hence it holds for all even $l \neq 0$. Together with $Y_0 = f_0$ this gives $\widehat{w}(j) = f_0\zeta^{jr_0}$ for all $j \in \mathbb{Z}/m$, that is, $w = f_0\delta_{r_0}$. □

By (12) and (13), a point of $W'_{S,f_0}(n)$ is determined by the $m/2$ values $Y_k$ with $k$ odd and $0 < k < m$: the values at the odd $k > m$ follow from $Y_{-k} = -Y_k^{-1}$, the values at the even $k \neq 0$ follow one 2-adic level at a time from $Y_{2k} = S\,Y_kY_{k+m}$, and $Y_0 = f_0$. In these coordinates, Lemma 9.6(b) says that the points with base $f_0\delta_{r_0}$ are the points of $W'_{S,f_0}(n)$ on the translate of a subtorus of dimension $m/4$ defined by the $m/4$ equations (14), each of which pairs $Y_k$ with $Y_{m-k}$. The value $r_0$ runs over the $m/2$ residues with $(-1)^{r_0} = Sf_0$.

**Conjecture 9.7** (DB)**.** *Let $e \ge 4$. Every point of $W'(2^e)$ has a delta base.*

*Remark* 9.8. (a) For odd $e$, $W'(2^e) = W(2^e)$, and by Lemma 9.5 no point of $W(2^e)$ has a delta base. So for odd $e$ Conjecture 9.7 is equivalent to $W(2^e) = \emptyset$, the strong form of Xia's Conjecture 5.4 for $n = 2^e$.

(b) The bound $e \ge 4$ is needed: $W(8)$ is not empty (Table 9), and by Lemma 9.5 none of its points has a delta base.

(c) For even $e$ we have $W(2^e) = i\,W'(2^e)$ (Subsection 9.1), and Conjecture 9.7 describes $W'(2^e)$. For $e = 4$ and $e = 6$ this variety is not empty: every point of $W'(16)$ has a delta base (Table 9), and Subsection 9.4 gives the evidence at $n = 64$. We state the conjecture for both parities of $e$ as one statement. The two parities differ in the value $d_{r_0}^2 = 1 - 1/n$ at a delta base, which is 0 for even $e$ and $-1$ for odd $e$, and Lemma 9.5 turns the second value into a contradiction.

**Corollary 9.9.** *Let $e \ge 5$ be odd. If Conjecture 9.7 holds for $e$, then there is no non-Desarguesian flag-transitive projective plane of order $2^e$. If it holds for every odd $e \ge 5$, then every finite flag-transitive projective plane whose order is a power of 2 is Desarguesian.*

*Proof.* Suppose that a non-Desarguesian flag-transitive projective plane of order $n = 2^e$ exists. By Theorem 2.1, $n \equiv 8 \pmod{24}$ and $n > 8$, so $e$ is odd (as $n \equiv 2 \pmod 3$) and $e \ge 5$; and there are an even $\sigma$ and $y_0, \dots, y_{n-1} \in \mathbb{F}_{3^{n/\sigma}}$ that satisfy (1). Then $y$ satisfies (L2), (L3) and (L4), so $y \in W(n) = W'(n)$. If Conjecture 9.7 holds for this $e$, then $y$ has a delta base, which Lemma 9.5 excludes. This proves the first statement, and the second follows from it, since Theorem 2.1 leaves no other powers of 2. □

The corollary does not use (L1). A proof of Conjecture 9.7 for one odd $e$ would therefore exclude the order $2^e$ by an argument about $W(2^e)$ alone.

9.4. **Evidence for Conjecture DB.** We use $\xi$, $Y_k$ and $Y(x)$ as in Subsection 9.1, and $\zeta = \xi^2$ and $\widehat{w}(j) = Y_{2j}$ as in Subsection 9.3. By Lemma 9.2(a), (L4) is the identity $Y(x)\,Y(-x) = S\,Y(x^2)$. Lemmas 9.10 and 9.12 hold for every $e \geq 3$, and Lemma 9.13 is about odd $e$. In Lemmas 9.14 and 9.15 and Proposition 9.16, $e$ is even, so $1/n = 1$ in $\mathbb{F}_3$, the line reads $y_s y_{s+m} = 1$, and $d_r^2 = w_r^2 - 1$; each remark after them states its $e$. For even $e$ the map $y \mapsto iy$ identifies $W(n)$ with $W'(n)$ (Subsection 9.1), so the results below describe $W(2^e)$ too, up to the factor $i$. By Proposition 9.3 it suffices to treat one class: the shift by 1 and $y \mapsto -y$ map delta bases to delta bases and $\mu_4$-valued points to $\mu_4$-valued points, and they normalise $G$; the shift by 1 exchanges the two loci in part (b) of Proposition 9.16 below, and $y \mapsto -y$ preserves each of them. The subsection ends with Corollary 9.20: for odd $e \geq 5$, every point of $W(2^e)$ that comes from a plane has trivial stabiliser in $G$.

**Lemma 9.10.** *Let $n = 2^e$ with $e \geq 3$. No point of $W'(n)$ is fixed by a reflection $t \mapsto s - t$ with $s$ even.*

*Proof.* Let $y$ be fixed. Then $Y_k = \xi^{ks} Y_{-k}$ for all $k$, and (12) gives $Y_k^2 = (-1)^k \xi^{ks} = \xi^{2kh}$ with $h = (s+m)/2$, an integer since $s$ and $m$ are even. So $Y_k = \varepsilon_k \xi^{kh}$ with $\varepsilon_k = \pm 1$. By (12), $\varepsilon_{-k} = (-1)^k \varepsilon_k$, and by (13), $\varepsilon_{2k} = \lambda\, \varepsilon_k \varepsilon_{k+m}$ for all $k$, with $\lambda = S(-1)^h$. By Lemma 9.2(b), the line gives $\sum_k (-1)^k \varepsilon_k \varepsilon_{2j-k} = 0$ in $\mathbb{F}_3$ for $0 < j < m$ (the factor $\xi^{2jh}$ drops out).

Now read the $\varepsilon_k$ as integers. Put $A(X) = \sum_k \varepsilon_k X^k$ in $\mathbb{Z}[X]/(X^n - 1)$ and $C(l) = \sum_k \varepsilon_k \varepsilon_{k+l}$, so that $A(X)A(X^{-1}) = \sum_l C(l) X^l$ and $C(0) = n$. Since $\varepsilon_{-k} = (-1)^k \varepsilon_k$, we have $A(X^{-1}) = A(-X)$. In $A(X)A(-X)$ the coefficient of $X^{2j}$ is $\sum_k (-1)^k \varepsilon_k \varepsilon_{2j-k}$, and the coefficient of an odd power is 0 (the terms $k$ and $l-k$ cancel). Hence $C(l) \equiv 0 \pmod 3$ for every $l \not\equiv 0 \pmod n$.

In $A(1) = \sum_k \varepsilon_k$ the terms with $k$ odd cancel in pairs, since $\varepsilon_{-k} = -\varepsilon_k$ and $-k \not\equiv k$. So

$$A(1) = \sum_{j=0}^{m-1} \varepsilon_{2j} = \lambda \sum_{j=0}^{m-1} \varepsilon_j \varepsilon_{j+m} = \tfrac{\lambda}{2}\, C(m) \equiv 0 \pmod 3.$$

But $A(1)^2 = A(1)A(1^{-1}) = \sum_l C(l) \equiv C(0) = n \pmod 3$, and $3 \nmid n$. This contradiction proves the lemma. □

*Remark* 9.11. The argument is a mod-3 analogue of the row-sum identity for a $\pm 1$ sequence of length $v$ whose periodic off-peak autocorrelations vanish: there $A(1)^2 = \sum_l C(l) = v$, so $v$ is a square (cf. [18, p. 330] for abelian Hadamard difference sets).

**Lemma 9.12.** *Let $e \geq 3$, and let $y \in W'(2^e)$ be fixed by $t \mapsto (m-1)t + s$ for some even $s$. Then, for some $r_0 \in \mathbb{Z}/m$, either $w = f_0 \delta_{r_0}$ or $w = f_0\big(\frac{2}{m} J - \delta_{r_0 + m/2}\big)$, where $J$ is the all-one vector.*

*Proof.* Being fixed means $Y_k = \xi^{-(m-1)ks} Y_{(m-1)k}$ for all $k$. For odd $k$ we have $(m-1)k \equiv m - k$ and $mks \equiv 0 \pmod n$, so $Y_{m-k} = \xi^{-ks} Y_k$. On the other hand $Y_{m-k} = -S\, Y_{-2k} Y_k$ for odd $k$ by Lemma 9.6(a). Hence $\widehat{w}(j) = -S\xi^{js}$ for every odd $j$, that is, $\widehat{w}(j) = f_0\, \zeta^{jr_0}$ for odd $j$, where $r_0 \equiv (s+m)/2$ if $S = f_0$ and $r_0 \equiv s/2$ if $S = -f_0$ (modulo $m$). The values at even $j$ follow from (13) at level $m$, $\widehat{w}(2j) = S\, \widehat{w}(j)\, \widehat{w}(j + m/2)$, and $\widehat{w}(0) = f_0$. If $f_0 = S(-1)^{r_0}$, this gives $\widehat{w}(j) = f_0 \zeta^{jr_0}$ for all $j$, so $w = f_0 \delta_{r_0}$. If $f_0 = -S(-1)^{r_0}$, it gives $\widehat{w}(j) = -f_0 \zeta^{jr_0}$ for all even $j \neq 0$, and the inverse transform is $w = f_0\big(\frac{2}{m} J - \delta_{r_0 + m/2}\big)$. □

**Lemma 9.13.** *Let $e \geq 3$ be odd. No point of $W(2^e)$ is fixed by $t \mapsto (m-1)t + s_0$ with $s_0$ even.*

*Proof.* Let $y$ be fixed by $g(t) = (m-1)t + s_0$. As $mt \equiv 0$ or $m \pmod n$ for $t$ even or odd, $g(t) = s_0 - t$ for even $t$ and $g(t) = s_0 - t + m$ for odd $t$; also $g(t+m) = g(t) + m$, since $m^2 \equiv 0 \pmod n$. Hence $d_{g(t)} = y_t - y_{t+m} = d_t$, and as $d$ is $m$-antiperiodic,

$$d_{s_0 - t} = (-1)^t\, d_t \qquad (t \in \mathbb{Z}/n).$$

If $s_0 \equiv 2 \pmod 4$, let $t_0 = s_0/2$; it is odd and $s_0 - t_0 = t_0$, so $d_{t_0} = -d_{t_0}$. If $s_0 \equiv 0 \pmod 4$, let $t_0 = (s_0 + m)/2$; it is even, as $4 \mid m$, and $s_0 - t_0 = t_0 - m$, so $d_{t_0} = d_{t_0 - m} = -d_{t_0}$. In both cases $d_{t_0} = 0$. Since $e$ is odd, $1/n = -1$ in $\mathbb{F}_3$, so $d_r^2 = w_r^2 + 1$, and $w_{t_0}^2 = -1$.

On the other hand, as $W(2^e) = W'(2^e)$ for odd $e$, Lemma 9.12 gives $w = f_0\delta_{r_0}$ or $w = f_0\big(\frac{2}{m}J - \delta_{r_0+m/2}\big)$. In either case $w$ is $\mathbb{F}_3$-valued, so $w_{t_0}^2 \in \{0, 1\}$. This contradiction proves the lemma. □

**Lemma 9.14.** *Let $e$ be even. If $y \in W'(2^e)$ has a delta base, then every $y_t$ lies in $\mu_4$, and $y_{t+m} = y_t^3$ for all $t$.*

*Proof.* The sign of the delta base is $f_0$, since $\sum_r w_r = \sum_t y_t = f_0$; so $w = f_0\delta_{r_0}$. Then $d_{r_0} = 0$ and $d_r^2 = -1$ for $r \neq r_0$. In characteristic 3, $y_r = -(w_r + d_r)$ and $y_{r+m} = -(w_r - d_r)$, so $y_{r_0} = y_{r_0+m} = -f_0$, and for $r \neq r_0$ the pair $(y_r, y_{r+m})$ is $(i, -i)$ or $(-i, i)$ with $i^2 = -1$. In both cases $y_{r+m} = y_r^3$. □

**Lemma 9.15.** *Let $e \geq 4$ be even, and let $y \in W'(2^e)$ be fixed by $t \mapsto (m-1)t + s$ for some even $s$. Then $y$ has a delta base.*

*Proof.* By Lemma 9.12, either $w = f_0\delta_{r_0}$, a delta base, or $w = f_0(J - \delta_{r'})$ with $r' = r_0 + m/2$ (here $2/m = 1$ in $\mathbb{F}_3$). We show that the second case does not occur. In it, $d_r = 0$ for $r \neq r'$ and $d_{r'} = \pm i$, so $y_t = -f_0$ for $t \not\equiv r' \pmod m$ and $(y_{r'}, y_{r'+m}) = (\mp i, \pm i)$. Write $Y(x) = -f_0 J(x) + E(x)$ with $J(x) = \sum_t x^t$ and $E(x) = (f_0 \mp i)x^{r'} + (f_0 \pm i)x^{r'+m}$. Since $J(x)J(-x) = 0$, $J(x)x^u = J(x)$, $J(-x)x^u = (-1)^u J(-x)$ and $E(x)E(-x) = (-1)^{r'}x^{2r'+m}$, we get

$$Y(x)\,Y(-x) = (-1)^{r'}\Big(x^{2r'+m} - \sum_{u \text{ even}} x^u\Big), \qquad S\,Y(x^2) = S f_0\Big(\sum_{u \text{ even}} x^u - x^{2r'}\Big).$$

The coefficient of $x^{2r'}$ is $-(-1)^{r'}$ on the left and 0 on the right, so (L4) fails, and this case does not occur. □

**Proposition 9.16.** *Let $n = 64$. In each class $W'_{S,f_0}(64)$:*

(a) *exactly 1024 points have a delta base;*
(b) *no point has $y_{t+m} = y_t$ for all odd $t$, and no point has $y_{t+m} = y_t$ for all even $t$;*
(c) *every point whose stabiliser in $G$ is not trivial has a delta base;*
(d) *a point has all its coordinates in $\mu_4$ if and only if it has a delta base.*

By the line $y_t y_{t+m} = 1$, a point has all its coordinates in $\mu_4$ exactly when $F(y) = (y_{t+m})_t$: if $y_t^4 = 1$ then $y_t^3 = y_t^{-1} = y_{t+m}$, and $y_t^3 = y_{t+m} = y_t^{-1}$ gives $y_t^4 = 1$. By Lemma 9.14, every point with a delta base is of this kind. So a point of $W'(64)$ without a delta base, if there is one, has a free $G$-orbit of 1024 points, and on it $F$ is not the shift by $m$.

*Proof.* (d) and (a). By Lemma 9.14 we must find all points with coordinates in $\mu_4$. For such a point $w$ is $\mathbb{F}_3$-valued and $d = i\,z$ with $z$ $\mathbb{F}_3$-valued, and the line becomes $w_r^2 + z_r^2 = 1$: exactly one of $w_r$, $z_r$ is non-zero. Conversely, $w$ and $d$ determine $y$, and $y$ lies in $W'(64)$ when the first three identities of Lemma 9.2(a) and the line hold. An $\mathbb{F}_3$-valued $w$ has $\widehat{w}(3j) = \widehat{w}(j)^3$, and $\widehat{w}(-j) = \widehat{w}(j)^{-1}$ by (12); since $(\mathbb{Z}/2^k)^\times = \langle -1\rangle \times \langle 3\rangle$, $w$ is determined by $b := \widehat{w}(1) \in \mathbb{F}_{3^8}^\times$ (the values at even $j$ follow from (13) at level $m$). In the same way $z$ is determined by $\alpha := \widehat{z}(1) \in \mathbb{F}_{3^{16}}^\times$, with $\widehat{z}(-1) = \alpha^{-1}$, where $\widehat{z}(k) = \sum_r z_r \xi^{kr}$ for odd $k$, so that $Y_k = i\,\widehat{z}(k)$. As $1 + m \equiv 3^8 \pmod{64}$, (13) at $k = 1$ reads $\alpha^{1+3^8} = -S\,b$, and at the other odd $k$ it is a Galois conjugate of this relation or of its inverse. So the $\mu_4$-valued points correspond to the $\alpha \in \mathbb{F}_{3^{16}}^\times$ for which the zero set of $z_r = m^{-1}\big(\mathrm{Tr}(\alpha\xi^{-r}) + \mathrm{Tr}(\alpha^{-1}\xi^r)\big)$, with Tr from $\mathbb{F}_{3^{16}}$ to $\mathbb{F}_3$, is the support of the base determined by $b = -S\alpha^{1+3^8}$. Two independent exhaustive searches over all $3^{16} - 1$ values of $\alpha$ find exactly 1024 such $\alpha$ in each class, and each of them gives a delta base. (The 6560 $\mathbb{F}_3$-valued bases of a class have supports of sizes $1, 16, 19, 22, 25, 28, 31$; 16 of them are delta bases.)

(b) It suffices to treat the class $S = f_0 = 1$: by the start of this subsection, the maps that permute the classes preserve or exchange the two loci. On these loci the coordinates at odd (resp. even) $t$ are $\pm 1$, since $y_t^2 = 1$ there. Up to $G$ there are 693 sign patterns on each locus. For each pattern the remaining equations have no solution. Two independent programs write the equations of each pattern, in different coordinates, and the Gröbner basis engine of Singular finds no solution for either; one of them did not finish six patterns, and for those msolve and an exact search also find no solution. The exact search solves (13) from the highest 2-power frequency down; each step takes a square root, and every square root that occurs lies in $\mathbb{F}_{3^{16}}$.

(c) $G$ is a 2-group, so a non-trivial stabiliser contains an element $t \mapsto ct + s$ of order 2. Then $c^2 \equiv 1$ and $(c+1)s \equiv 0 \pmod n$, so $c \in \{1, m-1, m+1, n-1\}$, with $s = m$ if $c = 1$, $s \in \{0, m\}$ if $c = m+1$, and $s$ any even number otherwise. For $c = 1$ a fixed point has $Y_k = -Y_k$ for odd $k$, which (12) forbids. For $c = m+1$ the fixed points are the two loci of (b). For $c = m-1$ use Lemma 9.15, and for $c = n-1$ use Lemma 9.10. □

*Remark* 9.17. For $n = 16$ the class $W'_{1,1}(16)$ has exactly 32 points (Table 9; two independent programs), and the method of (d) finds 32 points with a delta base in it; so every point of $W'(16)$ has a delta base (in each class, by Proposition 9.3). The 8 $\mathbb{F}_3$-valued bases of this class are the 4 delta bases and 4 bases of support 7. The 32 points of the class form one orbit of $G$, which has order $n^2/4 = 64$ (one program); so each point of $W'(16)$ is fixed by exactly one non-trivial element of $G$, namely by $t \mapsto 7t + s$ for one $s \equiv 0 \pmod 4$. For every even $e \geq 4$, Lemmas 9.10 and 9.15 show that a point of $W'(2^e)$ with a non-trivial stabiliser in $G$ has a delta base or lies on one of the two loci of (b). For every odd $e \geq 3$, Lemmas 9.10 and 9.13, with the involutions of $G$ listed in the proof of Proposition 9.16(c), show that a point of $W(2^e)$ with a non-trivial stabiliser in $G$ lies on one of these two loci, $\{y_t = y_{t+m} \text{ for all odd } t\}$ or $\{y_t = y_{t+m} \text{ for all even } t\}$. On the first locus $S = f_0$: there $d_r = 0$ for odd $r$, so $w_r^2 = -1$ for odd $r$, and $\sum_{r \text{ odd}} w_r = \frac{1}{2}\big(\widehat{w}(0) - \widehat{w}(m/2)\big) = \frac{1}{2}(f_0 - S)$ lies in $\mathbb{F}_3 \cap i\,\mathbb{F}_3 = \{0\}$. The shift by 1 exchanges the loci and $S$ with $-S$, so $S = -f_0$ on the second locus. A direct computation (Table 8) shows that for $n = 8$ every point of $W(8)$ lies on one of them. For $n = 32$ and $n = 128$ neither locus has a point, by Corollary 9.43 and Proposition 9.44; so no point of $W(32)$ or of $W(128)$ has a non-trivial stabiliser in $G$.

*Remark* 9.18. At odd $e$ the condition $F(y) = (y_{t+m})_t$ means that every $y_t$ is a primitive eighth root of unity, since the line gives $y_t^4 = -1$; equivalently, $w$ is $\mathbb{F}_3$-valued with no zero. Then $d = i\,z$ with $z$ a $\pm 1$-sequence, $z_{t+m} = -z_t$, and (12) at odd $k$ gives $Z(x)Z(x^{-1}) = 1$ in $\mathbb{F}_3[x]/(x^m + 1)$, where $Z(x) = \sum_{r<m} z_r x^r$. Two independent exhaustive searches over all $\pm 1$-sequences of length $m$ find no such sequence for $m = 4$ and $m = 16$. So for $n = 8$ and $n = 32$ no point of $W(n)$ has $F(y) = (y_{t+m})_t$, while for $n = 16$ and $n = 64$ the points of $W'(n)$ with this property are exactly those with a delta base (Proposition 9.16(d) and the remark above).

*Remark* 9.19. Let $y \in W(n)$ have trivial stabiliser in $G$. The integers $a$ with $F^a(y) \in G\,y$ form a non-zero subgroup $a_0\mathbb{Z}$, since the coordinates of $y$ lie in a finite field, and $F^a(y) = g_a(y)$ for a unique $g_a \in G$. As $F$ commutes with $G$, the $g_a$ form a cyclic 2-group. Either $g_{a_0} = 1$, and we call $y$ *Frobenius-free*; or this group has a unique involution $\iota$, and then $F^a(y) = \iota(y)$ for some $a > 0$, and we call $y$ *twisted*. As in the proof of Proposition 9.16(c), $\iota$ is $t \mapsto ct+s$ with $c \in \{1, m-1, m+1, n-1\}$; so there are four types of twisted points. Condition (L1) of (1) with $\sigma = 2$ is $F(y) = (y_{t+2})_t$, so it gives $F^{m/2}(y) = (y_{t+m})_t$; by Lemma 2.2, $\sigma = 2$ for planes of order $n = 2^e$. So the points that come from planes have $\iota$ equal to the shift by $m$ if their stabiliser in $G$ is trivial, and for odd $e \geq 5$ it always is (Corollary 9.20); Remark 9.18 is the case $a = 1$ of this type.

**Corollary 9.20.** *Let $n = 2^e$ with $e \geq 5$ odd. No solution of (1) with $\sigma = 2$ lies on the locus $\{y_t = y_{t+m}$ for all odd $t\}$ or on the locus $\{y_t = y_{t+m}$ for all even $t\}$. Hence every point of $W(2^e)$ that satisfies (L1) with $\sigma = 2$, in particular every point that comes from a plane of order $2^e$ (Lemma 2.2), has trivial stabiliser in $G$ and is twisted, with $\iota$ the shift by $m$.*

*Proof.* For odd $e$ the line of $W(n)$ is $y_t y_{t+m} = 1/n = -1$ for every $t$ (Definition 9.1). On the first locus it gives, at $t = 1$, $y_1^2 = -1$, that is $y_1 = \pm i$; on the second, at $t = 0$, $y_0 = \pm i$. A solution of (1) with $\sigma = 2$ is a solution of the norm-free system, and $8 \mid m = 2^{e-1}$ as $e \geq 5$; so Theorem 6.2(a) excludes both cases. By Remark 9.17, a point of $W(2^e)$ with a non-trivial stabiliser in $G$ lies on one of the two loci; so the stabiliser is trivial, and by Remark 9.19 the point is twisted, with $\iota$ the shift by $m$. □

9.5. **Xia's system for other values of $\sigma$.** Conjecture 5.2 of [19] is stated for every positive even divisor $\sigma$ of $n$. For a plane of order $n \equiv 8 \pmod{24}$, the proof of Lemma 2.2 gives $\sigma = 2\gcd(c, n_{\mathrm{odd}})$, so only $\sigma = 2d$ with $d \mid n_{\mathrm{odd}}$ occurs, and $\sigma = 2$ when $n$ is a power of 2. We now treat the values $\sigma > 2$ for $n = 128$; for $n = 32$ see the controls below, Corollary 9.29 and Subsection 9.9.

Let $y$ satisfy (L1) of (1) and put $Y_k = \widehat{y}(\xi^k)$ as in Subsection 9.1. As in the proof of (F1) in Proposition 2.4, (L1) is equivalent to

$$Y_{3k} = \xi^{3k\sigma}\, Y_k^3 \qquad (k \in \mathbb{Z}/n). \tag{15}$$

So on the orbit $\{3^a k\}$ of an odd $k$ under multiplication by 3 we have $Y_{3^a k} = \xi^{\sigma k a 3^a}\, Y_k^{3^a}$, and $Y_k$ lies in a finite set fixed by the length of the orbit. The relation (12) gives $Y$ on the orbit of $-k$, and (13) gives every $Y_{2j}$ from the odd values. Hence the points of (1) are described by one value per pair of orbits $\{O, -O\}$ of odd residues, and (L2) is then a further condition on these values; the base $w$ of Subsection 9.2 depends only on the products $Y_k Y_{k+m}$.

*The base test.* Let $\sigma \mid m$ and $q' = 3^{m/\sigma}$. Applying (L1) $m/\sigma$ times gives $y_{t+m} = y_t^{q'}$, so $d_t = y_t - y_{t+m}$ satisfies $d_t^{q'} = -d_t$. Hence $d_t^2 \in \mathbb{F}_{q'}$, and $d_t^2$ is 0 or a non-square of $\mathbb{F}_{q'}$. Since $d_t^2 = w_t^2 - 1/n$, for the base $w$ of a solution, $w_t^2 - 1/n$ is 0 or a non-square of $\mathbb{F}_{q'}$ for every $t$. By (L1), $w_{t+\sigma} = w_t^3$, so it suffices to test $t < \sigma$.

*A linear fibre for $n = 2^e$ with $e \geq 4$, and $4 \mid \sigma$.* Here the odd residues modulo $n$ are $\pm\langle 3\rangle$, so all odd $Y_k$ are fixed by $\beta := Y_1$, and $\nu := Y_2$ fixes the base. If $4 \mid \sigma$, then $\nu \in \mathbb{F}_{3^{n/8}}$. As $1 + m = 3^{n/8}$ in $\mathbb{Z}/n$, (13) at $k = 1$ gives $\beta^{-1} = \kappa\, \beta^{3^{n/8}}$ with $\kappa = S\, \xi^{\sigma(n/8)3^{n/8}}/\nu$. So, once $\nu$ is fixed, every odd $Y_k$, and hence every $d_t = m^{-1} \sum_{k \text{ odd}} Y_k \xi^{-kt}$, is an $\mathbb{F}_3$-linear function of $\beta$. Writing $d_t = \varepsilon_t r_t$ with $r_t^2 = w_t^2 - 1/n$ and $\varepsilon_t = \pm 1$ for $t < \sigma$ gives one homogeneous linear system over $\mathbb{F}_3$ in $\beta$ and the $\varepsilon_t$; a solution of (1) gives a kernel vector with every $\varepsilon_t \neq 0$.

*Programs.* (H) is for $n = 2^e$ with $e \geq 4$, and $4 \mid \sigma$: it runs over all $\nu$, applies the base test, solves the linear system, and tests each kernel vector with all $\varepsilon_t \neq 0$ (and the relation $\beta \cdot \xi^{\sigma(n/8)3^{n/8}} \beta^{3^{n/8}} = S\nu$) on all of (1). (H′) is a second program for the same case; over each base that passes the base test it runs through all sign vectors $(\varepsilon_t)_{t<\sigma}$, keeps those that satisfy (12) and (13) at $k = 1$, and tests each on all of (1). Controls: for $W'(16)$ with $\sigma = 8$, (H) and (H′) find all 32 points of each class, and none with $\sigma = 4$; for $W'(64)$ with $\sigma = 32$, (H) finds 1024 points in the class $(S, f_0) = (1, 1)$, as does an exhaustive search over $\beta$ (Table 8); at $n = 32$, (H) and (H′) find no solution for $\sigma = 4, 8, 16$, in each class.

The maps of Proposition 9.3 are shifts and $y \mapsto -y$; they commute with $F$ and with the shift by $\sigma$, so by Proposition 9.4 they also preserve (L1). Hence it suffices to treat one class. An even shift $y_t \mapsto y_{t+s}$ preserves (L1) and the class, and multiplies $\nu = Y_2$ by $\xi^{-2s}$, a $(n/4)$-th root of unity; so (H′) takes one $\nu$ in each orbit of these factors.

*The half shift.* For $\sigma = m$, (L1) reads $F(y) = (y_{t+m})_t$, which is the condition of Remark 9.18.

**Lemma 9.21.** *Let $e \geq 3$ be odd, and let $y \in W(2^e)$ satisfy $F(y) = (y_{t+m})_t$. Then $w \neq c\,(J + \delta_{r_0})$ for all $c \in \{\pm 1\}$ and $r_0 \in \mathbb{Z}/m$.*

*Proof.* By Remark 9.18, $d = i\,z$ with $z_r \in \{\pm 1\}$ and $z_{r+m} = -z_r$, and $Z(x)Z(x^{-1}) = 1$ in $\mathbb{F}_3[x]/(x^m + 1)$, where $Z(x) = \sum_{r<m} z_r x^r$. Put $W(x) = \sum_{r<m} w_r x^r$. For odd $k$ we have $Y_k = i\,Z(\xi^k)$, $Y_{k+m} = i\,Z(-\xi^k)$ and $Y_{2k} = W(\xi^{2k})$. The $\xi^k$ with odd $k$ are the roots of $x^m + 1$, so (13)

gives

$$Z(x)\,Z(-x) = -S\,W(x^2) \qquad \text{in } \mathbb{F}_3[x]/(x^m+1).$$

Suppose that $w = c\,(J+\delta_{r_0})$. Since $\sum_{r<m} x^{2r} = (1+x^m)\sum_{r<m/2} x^{2r}$, we get $W(x^2) = c\,x^{2r_0}$ modulo $x^m+1$, so $Z(x)Z(-x) = \varepsilon\,x^{2r_0}$ with $\varepsilon = -Sc$. Multiplying by $Z(x^{-1})$ gives $Z(-x) = \varepsilon\,x^{2r_0}Z(x^{-1})$. Extend $z$ to $\mathbb{Z}/n$ by $z_{r+m} = -z_r$; comparing the coefficients of $x^t$ gives $(-1)^t z_t = \varepsilon\,z_{2r_0-t}$ for all $t$. If $(-1)^{r_0} = -\varepsilon$, take $t = r_0$: then $z_{r_0} = -z_{r_0}$. Otherwise take $t = r_0 + m/2$, which has the parity of $r_0$ because $4 \mid m$; then $2r_0 - t = t - m$, so $z_{2r_0-t} = -z_t$ and $(-1)^{r_0} z_t = -\varepsilon z_t$, that is $z_t = -z_t$. In both cases $z_t = 0$, a contradiction. □

*Remark* 9.22. The proof of Lemma 9.21 does not use that $n$ is a power of 2, and it uses $w$ only through $W$ modulo $x^{m/2}+1$. Let $n \equiv 8 \pmod{24}$, so that $4 \mid m$ and $n \equiv -1 \pmod 3$, and let $y$ solve (1) with $\sigma = m$. Then $y_t^4 = -1$ by (L1) and (L2), so, as in Remark 9.18, $w_t = y_t + y_{t+m} = \pm 1$ and $d_t = y_t - y_{t+m} = i\,z_t$ with $z_t = \pm 1$ and $z_{t+m} = -z_t$. For odd $k$, (L4) gives $Y_k Y_{k+m} = S\,W(\xi^{2k})$, and (L2), (L3) give $Y_k Y_{-k} = n = -1$; as $Y_k = i\,Z(\xi^k)$, this means $Z(x)Z(-x) = -S\,W(x^2)$ and $Z(x)Z(x^{-1}) = 1$ in $\mathbb{F}_3[x]/(x^m+1)$. Modulo $x^m+1$, $W(x^2)$ depends only on $W$ modulo $x^{m/2}+1$. So if $W \equiv \pm x^{r_0} \pmod{x^{m/2}+1}$, the proof of Lemma 9.21 gives $z_t = 0$ for $t = r_0$ or $t = r_0 + m/2$ (this uses $4 \mid m$), a contradiction; and $W \equiv 0 \pmod{x^{m/2}+1}$ is impossible, since then $Z(x)Z(-x) = 0$ although $Z(x)$ and $Z(-x)$ are units ($x \mapsto -x$ is a ring automorphism of $\mathbb{F}_3[x]/(x^m+1)$, as $m$ is even).

**Proposition 9.23.** *Let $n = 128$. For every even $\sigma \geq 4$ that divides $n$, the system* (1) *has no solution.*

*Proof.* For $\sigma = 128$, (L1) gives $y_t^3 = y_t$, so $y_t \in \mathbb{F}_3$; since $y_t y_{t+m} = -1$ by (L2), this gives $y_{t+m} = -y_t$, so $Y_0 = \sum_t y_t = 0$, but $Y_0 = f_0 = \pm 1$.

For $\sigma = 64 = m$, Remark 9.18 shows that $w$ is $\mathbb{F}_3$-valued with no zero. By (12) and (13) at even $k$, and $Y_0 = f_0$, the base satisfies

$$W(x)\,W(x^{-1}) = 1, \qquad W(x)\,W(-x) = S\,W(x^2), \qquad W(1) = f_0 \qquad \text{in } \mathbb{F}_3[x]/(x^{64}-1).$$

Two independent programs, (Z) and (Z′), list all $\mathbb{F}_3$-valued solutions $w$ of these three relations, for each $(S, f_0)$. As the odd residues modulo 64 are $\pm\langle 3\rangle$, the value $b = \hat{w}(1) \in \mathbb{F}_{3^{16}}^{\times}$ fixes $\hat{w}$ at every odd residue, and the even residues give a solution at level 32. (Z) runs over all $b$ and all solutions at level 32; (Z′) builds every solution from $b$ level by level, from level 4 up, and checks directly on the three relations every solution with no zero that it finds. Both find that the only solutions with no zero are the 32 vectors $\pm(J + \delta_{r_0})$ with $r_0 \in \mathbb{Z}/64$, in each class. Lemma 9.21 excludes them.

For $\sigma = 4, 8, 16, 32$, the programs (H) and (H′) find no solution in the class $(S, f_0) = (1, 1)$, and this suffices by the remark before Lemma 9.21. □

*Remark* 9.24. Together with Section 8.1 ($\sigma = 2$, two programs), Proposition 9.23 shows that (1) has no solution at $n = 128$ for any even $\sigma$. The case $\sigma = n$ is excluded in the same way for every $n \equiv 2 \pmod 3$: (L1) gives $y_t \in \mathbb{F}_3$, so (L2) gives $y_{t+m} = -y_t$ and $Y_0 = 0$, while (L2) and (L3) give $Y_0^2 = -n = 1$. For $n = 56$, 80 and 104 we use two other independent programs, (G) and (G′), written for every $n$ with $8 \mid n$ and $3 \nmid n$ and every even $\sigma \mid m$. Each lists the bases from the Fourier values, one value per pair of orbits as above, applies the base test, and checks every point of each fibre on all of (1); (G) runs through the fibre by its Fourier values, (G′) by the signs $\varepsilon_t$ (or, where there are too many signs, by its Fourier values). Both find no solution of (1) for $\sigma = 14, 28$ ($n = 56$), $\sigma = 10, 20, 40$ ($n = 80$) and $\sigma = 26, 52$ ($n = 104$); for $\sigma = 52$, (G′) treats the class $(S, f_0) = (1, 1)$, which suffices as above (the proof of Proposition 9.3 does not use that $n$ is a power of 2). At $n = 80$, $\sigma = 40$, the 40 bases per class that pass the base test are also excluded by Remark 9.22, as $W$ modulo $x^{20}+1$ is $\pm$ a monomial for each of them. For these $n$, $\sigma = 2$ is in Table 5; the values $\sigma = 4$ and 8 (and $\sigma = 16$ for $n = 80$) were not computed.

9.6. **$\mathbb{F}_3$-valued bases with no zero.** For $\sigma = m$ the proof of Proposition 9.23 reduces to the $\mathbb{F}_3$-valued solutions $w$, with no zero, of three relations. Here we prove the needed statement by hand at level 16, and in general under one extra condition. For a power of two $M \geq 4$ call $w \in \mathbb{F}_3^M$ an $\mathbb{F}_3$-*base of level* $M$ if, with $W(x) = \sum_{r<M} w_r x^r$ and some $S, f_0 \in \{\pm 1\}$,

$$W(x)\,W(x^{-1}) = 1, \qquad W(x)\,W(-x) = S\,W(x^2), \qquad W(1) = f_0 \qquad \text{in } \mathbb{F}_3[x]/(x^M - 1).$$

The $\mathbb{F}_3$-bases of level $M$ form a group $B_M$ under multiplication, and the monomials $\pm x^r$ lie in $B_M$. Put $L = M/2$, and let $W^+ = W \bmod (x^L - 1)$ (the fold) and $W^- = W \bmod (x^L + 1)$ (the negafold), with coefficients $w_r^\pm = w_r \pm w_{r+L}$ $(r < L)$. Then $w_r = -(w_r^+ + w_r^-)$ and $w_{r+L} = -(w_r^+ - w_r^-)$, so

$$w \text{ has no zero} \iff \text{for every } r < L \text{ exactly one of } w_r^+,\ w_r^- \text{ is nonzero.} \tag{16}$$

The fold $W^+$ lies in $B_L$ with the same $S$ and $f_0$. Since $(x^L)^2 = 1$ modulo $x^L + 1$, we have $W(x^2) \equiv W^+(x^2)$ there, and the second relation gives

$$W^-(x)\,W^-(-x) = S\,W^+(x^2) \qquad \text{in } \mathbb{F}_3[x]/(x^L + 1), \qquad W^-(x)\,W^-(x^{-1}) = 1. \tag{17}$$

**Lemma 9.25.** *Let $M \geq 8$ and $w \in B_M$. If $W^+ = \varepsilon x^s$ with $\varepsilon = \pm 1$ and $s < L$, then $w_{s+M/4} = w_{s+3M/4} = 0$.*

*Proof.* Put $K = M/4$; it is even. As $W^+ \in B_L$, $\varepsilon^2(-1)^s x^{2s} = S\varepsilon x^{2s}$, so $S\varepsilon = (-1)^s$. By (17), $W^-(x)W^-(-x) = S\varepsilon x^{2s} = (-1)^s x^{2s}$. For $Y = x^{-s}W^-$ in $\mathbb{F}_3[x]/(x^L+1)$ this gives $Y(x)Y(-x) = 1$, and $YY^* = 1$; hence $Y(x^{-1}) = Y(-x)$. The coefficient of $x^K$ is $-y_K$ on the left (as $x^{-K} = -x^K$) and $(-1)^K y_K = y_K$ on the right, so $y_K = 0$, that is, $w_{s+K}^- = 0$ (up to sign, if $s + K \geq L$). Also $w_{s+K}^+ = 0$, as $K \not\equiv 0 \pmod L$. Thus $w_{s+K} = w_{s+K+L} = 0$. □

**Lemma 9.26.** *Let $L \geq 8$ be a power of two with $L \equiv 2 \pmod 3$, and let $\omega$ be a primitive $L$-th root of unity. If $u \in B_L$ and $U(\omega)$ is a 2-power root of unity, then $U = \pm x^r$ or $U = \pm(J - x^r)$ for some $r$, where $J = \sum_{r<L} x^r$.*

*Proof.* The values $U(\omega^j)$ are fixed by $(U(\omega), S, f_0)$. As $L \geq 8$, the odd residues are the $\pm 3^a$, and for odd $j$ we use $U(\omega^{3j}) = U(\omega^j)^3$ and $U(\omega^{-j}) = U(\omega^j)^{-1}$; for even $j \neq 0$ by $U(\omega^{2j'}) = S\,U(\omega^{j'})U(\omega^{j'+L/2})$, from smaller 2-adic valuation upwards; and $U(1) = f_0$. As $L$ is a unit of $\mathbb{F}_3$, $U$ is fixed by these values. The roots of unity in $\mathbb{F}_3(\omega) = \mathbb{F}_{3^{L/4}}$ of 2-power order form $\mu_L$, so at most $4L$ elements $u \in B_L$ have $U(\omega) \in \mu_L$. The $4L$ elements $\pm x^r$ and $\pm(J - x^r)$ have this property ($J(\omega) = 0$), are distinct, and lie in $B_L$: indeed $J - x^r = (J-1)x^r$, and $J - 1 \in B_L$, since $(J-1)(J^* - 1) = (L-2)J + 1 = 1$, and, with $J(x)J(-x) = 0$ and $J(x^2) = 2J_{\text{even}}$ where $J_{\text{even}} = \sum_{r \text{ even}} x^r$, $(J-1)(x)\,(J-1)(-x) = 1 + J_{\text{even}} = -\big(J(x^2) - 1\big)$, so $S = -1$. □

**Lemma 9.27.** *Let $M = 4^k \geq 4$ and let $w \in B_M$ have no zero. If $W^-$ is a monomial, then $W = c\,(J + x^t)$ for some $c = \pm 1$ and $t$.*

*Proof.* For $M = 4$ no hypothesis on $W^-$ is needed: the coefficients of $x$ and $x^2$ in $W(x)W(x^{-1}) = 1$ are $(w_0 + w_2)(w_1 + w_3)$ and $-(w_0 w_2 + w_1 w_3)$, so exactly one of the pairs $(w_0, w_2)$, $(w_1, w_3)$ has equal entries. Hence three entries of $w$ equal some $c$ and the fourth, at $t$ say, is $-c$; that is, $W = c\,(J + x^t)$.

Let $M \geq 16$, $L = M/2$, $K = M/4$, and induct on $k$. Let $W^- = \eta x^s$. By (17), $S\,W^+(x^2) = (-1)^s x^{2s}$ modulo $x^L + 1$, so $B := W^+ \bmod (x^K + 1)$ is a monomial $b\,x^{s'}$ with $s' \equiv s \pmod K$. By (16), $w^+$ vanishes only at $s$. For $r < K$, $r \neq s'$, the coefficient $w_r^+ - w_{r+K}^+$ of $B$ is 0, so $w_r^+ = w_{r+K}^+ \neq 0$; and exactly one of $w_{s'}^+$, $w_{s'+K}^+$ is 0. So the fold $W^{++}$ of $W^+$ (level $K$) has no zero. The negafold of $W^{++}$ is a monomial, by (17) for $W^+$, since $B(x)B(-x) = (-1)^{s'} x^{2s'}$. By induction, $W^{++} = c'(J + x^{r_1}) = c' x^{r_1}(J + 1)$; its value of $S$ is $c'(-1)^{r_1}$ (for $J + 1$ it is 1, since $(J+1)(x)(J+1)(-x) = 1 - J_{\text{even}} = J(x^2) + 1$), and it equals $S$. Now (17) for $W^+$, with $J \equiv 0$ modulo $x^{K/2} + 1$, reads $(-1)^{s'} x^{2s'} = S\,c' x^{2r_1}$ modulo $x^K + 1$. Hence $r_1 \equiv s' \pmod{K/2}$; and $r_1 \equiv s' + K/2 \pmod K$ would give $(-1)^{s'} = -Sc' = -(-1)^{r_1} = -(-1)^{s'}$, as $K/2$ is even. Hence $r_1 = s'$. Then

$w_r^+ = w_{r+K}^+ = -c'$ for $r \neq s'$, and $w^+ = -c'(J - x^s)$, since $w_s^+ = 0$. Finally $w_r = w_{r+L} = c'$ for $r \neq s$, and $\{w_s, w_{s+L}\} = \{-\eta, \eta\} = \{c', -c'\}$, so $W = c'(J + x^t)$ with $t \in \{s, s+L\}$. □

**Proposition 9.28.** *Let $M = 4^k \geq 16$, let $w \in B_M$ have no zero, and let $\omega$ be a primitive $(M/2)$-th root of unity. If $W^+(\omega)$ is a 2-power root of unity (equivalently, $W^+ \bmod (x^{M/4}+1)$ is a monomial), then $W = c\,(J + x^t)$ for some $c = \pm 1$ and $t$.*

*Proof.* By Lemma 9.26 for $L = M/2 \equiv 2 \pmod 3$, $W^+ = \pm x^u$ or $W^+ = \pm(J - x^u)$. The first case is excluded by Lemma 9.25. In the second, $w^+$ vanishes only at $u$, so $W^-$ is a monomial by (16), and Lemma 9.27 applies. □

**Corollary 9.29.** *Every $w \in B_{16}$ with no zero is $c\,(J + x^t)$. Hence for $n = 32$ the system (1) has no solution with $\sigma = 16$.*

*Proof.* Here $\omega$ is a primitive 8-th root of unity, and $W^+(\omega) \in \mathbb{F}_9^\times = \mu_8$; Proposition 9.28 applies. For $\sigma = m = 16$, Remark 9.18 makes the base $w$ an element of $B_{16}$ with no zero (the three relations as in the proof of Proposition 9.23), and Lemma 9.21 excludes $w = c\,(J + \delta_{r_0})$. □

*Remark* 9.30. At level 64 the two independent programs (Z) and (Z′) of Proposition 9.23 find the same answer as Corollary 9.29. There $W^+(\omega)$ lies in $\mathbb{F}_{3^8}^\times$, whose odd part has order 205, so Proposition 9.28 does not cover every base. We have no proof by hand for levels 64 and higher.

9.7. **The odd locus at odd $e$.** By Remark 9.17, for odd $e$ the points of $W(n)$ with a non-trivial stabiliser in $G$ lie on the odd locus $y_t = y_{t+m}$ ($t$ odd) or on its image under the shift by 1, and $S = f_0$ on the odd locus. By Corollary 9.20, for odd $e \geq 5$ no solution of (1) with $\sigma = 2$ lies on either locus, so this subsection and Subsection 9.8 concern only the strong form $W(2^e) = \emptyset$, not planes.

The plan is as follows. By Lemma 9.31, the base of a point on the odd locus lies in the set $P(m)$ defined below, and each element of $P(M)$ with $M \geq 8$ is in one of two cases, (I) or (II). In case (II) its fold lies in $P(M/2)$. For odd $e \geq 5$, folding repeatedly, the base first reaches case (I) at some level $M_0 \geq 8$ (Lemma 9.35). Lemma 9.32 treats $M_0 = m$, and Lemma 9.37 excludes $M_0 = 16$ for $e \geq 7$. Lemma 9.34 (for $n = 32$), Lemma 9.38 and Question 9.39 concern $M_0 = 8$, and Lemmas 9.42 and 9.45 give conditions on the other chains. With computations for $n = 128$, Corollary 9.43 and Proposition 9.44 use these to show that no point of $W(32)$ or $W(128)$ lies on the odd locus or on its shift by 1. Subsection 9.8 returns to $M_0 = 8$ for odd $e \geq 11$.

For a power of two $M \geq 2$ and $S = \pm 1$ let $P(M)$ be the set of $w \in \overline{\mathbb{F}}_3^{\mathbb{Z}/M}$ such that $W(x) = \sum_r w_r x^r$ satisfies, modulo $x^M - 1$,

$$W(x)W(x^{-1}) = 1, \qquad W(x)W(-x) = S\,W(x^2), \qquad W(1) = S,$$

and $w_r^2 = -1$ for every odd $r$. For $w \in P(M)$ with $M \geq 4$ we write $w_r^+ = w_r + w_{r+M/2}$ ($r \in \mathbb{Z}/(M/2)$) for its *fold*.

**Lemma 9.31.** *Let $e \geq 3$ be odd.*

(a) *The base $w$ of a point on the odd locus lies in $P(m)$.*

(b) *Let $M \geq 8$ and $w \in P(M)$. Then exactly one of the following holds. (I) $w_{r+M/2} = -w_r$ for every odd $r$, and $w^+ = S\,\delta_{2r_1}$ for some $r_1$. (II) $w_{r+M/2} = w_r$ for every odd $r$, and $w^+ \in P(M/2)$.*

(c) *$P(2) = \emptyset$, and $P(4)$ consists of the four vectors $(w_0, w_1, w_2, w_3) = \big(-(S + i\gamma),\ i\alpha,\ -(S - i\gamma),\ -i\alpha\big)$ with $\alpha, \gamma = \pm 1$.*

(d) *Let $n \geq 32$, let $y$ lie on the odd locus, and let its base $w$ be as in (II) (with $M = m$). Then $T(w) := \sum_{\rho \in \mathbb{Z}/(m/2)} (-1)^\rho w_{2\rho}^2$ lies in $\mathbb{F}_3$.*

*Proof.* (a) On the odd locus $d_r = 0$ for odd $r$, and $d_r^2 = w_r^2 + 1$ (as $1/n = -1$) gives $w_r^2 = -1$. The identities of $P(m)$ are those of Lemma 9.2(a) reduced modulo $x^m - 1$, and $W(1) = Y_0 = f_0 = S$.

(b) Let $\zeta$ be a primitive $M$-th root of unity and $\widehat{w}(j) = W(\zeta^j)$. The identities of $P(M)$ say $\widehat{w}(-j) = \widehat{w}(j)^{-1}$ and $\widehat{w}(j)\,\widehat{w}(j+M/2) = S\,\widehat{w}(2j) =: q(j)$. Write $w_{2\rho+1} = i\tau_\rho$ with $\tau_\rho = \pm 1$ and $\tau(v) = \sum_{\rho<M/2} \tau_\rho v^\rho$. For odd $j$ put $\delta(j) = \widehat{w}(j) - \widehat{w}(j+M/2) = -i\zeta^j \tau(\zeta^{2j})$. As $\tau$ has coefficients in $\mathbb{F}_3$, $\delta(3j) = -\delta(j)^3$; and $\delta(-j) = \widehat{w}(j)^{-1} - \widehat{w}(j+M/2)^{-1} = -\delta(j)/q(j)$. The odd residues modulo $M$ are the $\pm 3^a$, so $\delta$ vanishes at every odd $j$ or at none.

If $\delta$ vanishes at every odd $j$, then $\tau$ vanishes at every primitive $(M/2)$-th root of unity, so $v^{M/4}+1$ divides $\tau$ and $\tau_{\rho+M/4} = \tau_\rho$, that is, $w_{r+M/2} = w_r$ for odd $r$. Then $w_r^+ = 2w_r = -w_r$ for odd $r$, and reducing the identities of $P(M)$ modulo $x^{M/2}-1$ gives $w^+ \in P(M/2)$. This is (II).

Otherwise $\delta(-3j) = -\delta(3j)/q(3j) = \delta(j)^3/q(3j)$ and $\delta(-3j) = -\delta(-j)^3 = \delta(j)^3/q(j)^3$, so $q(3j) = q(j)^3$, that is, $\widehat{w}(6j) = \widehat{w}(2j)^3$ for odd $j$: the rule $\widehat{w}(3k) = \widehat{w}(k)^3$ holds for every $k$ of 2-adic valuation 1. We induct on the valuation $v$, starting at $v = 1$. If the rule holds for all $k$ of valuation $v < \log_2(M/2)$, then $\widehat{w}(6k) = S\,\widehat{w}(3k)\,\widehat{w}(3k+M/2) = \widehat{w}(2k)^3$, since $3(k+M/2) \equiv 3k + M/2$ and $k + M/2$ has valuation $v$ as well (here $M \geq 8$ is used at $v = 1$). With $\widehat{w}(0) = S$ and $S^3 = S$ this gives $\widehat{w}(3k) = \widehat{w}(k)^3$ for every even $k$, so the fold $w^+$, whose values are the $\widehat{w}(2j)$, is $\mathbb{F}_3$-valued. For odd $r$, $w_r^+ = w_r + w_{r+M/2} \in \mathbb{F}_3 \cap \{0, \pm i\} = \{0\}$, so $w_{r+M/2} = -w_r$, and $W^+(x) = A(x^2)$ with $A \in \mathbb{F}_3[v]/(v^{M/4}-1)$, $AA^* = 1$ and $A(v)^2 = S\,A(v^2)$. Put $\varphi(j) = S\,A(\theta^j)$ with $\theta$ a primitive $(M/4)$-th root of unity. Then $\varphi(2j) = \varphi(j)^2$, $\varphi(3j) = \varphi(j)^3$, $\varphi(-j) = \varphi(j)^{-1}$ and $\varphi(0) = S\,A(1) = 1$. Every residue modulo $M/4$ is $\pm 3^a 2^b$, so $\varphi(j) = \varphi(1)^j$, and $A = S\,v^{r_1}$ for some $r_1$. This is (I). The two cases exclude each other, since $w_r \neq 0$ for odd $r$.

(c) For $M = 2$, $w_1^2 = -1$ and $W(x)W(x^{-1}) = 1$ give $w_0^2 + w_1^2 = 1$ and $2w_0w_1 = 0$, so $w_0 = 0$ and $w_1^2 = 1$, a contradiction. For $M = 4$ the coefficient of $x$ in $W(x)W(x^{-1})$ is $(w_0+w_2)(w_1+w_3)$; if $w_3 = w_1$, then $w_1 + w_3 = \pm 2i \neq 0$, so $w_0 + w_2 = 0$ and $W(1) = \pm 2i \neq S$. Hence $w_3 = -w_1 = -i\alpha$ and $w_0 + w_2 = W(1) = S$. The coefficient of $x^2$ in $W(x)W(x^{-1})$ gives $w_0w_2 = -w_1w_3 = -1$, so $(w_0 - w_2)^2 = S^2 + 4 = -1$ and $w_0 - w_2 = i\gamma$. These four vectors satisfy all identities of $P(4)$.

(d) As in the proof of Lemma 9.32(a), $D(x) = E(x^2)$ with $E \in R = \overline{\mathbb{F}}_3[u]/(u^{m/2}+1)$, $EE^* = -1$ and $E^2 = S\,W^-$, where $W^-$ is $W$ mod $(x^{m/2}+1)$, written in the variable $u$. In (II), $W^- = C(u^2)$ with $C(v) = \sum_{\rho<m/4} c_\rho v^\rho$, $c_\rho = w_{2\rho} - w_{2\rho+m/2}$. Put $\Gamma(u^2) = E(u)E(-u)$. Then $\Gamma^2 = W^-(u)W^-(-u) = C(u^2)^2$, so $C(\eta)/\Gamma(\eta) = \pm 1$ at every root $\eta$ of $v^{m/4}+1$, and $\Gamma^* = 1/\Gamma$ by $EE^* = -1$. Sum the line $d_{2\rho}^2 = w_{2\rho}^2 + 1$ with signs $(-1)^\rho$ over $\rho \in \mathbb{Z}/(m/2)$. The right side is $T(w)$. The left side is the constant term of $E(u)E(-u^{-1})$, that is $\frac{2}{m}\sum_\theta E(\theta)E(-1/\theta)$ over the roots $\theta$ of $u^{m/2}+1$, with $\frac{2}{m} = -1$. Now $E(-1/\theta) = -E(\theta)/\Gamma(\theta^2)$, so $E(\theta)E(-1/\theta) = -S\,C(\theta^2)/\Gamma(\theta^2)$, and each $\eta$ is $\theta^2$ for two $\theta$. So the left side is $-S\sum_\eta C(\eta)/\Gamma(\eta)$, a sum of signs in $\mathbb{F}_3$. □

Let $e \geq 5$ be odd, $L = n/8$ (so $m = 4L$ and $L \equiv 1 \pmod 3$), and let $y \in W(n)$ lie on the locus $y_t = y_{t+m}$ ($t$ odd), so that $S = f_0$ (Remark 9.17). Then $d_r = 0$ and $w_r^2 = -1$ for odd $r$. We write $s_\rho = -i\,w_{2\rho+1} \in \{\pm 1\}$ and $c_\rho = w_{2\rho} - w_{2\rho+2L}$ for $\rho < L$, and $s(v) = \sum_{\rho<L} s_\rho v^\rho$, $C(v) = \sum_{\rho<L} c_\rho v^\rho$.

**Lemma 9.32.** *In this situation suppose that, for some $r_1$,*

$$w_r + w_{r+2L} = S \quad \text{if } r \equiv 2r_1 \pmod{2L}, \qquad w_r + w_{r+2L} = 0 \quad \text{otherwise.} \tag{18}$$

*For the $L$ roots $\eta$ of $v^L + 1$ put $h(\eta) = \eta^{-r_1} C(\eta)$.*

(a) *$h(1/\eta) = h(\eta)$ and $h(\eta)^2 = \Theta(\eta) := 1 - \eta^{1-2r_1} s(\eta)^2$, and there are signs $\Gamma(\eta) = \Gamma(1/\eta) \in \{\pm 1\}$ with*

$$S\sum_\eta \Gamma(\eta)\,h(\eta) \;=\; 1 + \sum_\eta h(\eta)\,h(-\eta).$$

(b) *For $n = 32$ there is no such $y$.*

(c) *For $n \geq 128$ there is no such $y$ if $\Theta(\eta)$ is a non-square in $\mathbb{F}_3(\eta)$ for one root $\eta$.*

*Proof.* (a) Put $W(x) = \sum_r w_r x^r$, $W^\pm = W$ mod $(x^{2L} \mp 1)$ and $D(x) = \sum_r d_r x^r$, so that $Y \equiv W \pmod{x^m - 1}$ and $Y \equiv D \pmod{x^m + 1}$. Reducing Lemma 9.2(a) gives $WW^* = 1$, $DD^* = -1$ (here

$P^*(x) = P(x^{-1})$), $W(x)W(-x) = S\,W^+(x^2)$ and $D(x)D(-x) = S\,W^-(x^2)$. By (18), $W^+ = S\,x^{2r_1}$, and $w_{r+2L} = -w_r$ for odd $r$, so $W^- = C(u^2) - i\,u\,s(u^2)$ in $R = \overline{\mathbb{F}}_3[u]/(u^{2L}+1)$. On the locus $D(x) = E(x^2)$ with $E \in R$, hence $E^2 = S\,W^-$ and $EE^* = -1$. Now $\Psi := u^{-2r_1}W^-$ satisfies $\Psi\Psi^* = 1$ and $\Psi(u)\Psi(-u) = u^{-4r_1}W^-(u)W^-(-u) = 1$, so $\Psi^* = \Psi(-u)$. The even part of $\Psi$ is $u^{-2r_1}C(u^2)$, so it is fixed by $^*$, which is $h(1/\eta) = h(\eta)$; and $1 = \Psi(u)\Psi(-u)$ evaluated at $u^2 = \eta$ is $h(\eta)^2 + \eta^{1-2r_1}s(\eta)^2$. Put $\Gamma(u^2) = u^{-2r_1}E(u)E(-u)$. Then $\Gamma^2 = \Psi(u)\Psi(-u) = 1$ and $\Gamma^* = 1/\Gamma = \Gamma$.

The line at $s = 2\rho$ reads $d_{2\rho}^2 = w_{2\rho}^2 + 1$. Multiply by $(-1)^\rho$ and sum over $\rho \in \mathbb{Z}/2L$. On the left we get the constant term of $E(u)E(-u^{-1})$, that is $\frac{1}{2L}\sum_\theta E(\theta)E(-1/\theta)$ over the roots $\theta$ of $u^{2L}+1$, and $\frac{1}{2L} = -1$. From $E(1/\theta) = -1/E(\theta)$ and $\Gamma$ we get $E(-1/\theta) = -\theta^{-2r_1}\Gamma(\theta^2)E(\theta)$, so $E(\theta)E(-1/\theta) = -S\,\Gamma(\theta^2)\Psi(\theta)$; the odd part of $\Psi$ cancels between $\theta$ and $-\theta$, and the left side is $-S\sum_\eta \Gamma(\eta)h(\eta)$. On the right, (18) gives $w_{2\rho} = -(S[\rho = r_1] + c_\rho)$ and $w_{2\rho+2L} = -(S[\rho = r_1] - c_\rho)$ for $\rho < L$, so the sum is $-\sum_{\rho<L}(-1)^\rho c_\rho^2 - (-1)^{r_1}$. In the same way $\sum_{\rho<L}(-1)^\rho c_\rho^2 = \sum_\eta C(\eta)C(-1/\eta) = (-1)^{r_1}\sum_\eta h(\eta)h(-\eta)$, using $\frac{1}{L} = 1$ and $C(1/\eta) = \eta^{-2r_1}C(\eta)$. Replacing $\Gamma$ by $(-1)^{r_1}\Gamma$ gives (a).

(b) Here $L = 4$. The odd part $\hat\sigma = u^{1-2r_1}s(u^2)$ of $i\Psi$ is antisymmetric (by $\Psi^* = \Psi(-u)$) with entries $\pm1$ at the odd places, so $\hat\sigma = a(u+u^7) + b(u^3+u^5)$ and $\hat\sigma^2 = -1 + ab(u^2 - u^6)$; thus $\Theta(\eta) = -1 - ab\,y(\eta)$ with $y(\eta) = \eta - \eta^3$. The $\eta$ are the primitive 8-th roots of unity, which lie in $\mathbb{F}_9$, and $y(\eta)^2 = -1$; so $\Theta(\eta) = -1 \pm i$, a non-square in $\mathbb{F}_9$, and $h(\eta)^9 = -h(\eta)$. As $y(-\eta) = -y(\eta)$, $\Theta(\eta)\Theta(-\eta) = 1 - y(\eta)^2 = -1$, so $h(\eta)h(-\eta) = \pm i$ and the right side of (a) lies in $\mathbb{F}_9$. The left side $A$ satisfies $A^9 = -A$. With $\eta_1$ one root, the roots are $\eta_1^{\pm1}, \eta_1^{\pm3}$, so $A = -S\big(\Gamma(\eta_1)h(\eta_1) + \Gamma(\eta_1^3)h(\eta_1^3)\big)$; $A = 0$ would give $\Theta(\eta_1) = \Theta(\eta_1^3)$, but $y(\eta_1^3) = -y(\eta_1) \neq 0$. So $A \notin \mathbb{F}_9$, and (a) fails.

(c) Here $L \geq 16$, $\mathbb{F}_3(\eta) = \mathbb{F}_{3^{L/2}}$, and $3^{L/4} \equiv 1 + L \pmod{2L}$. Let $\tau(x) = x^{3^{L/2}}$ and $\tau'(x) = x^{3^{L/4}}$; then $\tau(\eta) = \eta$ and $\tau'(\eta) = -\eta$ (again a root, as $L$ is even). Since $\Theta$ has coefficients in $\mathbb{F}_3$ and $\Theta(1/\eta) = \Theta(\eta)$ (by (a)), and every root is $\eta^{\pm 3^j}$, $\Theta$ is a non-square at every root. Hence $\tau(h(\eta)) = -h(\eta)$, so $\tau$ changes the sign of the left side of (a) and fixes the right side: both sides vanish. Next, $\tau'(h(\eta)) = \mu(\eta)h(-\eta)$ with $\mu(\eta) = \pm1$, as both square to $\Theta(-\eta)$; applying $\tau'$ twice gives $\mu(\eta)\mu(-\eta) = -1$. Hence $\tau'$ changes the sign of $\sum_\eta h(\eta)h(-\eta)$, which is $-1$ if the right side of (a) vanishes. But $\tau'(-1) = -1$. □

*Remark* 9.33. Lemma 9.32 needs $e \geq 5$ ($L \geq 4$); for $n = 8$ ($L = 1$) the proof does not apply, in line with $W(8)$ lying on the two loci. The identity in (a) was also checked numerically on all 2048 fibres with $EE^* = -1$ over the bases (18) at $n = 32$ (both classes $S = f_0 = \pm1$; one program, a second one checked 1024 of these fibres); the right side of (a) never equals the left side there. For $n = 128$, half of the 256 admissible $\hat\sigma$ satisfy the hypothesis of (c); the other half was checked by computation (two independent programs, Table 8): no fibre of a base satisfying (18) satisfies the whole even line.

The bases of case (II) of Lemma 9.31(b), with $w_{r+m/2} = w_r$ for odd $r$, are not covered by (18). For $n = 32$ the following lemma treats those whose fold $w_r^+ = w_r + w_{r+8}$ ($r \in \mathbb{Z}/8$) is in case (I) one level down.

**Lemma 9.34.** *Let $n = 32$ and let $y \in W(32)$ lie on the locus $y_t = y_{t+16}$ ($t$ odd). Suppose that $w_{r+8} = w_r$ for odd $r$, and that for some $r_1'$*

$$w_r^+ + w_{r+4}^+ = S \quad \text{if } r \equiv 2r_1' \pmod 4, \qquad w_r^+ + w_{r+4}^+ = 0 \quad \text{otherwise.}$$

*Then no such $y$ exists.*

*Proof.* Put $W^+(x) = \sum_{r<8} w_r^+ x^r$, $W^{+-} = W^+ \bmod (x^4+1)$, and $W^- = W \bmod (x^8+1)$. Reducing $WW^* = 1$ and $W(x)W(-x) = S\,W^+(x^2)$ gives $W^+W^{+*} = 1$ and $W^+(x)W^+(-x) = S\,W^{++}(x^2)$ with $W^{++} = W^+ \bmod (x^4-1) = S\,x^{2r_1'}$, hence $W^{+-}(x)W^{+-}(-x) = x^{4r_1'}$ and $W^{+-}W^{+-*} = 1$ modulo $x^4+1$. For odd $r$ we have $w_r^+ = 2w_r = -w_r$, so $(w_r^+)^2 = -1$ and $w_{r+4}^+ = -w_r^+$; write $w_1^+ = i\alpha$, $w_3^+ = i\beta$ with $\alpha, \beta \in \{\pm1\}$ and $ab := \alpha\beta$. As in the proof of Lemma 9.32(a), now with

$L$ replaced by 2, $\Psi' = x^{-2r_1'}W^{+-}$ satisfies $\Psi'^{*} = \Psi'(-x)$, so its odd part is $-i\,\varepsilon(x+x^3)$ for some $\varepsilon = \pm 1$, whose square is $-1$; since $\Psi'(x)\Psi'(-x) = 1$, the even part of $\Psi'$ squares to 0 and vanishes. Hence $W^{+-}(y) = -i(\alpha y + \beta y^3)$ in the level-8 variable $y$ ($y^4 = -1$), and $w^+_{2k} = w^+_{2k+4} = -S[k = r_1']$ $\in \mathbb{F}_3$.

Since $w_{r+8} = w_r$ for odd $r$, $W^-$ has only even powers: $W^- = C(x^2)$ with $C(v) = \sum_{k<4} c_k v^k$, $c_k = w_{2k} - w_{2k+8}$. Reducing the two identities modulo $x^8+1$ and putting $y = v = x^2$ gives $C(v)^2 = S\,W^{+-}(v) = -S\,i(\alpha v + \beta v^3)$ and $CC^* = 1$ in $\overline{\mathbb{F}}_3[v]/(v^4+1)$. At a root $\eta$ of $v^4+1$ (a primitive 8-th root of unity, in $\mathbb{F}_9$) we have $(\alpha\eta + \beta\eta^3)^2 = -2ab = ab$, so $C(\eta)^4 = -ab$ and $C(\eta)^3 = -ab\,C(1/\eta)$. As $c_k = \sum_\eta C(\eta)\eta^{-k}$ (here $\frac{1}{4} = 1$), cubing gives $c_k^3 = -ab\,\tilde{c}_{-3k}$, where $\tilde{c}$ is the extension of $c$ with $\tilde{c}_{k+4} = -\tilde{c}_k$. So the two $c_k$ with $(-1)^k = ab$ lie in $\{0, \pm i\}$ and the other two lie in $\mathbb{F}_3$. One of the first two is 0: the coefficients of $v^0$ and $v^2$ in $C^2$ vanish, $c_0^2 + c_1c_3 - c_2^2 = 0 = -c_0c_2 + c_1^2 - c_3^2$, and $\sum_k c_k^2 = 1$ (the constant term of $CC^*$). If $ab = 1$ and $c_0, c_2 \in \{\pm i\}$, the first equation gives $c_1c_3 = 0$; then $c_1 = c_3 = 0$ contradicts the second, and otherwise $\sum_k c_k^2 = -1 - 1 + 1 = -1$. If $ab = -1$ and $c_1, c_3 \in \{\pm i\}$, the second gives $c_0c_2 = 0$ and the first gives $c_0^2 - c_2^2 = -c_1c_3 = \pm 1$, so $\sum_k c_k^2 = 1 - 1 - 1 = -1$.

Let $k$ be such that $(-1)^k = ab$ and $c_k = 0$. On the locus $D(x) = E(x^2)$ with $E(u)^2 = S\,C(u^2)$ in $\overline{\mathbb{F}}_3[u]/(u^8+1)$, so $E(\theta)^8 = C(\theta^2)^4 = -ab$ at every root $\theta$ of $u^8+1$, and $\theta^9 = -\theta$. The line at $s = 2\rho$ reads $d_{2\rho}^2 = w_{2\rho}^2 + 1$, where $d_{2\rho} = -\sum_\theta E(\theta)\theta^{-\rho}$ (as $\frac{1}{8} = -1$); hence $d_{2\rho}^9 = -ab(-1)^\rho\, d_{2\rho}$. At $\rho = k$: $w_{2k} = -(w^+_{2k} + c_k) \in \mathbb{F}_3$, so $d_{2k}^2 = w_{2k}^2 + 1 \in \{\pm 1\}$ and $d_{2k}^8 = 1$, while $d_{2k}^9 = -d_{2k}$ gives $d_{2k}^8 = -1$. □

For every odd $e \geq 5$, Lemma 9.35 below uses Lemma 9.31(d) to exclude the bases that stay in case (II) down to level 4. For a power of two $M \geq 4$ and $u \in P(M)$ put $T_M(u) = \sum_{\rho \in \mathbb{Z}/(M/2)} (-1)^\rho u_{2\rho}^2$; thus $T_m(w) = T(w)$.

**Lemma 9.35.** *Let $e \geq 5$ be odd and let $y \in W(n)$ lie on the locus $y_t = y_{t+m}$ ($t$ odd), with base $w$. Put $w^{(m)} = w$ and, as long as $w^{(M)}$ is in case (II) of Lemma 9.31(b), $w^{(M/2)} = (w^{(M)})^+ \in P(M/2)$. Then $w^{(M)}$ is in case (I) for some $M \in \{8, 16, \dots, m\}$.*

*Proof.* Suppose that $w^{(M)}$ is in case (II) for every $M = m, m/2, \dots, 8$, so that $a = w^{(4)}$ is one of the vectors of Lemma 9.31(c). For $8 \leq M \leq m$ let $u = w^{(M)}$ and $U(x) = \sum_r u_r x^r$. In case (II), $U \bmod (x^{M/2}+1) = C_M(x^2)$ with $C_M(v) = \sum_{k<M/4} c_k v^k$ and $c_k = u_{2k} - u_{2k+M/2}$.

(1) As $u_{2k} = -(u^+_{2k} + c_k)$, $u_{2k+M/2} = -(u^+_{2k} - c_k)$ and $(-1)^{M/4} = 1$, pairing $\rho = k$ with $\rho = k + M/4$ gives

$$T_M(u) = -T_{M/2}(u^+) - K_M, \qquad K_M = \sum_{k<M/4} (-1)^k c_k^2.$$

(2) Let $M \geq 16$. Modulo $x^{M/2}+1$ we have $x^M = 1$, so $U(x^2) \equiv U^+(x^2)$, and $U^+(y) \bmod (y^{M/4}+1) = C_{M/2}(y^2)$ because $u^+$ is in case (II) as well. Thus the identity $U(x)U(-x) = S\,U(x^2)$ of $P(M)$ gives $C_M(v)^2 = S\,C_{M/2}(v^2)$ in $\overline{\mathbb{F}}_3[v]/(v^{M/4}+1)$. Let $\eta$ be a root of $v^{M/4}+1$; then $-\eta$ is a root too ($M/4$ is even), $C_M(\eta) \neq 0$ since $C_MC_M^* = 1$ (reduce $UU^* = 1$ modulo $x^{M/2}+1$), and $C_M(-\eta) = \pm C_M(\eta)$. Hence $K_M$, the constant term of $C_M(v)C_M(-1/v)$, is $\frac{4}{M}\sum_\eta C_M(\eta)/C_M(-\eta)$, a sum of signs times the unit $\frac{4}{M}$ of $\mathbb{F}_3$, and $K_M \in \mathbb{F}_3$.

(3) For $M = 8$, $u^+ = a$, and as in (2) $C_8(v)^2 = S\big((a_0 - a_2) + (a_1 - a_3)v\big)$ with $v^2 = -1$, so $K_8 = c_0^2 - c_1^2 = S(a_0 - a_2) = S\,i\gamma$, while $T_4(a) = (a_0 + a_2)(a_0 - a_2) = S\,i\gamma$. Hence $T_8(u) = -2S\,i\gamma = S\,i\gamma$.

By (1)–(3), $T_M(w^{(M)}) \equiv -T_{M/2}(w^{(M/2)})$ modulo $\mathbb{F}_3$ for $16 \leq M \leq m$, so $T(w) \equiv \pm S\,i\gamma$ modulo $\mathbb{F}_3$ and $T(w) \notin \mathbb{F}_3$. This contradicts Lemma 9.31(d). □

*Remark* 9.36. In the same way, if $w^{(M)}$ is in case (II) for $M = m, \dots, 2M_0$ and $w^{(M_0)}$ is in case (I) with $M_0 \geq 8$, then $T(w) \equiv \pm T_{2M_0}(w^{(2M_0)})$ modulo $\mathbb{F}_3$. For $M_0 = 8$ the right side lies in $\mathbb{F}_3$ (by the

first two paragraphs of the proof of Lemma 9.34, which use only the base $w^{(16)}$), so Lemma 9.31(d) gives no condition on these chains.

For odd $e \geq 7$, Lemma 9.37 below uses the transfer in Remark 9.36 to exclude the chains that reach case (I) at level 16.

**Lemma 9.37.** *Let $e \geq 7$ be odd and let $y \in W(n)$ lie on the locus $y_t = y_{t+m}$ ($t$ odd), with base $w$. Then it is not the case that $w^{(M)}$ is in case (II) for $M = m, m/2, \dots, 32$ and $w^{(16)}$ is in case (I).*

*Proof.* Suppose it is. Let $u = w^{(32)}$, so $u^+ = w^{(16)} \in P(16)$ satisfies (18) with $L = 4$, and let $h$, $\hat{\sigma}$, $\Psi$ be as in the proof of Lemma 9.32 for $u^+$. The parts of that proof used below (the first paragraph of the proof of (a): $h(1/\eta) = h(\eta)$, $h^2 = \Theta$, $\Psi(v)\Psi(-v) = 1$; its second paragraph: the evaluation of the right side of the line sum, which gives the formula for $T_{16}(u^+)$ used below; and the computation of $\Theta$ in (b)) use only the identities of $P(16)$, so they hold for $u^+$. By step (1) of the proof of Lemma 9.35, $T_{32}(u) = -T_{16}(u^+) - K_{32}$.

As in the proof of Lemma 9.32(a) (with $\frac{1}{L} = 1$), $T_{16}(u^+) = -(-1)^{r_1}\big(1 + \sum_\eta h(\eta)h(-\eta)\big)$, the sum over the roots of $v^4 + 1$. With $\eta_1$ one root, $-\eta_1 = \eta_1^{-3}$ and $-\eta_1^3 = \eta_1^{-1}$, so $h(1/\eta) = h(\eta)$ gives $\sum_\eta h(\eta)h(-\eta) = 4h(\eta_1)h(\eta_1^3) = h(\eta_1)h(\eta_1^3)$. By the proof of Lemma 9.32(b), $h(\eta_1)^2 h(\eta_1^3)^2 = (-1 - ab\,y)(-1 + ab\,y) = 1 - y^2 = -1$ with $y = y(\eta_1) = \pm i$, so the sum is $\pm i$ and $T_{16}(u^+) = -(-1)^{r_1}(1 \pm i)$.

Next, $U \bmod (x^{16} + 1) = C(x^2)$ with $C(v)^2 = S\, v^{2r_1}\Psi(v)$ and $CC^* = 1$ in $\overline{\mathbb{F}}_3[v]/(v^8 + 1)$ (reduce the relations of $P(32)$). Let $\eta$ be a root of $v^8 + 1$. As $\Psi(v)\Psi(-v) = 1$, $(C(\eta)/C(-\eta))^2 = \Psi(\eta)^2$, so $C(\eta)/C(-\eta) = \lambda(\eta)\Psi(\eta)$ with $\lambda(\eta) = \pm 1$, and $\lambda(-\eta) = \lambda(\eta)$. Hence, as in step (2) of the proof of Lemma 9.35, $K_{32} = \frac{1}{8}\sum_\eta \lambda(\eta)\Psi(\eta)$; the odd part $-i\hat{\sigma}$ cancels between $\eta$ and $-\eta$, so $K_{32} = \sum_\zeta \lambda(\zeta)h(\zeta)$ over the roots $\zeta = \eta^2$ of $z^4 + 1$ (with $\lambda$ read on $\zeta$). By the proof of Lemma 9.32(b), $h(\zeta) \in \mathbb{F}_{81} \setminus \mathbb{F}_9$ and $h(\zeta)^9 = -h(\zeta)$, while $\zeta \in \mathbb{F}_9$; so $\psi(x) = x^9$ gives $\psi(K_{32}) = -K_{32}$ and $\psi(T_{16}(u^+)) = T_{16}(u^+)$.

If $T_{32}(u)$ were in $\mathbb{F}_3$, then $\psi$ would fix it, so $K_{32} = 0$ and $T_{32}(u) = (-1)^{r_1}(1 \pm i) \notin \mathbb{F}_3$. Hence $T_{32}(u) \notin \mathbb{F}_3$, and by Remark 9.36 (here $m \geq 64$), $T(w) \notin \mathbb{F}_3$, against Lemma 9.31(d). □

The chains that reach case (I) at level 8 are not seen by $T$ (Remark 9.36). For them all spectral values are 2-power roots of unity, and two Frobenius powers act on the coefficients by explicit rules. For $M \geq 16$ in the chain write $c_k^{(M)} = w_{2k}^{(M)} - w_{2k+M/2}^{(M)}$, extended to all $k$ by $c_{k+M/4}^{(M)} = -c_k^{(M)}$, and $C_M(v) = \sum_{k<M/4} c_k^{(M)} v^k$.

**Lemma 9.38.** *Let $e \geq 7$ be odd and let $y \in W(n)$ lie on the locus $y_t = y_{t+m}$ ($t$ odd), with base $w$. Suppose that $w^{(M)}$ is in case (II) of Lemma 9.31(b) for $M = m, m/2, \dots, 16$ and that $w^{(8)}$ is in case (I), and write $w_1^{(8)} = i\alpha$, $w_3^{(8)} = i\beta$ with $\alpha, \beta \in \{\pm 1\}$. Then for every $k$ with $(-1)^k = \alpha\beta$ the four elements $z_t = \big(w_{2k+tm/8}^{(m/2)}\big)^2 + 1$ ($t \in \mathbb{Z}/4$) satisfy*

$$z_0 z_2 = z_1 z_3 \qquad \text{and} \qquad P^2 - P + z_0 z_2 = 0, \quad P = z_0^2 + z_1^2 + z_2^2 + z_3^2.$$

*Proof.* (1) *Spectra.* The first paragraph of the proof of Lemma 9.34 uses only the identities of $P(8)$, so the polynomial of $w^{(8)}$ modulo $x^4 + 1$ is $-i(\alpha x + \beta x^3)$ and the even entries of $w^{(8)}$ lie in $\mathbb{F}_3$. As in its second paragraph, $C_{16}(v)^2 = -S\, i(\alpha v + \beta v^3)$, and as in step (2) of the proof of Lemma 9.35, $C_M(v)^2 = S\, C_{M/2}(v^2)$ for $M \geq 32$, in $\overline{\mathbb{F}}_3[v]/(v^{M/4} + 1)$. Since $S^{M/16} = 1$ for $M \geq 32$, induction gives at every root $\eta$ of $v^{M/4} + 1$

$$C_M(\eta)^{M/8} = C_{16}(\eta^{M/16})^2 = -S\, i\big(\alpha\eta^{M/16} + \beta\eta^{3M/16}\big), \qquad C_M(\eta)^{M/4} = -\alpha\beta,$$

because $(\alpha\zeta + \beta\zeta^3)^2 = \alpha\beta$ when $\zeta^4 = -1$. On the locus $D(x) = E(x^2)$ with $E(u)^2 = S\, C_m(u^2)$ in $\overline{\mathbb{F}}_3[u]/(u^{m/2} + 1)$ (as in the proof of Lemma 9.32(a), now $W^- = C_m(x^2)$), so $E(\theta)^{m/4} = C_m(\theta^2)^{m/8} = -S\, i(\alpha\theta^{m/8} + \beta\theta^{3m/8})$ and $E(\theta)^{m/2} = -\alpha\beta$. All these values are roots of unity of 2-power order.

(2) *Frobenius.* Recall $v_2(3^{2^j}-1) = j+2$ for $j \geq 1$. Let $M \geq 32$. Then $3^{M/16} \equiv 1 + M/4 \pmod{M/2}$, so $\eta^{3^{M/16}} = -\eta$ and $C_M(\eta)^{3^{M/16}} = -\alpha\beta\, C_M(\eta)$; as $c_k^{(M)} = \frac{4}{M}\sum_\eta C_M(\eta)\eta^{-k}$ with $\frac{4}{M} \in \mathbb{F}_3$,

$$\big(c_k^{(M)}\big)^{3^{M/16}} = -\alpha\beta\,(-1)^k\, c_k^{(M)}.$$

Let $M \geq 64$. Then $3^{M/32} = 1 + M/8 + \delta M/4 \pmod{M/2}$ with $\delta \in \{0,1\}$, so $\eta^{3^{M/32}} = (-1)^\delta \eta^{1+M/8}$ and $C_M(\eta)^{3^{M/32}} = (-\alpha\beta)^\delta C_M(\eta)\, C_M(\eta)^{M/8}$; with the formula of (1),

$$\big(c_k^{(M)}\big)^{3^{M/32}} = \lambda_k\big(\alpha\, c_A^{(M)} + \beta\, c_{A-M/8}^{(M)}\big), \qquad A = k(1+\tfrac{M}{8}) - \tfrac{M}{16},$$

with $\lambda_k = -S\, i\,(-\alpha\beta)^\delta(-1)^{\delta k}$, so $\lambda_k^2 = -1$. The same computation for $e_\rho := d_{2\rho} = \frac{2}{m}\sum_\theta E(\theta)\theta^{-\rho}$ ($e_{\rho+m/2} = -e_\rho$) gives, with $q = 3^{m/8}$ and $q' = 3^{m/16} = 1 + m/4 + \delta' m/2 \pmod m$,

$$e_\rho^q = -\alpha\beta\,(-1)^\rho e_\rho, \qquad e_\rho^{q'} = \lambda'_\rho\big(\alpha\, e_{A'} + \beta\, e_{A'-m/4}\big), \quad A' = \rho(1+\tfrac{m}{4}) - \tfrac{m}{8}, \quad \lambda_\rho'^2 = -1.$$

By induction from $w^{(8)}$ (odd entries $\pm i$, even entries in $\mathbb{F}_3$, $c_k^{(16)} \in \mathbb{F}_9$ by the proof of Lemma 9.34, and $w_{2k}^{(M)} = -(w_{2k}^{(M/2)} + c_k^{(M)})$) the entries of $w^{(M)}$ lie in $\mathbb{F}_{3^{M/8}}$.

(3) *The filter and the couples.* Put $q'' = 3^{m/32}$ and $x_\rho = w_{2\rho}^2 + 1$, so the line reads $e_\rho^2 = x_\rho$. Squaring the $q'$-rule gives $x_\rho^{q'} = -(x_{A'} + x_{A'-m/4} - \alpha\beta\, e_{A'}e_{A'-m/4})$, and $\{A', A'-m/4\} \equiv \{\rho - m/8, \rho + m/8\} \pmod{m/2}$, hence

$$\big(x_\rho^{q'} + x_{\rho-m/8} + x_{\rho+m/8}\big)^2 = x_{\rho-m/8}\, x_{\rho+m/8}. \tag{F}$$

Now let $(-1)^k = \alpha\beta$ and write $a_k = w_{2k}^{(m/2)} \in \mathbb{F}_{q'}$, $c_k = c_k^{(m)}$, so that $x_k = (a_k + c_k)^2 + 1$ and $x_{k+m/4} = (a_k - c_k)^2 + 1$; by (2), $c_k^{q'} = -c_k$, so $x_k^{q'} = x_{k+m/4}$. Put $k' = k + m/8$, $s_\kappa = x_\kappa + x_{\kappa+m/4}$ and $N_\kappa = x_\kappa x_{\kappa+m/4}$. By (F) at $\rho = k$ and $\rho = k + m/4$, both $x_k$ and $x_{k+m/4}$ are roots of $(Z + s_{k'})^2 = N_{k'}$. If $a_k c_k \neq 0$ they are different, so $s_k = s_{k'}$ and $N_k + N_{k'} = s_k^2$, that is

$$a_k^2 + c_k^2 = a_{k'}^2 + c_{k'}^2, \qquad (a_k^2 + c_k^2 + 1)^2 = a_k^2 c_k^2 + a_{k'}^2 c_{k'}^2. \tag{F1, F2}$$

(4) *A field fact.* Call the couple $k$ special if $a_k c_k = 0$, and suppose it is not, so that (F1) and (F2) hold at $k$. Write $a_k = -(b+d)$, $a_{k'} = -(b-d)$ with $b = w_{2k}^{(m/4)} \in \mathbb{F}_{q''}$ and $d = c_k^{(m/2)}$, so $d^{q''} = -d$ by (2), and put $G = c_k^2$, $p = bd$; note $z_0 = a_k^2 + 1$ and $z_2 = a_{k'}^2 + 1$. Then (F1) reads $c_{k'}^2 = G + p$, and (F2) becomes $G^2 + (p-1)G + z_0^2 - p(z_2 - 1) = 0$. Here $c_k \notin \mathbb{F}_{q'}$, so $G$ is a non-square of $\mathbb{F}_{q'}$. If $p = 0$, then $z_0 \in \mathbb{F}_{q''}$ and $G^2 - G + z_0^2 = 0$, so $G \in \mathbb{F}_{q''}$ or $G\, G^{q''} = z_0^2$; in both cases $G$ is a square of $\mathbb{F}_{q'}$. Hence $p \neq 0$.

(5) *Special couples.* Now suppose that the couple $k$ is special. Then $x_k = x_k^{q'} \in \mathbb{F}_{q'}$, a square in $\mathbb{F}_q$, while $e_k^q = -e_k$ makes $x_k = e_k^2$ zero or a non-square of $\mathbb{F}_q$; so $x_k = 0$. If $a_k = 0$ this gives $c_k^2 = -1$, so $c_k \in \mathbb{F}_9 \subseteq \mathbb{F}_{q'}$, against $c_k^{q'} = -c_k \neq c_k$. So $c_k = 0$ and $a_k = \pm i$: special couples have $c = 0$. Then (F) at $\rho = k$ reads $(X+Y)^2 = XY$, i.e. $(X-Y)^2 = 0$, with $X = x_{k-m/8}$, $Y = x_{k+m/8} = x_{k-m/8+m/4}$: so the couple $k'$ is special too. The $q''$-rule at $k$ gives $\alpha c_A + \beta c_{A-m/8} = 0$, where $A \equiv k \pm m/16 \pmod{m/4}$; if $c_A \neq 0$ then $c_{A-m/8}^2 = c_A^2$, and (F1) at $A$ ($A$ is not special, since special couples have $c = 0$) together with (4) at $A$ gives a contradiction. Hence $c_A = c_{A-m/8} = 0$, and the couples $k \pm m/16$ are special as well. Applied to each of the four couples $k + t\, m/16$ (all have the parity of $k$), this shows that either all four are special or none is. If all four are special, then $w_{2k+tm/8}^{(m/2)} = \pm i$ for all $t$, so $z = (0,0,0,0)$ and the claim holds. From now on we assume that none is special.

(6) *Block support.* Put $j = k + m/16$, $j' = j + m/8$; the couples $k$ and $j$ are not special, so (F1) and (F2) hold at both. For $\kappa \in \{k, j\}$ let $b_\kappa = w_{2\kappa}^{(m/4)}$, $d_\kappa = c_\kappa^{(m/2)}$ as in (4), $p_\kappa = b_\kappa d_\kappa$, $r_\kappa = b_\kappa^2 + d_\kappa^2$

and $g_\kappa = c_\kappa^2 + c_{\kappa'}^2$. Since $a_\kappa^2 = r_\kappa - p_\kappa$ and $a_{\kappa'}^2 = r_\kappa + p_\kappa$ (as $2 = -1$), (F1) at $\kappa$ gives $c_\kappa^2 = p_\kappa - g_\kappa$ and $c_{\kappa'}^2 = -g_\kappa - p_\kappa$, and (F2) at $\kappa$ becomes

$$r_\kappa^2 - p_\kappa^2 - r_\kappa + (g_\kappa - 1)^2 = 0. \tag{F2$'$}$$

Put $\gamma_t = c_{k-tm/16}$ (so $\gamma_{t+4} = -\gamma_t$), $\zeta = 1 - i$ (so $\zeta^2 = i$) and $h_a = \sum_{t=0}^{3} \gamma_t \zeta^{-at}$ for odd $a$ modulo 8, so that $\gamma_t = \sum_a h_a \zeta^{at}$. As $c_{k'} = -\gamma_2$, $c_j = -\gamma_3$ and $c_{j'} = -\gamma_1$,

$$p_k = \gamma_2^2 - \gamma_0^2 = (h_1 + h_5)^2 + (h_3 + h_7)^2, \qquad p_j = \gamma_1^2 - \gamma_3^2 = -i\big((h_1 - h_5)^2 - (h_3 - h_7)^2\big),$$

$$g_k = \gamma_0^2 + \gamma_2^2 = (h_1 + h_5)(h_3 + h_7), \qquad g_j = \gamma_1^2 + \gamma_3^2 = -(h_1 - h_5)(h_3 - h_7).$$

For $x = k - tm/16$ the index in the $3^{m/32}$-rule of (2) (with $M = m$) is $A = x - (1-2k)m/16$, because $m^2/128 \equiv 0 \pmod{m/2}$, and $\lambda_x = \lambda_k$ (as $x \equiv k \pmod 2$). As $\zeta^{q''} = \zeta$, the rule gives $h_a^{q''} = \mu_a h_a$ with $\mu_a = \lambda_k \zeta^{a(1-2k)}(\alpha + \beta i^a)$. Using $(\alpha+\beta i^a)^2 = -\alpha\beta i^a$, $(\alpha - \beta i)/(\alpha + \beta i) = -\alpha\beta i$ and $(-1)^k = \alpha\beta$ one finds $\mu_{a+4} = -\mu_a$, $\mu_a^2 = -1$ and $\mu_3 = \mu_1$; so $\mu_1\mu_7 = \mu_3\mu_5 = 1$ and $\mu_1\mu_3 = \mu_5\mu_7 = -1$. By (2), as in (4), $b_\kappa^{q''} = b_\kappa$ and $d_\kappa^{q''} = -d_\kappa$ ($j$ has the parity of $k$), so $p_\kappa^{q''} = -p_\kappa$ and $r_\kappa^{q''} = r_\kappa$. Applying $q''$ to the formulas for $p_k$ and $p_j$ gives $h_1h_5 + h_3h_7 = 0$ and $h_1h_5 - h_3h_7 = 0$, so $h_1h_5 = h_3h_7 = 0$, and $h$ vanishes outside a set $\{a, a'\}$ with $a \in \{1,5\}$, $a' \in \{3,7\}$. If $\{a,a'\} = \{1,3\}$ or $\{5,7\}$, then $g_k^{q''} = \mu_a\mu_{a'} g_k = -g_k$, and $q''$ applied to (F2$'$) at $k$ gives $(g_k+1)^2 = (g_k-1)^2$, so $g_k = h_a h_{a'} = 0$. So in every case $h$ vanishes outside a block $\{a,a'\} = \{1,7\}$ or $\{5,3\}$ ($a \in \{1,5\}$). On it $p_k = h_a^2 + h_{a'}^2$, $p_j = -i(h_a^2 - h_{a'}^2)$ and $g_k = g_j = h_a h_{a'} =: g$, so $p_k^2 + p_j^2 = 4h_a^2 h_{a'}^2 = g^2$ (as $4 = 1$).

(7) *Conclusion.* Put $\nu = 1 - (g-1)^2 = -g(g+1)$; as $r^2 - r = (r+1)^2 - 1$, (F2$'$) reads $(r_\kappa + 1)^2 = p_\kappa^2 + \nu$. Since $z_0 = (b_k + d_k)^2 + 1$ and $z_2 = (b_k - d_k)^2 + 1$, we have $z_0 + z_2 = -(r_k + 1)$ and $z_0 z_2 = (r_k+1)^2 - p_k^2 = \nu$; in the same way $z_1 + z_3 = -(r_j + 1)$ and $z_1 z_3 = \nu$. Hence $z_0 z_2 = z_1 z_3$, and

$$P = (z_0 + z_2)^2 + (z_1 + z_3)^2 + z_0z_2 + z_1z_3 = (r_k+1)^2 + (r_j+1)^2 - \nu = p_k^2 + p_j^2 + \nu = g^2 + \nu = -g,$$

so $P^2 - P + z_0 z_2 = g^2 + g - g(g+1) = 0$. □

For a power of two $M \geq 16$ and $u \in P(M)$ put $u^{(M)} = u$ and, as long as $u^{(M')}$ is in case (II) of Lemma 9.31(b), $u^{(M'/2)} = (u^{(M')})^+ \in P(M'/2)$. Call $u$ a *chain base of level* $M$ if $u^{(M')}$ is in case (II) for $M' = M, M/2, \ldots, 16$ and $u^{(8)}$ is in case (I), and write $u_1^{(8)} = i\alpha$, $u_3^{(8)} = i\beta$ as in Lemma 9.38. In that lemma $w^{(m/2)}$ is a chain base of level $m/2$, and its four elements $z_t$ at $k$ are $u_{2k+tM/4}^2 + 1$ with $u = w^{(m/2)}$, $M = m/2$.

**Question 9.39.** Is it true that for every power of two $M \geq 32$ no chain base $u$ of level $M$ satisfies both equations of Lemma 9.38, for $z_t = u_{2k+tM/4}^2 + 1$, at every index $k$ with $(-1)^k = \alpha\beta$?

By Lemma 9.38, a positive answer to Question 9.39 implies that for every odd $e \geq 7$ no point of the odd locus has a chain that first reaches case (I) at level 8 (the zero tuple of step (5) satisfies both equations, so a positive answer covers that case as well). For $M = 32$ ($n = 128$) the answer is yes: for each class $S = f_0 = \pm 1$, at none of the 256 chain bases of level 32 do both equations hold at any index $k$ with $(-1)^k = \alpha\beta$ (computation over all these bases and indices; three independent programs, Table 8).

*Remark* 9.40. In Lemma 9.38 the entries $w_{2k}^{(m/2)}$ with $(-1)^k = \alpha\beta$ are not all $\pm i$. Thus the zero tuple of step (5) of its proof does not occur at every index $k$ with $(-1)^k = \alpha\beta$, and at some such index none of the four couples $k + tm/16$ is special. Indeed, let $u = w^{(8)}$ (in this remark only), with $u^+ = S\,\delta_{2r_1}$ and $r_1 \in \{0,1\}$ (Lemma 9.31(b)). By the first paragraph of the proof of Lemma 9.34 (see step (1) of the proof of Lemma 9.38), $u_{2r_1} = u_{2r_1+4} = -S$, the other two even entries vanish, $u_5 = -u_1 = -i\alpha$ and $u_7 = -u_3 = -i\beta$. In the identity $U(x)U(-x) = S\,U(x^2)$ of $P(8)$, with $U = \sum_r u_r x^r$ modulo $x^8 - 1$, the constant term on the left is $\sum_r (-1)^r u_r u_{-r} = 2S^2 - 4\alpha\beta = -1 - \alpha\beta$, and on the right

it is $S(u_0+u_4)$, that is 1 if $r_1=0$ and 0 if $r_1=1$. Hence $(-1)^{r_1}=\alpha\beta$. Folding down to level 8, $u_{2r_1}$ is the sum of the $m/16$ entries $w_r^{(m/2)}$ with $r\equiv 2r_1 \pmod 8$; these are the $w_{2k}^{(m/2)}$ with $k\equiv r_1 \pmod 4$, so $(-1)^k=\alpha\beta$. If they were all $\pm i$, their sum would lie in $i\,\mathbb{F}_3$, which meets $\mathbb{F}_3$ only in 0; but $u_{2r_1}=-S$.

*Remark* 9.41. For $n=512$ ($m=256$) there is no point of the odd locus whose chain first reaches case (I) at level 8. For such a point, by Lemma 9.38, both equations would hold for $u=w^{(128)}$ at every index $k$ with $(-1)^k=\alpha\beta$. The indices $k$ and $k+8$ of level 128 are linked by the $3^4$-rule of step (2) for $C_{128}$: if $\delta_0,\delta_1$ are the coefficients $c_k^{(128)}, c_{k+16}^{(128)}$, the two coefficients at $k+8$, $k+24$ have squares $-\phi((\delta_0\pm\delta_1)^2)$, $\phi(x)=x^{81}$. Allowing every $\delta$ with $\delta^{3^8}=-\delta$ gives a set $J$ of 6788 pairs $(w_{2k}^{(64)}, w_{2k+16}^{(64)})$ that the indices $k$ and $k+8$ allow; the same rule one level down then leaves no possible value at any index $k$ with $(-1)^k=\alpha\beta$ of any of the $2\cdot 256$ chain bases of level 32. Hence no chain base of level 128 satisfies both equations at every index $k$ with $(-1)^k=\alpha\beta$; that is, the answer to Question 9.39 is yes for $M=128$. (Computation; three independent programs, Table 8: two of them follow this route, and the third checks directly the lifts to level 128 of all chain bases of level 64, up to the Frobenius.)

The method of Lemma 9.37 also excludes part of the chains that first reach case (I) at a level $M_0\ge 32$.

**Lemma 9.42.** *Let $e\ge 7$ be odd, let $M_0$ be a power of two with $32\le M_0\le m/2$, and let $y\in W(n)$ lie on the locus $y_t=y_{t+m}$ ($t$ odd), with base $w$. Suppose that $w^{(M)}$ is in case (II) of Lemma 9.31(b) for $M=m,m/2,\dots,2M_0$ and that $w^{(M_0)}$ is in case (I), and let $h$ and $\Theta$ be as in Lemma 9.32 for $w^{(M_0)}$ (so $L=M_0/4$). Then $\Theta(\eta)$ is a square in $\mathbb{F}_3(\eta)$ for every root $\eta$ of $v^L+1$.*

*Proof.* Let $u=w^{(2M_0)}$, so $u^+=w^{(M_0)}$, and let $h$, $\hat\sigma$, $\Psi$ be as in the proof of Lemma 9.32 for $u^+$; as in the proof of Lemma 9.37, the parts of that proof used below use only the identities of $P(M_0)$. Write $L=4N$, so $N\ge 2$ is a power of two. As $v_2(3^{2^j}-1)=j+2$ for $j\ge 1$, we have $3^{L/2}\equiv 1+2L \pmod{4L}$ and $3^{L/4}\equiv 1+L \pmod{2L}$, and $\mathbb{F}_3(\eta)=\mathbb{F}_{3^{L/2}}$. Suppose that $\Theta(\eta)$ is a non-square in $\mathbb{F}_3(\eta)$ for one root $\eta$; as in the proof of Lemma 9.32(c), it is then a non-square at every root. By Remark 9.36 and Lemma 9.31(d), $T_{2M_0}(u)\in\mathbb{F}_3$, and by step (1) of the proof of Lemma 9.35, $T_{2M_0}(u)=-T_{M_0}(u^+)-K_{2M_0}$.

As in the proof of Lemma 9.32(a), now with $\frac{1}{L}=\pm 1$, we get $T_{M_0}(u^+)=-(-1)^{r_1}\big(1+\frac{1}{L}B\big)$, where $B=\sum_\eta h(\eta)h(-\eta)$ over the roots of $v^L+1$. As in the proof of Lemma 9.37, $U \bmod (x^{M_0}+1)=C(x^2)$ with $C=C_{2M_0}$, $C(v)^2=S\,v^{2r_1}\Psi(v)$ and $CC^*=1$ in $\overline{\mathbb{F}}_3[v]/(v^{2L}+1)$; as $\Psi(v)\Psi(-v)=1$, $C(\xi)/C(-\xi)=\lambda(\xi)\Psi(\xi)$ with $\lambda(\xi)=\pm 1$, and $K_{2M_0}=\frac{1}{2L}\sum_\xi \lambda(\xi)\Psi(\xi)$ over the roots $\xi$ of $v^{2L}+1$.

Let $\tau(x)=x^{3^{L/2}}$. The $\xi$ have order $4L$, so $\tau(\xi)=\xi^{1+2L}=-\xi$, while $\tau$ fixes $i$ and the roots $\eta=\xi^2$ of $v^L+1$. As $\Theta(\eta)$ is a non-square in $\mathbb{F}_{3^{L/2}}$, $\tau(h(\eta))=-h(\eta)$; and $\hat\sigma(v)=v^{1-2r_1}s(v^2)$ is odd with coefficients in $\mathbb{F}_3$. So $\tau(\Psi(\xi))=-h(\xi^2)-i\hat\sigma(-\xi)=-\Psi(\xi)$ and $\tau(K_{2M_0})=-K_{2M_0}$, while $\tau(B)=B$. Since $\tau$ fixes $T_{2M_0}(u)\in\mathbb{F}_3$, we get $K_{2M_0}=0$ and $B\in\mathbb{F}_3$.

Let $\tau'(x)=x^{3^{L/4}}$. Then $\tau'(\eta)=\eta^{1+L}=-\eta$, and $\tau'(h(\eta))=\mu(\eta)h(-\eta)$ with $\mu(\eta)=\pm 1$, as both square to $\Theta(-\eta)$; applying $\tau'$ twice gives $\mu(\eta)\mu(-\eta)=-1$. Hence $\tau'(B)=-B$, and with $B\in\mathbb{F}_3$ this gives $B=0$.

We now show that $B=0$ is impossible. Put $p(\eta)=h(\eta)h(-\eta)$ and $\mathrm{Fr}(x)=x^3$. As $h(1/\eta)=h(\eta)$, $p$ is constant on each of the $N$ sets $\{\pm\eta^{\pm 1}\}$ into which the roots fall; as the odd residues modulo $2L$ are the $\pm 3^j$ and $3^N\equiv 1+L \pmod{2L}$, these sets are the $\{\pm\eta_1^{\pm 3^j}\}$ with $j<N$, for one root $\eta_1$. As $\Theta$ has coefficients in $\mathbb{F}_3$, $p(\eta^3)^2=\Theta(\eta)^3\Theta(-\eta)^3=(p(\eta)^3)^2$, so $p(\eta_1^{3^j})=\delta_j\mathrm{Fr}^j(p_1)$ with $\delta_j=\pm 1$ and $p_1=p(\eta_1)$. Hence $B=4\sum_{j<N}\delta_j\mathrm{Fr}^j(p_1)=l(\mathrm{Fr})(p_1)$ (as $4=1$), with $l(t)=\sum_{j<N}\delta_j t^j$, and $\mathrm{Fr}^N(p_1)=\tau'(p_1)=\mu(\eta_1)\mu(-\eta_1)p_1=-p_1$. We show below that $l$ has no root $\omega$ with $\omega^N=-1$.

Then $l$ is prime to $t^N+1$ in $\mathbb{F}_3[t]$, so $gl = 1+(t^N+1)r$ for some $g, r \in \mathbb{F}_3[t]$, and $g(\mathrm{Fr})(B) = p_1 + r(\mathrm{Fr})\big(\mathrm{Fr}^N(p_1)+p_1\big) = p_1$. As $B=0$, this gives $p_1 = 0$, whereas $p_1^2 = \Theta(\eta_1)\Theta(-\eta_1) \neq 0$.

It remains to show that $l(\omega) \neq 0$ when $\omega^N = -1$; we use induction on $N$. If $N=2$, then $\omega = \pm i$ and $\delta_0 + \delta_1\omega \neq 0$. If $N=4$, then $\omega^2 = \varepsilon i$ with $\varepsilon = \pm 1$, so $\omega = a(1-\varepsilon i)$ with $a = \pm 1$, and $l(\omega) = \delta_0 + a(\delta_1+\delta_3) + \varepsilon i\big(\delta_2 + a(\delta_3-\delta_1)\big)$; as $\delta_1+\delta_3$ or $\delta_3-\delta_1$ is 0, one of the two parts is $\delta_0$ or $\delta_2$, which is not 0. If $N \geq 8$, then 3 has order $N/2$ modulo $2N$ and order $N/4$ modulo $N$, so $[\mathbb{F}_3(\omega) : \mathbb{F}_3(\omega^2)] = 2$. Writing $l(t) = l_0(t^2) + t\, l_1(t^2)$, $l(\omega) = 0$ gives $l_0(\omega^2) = 0$, where $l_0$ has $N/2$ coefficients $\pm 1$ and $(\omega^2)^{N/2} = -1$; this is excluded by the case $N/2$. □

With Lemma 9.32(c), which treats $M_0 = m$, this excludes for every odd $e \geq 7$ all chains that first reach case (I) at a level $M_0 \geq 32$ with $\Theta$ a non-square. When $\Theta$ is a square at every root, the argument gives no contradiction, and only the condition $T_{2M_0}(u) \in \mathbb{F}_3$ of Remark 9.36 and Lemma 9.31(d) remains; for $n = 128$ and $M_0 = 32$ it leaves 24576 bases, and these are excluded by Proposition 9.44(b).

**Corollary 9.43.** *No point of $W(32)$ lies on the odd locus or on its shift by 1. Hence $G$ acts freely on $W(32)$.*

*Proof.* By the shift, it is enough to treat the odd locus. Let $y$ lie on it, with base $w \in P(16)$ (Lemma 9.31(a)). If $w$ is as in Lemma 9.31(b)(I), Lemma 9.32(b) applies. Otherwise $w$ is as in (II) and $w^+ \in P(8)$. If $w^+$ is as in (I), Lemma 9.34 applies. If $w^+$ is as in (II) too, then $w$ and $w^+$ are both in case (II), against Lemma 9.35 with $m = 16$. With Remark 9.17, a point with a non-trivial stabiliser in $G$ would lie on one of the two loci. □

**Proposition 9.44.** *No point of $W(128)$ lies on the odd locus or on its shift by 1. Hence $G$ acts freely on $W(128)$.*

*Proof.* By the shift, and by $y \mapsto -y$ (Proposition 9.3), it is enough to treat the odd locus in the class $S = f_0 = 1$. Let $y$ lie on it, with base $w \in P(64)$ (Lemma 9.31(a)). By Lemma 9.35 the chain $w^{(M)}$ reaches case (I) at a level $M_0 \in \{8, 16, 32, 64\}$, with $w^{(M)}$ in case (II) for $M_0 < M \leq 64$; Lemma 9.37 excludes $M_0 = 16$. Cases (a) and (b) rest on computations, each done by two independent programs. Case (c) rests on Lemma 9.38 and the finite check at level 32 after Question 9.39, and, independently, on two programs at level 64. The programs and their logs are listed in Table 8.

(a) $M_0 = 64$, that is, $w$ in case (I): Lemma 9.32(c) and Remark 9.33; a second program walked the fibres of all 1048576 case (I) bases and found no point.

(b) $M_0 = 32$: $w$ is in case (II) and $w^+ \in P(32)$ is in case (I). Of the 524288 bases $w$ over the 2048 case (I) parents in $P(32)$, exactly 24576 have $T(w) \in \mathbb{F}_3$ (Lemma 9.31(d)). None of these 24576 bases is excluded by the base alone, and a search of the fibre of each of them found no point.

(c) $M_0 = 8$: by Lemma 9.38, $w^{(32)}$ would be a chain base of level 32 satisfying both equations of that lemma at every index $k$ with $(-1)^k = \alpha\beta$, and by the case $M = 32$ after Question 9.39 no chain base of level 32 does so at any such index. Independently, two programs excluded this case directly at level 64, in each class: one walked the fibres of all 65536 chain bases of level 64 with $M_0 = 8$, the other those of the 3072 bases that pass its Frobenius filter, the necessary condition proved in step (2) of the proof of Lemma 9.38.

With Remark 9.17, a point with a non-trivial stabiliser in $G$ would lie on one of the two loci. □

The condition $T_{2M_0}(w^{(2M_0)}) \in \mathbb{F}_3$ is the first of a family of conditions on the chain, one for each root of unity of 2-power order. For a power of two $M \geq 4$, $u \in P(M)$ and $\beta \in \overline{\mathbb{F}}_3$ with $\beta^{M/2} = 1$ put

$$F_\beta(u) = \sum_{\rho \in \mathbb{Z}/(M/2)} \beta^\rho u_{2\rho}^2,$$

so that $F_{-1} = T_M$. For a power of two $o$ let $\mu_o$ be the group of $o$-th roots of unity in $\overline{\mathbb{F}}_3$; thus $\mathbb{F}_3(\mu_2) = \mathbb{F}_3$, $\mathbb{F}_3(\mu_4) = \mathbb{F}_9$ and $\mathbb{F}_3(\mu_o) = \mathbb{F}_{3^{o/4}}$ for $o \geq 8$.

**Lemma 9.45.** *Let $e \geq 5$ be odd and let $y \in W(n)$ lie on the locus $y_t = y_{t+m}$ ($t$ odd), with base $w$ and chain $w^{(M)}$ as in Lemma 9.35. Suppose that $w^{(M)}$ is in case (II) of Lemma 9.31(b) for $M = m, m/2, \ldots, 2M_0$, where $M_0 \geq 8$, and let $\beta \in \overline{\mathbb{F}}_3$ have order $o$, a power of two with $2 \leq o \leq m/M_0$. Then:*

(a) $F_\beta(w^{(2M)}) + F_\beta(w^{(M)}) \in \mathbb{F}_3(\mu_o)$ *for every $M$ with $oM_0 \leq M < m$;*
(b) $\sum_{\rho \in \mathbb{Z}/(m/2)} \beta^\rho d_{2\rho}^2 \in \mathbb{F}_3(\mu_o)$*;*
(c) $F_\beta(w^{(oM_0)}) \in \mathbb{F}_3(\mu_o)$*.*

*Proof.* (a) Let $u = w^{(2M)}$, $u^+ = w^{(M)}$ and $C = C_{2M}$, with coefficients $c_k$ ($k < M/2$), extended by $c_{k+M/2} = -c_k$. As in step (1) of the proof of Lemma 9.35, $u_{2k} = -(u^+_{2k} + c_k)$ and $u_{2k+M} = -(u^+_{2k} - c_k)$. As $\beta^{M/2} = 1$, pairing $\rho = k$ with $\rho = k + M/2$ gives

$$F_\beta(u) = \sum_{k<M/2} \beta^k \big((u^+_{2k} + c_k)^2 + (u^+_{2k} - c_k)^2\big) = -F_\beta(u^+) - K, \qquad K = \sum_{k<M/2} \beta^k c_k^2.$$

Let $\eta$ run over the $M/2$ roots of $v^{M/2} + 1$. Then $c_k = \frac{2}{M} \sum_\eta C(\eta)\eta^{-k}$, and $\beta/(\eta\eta')$ is an $(M/2)$-th root of unity, so $\sum_{k<M/2}(\beta/(\eta\eta'))^k$ is $M/2$ if $\eta\eta' = \beta$ and 0 otherwise. Hence $K = \frac{2}{M}\sum_\eta C(\eta)C(\beta/\eta)$. Since $CC^* = 1$ (step (2) of the proof of Lemma 9.35), $C(\eta)C(1/\eta) = 1$, and with $\xi = 1/\eta$

$$K = \frac{2}{M} \sum_\xi \frac{C(\beta\xi)}{C(\xi)}.$$

For $L = 2M, M, \ldots, 4M/o$ the level $L/2 \geq 2M/o \geq 2M_0$ is in case (II), so step (2) of the proof of Lemma 9.35 gives $C_L(v)^2 = S\,C_{L/2}(v^2)$ in $\overline{\mathbb{F}}_3[v]/(v^{L/4} + 1)$. Applying this $\log_2 o$ times gives $C(z)^o = S^{o-1} C_{2M/o}(z^o)$ at every root $z$ of $v^{M/2} + 1$. As $\beta^o = 1$ and $C(\xi) \neq 0$, $\big(C(\beta\xi)/C(\xi)\big)^o = 1$. So $K$ is $\frac{2}{M} \in \mathbb{F}_3$ times a sum of $o$-th roots of unity, and $K \in \mathbb{F}_3(\mu_o)$.

(b) Since $w$ is in case (II), $W^- = C_m(x^2)$, and as in the proof of Lemma 9.32(a) $D(x) = E(x^2)$ with $E^2 = S\,C_m(u^2)$ and $EE^* = -1$ in $\overline{\mathbb{F}}_3[u]/(u^{m/2} + 1)$; so $d_{2\rho} = \frac{2}{m}\sum_\theta E(\theta)\theta^{-\rho}$ over the $m/2$ roots $\theta$ of $u^{m/2} + 1$. As in (a), since $\beta^{m/2} = 1$,

$$\sum_{\rho \in \mathbb{Z}/(m/2)} \beta^\rho d_{2\rho}^2 = \frac{2}{m} \sum_\theta E(\theta)E(\beta/\theta) = -\frac{2}{m} \sum_\xi \frac{E(\beta\xi)}{E(\xi)},$$

using $E(\theta)E(1/\theta) = -1$ and $\xi = 1/\theta$. For $o \geq 4$ the levels $L/2$ with $L = m, \ldots, 4m/o$ are in case (II) ($L/2 \geq 2m/o \geq 2M_0$), so as in (a) $C_m(v)^{o/2} = S^{o/2-1} C_{2m/o}(v^{o/2})$, and $E(z)^o = \big(S\,C_m(z^2)\big)^{o/2} = S^{o-1} C_{2m/o}(z^o)$; for $o = 2$ this is $E^2 = S\,C_m(u^2)$ itself. As $\beta^o = 1$ and $E(\xi) \neq 0$, every term is an $o$-th root of unity.

(c) The line at $s = 2\rho$ reads $d_{2\rho}^2 = w_{2\rho}^2 + 1$. Multiply by $\beta^\rho$ and sum over $\rho \in \mathbb{Z}/(m/2)$; as $\beta \neq 1$ and $\beta^{m/2} = 1$, $\sum_\rho \beta^\rho = 0$, so $F_\beta(w^{(m)}) = \sum_\rho \beta^\rho d_{2\rho}^2 \in \mathbb{F}_3(\mu_o)$ by (b). Now (a) for $M = m/2, m/4, \ldots, oM_0$ gives $F_\beta(w^{(M)}) \in \mathbb{F}_3(\mu_o)$ for each of these $M$. □

*Remark* 9.46. For $o = 2$, $\beta = -1$, Lemma 9.45 is Remark 9.36 together with Lemma 9.31(d). For larger $o$ the identity $F_\beta(w^{(2M)}) = -F_\beta(w^{(M)}) - K$ of its proof holds for every $M$ with $\max(2o, M_0) \leq M$ and $2M \leq m$, but the proof that $K \in \mathbb{F}_3(\mu_o)$ needs $M \geq oM_0$: below that level the halvings reach case (I). So (c) is one condition on the base $w^{(oM_0)}$ alone for each $\beta$ of order $o$, and it is the same for every $m \geq oM_0$. For $\beta = 1$ there is no condition: on the chain the odd entries are $\pm i$ and $\sum_r u_r^2 = 1$ (the constant term of $UU^* = 1$), so $F_1(u) = 1 + M/2$ at every level.

*Remark* 9.47. For $M_0 = 8$ these conditions are much weaker than the field degrees suggest. By step (1) of the proof of Lemma 9.38, every value $C_M(\eta)$ on such a chain is a root of unity of 2-power order, and so is every value $E(\theta)$; and the even entries of $w^{(8)}$ lie in $\mathbb{F}_3$. As $w^{(2M)}_{2k} = -(w^{(M)}_{2k} + c_k)$ and $w^{(2M)}_{2k+M} = -(w^{(M)}_{2k} - c_k)$ $(k < M/2)$ with $c_k = \frac{2}{M}\sum_\eta C_{2M}(\eta)\eta^{-k}$ (proof of Lemma 9.45(a)), induction on the level shows that every even entry of every $w^{(M)}$ is a sum of roots of unity of 2-power order. Hence every $K$ in (a) and every $F_\beta(w^{(M)})$ is such a sum, each term determined by the signs of the chain; with the lower levels fixed, the terms of the top level are fixed roots of unity times products of the new signs. Condition (c) is then a congruence on such sums, not a condition of generic codimension. For example, at level 128 ($o = 16$) each value $F_\beta(w^{(128)})$ lies in $\mathbb{F}_{3^{16}}$ (step (2) of the proof of Lemma 9.38) and (c) asks it to lie in $\mathbb{F}_{81}$, yet for each of the two level-64 bases we searched (the first two, in the program's order, that satisfy (c) for $o = 8$; class $S = 1$; one program, all $2^{16}$ sign choices) exactly 512 of the $2^{16}$ choices of the new signs satisfy (c) for all $\beta$ of order 16 together. For $M_0 \geq 32$ the values $C_M(\eta)$ also have odd-order factors, and this remark does not apply.

For $M_0 = 32$ and $\Theta$ a square, Lemma 9.45 gives conditions of orders $o = 2, 4, \ldots, m/32$. We make the first two explicit. They concern only the levels 32, 64 and 128, so we state them for a chain of bases. For $u \in P(M)$ we call $u' \in P(2M)$ a *child* of $u$ if $u'$ is in case (II) of Lemma 9.31(b) and $u'^{+} = u$. Let $w^{(32)} \in P(32)$ be in case (I), let $w^{(64)}$ be a child of $w^{(32)}$, and let $w^{(128)}$ be a child of $w^{(64)}$. Let $r_1$, $s$, $h$, $\Theta$, $\Psi$ and $\hat\sigma$ be as in Lemma 9.32 and its proof for $w^{(32)}$ (so $L = 8$ and $\Psi(u) = h(u^2) - i\,\hat\sigma(u)$), let $C = C_{64}$, and let $\eta$, $\xi$ and $x$ run over the roots of $v^8 + 1$, $v^{16} + 1$ and $v^{32} + 1$. We assume that $\Theta(\eta)$ is a square in $\mathbb{F}_3(\eta) = \mathbb{F}_{81}$ at every root, so that $h(\eta) \in \mathbb{F}_{81}$. This holds for the chain of a point: if $e \geq 9$ is odd, $y \in W(n)$ lies on the locus $y_t = y_{t+m}$ ($t$ odd), and its base $w$ has $w^{(M)}$ in case (II) for $M = m, m/2, \ldots, 64$ and $w^{(32)}$ in case (I), then $w^{(64)}$ is a child of $w^{(32)}$, $w^{(128)}$ is a child of $w^{(64)}$, and Lemma 9.42 shows that $\Theta(\eta)$ is a square at every root. Conversely, for $M = 32, 64$ every choice of signs gives a child of $w^{(M)}$: a child $u'$ of $u = w^{(M)}$ is determined by $u$ and $C_{2M}$ (for odd $r$, $u'_r = u'_{r+M} = -u_r$); modulo $x^M - 1$ the identities of $P(2M)$ are those of $P(M)$ for $u$, and modulo $x^M + 1$ they say $C_{2M}(v)^2 = S\,C_M(v^2)$ (for $M = 32$: $C_{64}(v)^2 = S\,v^{2r_1}\Psi(v)$, proof of Lemma 9.42) and $C_{2M}(v)C_{2M}(1/v) = 1$, which hold for either sign of $C_{2M}(\zeta)$, with $C_{2M}(1/\zeta) = 1/C_{2M}(\zeta)$, on each pair $\{\zeta, 1/\zeta\}$ of roots of $v^{M/2} + 1$. So $w^{(32)}$ has $2^8$ children and each $w^{(64)}$ has $2^{16}$. Fix a root $\xi_1$ with $\xi_1^8 = i$ and put $\eta_1 = \xi_1^2$, so that $\eta_1^4 = i$. Put $\tau(x) = x^{81}$ and $\tau'(x) = x^9$; then $\tau$ fixes $i$, $\eta$ and $h(\eta)$, $\tau(\xi) = -\xi$ and $\tau'(\eta) = -\eta$.

As $h(\xi^2) \in \mathbb{F}_{81}$, $\tau(i) = i$, $\tau(\xi) = -\xi$ and $\hat\sigma$ is odd with coefficients in $\mathbb{F}_3$, $\tau(\Psi(\xi)) = \Psi(-\xi)$, and $\Psi(-\xi) = 1/\Psi(\xi)$ as $\Psi(u)\Psi(-u) = 1$. Hence $\Psi(\xi)^{82} = 1$. In particular $h(\eta) \neq 0$ at every root: if $h(\xi^2) = 0$, then $\Psi(-\xi) = -\Psi(\xi)$, so $\Psi(\xi)^2 = -1$ and $\Psi(\xi)^{82} = -1$. As $h(\eta)^9$ and $h(-\eta)$ both square to $\Theta(-\eta)$, and $h(\eta)^3$ and $h(\eta^3)$ both square to $\Theta(\eta^3)$, we have $h(\eta)^9 = \mu(\eta)h(-\eta)$ and $h(\eta)^3 = \nu(\eta)h(\eta^3)$ with $\mu(\eta), \nu(\eta) = \pm 1$. Applying $\tau'$ to the first identity gives $h(\eta) = \mu(\eta)\mu(-\eta)h(\eta)$, so $\mu(-\eta) = \mu(\eta)$; and $h(1/\eta) = h(\eta)$ gives $\mu(1/\eta) = \mu(\eta)$. So $\mu$ is constant on each of the two sets $\{\pm\eta_1^{\pm 1}\}$ and $\{\pm\eta_1^{\pm 3}\}$. We call $w^{(32)}$ *good* if $\mu$ is constant, $\mu = \mu_0$, and then put $\lambda'_0 = (-1)^{r_1}\mu_0$; otherwise $\mu = \mu_A$ on the first set and $\mu = -\mu_A$ on the second.

Write $\Psi = \pi\omega$ with $\pi = \Psi^{41} = \pm 1$ and $\omega = \Psi^{42}$ of order dividing 41, and put $y = \omega + 1/\omega$. As $\Psi^* = \Psi(-u)$, also $\pi(-\xi) = \pi(1/\xi) = \pi(\xi)$ and $\omega(-\xi) = \omega(1/\xi) = 1/\omega(\xi)$; and as $\frac{1}{2} = -1$, $h(\xi^2) = \frac{1}{2}\big(\Psi(\xi) + \Psi(-\xi)\big) = -\pi(\xi)y(\xi)$. Next, $\Psi(\xi)^3 = \nu(\xi^2)h(\xi^6) + i\,\hat\sigma(\xi^3)$ is $\Psi(-\xi^3)$ or $-\Psi(\xi^3)$, so $\omega(\xi)^3 = \omega(\xi^3)^{\pm 1}$ and $y(\xi)^3 = y(\xi^3)$. Hence $\omega(\xi) \neq 1$ for every $\xi$: as $\xi \mapsto \xi^3$ and $\xi \mapsto 1/\xi$ generate a group that is transitive on the roots, $\omega = 1$ at one root would give $\omega = 1$ at all roots; then $\Psi = \pm 1$ and $\Psi(-\xi) = 1/\Psi(\xi) = \Psi(\xi)$, so $\hat\sigma(\xi) = 0$ at all 16 roots, whereas $\hat\sigma$ is a nonzero residue modulo $v^{16} + 1$. Thus $\omega(\xi)$ has order 41. As in the proof of Lemma 9.42, $C(\xi)/C(-\xi) = \pm\Psi(\xi)$, so $C(\xi)/C(-\xi) = \epsilon(\xi)\,\omega(\xi)$ with $\epsilon(\xi) = \pm 1$. For $\beta^{16} = 1$ put $K_{64}(\beta) = \sum_\xi C(\beta\xi)/C(\xi)$, and for $\beta^{32} = 1$ put $K_{128}(\beta) = -\sum_x C_{128}(\beta x)/C_{128}(x)$. These are the sums $K$ of the proof of Lemma 9.45(a)

($\frac{2}{32}=1$, $\frac{2}{64}=-1$). The first part of that proof uses only that the child is in case (II) and that $C_{2M}C_{2M}^*=1$; so, for $\beta=\pm1,\pm i$,

$$F_\beta(w^{(64)})=-F_\beta(w^{(32)})-K_{64}(\beta),\qquad F_\beta(w^{(128)})=-F_\beta(w^{(64)})-K_{128}(\beta).$$

Lemma 9.45(c) asks $F_{-1}(w^{(64)})\in\mathbb{F}_3$ ($o=2$) and $F_{\pm i}(w^{(128)})\in\mathbb{F}_9$ ($o=4$). First, a fact about $w^{(32)}$ alone.

**Lemma 9.48.** *In this situation let $\alpha=\omega(\xi_1)^{21}$, $Y_0=\alpha+1/\alpha$, $y_0=y(\xi_1)$, $p=Y_0+Y_0^9$, $g=Y_0^{10}$, $t_0=y_0+y_0^9$ and $\ell=y_0^{10}$, and write $\bar c=c^3$ for $c\in\mathbb{F}_9$. Then $p=1$, $g=\pm i$, $t_0=\pm i$ and $\ell=1\pm i$, with the same sign. Moreover $D=Y_0-Y_0^9$ satisfies $D^9=-D\neq0$ and $\delta=D^2=1\mp i$, and the conjugates $\theta^{3^j}$ ($j<8$) of $\theta=\omega(\xi_1)^{20}$ span an $\mathbb{F}_3$-space of dimension 7.*

*Proof.* As $\omega(\xi_1)$ has order 41 and $81\equiv-1\pmod{41}$, $\tau$ inverts $\alpha$ and $\gamma=\alpha^{21}$. So $Y_0$ and $y_0=\alpha^2+\alpha^{-2}=Y_0^2+1$ lie in $\mathbb{F}_{81}$, and $Y_0\notin\mathbb{F}_9$, as $Y_0^9=Y_0$ would give $\alpha^8=1$ or $\alpha^{10}=1$. Hence $D\neq0$, $D^9=-D$, and $\delta=D^2=p^2-4g=p^2-g$ lies in $\mathbb{F}_9$ but is not a square there. Next, $Y_0-1=(\gamma+1/\gamma)^2$ and $Y_0+1=(\gamma-1/\gamma)^2$ (note $\gamma^2=\alpha$), where $\tau$ fixes $\gamma+1/\gamma\neq0$ and negates $\gamma-1/\gamma\neq0$. As an element of $\mathbb{F}_{81}^*$ is a square if and only if its norm to $\mathbb{F}_9$ is, the norm $g-p+1$ of $Y_0-1$ is a nonzero square in $\mathbb{F}_9$ and the norm $g+p+1$ of $Y_0+1$ is not. Running these two norms over the 4 nonzero squares and the 4 non-squares of $\mathbb{F}_9$, solving for $p$ and $g$, and keeping $p^2-g$ a non-square leaves, up to the conjugation $c\mapsto\bar c$, the five pairs $(p,g)=(1,i)$, $(-i,-i)$, $(1-i,-1-i)$, $(-i,1-i)$ and $(-1-i,1)$.

Now $\hat\sigma(u)=u^{1-2r_1}s(u^2)$ is a residue modulo $u^{16}+1$ with the entries $\pm1$ at the 8 odd places, and $\hat\sigma(1/u)=-\hat\sigma(u)$, as $s(1/v)=-v^{1-2r_1}s(v)$. As $\sum_\xi\xi^d=0$ for $0<|d|<16$, $\sum_\xi\hat\sigma(\xi)\hat\sigma(1/\xi)=16\cdot8=-1$, so $\sum_\xi\hat\sigma(\xi)^2=1$. As $h(\xi^2)^2+\hat\sigma(\xi)^2=\Psi(\xi)\Psi(-\xi)=1$ and $h(\xi^2)=-\pi(\xi)y(\xi)$, this gives $\sum_\xi y(\xi)^2=0$. On the set $\{\pm\xi_1^{\pm3^k}\}$ the value of $y$ is $y_0^{3^k}$, so the trace of $y_0^2$ to $\mathbb{F}_3$ is 0. The trace of $y_0^2$ to $\mathbb{F}_9$ is $t_0^2-2\ell=t_0^2+\ell$, so $t_0^2+\ell+\overline{t_0^2+\ell}=0$. Here $t_0=p^2+g-1$ (the trace of $Y_0^2+1$) and $\ell=(g-1)^2+p^2$ (the norm of $y_0=(Y_0-i)(Y_0+i)$, using that $Y_0+c$ has norm $g+cp+c^2$ for $c\in\mathbb{F}_9$). For the five pairs, $t_0^2+\ell$ is $i$, $-1$, $1-i$, $1-i$ and $-1-i$, and only the first has $t_0^2+\ell+\overline{t_0^2+\ell}=0$. So $(p,g)=(1,\pm i)$, $t_0=\pm i$, $\ell=1\pm i$ and $\delta=p^2-g=1\mp i$.

Finally, let Fr be the Frobenius map of $\mathbb{F}_{3^8}$, which cubes each element. As $\mathbb{F}_3[\mathrm{Fr}]$-modules, $\mathbb{F}_{3^8}$ is the direct sum of $\mathbb{F}_{81}=\ker(\mathrm{Fr}^4-1)$ and $\ker(\mathrm{Fr}^4+1)$, and $\alpha=-(Y_0+z)$ with $z=\alpha-1/\alpha$ in the second. Thus the dimension of the span of the conjugates of $\theta$ (which is that of $\alpha=\theta^{81}$) is the sum of the dimensions for $Y_0$ and for $z$. For $Y_0$, the components for the factors $t^2+1$, $t-1$ and $t+1$ of $t^4-1$ are, up to units, $D\neq0$, $p+\bar p=-1\neq0$ and $p-\bar p=0$, so the dimension is 3. For $z$ it is 2 or 4, as $t^4+1=(t^2+t-1)(t^2-t-1)$. Dimension 2 would mean $(\mathrm{Fr}^2\pm\mathrm{Fr}-1)z=0$, that is $z^8=\mp z^2+1$, so that $z^2$ would be a root of $X^4\pm X-1$. This polynomial is irreducible over $\mathbb{F}_3$ (it has no root, and $(X^2+aX+b)(X^2-aX+c)=X^4\pm X-1$ would need $b+c=a^2=1$ and $bc=-1$) and has no $X^3$ term, so it would be the characteristic polynomial of $z^2$ over $\mathbb{F}_3$. But that coefficient is minus the trace of $z^2=y_0+1$ to $\mathbb{F}_3$, that is $-(t_0-1+\overline{t_0-1})=-1$. So the dimension for $z$ is 4, and the total is 7. □

**Lemma 9.49.** *In this situation:*

(a) *For $\beta^8=1$, $F_\beta(w^{(32)})=\beta^{r_1}(B_\beta-1)$ with $B_\beta=\sum_\eta h(\eta)h(\beta/\eta)$. Moreover $F_{-i}(w^{(32)})=(-1)^{r_1}F_i(w^{(32)})$, and $\tau$ fixes $F_i(w^{(32)})$. If $w^{(32)}$ is good, then $F_\beta(w^{(32)})\in\mathbb{F}_9$ for every $\beta$ with $\beta^8=1$, and $F_{-1}(w^{(32)})\in\mathbb{F}_3$. If $w^{(32)}$ is not good, then $F_{-1}(w^{(32)})\in\mathbb{F}_9\setminus\mathbb{F}_3$.*

(b) *$\big(C(i\xi)/C(\xi)\big)^{82}=(-1)^{r_1}\mu(\xi^2)$ for every $\xi$. If $w^{(32)}$ is good, then*

$$F_{-i}(w^{(64)})=\lambda_0'\,\tau\big(F_i(w^{(64)})\big)+\big(\lambda_0'-(-1)^{r_1}\big)F_i(w^{(32)}).$$

(c) *$\epsilon$ is constant on each set $\{\pm\xi^{\pm1}\}$. If $\epsilon$ is constant, $\epsilon=\epsilon_0$, then $K_{64}(-1)\in\mathbb{F}_3$, so $F_{-1}(w^{(64)})\in\mathbb{F}_3$ if and only if $F_{-1}(w^{(32)})\in\mathbb{F}_3$.*

(d) *If $w^{(32)}$ is good and $\epsilon = \epsilon_0$ is constant, then $\tau'(K_{64}(i)) = \epsilon_0\lambda_0' K_{64}(i)$. Hence $F_i(w^{(64)}) \in \mathbb{F}_9$ if $\epsilon_0 = \lambda_0'$. If $\epsilon_0 = -\lambda_0'$, then $K_{64}(i) \neq 0$ and $F_i(w^{(64)}) \notin \mathbb{F}_9$.*

(e) *If $w^{(32)}$ is good and $\epsilon = \epsilon_0$ is constant, then*

$$F_{-i}(w^{(128)}) = \epsilon_0\,\tau\big(F_i(w^{(128)})\big) + (\epsilon_0 - \lambda_0')\,\tau\big(F_i(w^{(64)})\big) - \big(\lambda_0' - (-1)^{r_1}\big)F_i(w^{(32)}).$$

*Hence $F_{\pm i}(w^{(128)}) \in \mathbb{F}_9$ if and only if $\epsilon_0 = \lambda_0'$ and $F_i(w^{(128)}) \in \mathbb{F}_9$.*

(f) *If $w^{(32)}$ is good and $\epsilon = \epsilon_0 = \lambda_0'$, then exactly $5184 = 72^2$ of the $2^{16}$ children $w^{(128)}$ of $w^{(64)}$ satisfy $F_{\pm i}(w^{(128)}) \in \mathbb{F}_9$.*

(g) *If $w^{(32)}$ is not good and $F_{-1}(w^{(64)}) \in \mathbb{F}_3$, then no child $w^{(128)}$ of $w^{(64)}$ satisfies $F_{\pm i}(w^{(128)}) \in \mathbb{F}_9$.*

*Proof.* (a) Let $w = w^{(32)}$. By (18), $w_{2\rho} = -(S[\rho = r_1] + c_\rho)$ and $w_{2\rho+16} = -(S[\rho = r_1] - c_\rho)$ for $\rho < 8$. As $\beta^8 = 1$, pairing $\rho$ with $\rho+8$ gives $F_\beta(w) = -\beta^{r_1} - \sum_{\rho<8}\beta^\rho c_\rho^2$. As in the proof of Lemma 9.45(a), now with $c_\rho = \frac{1}{8}\sum_\eta C_{32}(\eta)\eta^{-\rho}$ and $\eta\eta'$ an 8-th root of unity, $\sum_{\rho<8}\beta^\rho c_\rho^2 = \frac{1}{8}\sum_\eta C_{32}(\eta)C_{32}(\beta/\eta) = -\beta^{r_1}B_\beta$, as $C_{32}(\eta) = \eta^{r_1}h(\eta)$ and $\frac{1}{8} = -1$. As $h(1/\eta) = h(\eta)$, $B_i = \sum_\eta h(\eta)h(-i\eta)$, and the substitution $\eta \mapsto -i\eta$ turns $B_{-i} = \sum_\eta h(\eta)h(i\eta)$ into $B_i$; so $F_{-i}(w) = (-i)^{r_1}(B_i - 1) = (-1)^{r_1}F_i(w)$. The map $\tau$ fixes each term. If $\mu = \mu_0$, then $\tau'\big(h(\eta)h(\beta/\eta)\big) = \mu_0^2\,h(-\eta)h(-\beta/\eta)$, and $\eta \mapsto -\eta$ gives $\tau'(B_\beta) = B_\beta$; as $\beta^{r_1} \in \mathbb{F}_9$, $F_\beta(w) \in \mathbb{F}_9$. For $\beta = -1$, with $\nu$ as in the set-up, $h(\eta)^9 = \nu(\eta)\nu(\eta^3)h(-\eta)$, so $\mu(\eta) = \nu(\eta)\nu(\eta^3)$ and $\mu(\eta)\mu(\eta^3) = \nu(\eta)\nu(-\eta)$. Also $B_{-1} = \sum_\eta h(\eta)h(-\eta)$, as $h(-1/\eta) = h(-\eta)$. If $w$ is good, $\nu(\eta)\nu(-\eta) = 1$, so $B_{-1}^3 = \sum_\eta h(\eta^3)h(-\eta^3) = B_{-1}$, and $F_{-1}(w) = (-1)^{r_1}(B_{-1} - 1) \in \mathbb{F}_3$. If $w$ is not good, put $h_1 = h(\eta_1)$, $\nu = \nu(\eta_1)$ and $\ell = h_1^{10}$. Then $h(-\eta_1) = \mu_A h_1^9$, $h(\eta_1^3) = \nu h_1^3$ and $h(-\eta_1^3) = -\mu_A\nu h_1^{27}$, and grouping the eight terms of $B_{-1}$ by the two sets $\{\pm\eta_1^{\pm1}\}$, $\{\pm\eta_1^{\pm3}\}$ gives $B_{-1} = \mu_A(\ell - \ell^3)$. As $h_1 = -\pi(\xi_1)y_0$, $\ell = y_0^{10} = 1 \pm i$ by Lemma 9.48, so $\ell - \ell^3 = \mp i \neq 0$. Hence $B_{-1}$ is a nonzero element of $i\mathbb{F}_3$, and $F_{-1}(w) = (-1)^{r_1}(B_{-1} - 1) \in \mathbb{F}_9 \setminus \mathbb{F}_3$.

(b) Put $R(\xi) = C(i\xi)/C(\xi)$. We have $C(\xi)^2 = S\,\xi^{2r_1}\Psi(\xi)$ (proof of Lemma 9.42). Hence $R(\xi)^2 = (-1)^{r_1}\Psi(i\xi)/\Psi(\xi)$ and $R(\xi)^{82} = (R(\xi)^2)^{41} = (-1)^{r_1}\pi(\xi)\pi(i\xi)$. Now $\xi^8 = \pm i$, so $\xi^9 = \pm i\xi$ and $(\xi^9)^2 = -\xi^2$. As $\hat\sigma$ is odd with coefficients in $\mathbb{F}_3$,

$$\Psi(\xi)^9 = \mu(\xi^2)h(-\xi^2) - i\,\hat\sigma(\xi^9) = \begin{cases} \Psi(\xi^9) & \text{if } \mu(\xi^2) = 1, \\ -\Psi(-\xi^9) & \text{if } \mu(\xi^2) = -1. \end{cases}$$

Taking 41-st powers, $\pi(\xi) = \mu(\xi^2)\pi(\pm\xi^9) = \mu(\xi^2)\pi(i\xi)$, which gives the first claim. If $w^{(32)}$ is good, then $R^{82} = \lambda_0'$, that is $1/R = \lambda_0'\,\tau(R)$. The substitution $\xi \mapsto i\xi$ gives $K_{64}(-i) = \sum_\xi 1/R(\xi) = \lambda_0'\,\tau(K_{64}(i))$, and with $K_{64}(i) = -F_i(w^{(64)}) - F_i(w^{(32)})$ and (a) the formula follows.

(c) From $C(-\xi)/C(\xi) = 1/(\epsilon(\xi)\omega(\xi))$ we get $\epsilon(-\xi) = \epsilon(\xi)$, and from $C(1/\xi) = 1/C(\xi)$ we get $\epsilon(1/\xi) = \epsilon(\xi)$. Now $K_{64}(-1) = \sum_\xi \epsilon(\xi)/\omega(\xi)$. On the set $O = \{\pm\xi^{\pm1}\}$ the function $1/\omega$ takes the values $\omega(\xi)$ and $1/\omega(\xi)$, each twice, so the four terms of $O$ add up to $-\epsilon(O)y(O)$, where $y(O) = y(\xi)$. By the set-up, $y(O)^3 = y(O^3)$, and $\xi \mapsto \xi^3$ permutes the four sets. Hence, if $\epsilon = \epsilon_0$, $K_{64}(-1)^3 = K_{64}(-1)$.

(d) Let $\epsilon = \epsilon_0$, $\mu = \mu_0$, and $R$ as in (b). Put $\varphi(\xi) = R(\xi)\big(\omega(\xi)/\omega(i\xi)\big)^{21}$; as $\omega^{42} = \omega$, $\varphi(\xi)^2 = (-1)^{r_1}\pi(\xi)\pi(i\xi) = \lambda_0'$ by (b), so $\varphi(\xi)^4 = 1$. First, $R(\xi)R(i\xi) = C(-\xi)/C(\xi) = \epsilon_0/\omega(\xi)$, while $\big(\omega(\xi)/\omega(i\xi)\big)^{21}\big(\omega(i\xi)/\omega(-\xi)\big)^{21} = \omega(\xi)^{42} = \omega(\xi)$; so $\varphi(\xi)\varphi(i\xi) = \epsilon_0$. Next, let $\iota(\xi) = \mu_0\,\xi^9$. The display in (b) gives $\omega(\xi)^9 = \omega(\iota(\xi))$, and $\iota(i\xi) = i\,\iota(\xi)$, so $\tau'(R(\xi)) = \varphi(\xi)^9\big(\omega(i\iota(\xi))/\omega(\iota(\xi))\big)^{21} = \big(\varphi(\xi)/\varphi(\iota(\xi))\big)R(\iota(\xi))$. Finally $\iota(\xi) = \pm i\xi$. If $\iota(\xi) = i\xi$, then $\varphi(\xi)/\varphi(i\xi) = \varphi(\xi)^2/\epsilon_0 = \epsilon_0\lambda_0'$; if $\iota(\xi) = -i\xi$, then $\varphi(-i\xi)\varphi(\xi) = \epsilon_0$ and again $\varphi(\xi)/\varphi(-i\xi) = \epsilon_0\lambda_0'$. As $\iota$ permutes the roots $\xi$, $\tau'(K_{64}(i)) = \epsilon_0\lambda_0'K_{64}(i)$. With $F_i(w^{(64)}) = -F_i(w^{(32)}) - K_{64}(i)$ and (a), this gives $F_i(w^{(64)}) \in \mathbb{F}_9$ if $\epsilon_0 = \lambda_0'$; and, if $\epsilon_0 = -\lambda_0'$, $F_i(w^{(64)})$ is in $\mathbb{F}_9$ if and only if $K_{64}(i) = 0$.

Now let $\epsilon_0 = -\lambda_0'$. Write $r = R(\xi)$, $\varpi = \omega(\xi)$ and $\varpi' = \omega(i\xi)$. From $R(\zeta)R(i\zeta) = \epsilon_0/\omega(\zeta)$ at $\zeta = \xi, i\xi, -\xi$ and $\omega(-\xi) = 1/\varpi$, the values of $R$ at $\xi, i\xi, -\xi, -i\xi$ are $r$, $\epsilon_0/(\varpi r)$, $\varpi r/\varpi'$ and $\epsilon_0\varpi'/r$.

As $r^2 = \lambda_0'\varpi'/\varpi$, their sum is $r(1-\varpi)(1-1/\varpi')$. As $R(1/\zeta) = R(-i\zeta)$, the inverse points carry the same four values. Write the roots as $\xi_1^a$ ($a$ odd modulo 32). Multiplication by $i$ preserves $a$ modulo 8, and inversion maps $a$ to $-a$. So $K_{64}(i) = A_1 + A_2$, where $A_j = -r_j(1-\varpi_j)(1-1/\varpi_j')$ is the sum over $a \equiv \pm 1$ (for $j=1$, $\xi = \xi_1$) or $a \equiv \pm 3 \pmod 8$ (for $j=2$, $\xi = \xi_1^3$). Then $(1-\varpi)^2/\varpi = y(\xi)+1$ and $(1-1/\varpi')^2\varpi' = y(i\xi)+1$. As $i\xi_1 = \pm\xi_1^9$, the set-up gives $y(i\xi_1) = y(\xi_1)^9$, so $A_1^2 = \lambda_0' N$ with $N = (y(\xi_1)+1)(y(\xi_1)^9+1)$; in the same way $A_2^2 = \lambda_0' N^3$. Let $\alpha = \omega(\xi_1)^{21}$, so $\alpha^2 = \omega(\xi_1)$, and $z = \alpha - 1/\alpha$. Then $1-\omega(\xi_1) = -\alpha z$ and $1-\omega(\xi_1)^9 = -\alpha^9 z^9$, so $N = z^{20}$. As $81 \equiv -1 \pmod{41}$, $z^{81} = -z$, and $z \neq 0$. Hence $N^4 = z^{80} = -1$, so $N \notin \mathbb{F}_3$, $A_1^2 \neq A_2^2$ and $K_{64}(i) \neq 0$.

(e) Put $R_2(x) = C_{128}(ix)/C_{128}(x)$. As $C_{128}(v)^2 = SC(v^2)$,

$$R_2(x)^2 = C(-x^2)/C(x^2) = 1/\big(\epsilon(x^2)\,\omega(x^2)\big),$$

so $R_2^{82} = \epsilon_0$ and $1/R_2 = \epsilon_0\tau(R_2)$. As in (b), $K_{128}(-i) = \epsilon_0\tau(K_{128}(i))$, and the formula follows from $K_{128}(\pm i) = -F_{\pm i}(w^{(128)}) - F_{\pm i}(w^{(64)})$ and (b). As $\tau$ maps $\mathbb{F}_9$ onto itself and $F_i(w^{(32)}) \in \mathbb{F}_9$ by (a), if $\epsilon_0 = \lambda_0'$ then $F_{-i}(w^{(128)}) \in \mathbb{F}_9$ if and only if $F_i(w^{(128)}) \in \mathbb{F}_9$; if $\epsilon_0 = -\lambda_0'$, then modulo $\mathbb{F}_9$, $F_{-i}(w^{(128)}) \equiv \epsilon_0\tau\big(F_i(w^{(128)}) - F_i(w^{(64)})\big)$. By (d), $F_i(w^{(64)}) \notin \mathbb{F}_9$; so if $F_i(w^{(128)}) \in \mathbb{F}_9$, then $F_{-i}(w^{(128)}) \equiv -\epsilon_0\tau\big(F_i(w^{(64)})\big) \notin \mathbb{F}_9$, and the two conditions cannot both hold.

(f) By (d) and (e) we count the children with $K_{128}(i) \in \mathbb{F}_9$. For a root $x$ of $v^{32}+1$ put $\xi = x^2$, a root of $v^{16}+1$, and $\theta(\xi) = \omega(\xi)^{20}$, so $\theta(\xi)^2 = 1/\omega(\xi)$. With $R_2$ as in (e), $\varphi_2(x) = R_2(x)/\theta(\xi)$ satisfies $\varphi_2^2 = \epsilon_0$, and $K_{128}(i) = -\sum_\xi \theta(\xi)\big(\varphi_2(x) + \varphi_2(-x)\big)$ over the 16 roots $\xi$, where $\pm x$ are the roots over $\xi$. Call $\xi$ *active* if $\varphi_2(x) = \varphi_2(-x)$; then its term is $\theta(\xi)\varphi_2(x)$, and otherwise it is 0. Put $\Pi(x) = \prod_{u^4=1} C_{128}(ux)$. Then $\Pi(x)^2 = \big(C(\xi)C(-\xi)\big)^2$, and $\xi$ is active if and only if $\Pi(x) = C(\xi)C(-\xi)$. As $\Pi(ix) = \Pi(x)$ and $\Pi(1/x) = 1/\Pi(x)$, activity is constant on each set $O = \{\pm\xi^{\pm 1}\}$. Next, $R_2(1/x) = R_2(-ix)$ and $R_2(x)R_2(ix) = C_{128}(-x)/C_{128}(x) =: \kappa(x) = \pm 1$. Fix a root $x_O$ over a point $\xi_O$ of each set $O$, and fix $\varphi_0 \in \mathbb{F}_9$ with $\varphi_0^2 = \epsilon_0$. Then an active set contributes $-c\varphi_0\big(\theta_O + \kappa\epsilon_0\theta_O^{-1}\big)$, where $c = \varphi_2(x_O)/\varphi_0 = \pm 1$, $\kappa = \kappa(x_O)$ and $\theta_O = \theta(\xi_O)$. The 8 roots over $O$ form 4 sign pairs of $C_{128}$. Let $s_0, \dots, s_3$ be the signs at $x_O, ix_O, -x_O, -ix_O$. Up to fixed signs, activity, $c$ and $\kappa$ are $s_0s_1s_2s_3$, $s_0s_1$ and $s_0s_2$: three independent characters. So each of their 8 joint values comes from 2 of the 16 choices of these signs, and different sets use different pairs. Now $Y_O = \theta_O + \theta_O^{-1}$ is fixed by $\tau$ and $Z_O = \theta_O - \theta_O^{-1}$ is negated, while $\mathbb{F}_9$ is fixed; so $K_{128}(i) \in \mathbb{F}_9$ if and only if the terms with $Z_O$ add up to 0 and the terms with $Y_O$ add up to an element of $\mathbb{F}_9$.

Let $O_k = \{\pm\xi_1^{\pm 3^k}\}$ ($k < 4$) be the four sets, and $\theta = \theta_{O_0} = \omega(\xi_1)^{20}$. By the set-up, $\theta_{O_k} = \theta^{\pm 3^k}$, so $Y_k := Y_{O_k} = Y_0^{3^k}$ and $Z_{O_k} = \pm Z_0^{3^k}$; here $Y_0 = \theta + 1/\theta$ is the $Y_0$ of Lemma 9.48. $Y$-terms: by that lemma, $D = Y_0 - Y_2$ satisfies $D^9 = -D \neq 0$. Hence $D$ and $D^3 = Y_1 - Y_3$ are $\mathbb{F}_3$-independent (if $D^3 = cD$ with $c \in \mathbb{F}_3$, then $D^2 \in \mathbb{F}_3$, so $D \in \mathbb{F}_9$ and $D^9 = D$), and $\sum_k v_k Y_k \in \mathbb{F}_9$ ($v_k \in \mathbb{F}_3$) if and only if $v_0 = v_2$ and $v_1 = v_3$. $Z$-terms: with Fr as in the proof of Lemma 9.48, let $\chi$ be the monic divisor of $t^8 - 1$ of least degree with $\chi(\mathrm{Fr})\theta = 0$. Its degree is the dimension of the span of the conjugates of $\theta$, so $\deg\chi = 7$ by Lemma 9.48. Since the factors of $t^8-1$ of degree 1 divide $t^4-1$, $t^4+1$ divides $\chi$. As $Z_0 = (1-\mathrm{Fr}^4)\theta$, a relation $a(\mathrm{Fr})Z_0 = 0$ with $\deg a < 4$ gives $\chi \mid a(t)(1-t^4)$. Hence $t^4+1 \mid a(t)$, so $a = 0$: the $Z_{O_k}$ are $\mathbb{F}_3$-independent and no $Z$-term occurs. Thus the children counted are those in which every set is inactive or has a $Y$-term, with coefficients $(v_0, v_1, v_0, v_1)$. A set is inactive for 8 of its 16 sign choices, and has a $Y$-term with coefficient $+1$ or $-1$ for 2 each. The count is therefore $(8^2 + 2^2 + 2^2)^2 = 72^2 = 5184$.

(g) Let $w = w^{(32)}$, let $O_k = \{\pm\xi_1^{\pm 3^k}\}$ ($k < 4$), let $\mu_A$, $h_1$ and $\nu$ be as in the proof of (a), and let $Y_0$, $y_0$, $p$, $g$, $t_0$, $D$, $\delta$ be as in Lemma 9.48. By (a), $F_{-1}(w) \in \mathbb{F}_9 \setminus \mathbb{F}_3$.

Signs. As $F_{-1}(w^{(64)}) \in \mathbb{F}_3$, $K_{64}(-1) \in \mathbb{F}_9$, and by (c) $K_{64}(-1) = -\sum_k \epsilon(O_k) y_0^{3^k}$. The argument of (f) for $Y_0$ applies to $y_0$ ($y_0 \notin \mathbb{F}_9$, as for $Y_0$ in the proof of Lemma 9.48), so $\epsilon(O_0) = \epsilon(O_2)$ and $\epsilon(O_1) = \epsilon(O_3)$. If $\epsilon$ were constant, (c) would give $F_{-1}(w) \in \mathbb{F}_3$. So $\epsilon(O_k) = e'(-1)^k$ with $e' = \pm 1$.

Write the roots as $\xi_1^a$ ($a$ odd); then $O_0 \cup O_2$ and $O_1 \cup O_3$ are the roots with $a \equiv \pm 1$ and $a \equiv \pm 3$ (mod 8), and by (b) $R^{82} = \lambda'$ with $\lambda' = \lambda'_1 := (-1)^{r_1}\mu_A$ on the first half and $\lambda' = -\lambda'_1$ on the second. Hence $\epsilon\lambda' = \kappa_0 := e'\lambda'_1$ at every root.

Level 64. The second paragraph of the proof of (d) uses only that $\epsilon$ and $\lambda'$ are constant on each half. With $\kappa_0$ in place of $\epsilon_0\lambda'_0$ it gives $K_{64}(i) = A_1 + A_2$ with $A_j = -r_j(1 + \kappa_0\varpi_j)(1 + \kappa_0/\varpi'_j)$, $r_j^2 = \lambda'_j\varpi'_j/\varpi_j$ ($\lambda'_2 = -\lambda'_1$), $A_1^2 = \lambda'_1 N_0$ and $A_2^2 = -\lambda'_1 N_0^3$, where $N_0 = (y_0 - \kappa_0)(y_0^9 - \kappa_0)$. As $\tau(r_j) = \lambda'_j/r_j = r_j\varpi_j/\varpi'_j$, $\tau(\varpi) = 1/\varpi$ and $1 + \kappa_0\varpi = \kappa_0(\varpi + \kappa_0)$, we get $\tau(A_j) = A_j$. So $K_{64}(i) \in \mathbb{F}_{81}$, and $K_{64}(-i) = \sum_\xi 1/R(\xi) = \sum_\xi \lambda'(\xi)\tau(R(\xi)) = \lambda'_1(A_1 - A_2) \in \mathbb{F}_{81}$. If $\kappa_0 = 1$, then $N_0 = Y_0^2 Y_0^{18} = g^2$ (as $y_0 - 1 = Y_0^2$), so $A_1^2$ and $A_2^2$ are squares in $\mathbb{F}_9$ and $A_1, A_2 \in \mathbb{F}_9$. If $\kappa_0 = -1$, then $N_0$ is the $N$ of the proof of (d), $N^4 = -1$, and $A_j^9 = A_j(A_j^2)^4 = -A_j \neq 0$.

Level 32. As $i = \eta_1^4$, $\eta$ and $i/\eta$ always lie in different sets $\{\pm\eta_1^{\pm 1}\}$, $\{\pm\eta_1^{\pm 3}\}$, and the argument of (a) gives $\tau'(B_i) = -B_i$; so $F_{\pm i}(w) \equiv (\pm i)^{r_1}B_i$ modulo $\mathbb{F}_9$. Grouping the terms of $B_i$ with $h(1/\eta) = h(\eta)$ gives $B_i = -\big(h(\eta_1) + h(-\eta_1)\big)\big(h(\eta_1^3) + h(-\eta_1^3)\big) = -\nu\big(h_1 + \mu_A h_1^9\big)\big(h_1 - \mu_A h_1^9\big)^3$. As $h_1 = -\pi(\xi_1)y_0$ and $y_0 - y_0^9 = Y_0^2 - Y_0^{18} = pD$, we get $B_i = -\nu D\, p\bar{t}_0$ if $\mu_A = -1$ and $B_i = -\nu\delta D\, \bar{p}t_0$ if $\mu_A = 1$. Put $q = p\bar{t}_0$.

Level 128. In the proof of (f) each set $O$ has a single value $\epsilon(O)$, so the computation there holds with $\epsilon(O)$ in place of $\epsilon_0$ and $\varphi_O \in \{1, i\}$, $\varphi_O^2 = \epsilon(O)$, in place of $\varphi_0$; and as $1/R_2 = \epsilon\varphi_2/\theta$, the terms of $K_{128}(-i)$ are $\kappa$ times those of $K_{128}(i)$. So

$$K_{128}(i) = \sum_k \varphi_k(v_k Y_k + u_k Z_k), \qquad K_{128}(-i) = \sum_k \epsilon(O_k)\varphi_k(v_k Y_k - u_k Z_k),$$

with $Z_k = Z_{O_k}$, $\varphi_k = \varphi_{O_k}$ and $(v_k, u_k) \in \{(0,0), (\pm 1, 0), (0, \pm 1)\}$. Put $P = F_i(w) + K_{64}(i)$ and $P' = F_{-i}(w) + K_{64}(-i)$. They lie in $\mathbb{F}_{81}$, and $F_{\pm i}(w^{(128)})$ are $P - K_{128}(i)$ and $P' - K_{128}(-i)$. The parts of these negated by $\tau$ vanish only if $\sum_{\epsilon(O_k)=1} u_k Z_k = 0 = \sum_{\epsilon(O_k)=-1} u_k Z_k$. Each sum has two terms, $k$ and $k+2$, and $Z_{k+2} = \pm Z_k^9$; two nonzero terms would give $Z_k^8 = \pm 1$, so $Z_k \in \mathbb{F}_{81}$, which is false as $\tau(Z_k) = -Z_k \neq 0$. Thus every $u_k = 0$. As $Y_{k+2} = Y_k^9 \equiv -Y_k$, $Y_0 \equiv -D$ and $Y_1 \equiv -D^3 = -\delta D$ modulo $\mathbb{F}_9$, the conditions $F_{\pm i}(w^{(128)}) \in \mathbb{F}_9$ now read, modulo $\mathbb{F}_9$,

$$\begin{aligned} P + P' &\equiv (v_0 - v_2)D, \quad & P - P' &\equiv i(v_1 - v_3)\delta D \quad \text{if } e' = 1,\\ P + P' &\equiv (v_1 - v_3)\delta D, \quad & P - P' &\equiv i(v_0 - v_2)D \quad \text{if } e' = -1, \end{aligned}$$

where $P \pm P' = \big(1 \pm (-1)^{r_1}\big)F_i(w) + (1 \pm \lambda'_1)A_1 + (1 \mp \lambda'_1)A_2$. If $\kappa_0 = 1$, then $A_1, A_2 \in \mathbb{F}_9$, and as $F_i(w) \equiv i^{r_1}B_i$ with $B_i^9 = -B_i$, the conditions force $B_i/D \in \mathbb{F}_3$ or $B_i/D \in \delta\mathbb{F}_3$ (which one depends on $r_1$ and $e'$). As $\delta^{-1} = -\bar{\delta}$ ($\delta^4 = -1$), both fail if $q \notin \mathbb{F}_3 \cup \delta\mathbb{F}_3$. If $\kappa_0 = -1$, then in each of the four cases ($r_1$ even or odd, $e' = \pm 1$) one of $P \pm P'$ is $-A_1$ or $-A_2$ (as $\lambda'_1 = -e'$), a nonzero element with $A_j^9 = -A_j$; squaring, with $A_1^2 = \lambda'_1 N$ and $A_2^2 = -\lambda'_1 N^3$, gives $N = \bar{\delta}$. So it suffices that $q \notin \mathbb{F}_3 \cup \delta\mathbb{F}_3$ and $N \neq \bar{\delta}$. By Lemma 9.48, $p = 1$, $g = \pm i$, $t_0 = \pm i$ and $\delta = 1 \mp i$. Hence $q = \mp i$ is not in $\mathbb{F}_3 \cup \delta\mathbb{F}_3 = \{0, \pm 1, \pm(1 \mp i)\}$. As $Y_0 + c$ has norm $g + cp + c^2$ for $c \in \mathbb{F}_9$ and $y_0 + 1 = Y_0^2 - 1$, $N = (g - p + 1)(g + p + 1) = -1 \mp i = -\bar{\delta} \neq \bar{\delta}$. □

*Remark* 9.50. For each $S$, a computation (one program, run on each class) shows that 64 pairs $(r_1, s)$ of Lemma 9.32 have $\Theta(\eta)$ a square at every root; with the 16 choices of $h$ (one sign on each pair $\{\eta, 1/\eta\}$) this gives 1024 bases $w^{(32)}$ in case (I) with $\Theta$ a square. Each has $2^8$ children $w^{(64)}$ and each of these has $2^{16}$ children $w^{(128)}$. Flipping the sign of $C$ on one pair flips $\epsilon$ on one set $\{\pm\xi^{\pm 1}\}$, so each of the 16 functions $\epsilon$ comes from exactly 16 children. As $\mu$ is constant on each of the two sets $\{\pm\eta_1^{\pm 1}\}$, $\{\pm\eta_1^{\pm 3}\}$, and flipping $h$ on one pair $\{\eta, 1/\eta\}$ flips $\mu$ on its set, for each $(r_1, s)$ exactly 8 of the 16 choices of $h$ are good, and 512 of the 1024 bases are good.

A good $w^{(32)}$ has exactly 32 children $w^{(64)}$ with $F_{-1}(w^{(64)}) \in \mathbb{F}_3$, namely those with $\epsilon$ constant, and any other $w^{(32)}$ has 16. Indeed, $F_{-1}(w^{(32)}) \in \mathbb{F}_9$ by Lemma 9.49(a), so as in the proof of (g), $F_{-1}(w^{(64)}) \in \mathbb{F}_3$ forces $\epsilon(O_0) = \epsilon(O_2)$ and $\epsilon(O_1) = \epsilon(O_3)$. If $\epsilon(O_k) = e'(-1)^k$, then

$K_{64}(-1) = -e'(t_0 - \bar{t}_0)$ with $t_0 = \pm i$ (Lemma 9.48), a nonzero element of $i\mathbb{F}_3$. So on a good base only the two constant functions $\epsilon$ pass. On any other base the constant ones fail, as $F_{-1}(w^{(32)}) \notin \mathbb{F}_3$, and exactly one $e'$ passes, as $F_{-1}(w^{(32)})$ is congruent modulo $\mathbb{F}_3$ to the nonzero element $(-1)^{r_1}B_{-1}$ of $i\mathbb{F}_3$ (proof of (a)). Next, of the 32 children of a good $w^{(32)}$, the 16 with $\epsilon_0 = \lambda'_0$ have exactly 5184 children $w^{(128)}$ with $F_{\pm i}(w^{(128)}) \in \mathbb{F}_9$ each, by (e) and (f), and the 16 with $\epsilon_0 = -\lambda'_0$ have none, by (e); the 16 children of any other $w^{(32)}$ have none, by (g). Hence the bases $w^{(128)}$ that satisfy the conditions of Lemma 9.45(c) for $o = 2$ and $o = 4$ are exactly 5184 children of each of $512 \cdot 16 = 8192$ bases $w^{(64)}$, that is 42467328 of the $1024 \cdot 2^8 \cdot 2^{16} = 2^{34}$ bases $w^{(128)}$ whose chain reaches case (I) first at level 32 with $\Theta$ a square, in each class. The number of good bases, the counts 32 and 16 of children, the dimension 7 and the value of $Y_0 + Y_0^9$ in Lemma 9.48 were also checked by exhaustive search in both classes, and the count 5184 for each of the 8192 bases $w^{(64)}$ in the class $S = -1$ (each check by one program, run on each class named). Thus the conditions of Lemma 9.45(c) for $o = 2$ and $o = 4$ alone do not exclude the chains with $M_0 = 32$ and $\Theta$ a square.

*Remark* 9.51. For $n = 512$ ($m = 256$) Lemma 9.45(c) has one more stage, $o = 8$: $F_\beta(w^{(256)}) \in \mathbb{F}_9$ for the four $\beta$ of order 8. The identity $F_\beta(w^{(256)}) = -F_\beta(w^{(128)}) - K$ of Remark 9.46 still holds, but Lemma 9.45(a) says nothing about $K$ here (it needs $M \geq oM_0 = m$), so this is a condition on the $2^{32}$ children $w^{(256)}$ of each $w^{(128)}$. We checked it on a sample in the class $S = 1$, with one program. Call a base $w^{(128)}$ that passes the conditions for $o = 2$ and $o = 4$ *of the first kind* if $F_\beta(w^{(128)}) \in \mathbb{F}_9$ for the four $\beta$ of order 8, and *of the second kind* otherwise. We took four of the 8192 bases $w^{(64)}$ of Remark 9.50 (the first passing one over each of four good bases $w^{(32)}$). Three of them have $F_\beta(w^{(64)}) \in \mathbb{F}_9$ for the four $\beta$ of order 8, and each of these three has exactly 16 passing children $w^{(128)}$ of the first kind among its 5184; the fourth has none. Then we took four passing bases $w^{(128)}$, all over the first good base $w^{(32)}$ in the order of the program: going through its children among the 8192 bases $w^{(64)}$ in that order, we took from each one the first passing child of each kind that it has, until we had four. They come from three bases $w^{(64)}$, and two are of each kind. For each of the two of the first kind, exactly $7617600 = 2760^2$ of its $2^{32}$ children $w^{(256)}$ satisfy the four conditions of order 8; for each of the two of the second kind, none does. These children $w^{(256)}$ also meet the conditions for $o = 2$ and $o = 4$, which concern only $w^{(64)}$ and $w^{(128)}$. So, by this computation (one program), for $n = 512$ some bases meet all the conditions of Lemma 9.45(c), of orders 2, 4 and 8, and these conditions do not exclude the chains with $M_0 = 32$ and $\Theta$ a square.

9.8. **The odd locus with $M_0 = 8$ for every odd $e \geq 11$.** We reduce the chains with $M_0 = 8$, for every odd $e \geq 11$, to the three parts of Question 9.68. Theorem 9.65 shows that such a chain gives a swap pair (Definition 9.55) whose points, by Proposition 9.63, either lie (after zero coordinates are omitted) in one of finitely many sets of two kinds that do not depend on $e$, or fall in one remaining case. Theorem 9.67 pushes that case down to finer grids. In this subsection $e \geq 11$ is odd, $n = 2^e$ and $m = n/2$, so $m \geq 1024$, and $y$ is as in Lemma 9.38: its base has $w^{(M)}$ in case (II) for $M = m, m/2, \ldots, 16$ and $w^{(8)}$ in case (I). We use the notation of that lemma and its proof. In particular every value $C_M(\eta)$ is a root of unity of 2-power order, $C_M(v)^2 = S\,C_{M/2}(v^2)$ for $M \geq 32$, $C_M(v)C_M(1/v) = 1$, and $C_{16}(v)^2 = -S\,i(\alpha v + \beta v^3)$. Induction gives $C_M(\eta)^{2^j} = S\,C_{M/2^j}(\eta^{2^j})$ for $j \geq 1$ and $M/2^j \geq 16$, as $S^2 = 1$. Put $\zeta = 1 - i$, so $\zeta^2 = i$ and $\zeta$ has order 8, and fix $\vartheta \in \mathbb{F}_{81}$ with $\vartheta^2 = \zeta$. Put $\sigma_2 = 3^{m/128}$. Since $3^{2^j} \equiv 1 + 2^{j+2} \pmod{2^{j+3}}$ for $j \geq 1$, the number $u_2 = (\sigma_2 - 1)/(m/32)$ is an odd integer. It is used only as an exponent, and it is not the grid value $u_2$ below. As $m/128 \geq 8$, the map $x \mapsto x^{\sigma_2}$ fixes $\mathbb{F}_{3^8}$, so it fixes $i$, $\zeta$, $\vartheta$ and every root of unity of order dividing 16.

For a fixed index $k$ and the three levels $M = m, m/2, m/4$ we use the grids

$$\gamma_t = c^{(m)}_{k-tm/32}, \qquad \delta_t = c^{(m/2)}_{k-tm/32}, \qquad X_t = c^{(m/4)}_{k-tm/64} \qquad (t \in \mathbb{Z}),$$

and by the negacyclic rules $\gamma_{t+8}=-\gamma_t$, $\delta_{t+4}=-\delta_t$ and $X_{t+4}=-X_t$. For a root $z$ of $z^4+1$ (resp. $\psi$ of $\psi^8+1$) put $\hat X(z)=\sum_{t<4}X_tz^{-t}$, $\hat\delta(z)=\sum_{t<4}\delta_tz^{-t}$ and $\hat\gamma(\psi)=\sum_{t<8}\gamma_t\psi^{-t}$.

**Lemma 9.52.** *Let $k$ be an index. Define $K(\psi)=(S\,C_{32}(\psi))^{u_2}\psi^{-u_2k}$ for $\psi^8=-1$ and $F(z)=(S\,C_{16}(z))^{u_2}z^{-u_2k}$ for $z^4=-1$. Then, at every such root,*

$$\text{(a)}\ \ \widehat{\gamma^{\sigma_2}}(\psi)=K(\psi)\,\hat\gamma(\psi),\qquad \text{(b)}\ \ \widehat{\delta^{\sigma_2}}(z)=F(z)\,\hat\delta(z),\qquad \text{(c)}\ \ \widehat{X^{\sigma_2}}(z)=F(z)^2\,\hat X(z),$$

*where $\gamma^{\sigma_2}=(\gamma_t^{\sigma_2})_t$, and so on. Moreover (d) $K(\psi)^2=F(\psi^2)$, (e) $F(z)F(1/z)=1$, (f) $F(-z)^2=-F(z)^2$, and (g) $F(z)^4=-1$ if $(-1)^k=\alpha\beta$. (h) Let $\sigma_4=3^{m/256}$, $u_4=(\sigma_4-1)/(m/64)$ (odd), and $\delta_t^{(4)}=c_{k-tm/64}^{(m/2)}$ ($t\in\mathbb{Z}$, $\delta_{t+8}^{(4)}=-\delta_t^{(4)}$). Then $\widehat{\delta^{(4)\sigma_4}}(\psi)=F_4(\psi)\,\widehat{\delta^{(4)}}(\psi)$ with $F_4(\psi)=(S\,C_{32}(\psi))^{u_4}\psi^{-u_4k}$, where $\widehat{\delta^{(4)}}(\psi)=\sum_{t<8}\delta_t^{(4)}\psi^{-t}$ for $\psi^8=-1$.*

*Proof.* Let $M\in\{m,m/2,m/4\}$ and let $\eta$ run over the roots of $v^{M/4}+1$, so $c_x^{(M)}=\frac{4}{M}\sum_\eta C_M(\eta)\eta^{-x}$ with $\frac{4}{M}\in\mathbb{F}_3$. Write $\sigma_2=1+du_2$ with $d=m/32$. Then $\eta^{\sigma_2}=\eta\,(\eta^d)^{u_2}$ and $C_M(\eta)^{\sigma_2}=C_M(\eta)\,(C_M(\eta)^d)^{u_2}$. For $M=m$, $\eta^d=\psi$ is a root of $\psi^8+1$ and $C_m(\eta)^d=S\,C_{32}(\psi)$; for $M=m/2$, $\eta^d=z$ is a root of $z^4+1$ and $C_{m/2}(\eta)^d=S\,C_{16}(z)$; for $M=m/4$, $\eta^{d/2}=z$ is a root of $z^4+1$ and $C_{m/4}(\eta)^d=(S\,C_{16}(z))^2$. Hence $(c_x^{(M)})^{\sigma_2}=\frac{4}{M}\sum_\eta C_M(\eta)\eta^{-x}\,\Phi(\eta)$, where $\Phi(\eta)$ is $(S\,C_{32}(\psi))^{u_2}\psi^{-u_2x}$, $(S\,C_{16}(z))^{u_2}z^{-u_2x}$, or $(S\,C_{16}(z))^{2u_2}z^{-2u_2x}$, and depends on $\eta$ only through $\psi$ or $z$. For $x$ on the grid of $k$ the index $x$ enters $\Phi$ only through $x$ mod 16, which is $k$ mod 16 as $m/64\ge16$. Splitting the sum over $\eta$ by the value of $\psi$ or $z$ gives (a), (b), (c). For (d), $K(\psi)^2=(C_{32}(\psi)^2)^{u_2}\psi^{-2u_2k}=(S\,C_{16}(\psi^2))^{u_2}(\psi^2)^{-u_2k}=F(\psi^2)$. (e) follows from $C_{16}(z)C_{16}(1/z)=1$ and $S^2=1$. For (f), $F(z)^2=(C_{16}(z)^2)^{u_2}z^{-2u_2k}=(-S\,i(\alpha z+\beta z^3))^{u_2}z^{-2u_2k}$, and $\alpha z+\beta z^3$ is odd in $z$ while $u_2$ is odd. For (g), $(\alpha z+\beta z^3)^2=\alpha\beta$ when $z^4=-1$ (as $\alpha,\beta=\pm1$), so $F(z)^4=(-\alpha\beta)^{u_2}(-1)^{u_2k}=-\alpha\beta(-1)^k$. For (h), argue as for (b) with $\sigma_4=1+(m/64)u_4$, $\eta^{m/64}=\psi$ and $C_{m/2}(\eta)^{m/64}=S\,C_{32}(\psi)$; $\sigma_4$ fixes $\mathbb{F}_{81}$. □

From now on $k$ is an index with $(-1)^k=\alpha\beta$, $k'=k-m/64$, and $\gamma',\delta'$ and $u'$ (below) are the grids of $k'$. The even and the odd entries of $\gamma$ are the orbits $k-tm/16$ and $k-m/32-tm/16$ of Lemma 9.38, with spectra $\hat\gamma(\psi)\pm\hat\gamma(-\psi)$ at $\psi^2$. If no couple $k-tm/32$ is special, step (6) of the proof of that lemma puts each spectrum in a set $\{\zeta^a,\zeta^{-a}\}$ with $a\in\{1,3\}$. We say that $k$ has *block* $\{\pm a\}$ if the same $a$ serves both orbits, that is, if $\hat\gamma(\psi)=0$ unless $\psi^2\in\{\zeta^a,\zeta^{-a}\}$. Put $u_t=w_{2(k-tm/32)}^{(m/4)}$; then $u_{t+4}=u_t$, and, as $w_{2x}^{(m/4)}=-(w_{2x}^{(m/8)}+c_x^{(m/4)})$ and $c_{x-m/16}^{(m/4)}=-c_x^{(m/4)}$,

$$X_{2t}=u_t-u_{t+2}\qquad(t\in\mathbb{Z}).\tag{19}$$

The couple $k-tm/32$ has $a=-(u_t+\delta_t)$, $a'=-(u_t-\delta_t)$, $c=\gamma_t$ and $c'=\gamma_{t-4}=-\gamma_{t+4}$ (step (4) of the proof of Lemma 9.38), so (F1) of that proof reads $u_t\delta_t=\gamma_{t+4}^2-\gamma_t^2$ (as $4=1$). If the orbit of $\gamma$ through $t$ has its spectrum in $\{\zeta^{\pm b}\}$, write $\gamma_{t+2s}=\vartheta^{b(t+2s)}H_t^+ + \vartheta^{-b(t+2s)}H_t^-$ ($s\in\mathbb{Z}$); then $\gamma_{t+4}=i^b(\vartheta^{bt}H_t^+-\vartheta^{-bt}H_t^-)$, and as $2=-1$,

$$u_t\,\delta_t=\zeta^{bt}(H_t^+)^2+\zeta^{-bt}(H_t^-)^2.\tag{20}$$

Here $H_t^\pm=H_{t+2}^\pm$, and $H_t^+=h_b+(-1)^th_{b+8}$, $H_t^-=h_{-b}+(-1)^th_{8-b}$, where $h_f$ is the coefficient of $\vartheta^{ft}$ in $\gamma_t$. Put $\sigma=\sigma_2^2=3^{m/64}$. By step (2) of the proof of Lemma 9.38 for $M=m/4$ ($3^{M/16}=\sigma$), $(c_x^{(m/4)})^\sigma=-c_x^{(m/4)}$ when $(-1)^x=\alpha\beta$, and the entries of $w^{(m/8)}$ lie in $\mathbb{F}_{3^{m/64}}$; so, with (19),

$$u_t^\sigma=u_{t+2}\qquad(t\in\mathbb{Z}).\tag{21}$$

**Lemma 9.53.** *Let $(-1)^k=\alpha\beta$, and suppose that no couple $k-tm/32$ is special. Then $k$ has a block $\{\pm a\}$, and $\hat\delta(\zeta^{\pm3a})=0$.*

*Proof.* By step (6) of the proof of Lemma 9.38, the even entries of $\gamma$ (the orbit through $t=0$) have spectrum in a set $\{\zeta^{\pm a}\}$, and the odd entries in a set $\{\zeta^{\pm b}\}$. Put $f=F(\zeta^a)$. By Lemma 9.52(a), (d), $h_g^\sigma = K(\vartheta^g)^2 h_g = F(\zeta^g)h_g$, so $(H_0^\pm)^\sigma = f^{\pm1}H_0^\pm$, using (e). By (g), $f^{-2}=-f^2$. Apply $\sigma$ to (20) at $t=0$ and compare with (20) at $t=2$, which reads $u_2\delta_2 = i^a((H_0^+)^2-(H_0^-)^2)$; with (21) and $u_2\neq 0$ (step (4) of the proof of Lemma 9.38) this gives $\delta_0^\sigma = f^2 i^{-a}\delta_2$, and in the same way $\delta_2^\sigma = f^2 i^a \delta_0$. Write $\delta_t = \sum_c D_c\zeta^{ct}$ ($c$ odd modulo 8). By Lemma 9.52(b), $D_c^\sigma = F(\zeta^c)^2 D_c$, and by (e), (f), (g), $F(\zeta^c)^2 = f^2, -f^2, -f^2, f^2$ for $c = a, -a, a+4, 4-a$. The two relations become $f^2(D_{a+4}-D_{4-a})=0$ and $f^2 i^a(D_{a+4}+D_{4-a})=0$, so $D_c=0$ for $c\in\{a+4,4-a\}=\{\pm 3a\}$. The same argument for the odd entries, with $f_b=F(\zeta^b)$ and $t=1,3$ (now $\delta_1^\sigma = f_b^2 i^{-b}\delta_3$, $\delta_3^\sigma = f_b^2 i^b\delta_1$), gives $D_c\zeta^c=0$ for $c\in\{\pm 3b\}$. If $\{\pm b\}\neq\{\pm a\}$, then $\{\pm 3b\}=\{\pm a\}$, so $\delta=0$ and $\delta_0=0$, against step (4) of that proof. So $b=a$. □

At the four roots $\psi$ with $\psi^2\in\{\zeta^{\pm a}\}$ we have $K(-\psi)=\varsigma\,(-1)^k K(\psi)$ with $\varsigma = C_{32}(-\psi)/C_{32}(\psi)$, and $\varsigma=\pm1$ is the same at the four roots (as $C_{32}(v)^2 = S\,C_{16}(v^2)$ is even in $v$ and $C_{32}(1/v) = 1/C_{32}(v)$). We call $k$ *diagonal* if $\varsigma(-1)^k=1$ and a *swap index* if $\varsigma(-1)^k=-1$.

**Lemma 9.54.** *If $(-1)^k=\alpha\beta$, no couple $k-tm/32$ is special, and $k$ is diagonal, then $y$ does not exist.*

*Proof (computation).* By Lemma 9.53, $k$ has a block $\{\pm a\}$; write the even entries of $\gamma$ as $P\zeta^{as}+Q\zeta^{-as}$ and $\delta_t = R\zeta^{at}+T\zeta^{-at}$. As $k$ is diagonal, $\sigma_2$ maps each orbit of $\gamma$ to itself, and by Lemma 9.52 it multiplies $P,Q,R,T$ by roots of unity in $\mathbb{F}_{81}$. Put $A=R^2+T^2$, $A'=i(R^2-T^2)$, $B=P^4+Q^4$, $B'=i(P^4-Q^4)$, $\rho=RT$ and $g=PQ$. Eliminating $b$ by (F1), the equation (F2) at the couples $k$ and $k+m/16$ and its image under $\sigma_2$ become the four equations $\mathcal{E}(A,B)=\mathcal{V}(A,B)=0$ and $\mathcal{E}(A',B')=\mathcal{V}(A',B')=0$, where

$$\mathcal{E}(X,Y) = Y^2+(\rho-1)XY+X^4+(g+1)X^2+\rho^4+\rho^3+(g+1)\rho^2-g^2\rho+g^4,$$
$$\mathcal{V}(X,Y) = (X^2+\rho^2+\rho+g^2)\,Y-(\rho+1)X^3+(g^2+g\rho+\rho-\rho^3)\,X$$

have coefficients in $\mathbb{F}_3$. With $A^2+A'^2=\rho^2$ and $B^2+B'^2=g^4$ this gives six equations in $(A,A',B,B',\rho,g)$ that depend neither on $e$ nor on the class of the case. The ideal they generate in $\mathbb{F}_{81}[A,A',B,B',\rho,g]$ (not saturated) is zero-dimensional, with a quotient of dimension 480 over $\mathbb{F}_{81}$, and its eliminant in $A$ has degree 118 and irreducible factors over $\mathbb{F}_{81}$ of degrees $1,2,3,11$ only (two programs, Table 8: Gröbner bases by Singular and by msolve, factorizations by Singular and by FLINT; each run takes about a second). At a point $A\neq 0$ (else $R=T=0$), and $\sigma_2$ acts on $A$ with order exactly 4 ($A\mapsto\pm A'\mapsto -A$), so $[\mathbb{F}_{81}(A):\mathbb{F}_{81}] = m/128 = 2^{e-8}\geq 8$. No factor has such a degree. □

**Definition 9.55.** We call $(k,k')$ a *swap pair* with block $\{\pm a\}$ and shift $r$ if: no couple $k+tm/64$ ($t\in\mathbb{Z}$) is special; $k$ and $k'$ both have the block $\{\pm a\}$; $r$ is odd and $K(\psi)=\psi^r$ at the four roots $\psi$ with $\psi^2\in\{\zeta^{\pm a}\}$; and $\hat\delta$ and $\hat\delta'$ vanish at $\zeta^{\pm 3a}$.

**Lemma 9.56.** *Let $(-1)^k=\alpha\beta$, suppose that no couple $k-tm/32$ is special, and let $k$ be a swap index with block $\{\pm a\}$. Then $(k,k')$ is a swap pair with block $\{\pm a\}$.*

*Proof.* (1) *The shift.* By Lemma 9.52(d), (g), $K(\psi)^8 = F(\psi^2)^4 = -1$, so $K(\vartheta^a)=\vartheta^j$ with $j$ odd; put $r\equiv ja^{-1}$ (mod 16), which is odd. Then $K(\vartheta^a)=\vartheta^{ar}$, $K(-\vartheta^a)=-\vartheta^{ar}=(-\vartheta^a)^r$, and $K(\psi)K(1/\psi)=1$ gives the other two roots. (2) *$k'$ is not special.* $F_4(-\psi)/F_4(\psi) = \varsigma^{u_4}(-1)^{u_4 k} = \varsigma(-1)^k = -1$ at the four roots $\psi$ of (1). The entries $\delta_{2t}^{(4)}=\delta_t$ and $\delta_{2t+1}^{(4)}=\delta_t'$ give, for $z=\psi^2$, $\widehat{\delta^{(4)}}(\pm\psi) = \hat\delta(z)\pm\psi^{-1}\hat\delta'(z)$. Taking the even entries in Lemma 9.52(h), and as $\sigma_4$ fixes $\mathbb{F}_{81}$,

$$2\,\hat\delta(z)^{\sigma_4} = F_4(\psi)\widehat{\delta^{(4)}}(\psi)+F_4(-\psi)\widehat{\delta^{(4)}}(-\psi) = 2F_4(\psi)\,\psi^{-1}\hat\delta'(z) \qquad (z\in\{\zeta^{\pm a}\}).$$

By Lemma 9.53, $\hat\delta \neq 0$ at some $z \in \{\zeta^{\pm a}\}$, so $\delta' \neq 0$. A special couple has $c = 0$ and $a, a' \in \{\pm i\}$ (step (5) of the proof of Lemma 9.38), so $d = a - a' \in \{0, \pm i\}$ (as $a - a' = -2d$); as $d^{3^{m/32}} = -d$ (step (4)) and $i \in \mathbb{F}_9$ is fixed, $d = 0$. By step (5), the couples $k' - tm/16$ are all special or none is, and likewise the couples $k' - m/32 - tm/16$. By Lemma 9.52(b), (f), $\sigma$ acts on $\delta'$ by the odd polynomial $F^2$ (at $k'$; it equals $F^2$ at $k$, as $k' \equiv k \pmod{16}$), so it maps the even entries of $\delta'$ into the span of the odd entries; hence if one of the two sets of couples is special, $\delta' = 0$. Hence no couple of $k'$ is special. (3) *The block of $k'$.* By Lemma 9.53 at $k'$, $k'$ has a block $\{\pm a'\}$ and $\hat\delta'$ vanishes off it. If $a' \neq \pm a$, then $\hat\delta'(z) = 0$ for $z \in \{\zeta^{\pm a}\}$, so by the display $\hat\delta(z) = 0$ there, and $\delta = 0$: impossible. So $a' = \pm a$, and $K$, $F$ are the same at $k'$ as at $k$. □

**Lemma 9.57.** *Let $(k, k')$ be a swap pair with block $\{\pm a\}$ and shift $r$. Then $\gamma_t^{\sigma_2} = \gamma_{t+r}$, $\delta_t^{\sigma_2} = \delta_{t+r}$, $u_t^{\sigma_2} = u_{t+r}$ and $X_t^{\sigma_2} = X_{t+2r}$ for all $t$, the same holds for $\gamma'$, $\delta'$, $u'$ at $k'$, and $\hat X(z) = 0$ at $z = \zeta^{\pm 3a}$.*

*Proof.* As $k$ has the block $\{\pm a\}$, $\gamma_t = \vartheta^{at} H_t^+ + \vartheta^{-at} H_t^-$ for all $t$, in the notation of (20) with $b = a$, and $\delta_t = r_1\zeta^{at} + r_2\zeta^{-at}$. By Lemma 9.52(a), $h_f^{\sigma_2} = \vartheta^{rf} h_f$, and as $\vartheta^{8r} = -1$ this gives $(H_t^\pm)^{\sigma_2} = \vartheta^{\pm ar} H_{t+r}^\pm$, so $\gamma_t^{\sigma_2} = \gamma_{t+r}$. By (d), $F(\zeta^{\pm a}) = K(\vartheta^{\pm a})^2 = \zeta^{\pm ar}$, so (b) gives $r_1^{\sigma_2} = \zeta^{ar} r_1$, $r_2^{\sigma_2} = \zeta^{-ar} r_2$, and $\delta_t^{\sigma_2} = \delta_{t+r}$. Applying $x \mapsto x^{\sigma_2}$ to (20) gives $u_t^{\sigma_2}\delta_{t+r} = \zeta^{a(t+r)}(H_{t+r}^+)^2 + \zeta^{-a(t+r)}(H_{t+r}^-)^2 = u_{t+r}\delta_{t+r}$, and $\delta_{t+r} \neq 0$ by step (4) of that proof (no couple is special), so $u_t^{\sigma_2} = u_{t+r}$. The same holds for $\gamma'$, $\delta'$, $u'$ at $k'$, which has the same $K$ and $F$ (they depend on $k$ mod 16, and $k' \equiv k \pmod{16}$) and the same block. With (19) at $k$ and at $k'$ this gives $X_t^{\sigma_2} = X_{t+2r}$, so $\widehat{X^{\sigma_2}}(z) = z^{2r}\hat X(z)$. By Lemma 9.52(c), $(F(z)^2 - z^{2r})\hat X(z) = 0$. At $z = \zeta^{\pm a}$, $F(z)^2 = z^{2r}$. At $z = -\zeta^{\pm a} = \zeta^{\pm a + 4}$, which are the roots $\zeta^{\mp 3a}$, part (f) gives $F(z)^2 = -(-z)^{2r} = -z^{2r} \neq z^{2r}$; so $\hat X(z) = 0$ there. □

**Theorem 9.58.** *Let $(k, k')$ be a swap pair with block $\{\pm a\}$, and let $u$ be the grid of $k$. If $u_0 = u_2$ and $u_1 = u_3$, then the point $y$ of this subsection does not exist. This is the case if at every root $\eta$ of $v^{m/16} + 1$ with $\eta^{m/64} \in \{\zeta^a, \zeta^{-a}\}$ we have $C_{m/4}(-\eta) = -(-1)^k C_{m/4}(\eta)$; in particular, if there are $\nu = \pm 1$ and an integer $s \not\equiv k \pmod 2$ with $C_{m/4}(\eta) = \nu\,\eta^s$ at all these roots.*

*Proof.* The last statement is a case of the one before, as then $C_{m/4}(-\eta) = (-1)^s C_{m/4}(\eta)$. Step (1) shows that the sign condition gives $u_0 = u_2$ and $u_1 = u_3$; steps (2) and (3) show that these two equalities exclude $y$.

(1) *The sign condition gives $X = 0$.* As $c_x^{(m/4)} = \frac{16}{m}\sum_\eta C_{m/4}(\eta)\eta^{-x}$ and $\sum_{t<4} w^t = 0$ for $w^4 = 1$, $w \neq 1$, we have $\hat X(z) = \frac{64}{m}\sum_{\eta^{m/64} = z} C_{m/4}(\eta)\eta^{-k}$. For $z = \zeta^{\pm a}$ the set of these $\eta$ is closed under $\eta \mapsto -\eta$ (as $m/64$ is even), and $\eta \neq -\eta$, so it is a disjoint union of pairs $\{\eta, -\eta\}$; as $C_{m/4}(-\eta)(-\eta)^{-k} = -C_{m/4}(\eta)\eta^{-k}$, the sum is 0. Together with Lemma 9.57, $\hat X = 0$ at all four roots, so $X = 0$, and by (19) $u_0 = u_2$ and $u_1 = u_3$.

(2) *The couples.* From now on we assume only $u_0 = u_2$ and $u_1 = u_3$. Put $P = r_1 r_2$, $\Sigma = r_1^2 + r_2^2$, $\Delta = r_1^2 - r_2^2$, $g_0 = H_0^+ H_0^-$ and $g_1 = H_1^+ H_1^-$. In (20), $\delta_0 = r_1 + r_2$ and $\delta_2 = i^a(r_1 - r_2)$, $\zeta^{\pm 2a} = \pm i^a$ and $H_2^\pm = H_0^\pm$; so the equations for $t = 0, 2$ with $u_2 = u_0$ give $u_0 r_1 = (H_0^+)^2$ and $u_0 r_2 = (H_0^-)^2$. For $t = 1, 3$ with $u_3 = u_1$ they give $u_1 r_1 = (H_1^+)^2$ and $u_1 r_2 = (H_1^-)^2$, because the determinant $\zeta^a\zeta^{-3a} - \zeta^{-a}\zeta^{3a} = -2i^a = i^a$ is not 0. Hence $g_0^2 = u_0^2 P$ and $g_1^2 = u_1^2 P$. At the couple $t$, (F2′) of the proof of Lemma 9.38 reads $(U - D)^2 - (U + D) + (g - 1)^2 = 0$ with $U = u_t^2$, $D = \delta_t^2$ and $g = \gamma_t^2 + \gamma_{t+4}^2 = g_{t \bmod 2}$ (as $(U + D)^2 - UD = (U - D)^2$ in characteristic 3). Here $\delta_0^2 = \Sigma - P$, $\delta_2^2 = -\Sigma - P$, $\delta_1^2 = i^a\Delta - P$ and $\delta_3^2 = -i^a\Delta - P$. Subtracting the equations for $t = 0$ and $t = 2$ gives $(\delta_2^2 - \delta_0^2)(2u_0^2 - \delta_0^2 - \delta_2^2 + 1) = 0$, that is $\Sigma\,(1 - P - u_0^2) = 0$; in the same way $\Delta\,(1 - P - u_1^2) = 0$. If $\Sigma = \Delta = 0$ then $r_1 = r_2 = 0$, so $\delta_0 = 0$, which is impossible by step (4) of the proof of Lemma 9.38. Using $(g - 1)^2 = g^2 + g + 1$:

(i) If $\Sigma = 0$, then $u_1^2 = 1 - P$, $g_1^2 = P - P^2$, and the equation for $t = 1$ gives $(g_1 - 1)^2 = P + \Delta^2 = P - P^2 = g_1^2$ (as $\Delta^2 = \Sigma^2 - 4P^2$); so $g_1 = -1$, $P^2 - P + 1 = (P + 1)^2 = 0$, $P = -1$, and $r_1^4 = -1$.

(ii) If $\Delta = 0$, then in the same way, from $t = 0$, $P = -1$ and $r_1^4 = P^2 = 1$.
(iii) Otherwise $u_0^2 = u_1^2 = 1 - P$, and the equations for $t = 0$ and $t = 1$ give $g_0 = P^2 - \Sigma^2 - 1$ and $g_1 = \Sigma^2 - 1$. As $g_0^2 = g_1^2 = P - P^2$, we get $(\Sigma^2 + P^2)(P^2 + 1) = 0$. If $P^2 = -\Sigma^2$, then $P = \pm i\Sigma \neq 0$ (here $\Sigma \neq 0$), and $\Sigma^4 \mp i\Sigma + 1 = 0$. If $P^2 = -1$, then $\Sigma^4 + \Sigma^2 - P = 0$. In both cases $\Sigma$ is a root of a nonzero polynomial of degree 4 over $\mathbb{F}_9$, $P \in \mathbb{F}_9(\Sigma)$, and $r_1^2$ is a root of $T^2 - \Sigma T + P^2$.

In every case $P \neq 0$, so $r_1 \neq 0$ (as $r_1^2 r_2^2 = P^2$), and $[\mathbb{F}_9(r_1) : \mathbb{F}_9] \leq 16$, so $d = [\mathbb{F}_3(r_1) : \mathbb{F}_3] \leq 32$.

(3) *Degree.* From the proof of Lemma 9.57, $r_1^{\sigma_2} = \zeta^{ar} r_1$ with $\zeta^{ar}$ of order 8; as $\sigma_2$ fixes $\zeta$, $r_1^{\sigma_2^j} = \zeta^{jar} r_1$ for all $j$. So $r_1^{3^{m/16}} = r_1^{\sigma_2^8} = r_1$, and $d$ divides $m/16$; hence $d$ is a power of 2 with $d \leq 32$, so $d$ divides 32, which divides $m/32$. Then $r_1 = r_1^{3^{m/32}} = r_1^{\sigma_2^4} = \zeta^{4ar} r_1 = -r_1$, so $r_1 = 0$: a contradiction. □

We now turn to the fibre values $e_\rho = \frac{2}{m} \sum_\theta E(\theta)\theta^{-\rho}$ of step (2) of the proof of Lemma 9.38, where $\theta$ runs over the roots of $u^{m/2} + 1$ and $E(u)^2 = S\, C_m(u^2)$; recall $e_{\rho + m/2} = -e_\rho$ and $e_\rho^2 = x_\rho = w_{2\rho}^2 + 1$ (step (3)).

**Lemma 9.59.** *Let $k$ be an index and put $\phi_t = e_{k - tm/32}$ ($t \in \mathbb{Z}$), so that $\phi_{t+16} = -\phi_t$. For a root $y$ of $y^{16} + 1$ put $\hat{\phi}(y) = \sum_{t<16} \phi_t y^{-t}$ and $K_E(y) = (S\, C_{64}(y))^{u_2} y^{-u_2 k}$. Then $\widehat{\phi^{\sigma_2}}(y) = K_E(y)\, \hat{\phi}(y)$, $K_E(y)^2 = K(y^2)$ and $K_E(y) K_E(1/y) = 1$; and $K_E(y)^{16} = -1$ if $(-1)^k = \alpha\beta$.*

*Proof.* Put $d = m/32$. For each $\theta$, $y = \theta^d$ is a root of $y^{16} + 1$, and $E(\theta)^d = (S\, C_m(\theta^2))^{m/64} = C_m(\theta^2)^{m/64} = S\, C_{64}(y)$, by $S^{m/64} = 1$ and the identity $C_m(\eta)^{2^j} = S\, C_{m/2^j}(\eta^{2^j})$ with $2^j = m/64$. As $\sigma_2 = 1 + du_2$, $E(\theta)^{\sigma_2} = E(\theta)(S\, C_{64}(y))^{u_2}$ and $\theta^{\sigma_2} = \theta y^{u_2}$. Hence $Z(y) = \frac{2}{m} \sum_{\theta^d = y} E(\theta)\theta^{-k}$ satisfies $Z(y)^{\sigma_2} = K_E(y) Z(y)$. As $\theta^{-(k-td)} = \theta^{-k} y^t$, $\phi_t = \sum_y Z(y) y^t$, so $\hat{\phi}(y) = 16 Z(y) = Z(y)$; and $\sigma_2$ fixes $y \in \mathbb{F}_{3^8}$, which gives the first claim. The other claims follow from $C_{64}(y)^2 = S\, C_{32}(y^2)$, $C_{64}(y) C_{64}(1/y) = 1$ and Lemma 9.52(d), (g): $K_E(y)^{16} = K(y^2)^8 = F(y^4)^4 = -1$. □

**Lemma 9.60.** *Let $(k, k')$ be a swap pair with block $\{\pm a\}$ and shift $r$, let $\kappa \in \{k, k'\}$, and let $\phi$, $\hat{\phi}$ and $K_E$ be as in Lemma 9.59 for the index $\kappa$. Then there is $c \in \{\pm 1\}$ such that $\phi_t^{\sigma_2} = c\, \phi_{t+r}$ for all $t$, and $\hat{\phi}(y) = 0$ unless $K_E(y) = c\, y^r$. Every $y$ with $K_E(y) = \pm y^r$ satisfies $y^4 \in \{\zeta^a, \zeta^{-a}\}$, and the set of the $y$ with $K_E(y) = c\, y^r$ is a union of pairs $\{y, 1/y\}$.*

*Proof.* Here $r$ is the odd integer of Definition 9.55; it is also the shift in Lemma 9.57.

(1) *The copy.* Let $\gamma, \delta, u$ be the grids of $\kappa$. For $\rho = \kappa - tm/32$, $w_{2\rho} = -(w_{2\rho}^{(m/2)} + c_\rho^{(m)}) = u_t + \delta_t - \gamma_t$, so Lemma 9.57 gives $x_\rho^{\sigma_2} = x_{\rho - rm/32}$. Hence $\phi_t^{\sigma_2} = \epsilon_t \phi_{t+r}$ with $\epsilon_t \in \{\pm 1\}$ (we take $\epsilon_t = 1$ if $\phi_{t+r} = 0$), and $\epsilon_{t+16} = \epsilon_t$. Moreover $\phi \neq 0$: otherwise $x_\kappa = x_{\kappa + m/4} = 0$, so $(a_\kappa \pm c_\kappa)^2 = -1$ in the notation of step (3) of the proof of Lemma 9.38; then $c_\kappa \in \{0, \pm i\}$, and as $c_\kappa^{3^{m/16}} = -c_\kappa$ (step (2)) while $3^{m/16}$ fixes $i$, $c_\kappa = 0$, so the couple $\kappa$ would be special.

(2) *An eigenvector.* Let $V$ be the space of sequences $f$ over $\overline{\mathbb{F}}_3$ with $f_{t+16} = -f_t$. Let $K_E$ act on $V$ by multiplying $\hat{f}(y)$ by $K_E(y)$, and put $(Af)_t = \epsilon_t f_{t+r}$. The matrix of $K_E$ has entries in $\mathbb{F}_{3^8}$, which $\sigma_2$ fixes, and $A$ has entries $\pm 1$. By (1) and Lemma 9.59, $K_E \phi = \phi^{\sigma_2} = A\phi$; applying $\sigma_2$ repeatedly, $K_E \phi^{\sigma_2^j} = A\phi^{\sigma_2^j} = \phi^{\sigma_2^{j+1}}$ for all $j$. Thus on the span $U$ of the $\phi^{\sigma_2^j}$ we have $K_E = A$, and $U$ is stable under $K_E$. As $K_E$ is diagonal in the basis $(y^t)_t$ and $U \neq 0$ (a subspace stable under a diagonalisable map contains an eigenvector of it), there are $\mu$ and $f \in U$, $f \neq 0$, with $K_E f = Af = \mu f$.

(3) *A sign function.* $Af = \mu f$ reads $f_{t+r} = \mu\, \epsilon_t f_t$. As $f$ has period 32 and $t \mapsto t + r$ is transitive on $\mathbb{Z}/32$ ($r$ is odd), $f_0 = 0$ would give $f = 0$; so $f_0 \neq 0$. By Lemma 9.59 $\mu^{16} = -1$, so $\mu = y_0^r$ for a root $y_0$ of $y^{16} + 1$. Then $g_t = f_t y_0^{-t} / f_0$ satisfies $g_{t+r} = \epsilon_t g_t$, $g_{t+16} = g_t$ and $g_0 = 1$, so $g_t \in \{\pm 1\}$ for all $t$.

(4) *Frequencies.* Put $\lambda(y) = K_E(y)y^{-r}$. If $y^4 \in \{\zeta^{\pm a}\}$, then $\lambda(y)^2 = K(y^2)y^{-2r} = 1$ by Definition 9.55. Otherwise $z = y^4 \in \{\zeta^{\pm 3a}\}$, where $F(z)^2 = -z^{2r}$ (proof of Lemma 9.57), so $\lambda(y)^8 = F(z)^2 z^{-2r} = -1$ and $\lambda(y)$ has order 16. Write $g_t = \sum_\omega p_\omega \omega^t$ over the 16-th roots of unity $\omega$, which lie in $\mathbb{F}_{81}$. Then $f_t = f_0 \sum_\omega p_\omega (\omega y_0)^t$, so $K_E(\omega y_0) = \mu$, that is $\lambda(\omega y_0) = \omega^{-r}$, whenever $p_\omega \neq 0$. If $(\omega y_0)^4 \in \{\zeta^{\pm a}\}$ this gives $\omega^{2r} = 1$, so $\omega = \pm 1$; otherwise $\omega$ has order 16, $\omega^4 = \pm i$, and of the two elements $\pm i\, y_0^4$ exactly one lies outside $\{\zeta^{\pm a}\}$ (as $a + 4 \not\equiv \pm a \pmod 8$). So $p_\omega \neq 0$ only for $\omega = \pm 1$ and for the $\omega$ with $\omega^4 = \iota$, for one fixed $\iota \in \{i, -i\}$.

(5) *Conclusion.* Write $g = g' + g''$ with $g'_t = p_1 + p_{-1}(-1)^t$; then $g''_{t+4} = \iota g''_t$ and $g''_{t+8} = -g''_t$. From $g_t^2 = g_{t+8}^2 = 1$ we get $g_t'^2 + g_t''^2 = 1$, so $g''^2$ has period 2, while $g''^2_{t+4} = -g''^2_t$. Hence $g'' = 0$, and as $g_0 = 1$, either $g_t = 1$ for all $t$ or $g_t = (-1)^t$. (In particular $y_0^4 \in \{\zeta^{\pm a}\}$.) So $\epsilon_t = g_t g_{t+r}$ is a constant $c$, and $K_E\phi = A\phi$ reads $\hat\phi(y)(K_E(y) - c\, y^r) = 0$. Finally, $K_E(y) = \pm y^r$ means $\lambda(y) = \pm 1$, which by (4) forces $y^4 \in \{\zeta^{\pm a}\}$; and $\lambda(1/y) = 1/\lambda(y)$, as $K_E(1/y) = 1/K_E(y)$, so $\lambda(1/y) = \lambda(y)$ when $\lambda(y) = \pm 1$. □

For $a \in \{1, 3\}$ let $B_a$ be the set of the eight roots $y$ of $y^{16} + 1$ with $y^4 \in \{\zeta^a, \zeta^{-a}\}$; it is the union of four pairs $\{y, 1/y\}$. For $\Omega \subseteq B_a$ let $\Sigma_a(\Omega)$ be the set of points

$$P = \big(H_0^+, H_1^+, H_0^-, H_1^-,\, r_1, r_2,\, u_0, u_1, u_2, u_3,\, (z_y)_{y\in\Omega},\, s\big)$$

over $\overline{\mathbb{F}}_3$ such that, with $\gamma_t = \vartheta^{at} H_t^+ + \vartheta^{-at} H_t^-$, $H^\pm_{t+2} = H_t^\pm$, $\delta_t = r_1\zeta^{at} + r_2\zeta^{-at}$, $u_{t+4} = u_t$ and $\phi_t = \sum_{y\in\Omega} z_y y^t$, for all $t$

$$u_t\delta_t = \gamma_{t+4}^2 - \gamma_t^2, \quad \big((u_t+\delta_t)^2 + \gamma_t^2 + 1\big)^2 = (u_t+\delta_t)^2\gamma_t^2 + (u_t-\delta_t)^2\gamma_{t+4}^2, \quad \phi_t^2 = (u_t + \delta_t - \gamma_t)^2 + 1,$$

and $s\gamma_0\gamma_1\delta_0\delta_1 = 1$. Put $X_a = \Sigma_a(B_a)$, and for $P \in X_a$ put $\chi_P(v) = (u_0 - u_2) + (u_1 - u_3)v^{-1}$. For a pair $p = \{y_0, 1/y_0\} \subseteq B_a$ let $J_a(p)$ be the set of the $(P, P') \in X_a \times X_a$ with

$$\chi_{P'}(v)^2 = v\,\chi_P(v)^2 \ (v = \pm i), \qquad z'^2_{y_0} = y_0 z_{y_0}^2, \quad z'^2_{1/y_0} = y_0^{-1} z^2_{1/y_0}, \quad z'_{y_0} z'_{1/y_0} = z_{y_0} z_{1/y_0},$$

where $z$ and $z'$ are the coordinates of $P$ and $P'$. These sets are defined over $\mathbb{F}_3(\vartheta, B_a) \subseteq \mathbb{F}_{3^8}$ and do not depend on $e$. Write $\gamma_t = \sum_f h_f \vartheta^{ft}$ ($f \in \{\pm a, \pm a + 8\}$ modulo 16); thus $h_{\pm a} = -(H_0^\pm + H_1^\pm)$ and $h_{\pm a+8} = -(H_0^\pm - H_1^\pm)$, as $\frac{1}{2} = -1$. We say that $P$ has the *degrees of* $e$ if every nonzero $z_y$, $h_f$, $r_i$ has degree exactly $2^{e-3}$, $2^{e-4}$, $2^{e-5}$ over $\mathbb{F}_3$, respectively, and that $(P, P')$ has them if $P$ and $P'$ do.

**Lemma 9.61.** *Let $\Omega \subseteq B_a$, let $H_t^\pm$, $r_i$, $u_t$, $z_y$ be given with $\gamma_0\gamma_1\delta_0\delta_1 \neq 0$, and let $\gamma$, $\delta$, $\phi$ be as in the definition of $\Sigma_a(\Omega)$. (a) If $\phi_t^2 = (u_t + \delta_t - \gamma_t)^2 + 1$ for all $t$, then the first two equations of $\Sigma_a(\Omega)$ hold for all $t$. (b) At every point of $\Sigma_a(\Omega)$, $\phi \neq 0$.*

*Proof.* Put $v_t = u_t + \delta_t$ and $x_t = (v_t - \gamma_t)^2 + 1$; then $v_{t+4} = u_t - \delta_t$, $v_{t+8} = v_t$ and $\gamma_{t+8} = -\gamma_t$, so $x_t + x_{t+8} = -(v_t^2 + \gamma_t^2 + 1)$ and $x_t - x_{t+8} = -v_t\gamma_t$.

(a) Write $\phi = \phi^+ + \phi^-$, where $\phi_t^\pm$ is the sum of the $z_y y^t$ with $y^4 = \zeta^{\pm a}$. Then $\phi^\pm_{t+4} = \zeta^{\pm a}\phi_t^\pm$, and as $a$ is odd, $\zeta^{\pm 2a} = \pm i^a$; so $\phi_{t+8} = i^a(\phi_t^+ - \phi_t^-)$. Hence $\phi_t^2 + \phi_{t+8}^2 = 4\phi_t^+\phi_t^-$, which has period 4, and $\phi_t\phi_{t+8} = i^a\big((\phi_t^+)^2 - (\phi_t^-)^2\big) = (\phi^+_{t+4})^2 + (\phi^-_{t+4})^2 = -(\phi^2_{t+4} - \phi^2_{t+12})$. Now let $\phi_t^2 = x_t$ for all $t$. The first identity shows that $x_t + x_{t+8}$ has period 4, that is $v_t^2 + \gamma_t^2 = v^2_{t+4} + \gamma^2_{t+4}$, which is $u_t\delta_t = \gamma^2_{t+4} - \gamma_t^2$ (as $4 = 1$). The second gives $\phi_t\phi_{t+8} = -(x_{t+4} - x_{t+12}) = v_{t+4}\gamma_{t+4}$, so $x_t x_{t+8} = v^2_{t+4}\gamma^2_{t+4}$; as $x_t x_{t+8} = (v_t^2 + \gamma_t^2 + 1)^2 - v_t^2\gamma_t^2$ in characteristic 3, this is the second equation.

(b) If $\phi = 0$, then $x_t = x_{t+8} = 0$, so $v_t\gamma_t = 0$ and $v_t^2 + \gamma_t^2 = -1$ for every $t$; thus $\gamma_t \in \{0, \pm i\}$. As $\gamma_0 \neq 0$, $v_0 = 0$, so $v_4 = u_0 - \delta_0 = \delta_0 \neq 0$ and $\gamma_4 = i^a(H_0^+ - H_0^-) = 0$; that is, $H_0^+ = H_0^- =: h$, with $h^2 = \gamma_0^2 = -1$. Then $\gamma_2 = h(\zeta^a + \zeta^{-a}) = \pm i\, h = \pm 1$ (as $\zeta + \zeta^{-1} = i$ and $\zeta^3 + \zeta^{-3} = -i$), which is neither 0 nor $\pm i$. □

**Lemma 9.62.** *Let $(k, k')$ be a swap pair with block $\{\pm a\}$. For $\kappa \in \{k, k'\}$ let $P_\kappa$ be the point formed by the $H_t^\pm$ and $r_i$ of the grids $\gamma$, $\delta$ of $\kappa$ (as in (20) and in the proof of Lemma 9.57), by $u_0, \dots, u_3$*

*of $\kappa$, by $z_y = \hat{\phi}(y)$ ($y \in B_a$) for the grid $\phi$ of $\kappa$, and by $s = 1/(\gamma_0\gamma_1\delta_0\delta_1)$. Then $P_k, P_{k'} \in X_a$, both have the degrees of $e$, and $\chi_{P_{k'}}(v)^2 = v\,\chi_{P_k}(v)^2$ for $v = \pm i$.*

*Proof.* The couples $\kappa - tm/32$ are not special, so (F1) and (F2) of step (3) of the proof of Lemma 9.38 hold there; in the notation of that step the couple has $a = -(u_t + \delta_t)$, $a' = -(u_t - \delta_t)$, $c = \gamma_t$, $c' = -\gamma_{t+4}$, so (F1) and (F2) are the first two equations, and $c \neq 0$ and $d = \delta_t \neq 0$ (step (4)) give $\gamma_t\delta_t \neq 0$. By Lemma 9.60, $\phi_t = \sum_{y\in B_a} z_y y^t$, and $\phi_t^2 = x_{\kappa - tm/32} = (u_t + \delta_t - \gamma_t)^2 + 1$ by step (1) of its proof. Next, $\sigma_2$ multiplies $z_y$ by $cy^r$ (Lemma 9.60), $h_f$ by $K(\vartheta^f) = \vartheta^{fr}$ (Lemma 9.52(a) and Definition 9.55), and $r_1, r_2$ by $\zeta^{\pm ar}$ (proof of Lemma 9.57): by elements of $\mathbb{F}_{3^8}$ of orders 32, 16, 8. If $x \neq 0$ and $x^{\sigma_2} = \omega x$ with $\omega \in \mathbb{F}_{3^8}$ of order $N$, then $x^{\sigma_2^j} = \omega^j x$, so $x$ lies in $\mathbb{F}_{3^{N2^{e-8}}}$ (as $\sigma_2 = 3^{2^{e-8}}$) but not in $\mathbb{F}_{3^{N2^{e-9}}}$, and its degree over $\mathbb{F}_3$ is $N2^{e-8}$. Finally, by (19) at $k$ and at $k'$, $X_{2t} = u_t - u_{t+2}$ and $X_{2t+1} = u'_t - u'_{t+2}$, so $\hat{X}(z) = \chi_{P_k}(z^2) + z^{-1}\chi_{P_{k'}}(z^2)$. By Lemma 9.57 this vanishes at $z = \zeta^{\pm 3a}$, whose squares are $\pm i$; so $\chi_{P_{k'}}(z^2) = -z\,\chi_{P_k}(z^2)$ there. □

**Proposition 9.63.** *Let $(k, k')$ be a swap pair with block $\{\pm a\}$, and let $P = P_k$ and $P' = P_{k'}$ be as in Lemma 9.62. Then $\chi_P \neq 0$, and $C_{m/4}(-\eta) \neq -(-1)^k C_{m/4}(\eta)$ for some root $\eta$ of $v^{m/16} + 1$ with $\eta^{m/64} \in \{\zeta^{\pm a}\}$. Moreover $(P, P')$ is in one of the following cases, where (iii) only names what is left:*

- (i) *for pairs $p$ and $p'$ of $B_a$, the coordinates $z_y$ of $P$ vanish on $p$ and those of $P'$ vanish on $p'$; omitting them gives a point $(P, P')$ of $\Sigma_a(B_a \setminus p) \times \Sigma_a(B_a \setminus p')$ with $\chi_{P'}(v)^2 = v\,\chi_P(v)^2$ ($v = \pm i$) and the degrees of $e$;*
- (ii) *$(P, P')$ is a point of $J_a(p)$ with the degrees of $e$, for a pair $p$;*
- (iii) *neither (i) nor (ii) holds.*

*Proof.* As the point $y$ exists, Theorem 9.58 gives $\chi_P \neq 0$ (that is, $(u_0, u_1) \neq (u_2, u_3)$) and the statement about $C_{m/4}$. By Lemma 9.62, $P, P' \in X_a$ have the degrees of $e$ and satisfy $\chi_{P'}(v)^2 = v\,\chi_P(v)^2$ ($v = \pm i$). The $z_y$ enter the equations of $\Sigma_a$ only through $\phi_t$, so omitting coordinates that vanish on a pair $p$ gives a point of $\Sigma_a(B_a \setminus p)$, with the same $\chi_P$ and the same nonzero coordinates. The rest is a case distinction. □

A point at which only one of $P$, $P'$ vanishes on a pair lies in (ii) or (iii). If $P$ vanishes on no pair, then by Lemma 9.60 the set of the $y$ with $K_E(y) = cy^r$ at $k$ is all of $B_a$; the same holds for $P'$ at $k'$.

**Lemma 9.64.** *There is an index $k$ with $(-1)^k = \alpha\beta$ such that no couple $k - tm/32$ ($t \in \mathbb{Z}$) is special.*

*Proof.* By Remark 9.40 there is $k$ with $(-1)^k = \alpha\beta$ such that no couple $k - tm/16$ is special. By step (5) of the proof of Lemma 9.38, the couples $k - m/32 - tm/16$ are all special or none is. Suppose all are. A special couple has $c = 0$ and $a, a' \in \{\pm i\}$, so $d = a - a' \in \{0, \pm i\}$, and $d^{3^{m/32}} = -d$ (step (4)) gives $d = 0$; so $\delta_t = 0$ for odd $t$, and $\hat{\delta}(-z) = \hat{\delta}(z)$. By Lemma 9.52(b) applied twice ($F$ takes values in $\mathbb{F}_{81}$, which $\sigma_2$ fixes), $\widehat{\delta^\sigma}(z) = F(z)^2\hat{\delta}(z)$, which is odd in $z$ by (f). Hence $\delta^\sigma$ has no even entries, and no odd ones as $\delta_t^\sigma = 0$ for odd $t$. Hence $\delta = 0$, against $\delta_0 \neq 0$ (step (4)). □

**Theorem 9.65.** *Let $e \geq 11$ be odd and let $y \in W(n)$ lie on the locus $y_t = y_{t+m}$ ($t$ odd), with base $w$, such that $w^{(M)}$ is in case (II) of Lemma 9.31(b) for $M = m, m/2, \ldots, 16$ and $w^{(8)}$ is in case (I). Then there are $a \in \{1, 3\}$ and a swap pair $(k, k')$ with block $\{\pm a\}$, and the points $P = P_k$ and $P' = P_{k'}$ of Lemma 9.62 lie in $X_a$, have the degrees of $e$, and satisfy $\chi_P \neq 0$ and $\chi_{P'}(v)^2 = v\,\chi_P(v)^2$ ($v = \pm i$), so that Proposition 9.63 applies to them.*

*Proof.* Take $k$ as in Lemma 9.64. By Lemma 9.53 it has a block $\{\pm a\}$, where we may take $a \in \{1, 3\}$; by Lemma 9.54 it is not diagonal, so it is a swap index, and by Lemma 9.56 $(k, k')$ is a swap pair. Now apply Lemma 9.62 and Proposition 9.63. □

Case (iii) can be pushed down to finer grids. For this we use the fibre values at all levels.

**Definition 9.66.** For $1 \le i \le e-8$ put $d_i = m/2^{i+4}$ and $\tau_i = 3^{m/2^{i+6}}$. Then $\tau_i = 1 + d_i n_i$ with $n_i$ odd, $\tau_{i-1} = \tau_i^2$, $d_1 = m/32$, $\tau_1 = \sigma_2$, $n_1 = u_2$ (the odd number defined before Lemma 9.52), $d_{e-8} = 8$ and $\tau_{e-8} = 9$. Let $R_i$ be the set of the roots of $v^{2^{i+3}} + 1$, and $A_i$ the set of the $v \in R_i$ with $v^{2^{i+1}} \in \{\zeta^a, \zeta^{-a}\}$; so $A_1 = B_a$. For an index $b$ and $v \in R_i$ put

$$B_i^b(v) = S\,C_{2^{i+5}}(v)\,v^{-b}, \qquad K_i^b(v) = B_i^b(v)^{n_i}, \qquad Z_i^b(v) = \tfrac{2}{m}\textstyle\sum_{\theta^{d_i}=v} E(\theta)\,\theta^{-b},$$

where $\theta$ runs over the roots of $x^{m/2}+1$. Thus $K_1^k = K_E$ and $Z_1^k = \hat{\phi}$ in Lemma 9.59, and $e_{b-sd_i} = \sum_{v\in R_i} Z_i^b(v)\,v^s$ for all $s \in \mathbb{Z}$. We say that $(H_i)$ *holds at* $b$ if there are $c \in \{\pm 1\}$ and an odd integer $\rho$ with $K_i^b(v) = c\,v^\rho$ for every $v \in A_i$.

**Theorem 9.67.** *Let $(k,k')$ be a swap pair with block $\{\pm a\}$ such that $P = P_k$ and $P' = P_{k'}$ are in case (iii) of Proposition 9.63. Then there are $\ell$ with $3 \le \ell \le e-8$ and $y \in A_{\ell-1}$ such that, with $q = 2^{\ell-1}$ and $\kappa_g = k - g\,d_\ell$ $(0 \le g < q)$:*

(a) *each $(\kappa_g, \kappa_g - m/64)$ is a swap pair with block $\{\pm a\}$; the point $P_g = P_{\kappa_g}$ of Lemma 9.62 lies in $X_a$, has the degrees of $e$ and satisfies $\chi_{P_g} \ne 0$; and $P_0 = P$, $P_{q/2} = P'$;*

(b) *for $2 \le i \le \ell$ and $0 \le h < 2^{\ell-i}$, the grid $Y_s = c^{(m/2^i)}_{\kappa_h - sd_i}$ satisfies $\sum_{s<4} Y_s z^{-s} = 0$ at $z = \zeta^{3a}$ and at $z = \zeta^{-3a}$; and, with $u_{g+qt} = u_t(P_g)$ $(0 \le g < q,\ t \in \mathbb{Z})$, $D = 2^{\ell-i}$ and $K = 2^{i-2}$,*

$$Y_s = \textstyle\sum_{j<K}\big(u_{h+D(s+8j)} - u_{h+D(s+4+8j)}\big);$$

(c) *let $Q = q/2$, let $z_{y'}(P_g)$ denote the coordinate $z_{y'}$ of $P_g$ $(y' \in B_a)$, and for $x \in \{y, 1/y\}$ put*

$$\mathcal{A}(x) = \tfrac{1}{Q}\textstyle\sum_{j<Q} z_{x^Q}(P_{2j})\,x^{-j}, \qquad \mathcal{B}(x) = \tfrac{1}{Q}\textstyle\sum_{j<Q} z_{x^Q}(P_{2j+1})\,x^{-j};$$

*then*

$$\mathcal{B}(y)^2 = y\,\mathcal{A}(y)^2, \qquad \mathcal{B}(1/y)^2 = y^{-1}\mathcal{A}(1/y)^2, \qquad \mathcal{B}(y)\,\mathcal{B}(1/y) = \mathcal{A}(y)\,\mathcal{A}(1/y).$$

*For fixed $\ell$, $a$ and $y$, the conditions $P_g \in X_a$ $(0 \le g < q)$, (b) and (c) are polynomial equations in the coordinates of $(P_0, \dots, P_{q-1})$ with coefficients in $\mathbb{F}_{3^8}(y)$, the same for every $e$; let $E_{\ell,a,y}$ be the set that they define. If $e = 11$, then $\ell = 3$.*

*Proof.* Write $K_i = K_i^k$ and $Z_i = Z_i^k$. Since $B_i^b(v)^2 = B_{i-1}^b(v^2)$, $(H_i)$ at $b$ implies $(H_{i'})$ at $b$ for all $i' < i$; and $K_i^b(v) = K_i^k(v)\,v^{n_i(k-b)}$, so $(H_i)$ moves between indices that differ by an even number.

(1) $(H_1)$ *holds at* $k$. As (i) fails, one of $P$, $P'$, say $P_\kappa$, has a nonzero coordinate on every pair $\{y, 1/y\}$ of $B_a$. By Lemma 9.60 at $\kappa$ every such pair lies in the set where $K_E^\kappa(y) = c\,y^r$, so $(H_1)$ holds at $\kappa$, and hence at $k$ ($k - k' = m/64$ is even).

(2) *Frobenius on the fibre values.* As in the proof of Lemma 9.59, $E(\theta)^{d_i} = S\,C_{2^{i+5}}(\theta^{d_i})$; so $Z_i^b(v)^{\tau_i} = K_i^b(v)\,Z_i^b(v)$ and $Z_i^b(v)^{\tau_i^2} = K_{i-1}^b(v^2)\,Z_i^b(v)$ for every $v \in R_i$, whether or not $\tau_i$ fixes $v$.

(3) *Families and support.* Let $2 \le i \le e-8$ and suppose that $(H_{i-1})$ holds at $k$. We show by induction on $i$ that each $\kappa = k - g\,d_i$ $(0 \le g < 2^{i-1})$ has no special couple $\kappa - tm/32$ $(t \in \mathbb{Z})$ and the block $\{\pm a\}$, and that the $\hat{\delta}$ of $\kappa$ vanishes at $\zeta^{\pm 3a}$. Each $\kappa$ has the parity of $k$, as $d_i$ is even. For $i = 2$ these are $k$ and $k'$, and the claim holds as $(k,k')$ is a swap pair. Let $i \ge 3$. Then $(H_{i-2})$ holds at $k$, so, by induction, the claim holds for the $\kappa$ with $g$ even, which are those of step $d_{i-1}$. Let $\delta_s = c^{(m/2)}_{k-sd_i}$ $(s \in \mathbb{Z})$ be the $\delta$ grid of step $d_i$. Its entries $\delta_s$ with $s \equiv g \pmod{2^{i-1}}$ form the $\delta$ grid of $\kappa$. As in the proof of Lemma 9.52, $\delta_s$ is the sum of the terms $\frac{8}{m}\,C_{m/2}(\eta)\,\eta^{-k}v^s$ with $v = \eta^{d_i} \in R_{i-2}$, over the roots $\eta$ of $x^{m/8}+1$. Let $\tilde{\delta}_s$ be the sum of the terms with $v \in A_{i-2}$. The $\tilde{\delta}_s$ with $s \equiv g$ form the part of the $\delta$ grid of $\kappa$ with spectrum in $\{\zeta^{\pm a}\}$. As $C_{m/2}(\eta)^{d_i} = S\,C_{2^{i+3}}(v)$, the computation of (2) shows that $\tau_i$ multiplies $C_{m/2}(\eta)\,\eta^{-k}$ by $B_{i-2}^k(v)^{n_i}$. By $(H_{i-2})$, $B_{i-2}^k(v)^{n_{i-2}} = c_{i-2}\,v^\rho$ for all $v \in A_{i-2}$, with $c_{i-2} = \pm 1$ and $\rho$ odd. As $B_{i-2}^k(v)$ is a root of unity of 2-power order and $n_{i-2}$, $n_i$

are odd, this gives $B^k_{i-2}(v)^{n_i} = c_{i-2}\, v^{\rho''}$ on $A_{i-2}$ with $\rho''$ odd. So $\tilde\delta_s^{\tau_i} = c_{i-2}\,\tilde\delta_{\tau_i s+\rho''}$ for all $s$. The map $s \mapsto \tau_i s + \rho''$ permutes the classes modulo $2^{i+2}$, a period of $\tilde\delta$, and maps the even classes onto the odd ones. For even $s$, $\tilde\delta_s = \delta_s$, as the $\hat\delta$ of the $\kappa$ with $g$ even vanishes at $\zeta^{\pm 3a}$, and $\delta_s \neq 0$, as no couple of these $\kappa$ is special (step (4) of the proof of Lemma 9.38). So $\tilde\delta_s \neq 0$ for every odd $s$. Now let $g$ be odd. If a couple of $\kappa$ were special, the $\delta$ grid of $\kappa$ would be 0, as in step (2) of the proof of Lemma 9.56, and so would every $\tilde\delta_s$ with $s \equiv g$. Hence no couple of $\kappa$ is special. By Lemma 9.53, $\kappa$ has a block $\{\pm a_\kappa\}$ and its $\hat\delta$ vanishes at $\zeta^{\pm 3a_\kappa}$. If $a_\kappa \neq \pm a$, then $\{\pm 3a_\kappa\} = \{\pm a\}$, so this $\hat\delta$ vanishes on $\{\zeta^{\pm a}\}$, and $\tilde\delta_s = 0$ for every $s \equiv g$, which is impossible. This proves the claim. By Lemmas 9.54 and 9.56, as for $k$ in the proof of Theorem 9.65, each $(\kappa, \kappa - m/64)$ is then a swap pair with block $\{\pm a\}$. Lemma 9.60 at all these $\kappa$ and the Vandermonde matrix of the $2^{i-1}$ roots $v$ of $v^{2^{i-1}} = y'$ ($y' \in R_1$) give $Z_i = 0$ outside $A_i$.

(4) *One sign.* Under the same hypothesis there are $c_i = \pm 1$ and an odd $h_i$ with $(K_i(v) - c_i\, v^{h_i})\, Z_i(v) = 0$ for all $v \in R_i$. Indeed, let $h_i$ be an odd integer with $B^k_{i-1}(w)^{n_i} = w^{h_i}$ for all $w \in A_{i-1}$ (it exists by $(H_{i-1})$, as $w^{2^{i+2}} = -1$), and put $f(s) = \tau_i s + h_i$. As $n_{i-1} = n_i(\tau_i + 1)/2$, this gives $K_{i-1}(v^2) = v^{(\tau_i+1)h_i}$ on $A_i$. By (3) and the Vandermonde argument at its end, the grids $\gamma_s = c^{(m)}_{k-sd_i}$ and $\delta_s = c^{(m/2)}_{k-sd_i}$ of step $d_i$ have their spectra in $A_{i-1}$ and in $A_{i-2} = \{w^2 : w \in A_{i-1}\}$. By the computation of (2), $\tau_i$ multiplies their terms at $w$ and at $w^2$ ($w \in A_{i-1}$) by $B^k_{i-1}(w)^{n_i} = w^{h_i}$ and by $B^k_{i-2}(w^2)^{n_i} = B^k_{i-1}(w)^{2n_i} = (w^2)^{h_i}$. So $\gamma_s^{\tau_i} = \gamma_{f(s)}$ and $\delta_s^{\tau_i} = \delta_{f(s)}$. As no couple is special, by (3), the relation $u_t\delta_t = \gamma^2_{t+4} - \gamma^2_t$ holds at every couple. On the grids of step $d_i$ it reads $u_s\delta_s = \gamma^2_{s+2^{i+1}} - \gamma^2_s$, and with $\delta_{f(s)} \neq 0$ it gives $u_s^{\tau_i} = u_{f(s)}$, as in the proof of Lemma 9.57. Hence the time values $t_s = e_{k-sd_i}$, with $t_s^2 = (u_s + \delta_s - \gamma_s)^2 + 1$, satisfy $(t_s^{\tau_i})^2 = t^2_{f(s)}$. The map $f$ is one cycle modulo $2^{i+3}$ (as $\tau_i \equiv 1 \pmod 4$ and $h_i$ is odd); as $t$ contains the grid $\phi \neq 0$ of $k$ (step (1) of the proof of Lemma 9.60), no $t_s$ is 0. The signs $\epsilon_s$ with $t_s^{\tau_i} = \epsilon_s\, t_{f(s)}$ satisfy $\epsilon_s\epsilon_{f(s)} = 1$, by comparing the two values of $t_s^{\tau_i^2}$ given by (2), (3) and $(H_{i-1})$; so $\epsilon$, which has period $2^{i+3}$, is constant, and comparing coefficients in the basis $\big((v^{\tau_i})^s\big)_{v\in R_i}$ gives the claim. Put $\lambda(v) = K_i(v)v^{-h_i}$. Then $\lambda = \pm 1$ on $A_i$ (as $\lambda(v)^{\tau_i+1} = K_{i-1}(v^2)v^{-(\tau_i+1)h_i} = 1$ and $(\tau_i+1)/2$ is odd) and $\lambda(1/v) = \lambda(v)$, and for $w \in A_{i-1}$ with square roots $\pm v$ we call $w$ *single* if $\lambda(-v) = -\lambda(v)$, *double* if $\lambda(-v) = \lambda(v) = c_i$, and *none* if $\lambda(-v) = \lambda(v) = -c_i$. If every $w$ is double, $(H_i)$ holds at $k$.

(5) *The descent stops.* Start from $(H_1)$ and apply (4) for $i = 2, 3, \dots$. If $(H_{e-8})$ held at $k$, then, as $n_{e-8} = 1$ and $A_{e-8}$ is the set of the roots $\eta$ of $v^{m/16} + 1$ with $\eta^{m/64} \in \{\zeta^{\pm a}\}$, we would have $C_{m/4}(\eta) = S\, c\, \eta^{k+\rho}$ on this set with $k + \rho \not\equiv k \pmod 2$, which Theorem 9.58 excludes. So there is a smallest $j \leq e - 8$ such that some $w \in A_{j-1}$ is single or none, and $(H_{j-1})$ holds at $k$.

(6) *The link.* As $\theta^{d_{j-1}} = (\theta^{d_j})^2$, we have $Z^k_{j-1}(w) = Z_j(v) + Z_j(-v)$ and $Z^{k-d_j}_{j-1}(w) = v\big(Z_j(v) - Z_j(-v)\big)$. If $w$ is single, choose $v$ with $\lambda(v) = c_j$; then $Z_j(-v) = 0$, so $Z^{k-d_j}_{j-1}(w) = v\, Z^k_{j-1}(w)$, and the same at $1/w$ with $1/v$. If $w$ is none, $Z_j$ vanishes at $\pm v$ and $\pm 1/v$, and one step lower, at $x = w^2$, $Z^{k-d_{j-1}}_{j-2}(x) = -w\, Z^k_{j-2}(x)$, and the same at $1/x$. By the inverse Fourier transform over the $Q$ roots of $x'^Q = y'$, $\mathcal{A}(x') = Z^k_{\ell-1}(x')$ and $\mathcal{B}(x') = Z^{k-d_\ell}_{\ell-1}(x')$; so (c) holds with $\ell = j$, $y = w$ in the first case and with $\ell = j - 1$, $y = x$ in the second. For $j = 2$ a none makes $P$ and $P'$ vanish on $\{w, 1/w\}$, which is case (i), and a single gives $(P, P') \in J_a(\{w, 1/w\})$, which is case (ii); for $j = 3$ a none gives (c) with $\ell = 2$, case (ii) again. Hence $3 \leq \ell \leq e - 8$.

(7) *The tuple.* In both cases $(H_{\ell-1})$ holds at $k$, hence at every $\kappa_g$. Part (a) follows from (3), from Lemma 9.62 and from Proposition 9.63 at each $(\kappa_g, \kappa_g - m/64)$. For (b) with $i = 2$, $Y$ is the grid $X$ of $\kappa_h$, and $\hat Y(\zeta^{\pm 3a}) = 0$ is Lemma 9.57 at $\kappa_h$. For $i \geq 3$, the indices $\kappa_h - g\, d_i = \kappa_{h+gD}$ ($0 \leq g < 2^{i-1}$) lie in the family of (a), so the grids of step $d_i$ at the base $\kappa_h$ have their spectra as in (4), and no couple of these indices is special. Let $\rho' = h_{i-1}$ at the base $\kappa_h$ (it exists by $(H_{i-2})$ at $\kappa_h$). As $\tau_{i-1} = 1 + 2d_i n_{i-1}$, the computation of (2) shows that $\tau_{i-1}$ multiplies the term of $\gamma$

at $w \in A_{i-1}$ by $B_{i-2}^{\kappa_h}(w^2)^{n_{i-1}} = w^{2\rho'}$, and the term of $\delta$ at $w^2$ by $w^{4\rho'}$. So, as in (4), $\tau_{i-1}$ acts on the $\gamma$, $\delta$ and $u$ grids of step $d_i$ by $s \mapsto \tau_{i-1}s + 2\rho'$ with $\tau_{i-1} \equiv 1 \pmod 8$; summing $u$ over the classes modulo 8 removes the twist, so $\hat{Y}(z)^{\tau_{i-1}} = z^{2\rho'}\hat{Y}(z)$ at the roots $z$ of $z^4+1$, while the argument of Lemma 9.52(c), with $\tau_{i-1}$ in place of $\sigma_2$, gives $\hat{Y}(z)^{\tau_{i-1}} = \left(S\,C_{16}(z)\,z^{-\kappa_h}\right)^{2n_{i-1}}\hat{Y}(z)$. This is $F(z)^2\hat{Y}(z)$, as $\left(S\,C_{16}(z)\,z^{-\kappa_h}\right)^4 = -1$ (proof of Lemma 9.52(g), as $(-1)^{\kappa_h} = \alpha\beta$) and $n_{i-1} \equiv n_1 = u_2 \pmod 4$ (by the congruence $(\tau_{i'}+1)/2 \equiv 1 \pmod 4$ below). Moreover $F(z)^2 = -z^{2\rho'}$ at $z = \zeta^{\pm 3a}$ (proof of Lemma 9.57), as $\rho' \equiv r \pmod 4$. Indeed, $\rho' = h_{i-1}$ by definition, and $h_{i'-1} \equiv h_{i'} \pmod 4$ for $2 \le i' < i$, as $n_{i'-1} = n_{i'}(\tau_{i'}+1)/2$ and $(\tau_{i'}+1)/2 \equiv 1 \pmod 4$. The definition of step (4) at $i = 1$, with $B_0^k(\psi) = S\,C_{32}(\psi)\,\psi^{-k}$ at the four roots $\psi$ of Definition 9.55, allows $h_1 = r$, as $B_0^k(\psi)^{n_1} = K(\psi) = \psi^r$. Here $h_{i'}$, $K$ and $F$ are taken at the base $\kappa_h$ (with $B_{i'}^{\kappa_h}$ in place of $B_{i'}^k$), and $r$ is the shift of the swap pair $(\kappa_h, \kappa_h - m/64)$. The formula for $Y_s$ follows from the case (II) relations between the levels $m/4, \dots, m/2^i$, as for (19). □

**Question 9.68.** Let $p$ and $p'$ be pairs in $B_1$. (a) Is there an odd $e \ge 11$ such that some point $(P, P')$ of $\Sigma_1(B_1 \setminus p) \times \Sigma_1(B_1 \setminus p')$ with $\chi_P \ne 0$ and $\chi_{P'}(v)^2 = v\,\chi_P(v)^2$ ($v = \pm i$) has the degrees of $e$? (b) Is there an odd $e \ge 11$ such that $J_1(p)$ has a point $(P, P')$ with $\chi_P \ne 0$ and the degrees of $e$? (c) Does case (iii) of Proposition 9.63 occur?

The question needs only $a = 1$. The map $x \mapsto x^3$ on all coordinates (a coordinate $z_y$ moving to the index $y^3$) maps $\Sigma_1(\Omega)$ onto $\Sigma_3(\Omega^3)$, $J_1(p)$ onto $J_3(p^3)$ and the sets of (a) onto those for $a = 3$, as it maps $\vartheta$, $\zeta$, $B_1$ to $\vartheta^3$, $\zeta^3$, $B_3$ and $\{i, -i\}$ onto itself; it preserves $\chi_P \ne 0$ and all degrees. In the same way $x \mapsto x^9$, together with $H_t^{\pm} \mapsto (-1)^t H_t^{\pm}$ (as $\vartheta^9 = -\vartheta$), maps the sets for $p, p'$ onto those for $p^9, p'^9$; and since $y^9$ and $y^{81} = -y$ differ from $y^{\pm 1}$ for $y \in B_1$, the map $y \mapsto y^9$ permutes the four pairs of $B_1$ in one cycle. So, up to these maps, (b) concerns one set, and (a) four sets ($p$ fixed, $p'$ any of the four pairs).

By Theorem 9.65, if the answer to all three questions is no, then for no odd $e \ge 11$ does a point of the odd locus have a chain that first reaches case (I) at level 8. The sets in (a) and (b) are fixed algebraic sets over $\mathbb{F}_{3^8}$ (with the open condition $\chi_P \ne 0$), the same for every $e$; a point of one of them with some $z_y \ne 0$ has the degrees of $e$ for at most one $e$. We have not computed these sets. By Theorem 9.67, a point in case (iii) gives a point with the degrees of $e$ of one of the fixed algebraic sets $E_{\ell,a,y}$ with $3 \le \ell \le e - 8$; but $\ell$ may grow with $e$, so even the finiteness of every $E_{\ell,a,y}$ would not by itself bound $e$. All three questions are open. They concern only the strong form $W(2^e) = \emptyset$: by Corollary 9.20, no solution of (1) with $\sigma = 2$, and so no point that comes from a plane, lies on the odd locus.

*Remark* 9.69. If $\Sigma_1(B_1 \setminus p)$ and $J_1(p)$ are finite, then parts (a) and (b) of Question 9.68 can hold only for finitely many $e$. Part (c) is not affected. By Lemma 9.61(a), in the open set where $\gamma_0\gamma_1\delta_0\delta_1 \ne 0$ the set $\Sigma_1(B_1 \setminus p)$ is the zero set of the 16 quadrics $\phi_t^2 - (u_t + \delta_t - \gamma_t)^2 - 1$ ($t < 16$) in its 16 coordinates other than $s$; and in the open set where $\gamma_0\gamma_1\delta_0\delta_1 \ne 0$ for $P$ and for $P'$ and $\chi_P \ne 0$, the set $J_1(p)$ is the zero set of 37 quadrics in 36 coordinates. A point that is isolated in such a set is an irreducible component of the zero set of these quadrics in affine space, since a component of positive dimension through it would meet the open set in a neighbourhood of the point. We apply the refined Bézout inequality [4, Example 8.4.6] to the projective closures of the quadrics, one irreducible component of each at a time: each component of the intersection is a component of such an intersection, and the components of a quadric have degrees adding up to at most 2. Thus if $\Sigma_1(B_1 \setminus p)$ is finite it has at most $2^{16}$ points, and if $J_1(p)$ (with $\chi_P \ne 0$) is finite it has at most $2^{37}$. On the other hand, by Lemma 9.61(b) a point with the degrees of $e$ has a coordinate $z_y \ne 0$, of degree $2^{e-3}$ over $\mathbb{F}_3$ and so $2^{e-6}$ over $\mathbb{F}_{3^8}$; so the point has at least $2^{e-6}$ conjugates over $\mathbb{F}_{3^8}$, and they lie in the same set, which is defined over $\mathbb{F}_{3^8}$. Hence, if $\Sigma_1(B_1 \setminus p)$ is finite, part (a) of Question 9.68 can hold only for odd $e \le 21$, and if $J_1(p)$ is finite, part (b) only for odd $e \le 43$. We have not shown that these sets are finite.

*Remark* 9.70. We do not know whether the sets $E_{\ell,a,y}$ of Theorem 9.67 are finite; equal numbers of equations and unknowns do not decide it. Near infinity $X_a$ looks as follows. Let a curve on the closure of $X_a$ (without the coordinate $s$) have a place at which some coordinate has a pole, and let bars denote the leading coefficients at that place, with $w_t = u_t + \delta_t - \gamma_t$. The leading terms of the equations of $\Sigma_a(B_a)$ give $\bar\phi_t^2 = \bar w_t^2$, so $\bar\phi_t = \epsilon_t \bar w_t$ for a sign function $\epsilon$. The condition that $\epsilon\bar w$ has its Fourier support in $B_a$ splits according to $t$ mod 4, and for every $\epsilon$ it determines $\bar u$ and $\bar\gamma$ as linear functions of $\bar\delta$ (a case distinction on the signs of each residue class). So $\delta$ has the top pole order, and the leading coefficients lie in one of $2^{16}$ two-dimensional linear subspaces, each a graph over $(\bar r_1, \bar r_2)$. Whether such leading terms can satisfy the linear equations (b), (c) of Theorem 9.67 for all points of a tuple at once is not decided by this first-order description.

9.9. **The case $n = 32$.** At $n = 32$, $G$ acts freely on $W(32)$ by Corollary 9.43 (with Remark 9.17, that is, Lemmas 9.10 and 9.13): every finite non-empty class has a multiple of 256 points. Since $F$ commutes with $G$, $F$ permutes the $G$-orbits. If $F$ fixed an orbit, a point $y$ of it would satisfy $F(y) = g(y)$ for some $g \in G$, a system of the same kind as (1), with $g$ in place of the shift by $\sigma$. These systems are all empty, in each class $(S, f_0)$, by two independent programs (Table 8). One treats one $g$ in each of the 31 classes of $G$ under conjugation by all substitutions $t \mapsto ct + s$ with $c$ odd and $s$ any: a Gröbner basis computation for 29 of them and an exhaustive search for the other 2. (By Proposition 9.3 the odd shifts permute the classes $(S, f_0)$, and all classes are treated.) The other program is an exact search in the time domain over all 256 elements $g$ of $G$. Thus every $F$-cycle of orbits has length at least 2, and each class of $W(32)$ is empty, infinite, or has at least 512 points. Proposition 9.72 below excludes a part of $W(32)$; whether $W(32)$ is empty is open.

*Even and odd entries of the fibre.* (Not the halves of Remark 2.6.) On $W(n)$ we have $Y_m = S$, $Y_k Y_{-k} = -1$ and $Y_{2k} = S Y_k Y_{k+m}$ for odd $k$. For odd $k < m$ put $u_k = Y_k + Y_{k+m}$ and $v_k = Y_k - Y_{k+m}$. The even entries $d_{2\rho}$ are linear forms in the $u_k$ alone and the odd entries $d_{2\rho+1}$ are linear forms in the $v_k$ alone, and

$$u_{m-k} = -S\,Y_{-2k}\,u_k, \qquad v_{m-k} = -S\,Y_{-2k}\,v_k, \qquad u_k^2 - v_k^2 = S\,Y_{2k} \qquad (k \text{ odd}). \tag{22}$$

So over a fixed base $w$ (that is, fixed $Y_{2k}$) the even part $(d_{2\rho})_\rho$ lies in a space of dimension $m/4$ and has prescribed squares, and so has the odd part $(d_{2\rho+1})_\rho$; the two parts are coupled only by the $m/4$ conics $u_k^2 - v_k^2 = SY_{2k}$. The time shift $y_t \mapsto y_{t+1}$ exchanges the two parts and changes $S$ to $-S$.

**Proposition 9.71.** *No point of $W(32)$ has a base $w$ with values in $\mathbb{F}_{81}$.*

*Computation.* The base is $\mathbb{F}_{81}$-valued exactly when $Y_2, Y_6, Y_{10}, Y_{14} \in \mathbb{F}_{81}^\times$, since a primitive 16-th root of unity lies in $\mathbb{F}_{81}$. Hence each class has $80^4 = 40\,960\,000$ such bases. For every one of them, and for every choice of signs $d_r = \pm(w_r^2 + 1)^{1/2}$, two independent programs (Table 8) test whether the even part and the odd part lie in their spaces. In no class does any base pass both tests; the even test alone is passed by 136 or 216 bases, and the odd test by 216 or 136, as the time shift predicts. Both programs recover the 8 points per class of $W(8)$ and the 32 points per class of $W'(16)$ from their $\mathbb{F}_{81}$-bases, and find none for the line $y_s y_{s+8} = -1$ at $n = 16$ (that is, for $W(16)$, whose points have $f_0 = \pm i$) in the classes $S, f_0 = \pm 1$. □

**Proposition 9.72.** *No point of $W(32)$ has $u_1 v_1 = 0$.*

*Computation.* The shift $y \mapsto (y_{t+1})_t$ multiplies $Y_j$ by $\xi^{-j}$, so it sends $(u_k, v_k)$ to $(\xi^{-k} v_k, \xi^{-k} u_k)$, and $y \mapsto -y$ sends $(u_k, v_k)$ to $(-u_k, -v_k)$. Both maps preserve the condition $u_1 v_1 = 0$, and by Proposition 9.3 they map the four classes onto each other. So it suffices to treat the class $S = f_0 = 1$. We use the 16 unknowns $a_k = Y_{2k}$, $b_k = Y_{-2k}$, $u_k$ and $v_k$ for $k = 1, 3, 5, 7$. By (F3), (F4) and (22), every $Y_j$ is a polynomial in them with coefficients in $\mathbb{F}_3$. Thus $W'_{1,1}(32)$ is the zero set of the ideal $I$ over $\mathbb{F}_3$ generated by $a_k b_k - 1$, the four conics $u_k^2 - v_k^2 - a_k$, and the 15 equations of Lemma 9.2(b)

for the line. The points with $u_1 v_1 = 0$ form two pieces: $u_1 = 0$, and $u_1 \neq 0 = v_1$. On the first piece the conic gives $v_1^2 = -a_1 \neq 0$.

Two symmetries reduce the size of each piece. (i) The shift $y_t \mapsto y_{t+2}$, an element of $G$ of order $m$, multiplies $Y_j$ by $\xi^{-2j}$; so it multiplies $u_k$, $v_k$ by $\zeta^{-k}$ and $a_k$ by $\zeta^{-2k}$, with $\zeta = \xi^2$. On the first piece the cyclic group it generates acts freely, through $v_1$. On the second piece it acts freely on the double cover $r^2 = a_1$ (note $r \neq 0$, as $r^2 b_1 = 1$), through $r \mapsto \zeta^{-1} r$. We replace each piece by its quotient: $v_1^m$ (resp. $r^m$) becomes a new unknown, and every other unknown $z$, which the shift multiplies by $\zeta^{-\ell}$ for some $\ell$, is replaced by $z\, v_1^{-\ell}$ (resp. $z\, r^{-\ell}$). (ii) Every generator of $I$ is even in $(u_k)_k$ and even in $(v_k)_k$ (we checked this term by term). This reflects two elements of $G$: the map $t \mapsto (m+1)t$ fixes the base and exchanges $Y_k$ and $Y_{k+m}$ for odd $k$, so it sends $v$ to $-v$, and its composite with $t \mapsto t + m$ sends $u$ to $-u$. So on the second piece we replace $(u_k)$ by $u_1^2$ and the ratios $u_k/u_1$.

For both resulting ideals over $\mathbb{F}_3$, a Gröbner basis computation gives the unit ideal, in each of two encodings of the system; the encodings are written by two independent programs, and both are solved by the Gröbner basis engine of Singular (Table 8). On the remaining part $u_1 v_1 \neq 0$ the same computation, with the halving in $(v_k)$ as well, did not finish; whether $W(32)$ is empty is open. At $n = 16$ the same reductions applied to $W'(16)$, in all four classes, return the known 32 points per class: 8 points on the quotient of the cover, 4 after the halving in $u$, none with $v_1 = 0$, and 2 after both halvings. □

## 10. Why the standard routes stop

We explain why the known methods do not reach Question 1.1, and where the results of this paper sit among them. Let $K \subset \mathbb{Q}(\zeta_p)$ be the fixed field of $H$; it has degree $n$. For a coset $c$ of $H$ in $\mathbb{F}_p^\times$ let $\eta_c = \sum_{x \in c} \zeta_p^x$ be its Gauss period, and put $\eta := \eta_H$. The $n$ periods are conjugate, their sum is $-1$, and they form an integral basis of the ring of integers $\mathcal{O}_K$ (the trace from $\mathbb{Z}[\zeta_p]$ to $\mathcal{O}_K$ is onto, because $p$ is tamely ramified).

**Proposition 10.1.** *Let $M \geq 2$ be an integer. Then $H$ is a planar difference set if and only if $\eta\,\overline{\eta} \equiv n \pmod{M\mathcal{O}_K}$.*

*Proof.* For $x \neq 0$ let $t_x$ be the number of pairs $(h, h') \in H^2$ with $h - h' = x$. It depends only on the coset $c = xH$; write $t_c$. Then $\eta\overline{\eta} = \sum_{h,h'} \zeta_p^{h-h'} = (n+1) + \sum_c t_c\, \eta_c$, and $\sum_c t_c = n$, since the $n(n+1)$ pairs with $h \neq h'$ fall into cosets of size $n+1$. With $\sum_c \eta_c = -1$ this gives $\eta\overline{\eta} - n = \sum_c (t_c - 1)\, \eta_c$. As the $\eta_c$ are an integral basis, the congruence holds if and only if $t_c \equiv 1 \pmod{M}$ for every $c$. Then every $t_c \geq 1$ (as $t_c \geq 0$), and $\sum_c (t_c - 1) = 0$ forces $t_c = 1$ for all $c$, which is planarity. The converse is clear. □

After Kantor's reduction no group theory is left: the group is a Frobenius group of order $p(n+1)$ [12, Theorem A]. Every arithmetic route we know is of one of four kinds.

**(i) Equivalent forms.** The identities $|\eta_c|^2 = n$ for all $c$, the vanishing of the autocorrelations of the Gauss sums of order $n$, the corresponding Jacobi-sum identities, the power sums $\sum_{h \in H} (h-1)^{a(n+1)} \equiv 0 \pmod{p}$, and the point counts of Fermat curves [17, Theorem 3.1] are all equivalent to $\eta\overline{\eta} = n$. They restate the problem. The Weil bound does not help: the Fermat curve of degree $n$ has genus about $n^2/2$, so the error term, about $n^2\sqrt{p} \approx n^3$, is larger than the main term $p \approx n^2$.

**(ii) Reduction at one prime.** By Proposition 10.1, reducing $\eta\overline{\eta} = n$ modulo any $M$ loses nothing if the actual periods are kept. For a prime $\ell \neq p$ the reduction modulo $\ell\mathcal{O}_K$ is the set of the $n$ conjugate congruences modulo one prime above $\ell$, since the Galois group of $K$ acts transitively on these primes. In particular the periods modulo any prime $\ell \mid n$, for example the binary periods ($\ell = 2$), carry exactly the information of planarity and nothing beyond it (if $H$ is planar, such primes lie in $H$ [3], so they split completely in $K$); the higher $\ell$-adic digits of the periods add

nothing either. A reduction can give an obstruction only by forgetting information, as Xia does at $\ell = 3$: the Gauss sums become free unknowns in a finite field, and the result is the system (1). Its insolvability must then be proved for the system itself; Xia reports no solution for $n = 32$, and for subgroups of fixed index $N$ Xia's Gröbner computations settled $N = 26$ and 32 over prime fields [19, Theorem 3.7] and failed at $N = 38$ [19]. Xia's Theorem 3.4 needs a prime $r \nmid pn$, so it gives no system at $r = 2$ or at the primes dividing $n$.

**(iii) Multiplier tests.** Every prime divisor of $n$ is a multiplier (Hall's multiplier theorem [8]) and lies in $H$ (Feit [3]; see [17, p. 175]). The known exclusions test that differences of these known elements of $H$ are unique: $8 \mid n$ [17, p. 189], and $2q \nmid n$ (so $q \nmid n$, as $n$ is even) for an explicit list of 30 odd primes $q \leq 449$, among them every odd prime $q \leq 31$ [7]. Each test excludes fixed divisors, not all $n$. The multiplier-group argument for $n = 2^e$ [10] is discussed in the introduction.

**(iv) Fixed index.** For subgroups of small fixed index $N$ the analogous question is settled for even $N \leq 22$, and for $N = 24$ over prime fields, by Lehmer's criterion with cyclotomic numbers and by later methods [14, Theorems 2.1 and 2.5, and the paragraph after Theorem 2.5]; exact Gauss sums settle $N < 10$ [17, Theorem 5.1]. Here the index of $H$ is $n$ itself, and $n \geq 10^{14}$ (Proposition 8.4; $n \geq 2 \cdot 10^{11}$ by [17, Appendix]).

The two classical global methods for $|X|^2 = n$ in cyclotomic fields are vacuous here. Field descent [15, 13] cannot move $\eta$ to a smaller field, because for a prime modulus $p$ the descent field is $\mathbb{Q}(\zeta_p)$ itself. Self-conjugacy would need a prime $q \mid n$ with $q^j \equiv -1 \pmod{p}$; but $q \in H$ and $-1 \notin H$, since $|H| = n + 1$ is odd.

Our results stay inside route (ii) at $\ell = 3$ and locate the obstruction there. The norm-free system, in which (L2) is replaced by its consequence $R(m) = 1$ (Definition 2.3), always has solutions, for every $n \equiv 8 \pmod{24}$ and every even $\sigma$ (Theorem 4.1 and Proposition 4.3); so any proof along this route must use (L2) beyond $R(m) = 1$ (Corollary 4.2). For $\sigma = 2$ the norm equation splits, when $n = 2^e$ with $e \geq 5$ odd, into two conditions on the two components $\theta_+$, $\theta_-$ of one parameter, which stay coupled through a conic (Theorem 3.5), and for every $n$ in Xia's range, inside each fibre, into two conditions, each involving only one eigenspace of an involution of the fibre's parameters (Theorem 5.1). In the slice $y_1 = \pm i$ the norm-free equations already give arithmetic conditions (Theorem 6.2). What is missing is a uniform argument that the two norm conditions never hold together on the explicit solution set of the norm-free system. The alternative is a global argument that uses the actual periods at several primes at once (Question 11.3); by Proposition 10.1, a reduction of the actual periods modulo a single prime is equivalent to the problem itself, so it is no easier on its own.

## 11. Open questions

By Theorem 4.1 and Corollary 4.2, every remaining difficulty in Xia's system lies in the norm equation. We record the questions that our results isolate.

**Question 11.1** (Question P)**.** Let $n = 2^e$ with $e \geq 5$ odd. Is it true that $\mathrm{N}(y_0) \notin \mu_n$ for every solution of the norm-free system?

By the translation (Remark 3.3), a positive answer gives the same for $\mathrm{N}(y_1)$. Since $-1 \in \mu_n$, a positive answer implies, by Corollary 3.2 and Lemma 2.2, that there is no non-Desarguesian flag-transitive projective plane of order $2^e$; this is the case that, as explained in the introduction, appears to be open in the literature. Two facts constrain any proof.

(a) It must use that $e$ is odd. For $n = 16$ the norm $\mathrm{N}(y_0)$ lies in $\mu_{16}$ for 80 of the 320 solutions (a random element of $k_0^\times$ would give 64), and for $n = 64$ random sampling finds such solutions at about the chance rate (3 of $10^6$ samples, against 1.5 expected; Table 6). In the norm-free system $n$ enters only through the sizes of the fields and groups involved: no constant in (F1), (F3), (F4) or in $\mathrm{N}(y_0)$ depends on the parity of $e$. So a proof that uses only these laws

would also apply to $e = 4$ and $e = 6$, where the answer is no; it must use the arithmetic of the tower $\mathbb{F}_3 \subset \mathbb{F}_9 \subset \cdots \subset k_0$, for instance the factors $(3^{2^j}+1)/2$ of the odd part of $|k_0^\times|$.

(b) It must use the joint condition. For $n = 32$, $\mathrm{N}(y_0)$ is a fifth power in $k_0^\times$ for 5344 of the 26240 solutions (chance: 5248), and a 41st power for 768 (chance: 640); only the joint event $(\mathrm{N}(y_0) \in \mu_{32})$ never occurs.

A positive answer would also impose congruences on auxiliary Gauss periods. Let $p'$ be a prime with $p' \equiv 1 \pmod n$ and $(p'-1)/n$ odd, and let $\chi$ be a character of order $n$ of $\mathbb{F}_{p'}^\times$ such that $\chi(3)$ has order $n/2$ and $\chi(4) = 1$ (then 3 is a square modulo $p'$ and $p' \equiv 1 \pmod 4$, so $p' \equiv 1 \pmod 3$ by quadratic reciprocity). Put $g(\psi) := \sum_{x \in \mathbb{F}_{p'}^\times} \psi(x)\, \zeta_{p'}^x$ for a primitive $p'$-th root of unity $\zeta_{p'}$, so that $g(1) = -1$; reduce at a prime $\mathfrak{P}$ above 3, and fix $\varpi \in \mu_n$ with $\varpi^2 = \chi(3)$. Then $\widehat{y}(\varpi^a) := g(\chi^a) \bmod \mathfrak{P}$ satisfies (F1), (F3) and (F4), by the congruence $g(\chi^a)^3 \equiv \chi(3)^{-3a} g(\chi^{3a})$, the reflection law $g(\chi^a)g(\chi^{-a}) = \chi^a(-1)\, p' = (-1)^a p'$ for $a \not\equiv 0 \pmod n$ (as $(p'-1)/n$ is odd, $\chi(-1) = -1$; and $g(1)^2 = 1$), and the Hasse–Davenport product formula $g(\psi)g(\psi\chi^m) = \overline{\psi}(4)\, g(\psi^2)\, g(\chi^m)$, which with this $g$ also holds for $\psi = 1$ and $\psi = \chi^m$ (compare Remark 2.5). By Proposition 2.4 this is a solution of the norm-free system, with $y_0 = \eta \bmod \mathfrak{P}$ for the Gauss period $\eta = \sum_{x \in H'} \zeta_{p'}^x$ of the subgroup $H' = \ker \chi$ of index $n$, and $\mathrm{N}(y_0) = \eta\overline{\eta} \bmod \mathfrak{P}$ with $\overline{\eta}$ the complex conjugate, since $\chi(3^{m/2}) = -1 = \chi(-1)$ gives $3^{m/2}H' = -H'$. So a positive answer to Question 11.1 would imply that $\eta\overline{\eta} \bmod \mathfrak{P} \notin \mu_n$ for every such $p'$: a congruence for Gauss periods of index $n$ modulo the primes above 3, for which we know no mechanism. For the prime $p = n^2 + n + 1$ of a plane of order $n$, $H' = H$ and $\eta\overline{\eta} = n = -1$ in $\mathbb{F}_3$, which lies in $\mu_n$. The analogous assertion at $n = 8$ fails for $p' = 73$, the prime of $\mathrm{PG}(2, 8)$.

The question arose from the case $n = 32$, where $\mathrm{N}(y_0) \notin \mu_{32}$ for all 26240 solutions. We then tested $n = 128$ with one program: by Theorem 3.5(c) and the translation, the search reduces to 1345210 values of $\nu$, and no solution has $\mathrm{N}(y_0) \in \mu_{128}$ (Section 8.2). If the norms behaved like random elements, about 512 such solutions would be expected. As $\theta$ and $T\theta$ give the same $y_0$ (Theorem 3.5(c)), these are about 256 values of $y_0$, that is, about two classes of values of $y_0$ under Frobenius and sign, so this is evidence of a modest kind (a chance of about one in seven). Random sampling points the other way (Table 6): at $n = 64$ and at $n = 128$ (with $10^7$ samples) the components of $\mathrm{N}(y_0)$ in the factors 5, 41 and 3281 of the odd part of $|k_0^\times|$ are trivial at the chance rate within sampling error, singly and in pairs, and at $n = 64$ the full event occurs at about the chance rate. At $n = 128$ sampling cannot decide the joint event that Question 11.1 forbids: agreement with chance singly and in pairs does not determine the joint distribution, and the component in the largest factor 21523361 is out of reach of sampling.

**Question 11.2.** For $n \equiv 8 \pmod{24}$, $n > 8$, does every solution of (L1)–(L3) of (1) with $\sigma = 2$ have $y_0 = \pm i$ or $y_1 = \pm i$ (Claim C)?

By Corollary 6.4, if the answer is positive at $n$, then Xia's system with $\sigma = 2$ can have a solution at $n$ only if $n/8$ is 3511 or has a base-2 Wieferich prime factor larger than $6.7 \times 10^{15}$. Claim C holds at $n = 8, 32, 56, 80$ by computation (Section 8.1). We expect, however, that it fails for some large $n$. Write $y_j = i\omega_j$ with $\mathrm{N}(\omega_j) = 1$. For fixed $\omega_0$ the odd shifts of (L3) are $m/2$ linear conditions on $\omega_1$ over $\mathbb{F}_3$, of full rank unless $\omega_0$ lies in a proper submodule for the Frobenius (they hold identically at $\omega_0 = \pm 1$, which is why the known solutions lie in the slice), and once the even shifts hold, the last odd shift follows from the others. A random model built on these facts matches the pass rates of the odd shifts in the exhaustive searches of Section 8.1, (X′) at $n = 56$ and (X) and (X′) at $n = 80$ (up to a small, unexplained excess of near-solutions at $n = 56$), and predicts about $2/m$ classes of solutions outside the slice at each $m = n/2 \equiv 4 \pmod{12}$; the sum over $m$ diverges. Under this model the computations up to $n = 80$ come out as observed with probability about 0.8, so they are no evidence for Claim C. A proof that (1) has no solution at $\sigma = 2$ should therefore use (L2) and (L4) together; it must use (L2) beyond $R(m) = 1$ (Corollary 4.2), since the norm-free system has

solutions (Theorem 4.1). (In the slice, the norm-free equations alone already give the restrictions of Theorem 6.2.) One program points the same way: without the odd shifts of (L3), the equations (L1), (L2), (L4) and the even shifts of (L3) have only the 16 solutions of (1) at $n = 8$ (those from $\mathrm{PG}(2, 8)$ and their negatives), and none at $n = 32$ (none of 32896 pairs $(y_0, y_1)$ that pass the even shifts passes (L4)) or at $n = 56$ (none of 23363424).

**Question 11.3.** A plane of order $2^e$ gives solutions of Xia's systems for $r = 3$ and for $r = 5$ at once (Proposition 7.1), and both are reductions of the same Gauss periods. Can the two norm conditions be played against each other? Reductions at different primes alone cannot clash, by the Chinese remainder theorem; any argument must use the Gauss periods themselves, for instance through the Jacobi sums of the characters of order $n$ of $\mathbb{F}_p$.

For powers of 2, Section 9 replaces (1) by the larger variety $W(2^e)$, which forgets (L1).

**Question 11.4.** Does Conjecture 9.7 hold for every $e \geq 4$? For odd $e$ it says $W(2^e) = \emptyset$, and then no non-Desarguesian flag-transitive projective plane of order $2^e$ exists.

For odd $e$, a point of $W(2^e)$ with a non-trivial stabiliser in $G$ lies on one of two explicit loci (Lemmas 9.10 and 9.13); for $e = 5$ and $e = 7$ both loci are empty (Corollary 9.43 and Proposition 9.44). By Remark 9.19, a point with trivial stabiliser is either Frobenius-free or twisted, of one of four types; the points that come from planes are twisted, with $\iota$ the shift by $m$. The simplest case of that type asks:

**Question 11.5.** Is there, for some odd $e \geq 9$, a point of $W(2^e)$ with $F(y) = (y_{t+m})_t$? By Remark 9.18 and Lemma 9.21, there is none if every $\mathbb{F}_3$-valued solution $w$, with no zero, of the three relations in the proof of Proposition 9.23, at level $m = 2^{e-1}$ in place of 64, is of the form $\pm(J + \delta_{r_0})$; this holds for $m = 16$ by Corollary 9.29, and for $m = 64$ by two independent programs (for $e = 7$ this is the case $\sigma = 64$ of Proposition 9.23). There is also none if there is no $z \in \{\pm 1\}^m$ with $Z(x)Z(x^{-1}) = 1$ in $\mathbb{F}_3[x]/(x^m + 1)$; for $e = 3$ and $e = 5$ there is no such $z$.

The points with a non-trivial stabiliser matter only for the strong form of [19, Conjecture 5.4]: by Corollary 9.20, no point that comes from a plane of order $2^e$ ($e \geq 5$ odd) has one, so the rest of this paragraph does not concern planes. For these points, Section 9 leaves two families of chains open; Subsection 9.7 excludes all other chains for every odd $e \geq 7$. The first family, open for odd $e \geq 11$, consists of the chains that first reach case (I) of Lemma 9.31 at level 8. Question 9.39 asks whether the condition that Lemma 9.38 puts on their base can hold; for $n = 128$ and $n = 512$ it cannot, by three independent programs in each case, and for every odd $e \geq 11$ Theorem 9.65 reduces these chains to the three parts of Question 9.68. The second family, open for odd $e \geq 9$, consists of the chains that first reach case (I) at a level $M_0 \geq 32$ with $\Theta(\eta)$ a square at every root ($\Theta$ as in Lemma 9.32; for $e = 7$ these chains are excluded by Proposition 9.44). Lemma 9.45 gives one condition on them for each root of unity $\beta \neq 1$ of 2-power order at most $m/M_0$, but for $n = 512$ a computation with one program finds bases $w^{(256)}$ that meet all of them (Remark 9.51). So, at least for $n = 512$, a proof for these chains must use more of the line at $s = 2\rho$ than its sums weighted by $\beta^\rho$.

## Acknowledgments

This work was done overwhelmingly by AI models, steered by the author in a continuous critical dialogue with Google's Gemini, Anthropic's Claude and OpenAI's ChatGPT. The author takes full responsibility for the paper.

## References

1. Dario Alpern, *Factors of generalized Fermat numbers*, https://www.alpertron.com.ar/MODFERM.HTM, Web table, last updated December 16, 2022; accessed October 20, 2026.

2. François G. Dorais and Dominic Klyve, *A Wieferich prime search up to* $6.7 \times 10^{15}$, J. Integer Seq. **14** (2011), Article 11.9.2.
3. W. Feit, *Finite projective planes and a question about primes*, Proc. Amer. Math. Soc. **108** (1990), 561–564.
4. William Fulton, *Intersection theory*, second ed., Springer, New York, 1998.
5. D. Goel, *Xia's equations for the Higman–McLaughlin (1961) conjecture: exact solution counts when the norm equation is replaced by its sum*, Zenodo, 2026, https://doi.org/10.5281/zenodo.23874481.
6. B. Gordon, W. H. Mills, and L. R. Welch, *Some new difference sets*, Canad. J. Math. **14** (1962), 614–625.
7. Daniel M. Gordon, *Some restrictions on orders of abelian planar difference sets*, J. Combin. Math. Combin. Comput. **29** (1999), 241–246.
8. Marshall Hall, Jr., *Cyclic projective planes*, Duke Math. J. **14** (1947), 1079–1090.
9. D. G. Higman and J. E. McLaughlin, *Geometric ABA-groups*, Illinois J. Math. **5** (1961), 382–397.
10. C. Y. Ho and A. Pott, *Multiplier groups of planar difference sets and a theorem of Kantor*, Proc. Amer. Math. Soc. **109** (1990), 803–808.
11. Dieter Jungnickel and Klaus Vedder, *On the geometry of planar difference sets*, European J. Combin. **5** (1984), 143–148.
12. William M. Kantor, *Primitive permutation groups of odd degree, and an application to finite projective planes*, J. Algebra **106** (1987), 15–45.
13. Ka Hin Leung and Bernhard Schmidt, *The field descent method*, Des. Codes Cryptogr. **36** (2005), no. 2, 171–188.
14. Koji Momihara, Qi Wang, and Qing Xiang, *Cyclotomy, difference sets, sequences with low correlation, strongly regular graphs and related geometric substructures*, Combinatorics and Finite Fields: Difference Sets, Polynomials, Pseudorandomness and Applications (Kai-Uwe Schmidt and Arne Winterhof, eds.), Radon Ser. Comput. Appl. Math., vol. 23, De Gruyter, Berlin, 2019, arXiv:1809.03007, pp. 173–198.
15. Bernhard Schmidt, *Cyclotomic integers and finite geometry*, J. Amer. Math. Soc. **12** (1999), 929–952.
16. K. Thas, *Finite flag-transitive projective planes: a survey and some remarks*, Discrete Math. **266** (2003), 417–429.
17. Koen Thas and Don Zagier, *Finite projective planes, Fermat curves, and Gaussian periods*, J. Eur. Math. Soc. (JEMS) **10** (2008), 173–190.
18. Richard J. Turyn, *Character sums and difference sets*, Pacific J. Math. **15** (1965), no. 1, 319–346.
19. Binzhou Xia, *New necessary conditions for the existence of finite non-Desarguesian flag-transitive projective planes*, European J. Combin. **110** (2023), Paper No. 103687, cited from the preprint arXiv:1707.05486v7 (11 January 2023); section, equation and result numbers refer to that version. The first version, arXiv:1707.05486v1 (18 July 2017), has the system as (25) in Theorem 4.7 and the conjecture as Conjecture 4.8.