hexagon:2611.00915v2

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

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 σ 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. Both conjectures remain open. Every result that this paper proves has also been proved in the Lean 4 proof assistant, where Proposition 6.1 assumes Xia's Proposition 1.2.

1. Introduction

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 [4] in 1961 (see [9, p. 174]), that among the finite 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 [7, Theorem A] showed, using the classification of finite simple groups, that a finite flag-transitive plane of order n is Desarguesian, or else 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 (Thas and Zagier [9, Proposition 2.1, Theorem 2.4]) the plane is the development of the subgroup H of order $n+1$ of $\mathbb{F}_p^\times$: its lines are the translates $H + x$ with $x \in \mathbb{F}_p$. So the question is whether H can be a planar difference set, that is, whether every non-zero element of $\mathbb{F}_p$ can be written as 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 $n = 8$ it can, and the planes are $\mathrm{PG}(2,2)$ and

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.

Expanded version, with further results [2]: https://doi.org/10.5281/zenodo.23609692

The Lean proof:
https://github.com/david44hello/paper_higman-mclaughlin-1961-xia-equations/tree/v3.71

PG$(2,8)$. In a counterexample, $8 \mid n$ (Jungnickel and Vedder [6]; also Feit [1]); every divisor of n lies in H (Feit [1]; see also [9, p. 175]); $n \equiv 2 \pmod 3$ ([9, p. 189], [10, Lemma 4.1]); and $n \geq 2 \cdot 10^{11}$ ([9, Appendix]). K. Thas [8] gave an elementary proof of the divisor condition.

For the orders $n = 2^e$ the published non-existence proofs of Feit [1] and of Ho and Pott [5] use a result of Gordon, Mills and Welch [3] beyond the hypotheses under which it is proved. For Feit's argument (in the proof of [1, Theorem A]) this is pointed out by Thas and Zagier [9, Remark 1.2]. Ho and Pott state in [5, Theorem 2.2] that for every cyclic projective plane of order ℓ^k (ℓ prime) the multipliers are the powers of ℓ, and use this in the proof of their Lemma 3.1(2). Gordon, Mills and Welch [3, Theorem 5] prove this statement only for the difference sets that they construct, a class that includes the Singer difference sets. So the orders $n = 2^e$ with p prime and $n \geq 2 \cdot 10^{11}$ appear to remain open. If $p = 2^{2e} + 2^e + 1$ is prime, e is a power of 3: if $e = 3^k m$ with $m > 1$ and $3 \nmid m$, then $2^{2 \cdot 3^k} + 2^{3^k} + 1$ is a proper divisor of p. Hence $e \geq 3^8$, as $n \geq 2 \cdot 10^{11}$ and p has a prime factor below $3 \cdot 10^5$ for $e = 3^4, \ldots, 3^7$. Our results do not exclude any of these orders.

Xia [10, Theorem 1.3(b)] derived a necessary condition from the Gauss periods of H. If a counterexample of order $n > 8$ exists, then $n \equiv 8 \pmod{24}$, and for some even divisor σ of n the system (1) below, 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 σ, a norm equation (L2), an autocorrelation equation (L3) and a doubling equation (L4):

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

Xia conjectured, already in the first arXiv version of [10] (2017), that for $n > 8$ with $n \equiv 8 \pmod{24}$ the system has no solution for any even $\sigma \mid n$ [10, Conjecture 5.2]. We call (1) Xia's system and this conjecture Xia's conjecture. Xia reports that it holds for $n = 32$ [10, Section 5]. Figure 1 shows the chain of reductions from a counterexample to Xia's system, and where the results of this paper sit in it.

Our results separate what the norm equation contributes from what the other three equations force. Summing $y_s\, y_{s+n/2} = -1$ 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. As $n \equiv 2 \pmod 3$, $-n = 1$ in $\mathbb{F}_3$. We call the system (L1), (L3), $R(n/2) = 1$, (L4), for $y \in \mathbb{F}_{3^{n/\sigma}}^n$, the *norm-free system with shift* σ, and for $\sigma = 2$ simply

TABLE 1. The best results before this paper, and the new results. Here 2^a is the 2-part of n, the L_i are lengths of explicit Frobenius orbits on roots of unity, and σ_r is Xia's shift in characteristic r (Theorems A–C below).

Best result before this paper	New result
No count; Xia's heuristic compares n unknowns with $5n/2$ equations [10, Section 5]	The norm-free system, for every even divisor σ of every n with $8 \mid n$ and $3 \nmid n$, in particular every $n \equiv 8 \pmod{24}$: exactly $4 \prod_i (3^{L_i} - 1)$ solutions, always at least one (Theorem A)
No solution for $n = 32$, reported in [10, 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, 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 before Theorem B), $b = 0$ when $16 \mid n$ (Theorem B)
No count; the systems exist [10, Theorem 3.4], and Xia's shift satisfies a sign condition [10, 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 σ_r, none for a shift of the other parity (Theorem C)

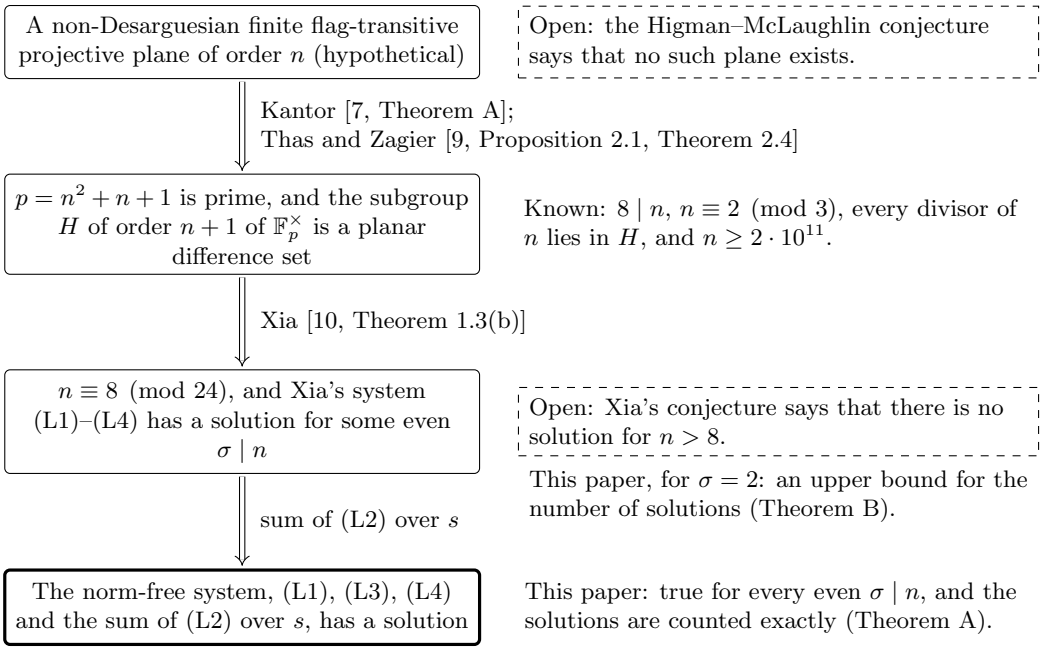


FIGURE 1. The known chain of reductions, and where the results of this paper sit. The first three boxes concern a hypothetical plane of order n; the last holds for every $n \equiv 8 \pmod{24}$ (Theorem A). Each double arrow is an implication for such a plane: the first two are proved in the cited works, 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.

the *norm-free system*. It makes sense for every even n. Every solution of Xia's system solves the norm-free system with the same σ, and for $\sigma = 2$ the solutions of Xia's system are exactly those of the norm-free system that satisfy 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 with these values form a *fibre*, and Theorem B places it in an $\mathbb{F}_3$-vector space V with an involution T whose eigenspaces are V_+ and V_-. Table 1 and Figure 2 compare our results with earlier work.

To state the results, write $n = 2^a n_{\mathrm{odd}}$ with $a \geq 3$, n_{odd} odd and $3 \nmid n$, and let μ_n be the group of n-th roots of unity in an algebraic closure of $\mathbb{F}_3$. The elements of μ_n whose order has a given 2-part form a *layer*. The map $\xi \mapsto \xi^3$ permutes the *top layer*, the layer of 2-part 2^a; its orbits there come in pairs $\{O, O^{-1}\}$ with $O \neq O^{-1}$, and for each pair $i \in I$ (I indexes the pairs) we write L_i for the common length of O and O^{-1}, so that $\sum_{i \in I} L_i = n/4$. For $y \in \mathbb{F}_{3^{n/\sigma}}^n$ put $\widehat{y}(\xi) := \sum_t y_t \xi^t$ ($\xi \in \mu_n$).

Theorem A. *Let $8 \mid n$ and $3 \nmid n$. For every even divisor σ of n, the norm-free system with shift σ (Definition 2.3) has exactly*

$$4 \prod_{i \in I} \left(3^{L_i} - 1\right)$$

solutions. In particular it always has a solution. For an odd divisor σ of n, the norm-free system with shift σ has no solution. For $n \equiv 8 \pmod{24}$ every solution of Xia's system solves the norm-free system with the same σ, so any proof that Xia's system has no solution must use the norm equation itself, beyond its consequence $R(n/2) = 1$.

Xia also conjectured that such systems have no solution "even after deleting some equations" [10, Section 1]. Without the norm equation, the system has the trivial solution $y = 0$. Theorem A

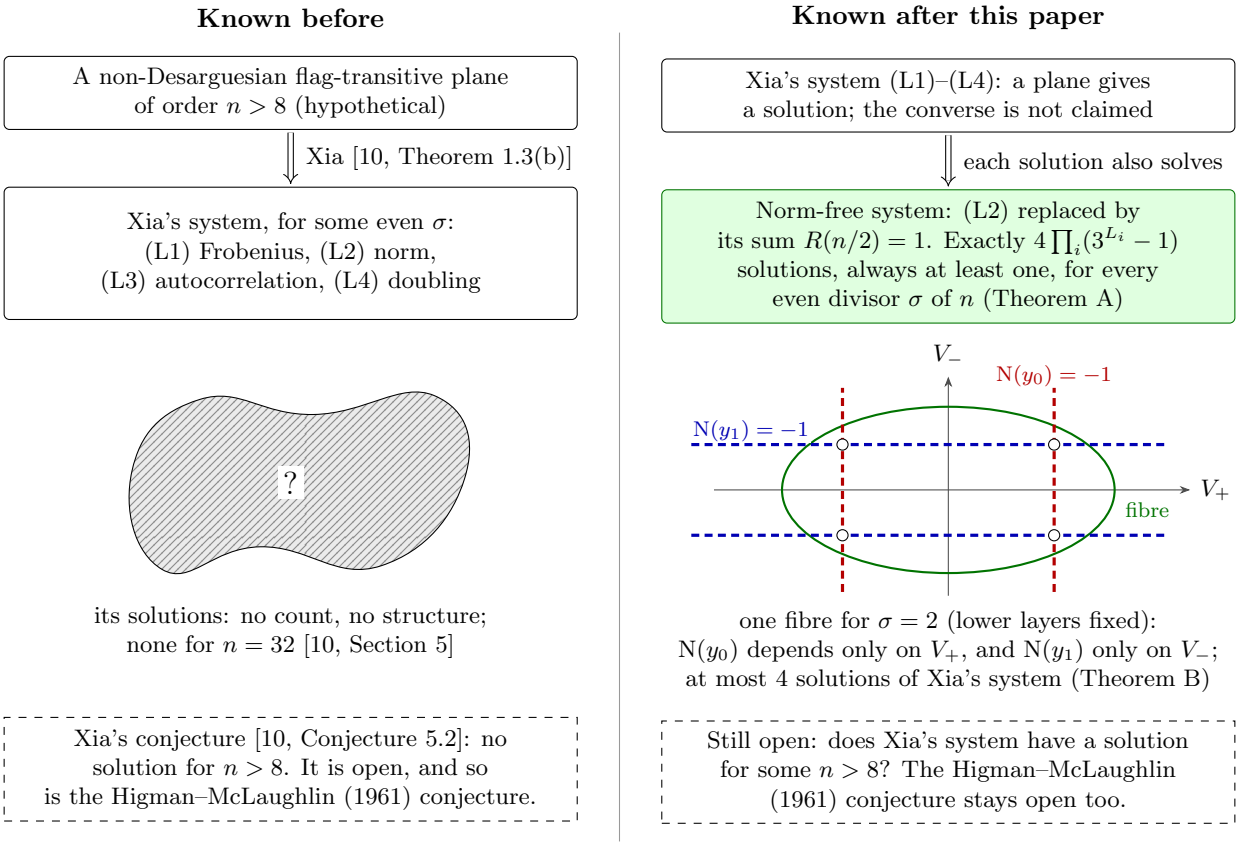


FIGURE 2. Xia's system before and after this paper. Left: a plane gives a solution of Xia's system (one-way arrow); the solutions were not classified. Right: with the norm equation replaced by its sum $R(n/2) = 1$, the solutions are counted exactly (Theorem A); for $\sigma = 2$ each of the two norm conditions depends on one eigenspace of an involution T, and each fibre contains at most 4 solutions of Xia's system (Theorem B). 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 $v \mapsto -v$.

says more: replacing the norm equation by its consequence $R(n/2) = 1$, which excludes $y = 0$, still leaves solutions. Hence Xia's statement cannot extend to deleting the norm equation, even with $y = 0$ 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).

The proof of Theorem A (Section 4, with Proposition 4.3 for $\sigma \neq 2$) works in the Fourier coordinates of Proposition 2.4, in which the equations of the norm-free system take the form of the Frobenius, reflection and product laws for Gauss sums (Remark 2.5), and it constructs every solution layer by layer (Figure 3 shows the layers for $n = 80$). The construction is not a free choice of parameters: when $n_{\mathrm{odd}} > 1$ the values of $\widehat{y}$ on the top layer (the *top data*) must be compatible with the bottom layer $\mu_{n_{\mathrm{odd}}}$. The key observation is that the quotient $\widehat{y}'/\widehat{y}$ of the Fourier transforms of two solutions satisfies homogeneous versions of these laws. Hence the set of solutions is either

empty or a *torsor* under the finite group K_n of functions that satisfy the homogeneous laws (K_n acts on it by multiplication, freely and transitively), and in the second case it has exactly $|K_n|$ elements. We compute $|K_n| = 4\prod_{i\in I}(3^{L_i}-1)$ with a surjective homomorphism from the group of homogeneous top data onto a finite group attached to the bottom layer; the same surjectivity gives top data that are compatible with the bottom layer, so the set is not empty. For $n = 2^e$ every solution is given by one parameter and two signs (Theorem 3.1).

Theorem B concerns $\sigma = 2$. Xia's proof fixes σ for each n (n/σ is the order of 3 in $\mathbb{F}_p^\times/H$), and we call it the σ of n (Section 2). It is 2 when $n = 2^e \geq 8$ with p prime (Lemma 2.2) and 10 for $n = 80$. To state the bound, note that $\xi \mapsto -\xi$ permutes the orbits of $\xi \mapsto \xi^3$ on the top layer. 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*. We write $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$ for the sets of blocks of each case and $b := |\mathcal{B}|$. In cases A and B the length L of O is even, and we put $q_O := 3^{L/2}$. Case B occurs only when $a = 3$, so $b = 0$ when $16 \mid n$ (Theorem 5.1(b)).

Theorem B. *Let $n \equiv 8 \pmod{24}$ and $\sigma = 2$. The substitution $y \mapsto y^{(u)}$, $y_t^{(u)} := y_{ut}$ with $u := 1 + n/2$, is an involution of the solution set of the norm-free system. Fix the values of $\widehat{y}$ on $\mu_{n/2}$, the lower layers (all of μ_n except the top layer); the solutions with these values form a* fibre. *Its points are given by top data in an explicit $\mathbb{F}_3$-vector space V attached to the fibre. This space is the direct sum of the block parameter spaces of Section 5. The substitution acts on the points of the fibre as an $\mathbb{F}_3$-linear involution T of V with eigenspaces V_+ and V_- (Theorem 5.1(c),(d)). For $n = 2^e$ with $e \geq 5$, the space V is $\{x \in \mathbb{F}_{3^{n/2}} : x^{3^{n/4}} = -x\}$, a point of the fibre is given by $x = \widehat{y}(\xi_0)$ for a fixed ξ_0 of order n, and $T(x) = \xi_0^{n/4} x^{3^{n/8}}$ (Theorem 3.4). On each fibre, y_0 is an injective function of the V_+-component alone and y_1 an injective function of the V_--component alone, so the condition $\mathrm{N}(y_0) = -1$ involves only V_+ and $\mathrm{N}(y_1) = -1$ only V_-. Each fibre contains at most 4 solutions of Xia's system, and Xia's system has at most*

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

solutions, where the products run over the blocks of each case and L is the length of an orbit in the block (Section 5). For $n = 2^e$ with $e \geq 5$ odd this bound is $16(3^{n/8} - 1)$, compared with the $4(3^{n/4} - 1)$ solutions of the norm-free system.

Theorem B is Theorem 5.1 with Corollary 5.2; for $n = 2^e$ with $e \geq 5$ it is Theorem 3.4 with Corollary 3.5. It bears on a counterexample of order n only when the σ of n is 2. The bound of 4 solutions per fibre is elementary. In $y_t = n^{-1}\sum_{\xi\in\mu_n}\widehat{y}(\xi)\xi^{-t}$, we call the sum over the lower layers the *lower-layer part* of y_t and the sum over the top layer its *top-layer part* (Remark 2.6). On a fibre the lower-layer parts of y_0 and y_1 are constant, and $\mathrm{N}(y_j)$ is the square of the lower-layer part of y_j minus the square of its top-layer part, so each norm condition determines one top-layer part up to sign. By (L1), y is a function of (y_0, y_1). The work lies in counting the fibres: their number is the count of Theorem A divided by the size of a fibre (Theorem 5.1(c)).

The split $V = V_+ \oplus V_-$ comes from the substitution $y \mapsto y^{(u)}$ of Theorem B. Once a fibre is fixed, the proof extends the top data $\mathbb{F}_3$-linearly from the fibre to all of V (the *formal top function* of Section 5). On the formal top function, T acts by composition with the map $\xi \mapsto -\xi$ of the top layer, and at the points of the fibre it is the substitution itself, which preserves y_0 and replaces y_1 by its conjugate $\overline{y_1} = y_{1+n/2}$. The top-layer part of y_0, a plain sum over the top layer, is fixed by T, while that of y_1, which carries the factor ξ^{-1}, changes sign. So the first vanishes on V_-, where $T = -1$, and the second on V_+, where $T = 1$. Together the two parts determine the point of V: by (L1), which the formal top function also satisfies in Fourier form (Section 5), they determine the whole top-layer part of y, and Fourier inversion turns this into the top data, which give the point. Hence the top-layer part of y_0 alone determines the V_+-component, and that of y_1 the V_--component, which is the injectivity in Theorem B. So the condition $\mathrm{N}(y_0) = -1$ determines the

V_+-component of a point of the fibre up to sign, and $\mathrm{N}(y_1) = -1$ determines its V_--component up to sign.

For $n = 2^e$ with $e \geq 5$ odd the two conditions are not independent: the points of a fibre form a conic in V (Theorem 3.4(c)), not a product of a subset of V_+ and a subset of V_-, so the V_+- and V_--components allowed by the two conditions need not combine to a point of the fibre. For other n, Theorem 5.1(c) describes the points of a fibre block by block (Table 4 lists the blocks for the five smallest $n \equiv 8 \pmod{24}$). For every $n \equiv 8 \pmod{24}$ 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 also derived systems in every characteristic $r \nmid pn$ [10, Theorem 3.4]. They have the same shape as (1) because $2 \in H$ [10, Lemma 4.1]. In these systems, (L1) becomes $y_{s+\sigma_r} = y_s^r$, with a shift σ_r in place of σ, and (L2), (L3) read $y_s y_{s+n/2} = n^3$ and $\sum_t y_t y_{s+t} = n(1-p)$. Here Xia's shift σ_r is defined by $\chi_r(r) = \varpi_r^{\sigma_r}$ for an r-adic multiplicative character χ_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 ϖ_r. For $r = 3$, with ϖ_3 chosen so that $\sigma_3 \mid n$ (as in Section 2), it is the σ of n. The character $\chi_r^{n/2}$ is the quadratic character of $\mathbb{F}_p$, so $(-1)^{\sigma_r} = \chi_r(r)^{n/2} = (r/p)$. Since $4 \mid n$, we have $p \equiv 1 \pmod 4$, and r is odd as $r \nmid n$, so $(r/p) = (p/r)$ by quadratic reciprocity. Hence σ_r satisfies the *sign condition* $(-1)^{\sigma_r} = (p/r)$, which is [10, Lemma 3.5] in our setting. This argument needs only that p is prime, not that a counterexample exists. In the *norm-free system in characteristic* r, (L2) is again replaced by its sum, $R(n/2) = n^4$; (L4) is unchanged, and the unknowns lie in $\mathbb{F}_{r^{n/g}}$ with $g = \gcd(\sigma_r, n)$.

Theorem C. *Let $8 \mid n$ (here $3 \mid n$ is allowed), let 2^a be the 2-part of n, and let r be a prime with $r \nmid pn$ and $r \not\equiv -1 \pmod{2^a}$. Let σ_r be any integer (Xia's shift is one choice), and let L_i be the common length of O and O^{-1} for the i-th pair $\{O, O^{-1}\}$ of orbits of $\xi \mapsto \xi^r$ on the elements of μ_n (in an algebraic closure of $\mathbb{F}_r$) whose order is divisible by 2^a. If $(-1)^{\sigma_r} \neq (p/r)$, the norm-free system in characteristic r (Section 6.4) has no solution; if $(-1)^{\sigma_r} = (p/r)$, it has exactly $4\prod_i (r^{L_i} - 1)$ solutions.*

Theorem C is Theorem 6.4. Its proof follows that of Theorem A with 3 replaced by r; the new point is where the sign condition enters. Here $S := \widehat{y}(-1)$ satisfies $S^2 = \kappa := n^2 p$, and at the first step down from the top layer the Frobenius law picks up the factor $(-1)^{\sigma_r} S^{r-1}$, which is $(-1)^{\sigma_r}(p/r)$ by Euler's criterion ($S^{r-1} = \kappa^{(r-1)/2}$). Thus the descent (the construction from the top layer down) closes exactly when $(-1)^{\sigma_r} = (p/r)$; otherwise the forced values contradict the reflection law. Xia's own shift σ_r always satisfies the sign condition, so the case without solutions concerns only other shifts. Hence, for $r \not\equiv -1 \pmod{2^a}$, and for every r when $n = 2^a$, no argument that uses one of these systems without its norm equation can exclude a counterexample (Corollary 6.5). What is new in Theorem C is the exact count and the sufficiency of the sign condition for the norm-free system, not the systems or the sign condition themselves.

The proofs use the discrete Fourier transform on μ_n, finite group theory and linear algebra over finite fields. Section 2 recalls Xia's system and puts it in Fourier form. Section 3 treats $n = 2^e$, and Sections 4 and 5 prove Theorems A and B. Section 6 first treats $r = 5$ for $n = 2^e$, where one norm condition on y_0 remains (Corollary 6.3), and then proves Theorem C. An expanded version of this paper, with further results, is posted on Zenodo [2].

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 [10, 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 σ dividing n and $y_0, \dots, y_{n-1} \in \mathbb{F}_{3^{n/\sigma}}$ such that (1) of the introduction holds.*

The system (1) is the system (12) in [10, Conjecture 5.2]. In (L4) the factor $y_s + y_{s+n/2}$ multiplies the whole alternating sum. The integer σ comes from the proof of Theorem 1.3 in [10]: if χ 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 ϖ in $\mathbb{C}_3$ and a positive divisor σ of n. Here $\mathbb{C}_3$ is the completion of an algebraic closure of $\mathbb{Q}_3$. This σ is determined by n (see the proof of Lemma 2.2), and we call it the *σ of n*. By Theorem 2.1 and its proof in [10], to exclude the planes of order n it suffices to prove that (1) has no solution for this n and the σ 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 σ 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 ϖ primitive and $\sigma \mid n$ with $\chi(3) = \varpi^\sigma$ [10, proof of Theorem 1.3], so ϖ^σ has order n/σ, and $\sigma = \gcd(c,n)$. As $H = \ker\chi$, n/σ 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_{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 σ of n is 2 (Lemma 2.2). For $n_{\mathrm{odd}} > 1$ the σ 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 σ for every even divisor σ 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 σ be a divisor of n. The *norm-free system with shift* σ 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 μ_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 μ_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 μ_n, then cubing the inversion formula and using that $\xi \mapsto \xi^3$ permutes μ_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 μ_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 $0 \leq s < m$; for $s \geq m$ 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 μ_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 [10, Lemma 2.1]). This is expected: in Xia's proof the y_s are reductions of the sums g_s of [10, (1)], which are n times Gauss periods [10, §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 μ_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 μ_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. Theorem B fixes the first and studies the second.

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 σ of n is 2 (Lemma 2.2), so that Theorem B 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 θ 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 μ_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 μ_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 θ 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 η of order 2^j write $\eta = \xi^2$ with ξ 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 η: 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 ξ 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 [10, Lemma 2.1(b)]).

Step 4 (bottom). The elements of order 4 of μ_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 ι, 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 θ 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.

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 θ_+, θ_- of the parameter (Theorem 3.4(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 $Q = q^2$, ι 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 θ 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 θ 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 3.4. For $\nu \in k_0$ with $\nu^{q-1} = -1$ define the $\mathbb{F}_3$-linear maps $F \to F$ below; by Theorem 3.4(b) they give the top-layer parts y_0^-, y_1^- of y_0, y_1 in terms of the parameter θ:

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

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

Theorem 3.4. *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* ν*, 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* $\nu^{q-1} = -1$*,* Λ_ν *is injective on* V_+ *and* Λ'_ν *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 θ_+, θ_- of the parameter:

Corollary 3.5. *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* ν *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* θ_+*, the second only* θ_-*.*

(ii) *Above each triple* $(\nu, S, \widehat{y}(1))$*, that is, in each fibre of Theorem B, 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 3.4. (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 ξ^{-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 ν 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 μ_m (Remark 2.6). Every element η of order m is ρ^2 with $\rho = \xi_0^{\pm 3^k}$, and by (2) $-\rho = \rho^{1+n/2} = \rho^q$ lies in the same orbit as ρ. 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 μ_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 ν. 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 Λ_ν is injective on V_+; for $x \in V_-$ it is $(0, \Lambda'_\nu(-x))$, so Λ'_ν 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 3.5. (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 3.4(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 3.4(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 Λ_ν is injective and $\mathbb{F}_3$-linear on V_+ (Theorem 3.4(d)), θ_+ is one of two values $\pm x_0$. Likewise $\mathrm{N}(y_1) = -1$ fixes θ_- 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 ν, 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 ν (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 3.6. (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. (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 3.4 the two components remain coupled through ν, which enters y_0^+, y_1^+, Λ_ν, Λ'_ν and the conic.

4. The norm-free system for general n

This section proves Theorem A (Theorem 4.1 and Proposition 4.3). Here $n = 2^a n_{\mathrm{odd}}$ with $a \geq 3$, n_{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, μ_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 $\alpha \in \mu_{n_{\mathrm{odd}}}$; ξ 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 Ξ_a be the set of the 2^{a-1} elements of order 2^a of μ_{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's heuristic [10, 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 λ 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 $\lambda(\xi)^{3^{\mathrm{ord}_n(3)}-1} = 1$.

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.

TABLE 2. The layers of μ_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^τ, 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^τ-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

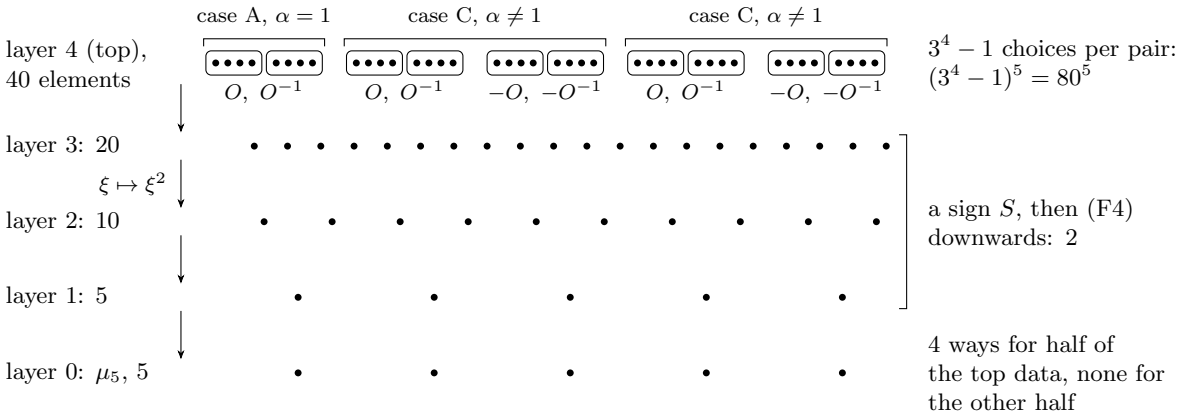


FIGURE 3. The layers of μ_n for $n = 80$ (Remark 4.4: $a = 4$, $n_{\mathrm{odd}} = 5$). An element $\xi = \zeta\alpha$ lies in layer j when ζ has order 2^j. The top layer has 40 elements and splits into ten orbits of $\xi \mapsto \xi^3$, each of length 4, in five inverse pairs $\{O, O^{-1}\}$. The pair 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 $4 \cdot 80^5$.

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 $1 \le j(\xi) \le a-1$ both square roots $\pm\eta$ of ξ lie in layer $j+1$, and (F4) at η defines $\widehat{y}(\xi) := S\,\widehat{y}(\eta)\widehat{y}(-\eta)$. By induction,

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

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 ζ with ζ^{-1}, we get from (F3)

$\prod_{\zeta\in\Xi_a}\widehat{y}(\zeta)=\prod_{\{\zeta,\zeta^{-1}\}}\zeta^m=(-1)^{2^{a-2}}=1$ ($\zeta^m=(-1)^{n_{\mathrm{odd}}}=-1$; $a\ge 3$). 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 α 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 $f(1)=\pm1$, 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 $P(\alpha^3)=\alpha^6P(\alpha)^3$ 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 τ 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 $P(\alpha^3)=\alpha^6P(\alpha)^3$, $P(\alpha)P(\alpha^{-1})=\alpha^m$; 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 $f=f_0g$ 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^τ-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 $\langle3\rangle$ of length ℓ choose $f(\alpha)$ with $f(\alpha)^{3^\ell-1}=\alpha^{-2\ell3^\ell}$ 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 α; $3\nmid 3^h+1$). 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 ℓ be the length of its $\langle3\rangle$-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 β_0 (that is, with odd part β_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 β_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 β_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 β_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 $O^{-1}\ne O$ by Step 1. So $\widetilde{P}_\lambda(\beta_0)=s^{1-3^h}$, which runs over μ_{3^h+1}. This is again the set of values at β_0 of the $g\in G$, since every $g\in G$ satisfies $g(\beta_0)^{-1}=g(\beta_0)^{3^h}$. For such λ, $\widetilde{P}_\lambda$ is 1 off the orbit of β_0 and its inverse, and $g\in G$ is determined by its values at one β_0 in each $\langle3,-1\rangle$-orbit; as Π is a homomorphism, its image contains a generating set of G, so Π is onto.

Step 7 (count). Consider first the homogeneous laws; here S stands for $\lambda(-1)=\pm1$. 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 λ 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 Π is onto, the number of λ 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 σ)**.** *Let σ be a divisor of n. If σ is even, the norm-free system with shift σ (Definition 2.3) has exactly $4\prod_{i\in I}(3^{L_i}-1)$ solutions. If σ 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 σ, so K_n and Steps 1, 6 and 7 are unchanged; we check that the other steps still close for even σ. 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 σ 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 σ, (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.

5. The two norm conditions for general n

This section proves Theorem B. 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_{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 *ν-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 ν-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 ν-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 3.4, 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 Φ 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	ν-datum	T	Factor in Φ	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_{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 μ_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 ν-datum (in case B, preserves xx'), and is the action of $y \mapsto y^{(u)}$. The values of $\widehat{y}$ on μ_m depend only on the ν-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 ν-data. Call the set of solutions of the norm-free system with given ν-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 ν-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 $y_1^- = \mathcal{Y}_1(v_-)$.*

These fibres are those of Theorem B: a fibre is the set of solutions with given values of $\widehat{y}$ on μ_m, since by (c) these values are fixed by the ν-data, S and f; conversely they give $S = \widehat{y}(-1)$, f, and the ν-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*

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

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 $e \geq 5$ odd it is the bound $16(q - 1)$ of Corollary 3.5. 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 $n \geq 2 \cdot 10^{11}$. For $n = 80$ the σ 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 ξ on μ_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 $a \geq 4$, 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 ρ_O would have order 4, while its order is a multiple of $2^a \geq 8$. 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 ξ in layer $a-1$ is ρ^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 ν-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 ρ, so P is a product of values $\widehat{y}(\rho)\widehat{y}(-\rho)$, a function of the ν-data. Hence, for ν-data, S and f that occur, all top data with these ν-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* 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) 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 ϕ^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 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 ε that differ by $2k3^k(1+q_O)$; so the two values

agree by (6). On O^{-1}: $\operatorname{top}_{Tv}(\rho_O^{-3^k}) = -\rho_O^{-2k3^k}(t_0^{-1}x/\delta_O)^{3^k}$, while $-\rho_O^{-3^k} = \rho_O^{3^{g+k}} \in O$ gives $\operatorname{top}_v(-\rho_O^{-3^k}) = \rho_O^{2(g+k)3^{g+k}} t_0^{3^{g+k}} x^{3^k}$ (as $x \in \mathbb{F}_{q_O}$); with $\delta_O^{-3^k} = -\rho_O^{Lq_O3^k} t_0^{3^k+3^{g+k}}$ both are $\rho_O^{\varepsilon'} t_0^{3^{g+k}} x^{3^k}$, and again the exponents ε' differ by $2k3^k(1+q_O)$, so the two values agree.

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

Separation. By (P2), $\mathcal{Y}_0(Tv) = \mathcal{Y}_0(v)$ and $\mathcal{Y}_1(Tv) = n^{-1}\sum_\xi \operatorname{top}_v(-\xi)\xi^{-1} = -\mathcal{Y}_1(v)$. 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 $\operatorname{top}_v = 0$ (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 μ_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 $L \ge 2$. □

6. 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 (7) below (Proposition 6.1), so the solvability of (7) 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 6.3). The Fourier form for $r = 5$ carries over to every prime r. For $8 \mid n$, Section 6.4 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 $r \nmid pn$.

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

Proposition 6.1. *Let $n = 2^e$ with $e \ge 3$ 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 $s = 0, \dots, n/2 - 1$:*

$$\begin{aligned} &(L1_5)\quad y_{s+1} = y_s^5, \qquad (L2_5)\quad y_s\, y_{s+n/2} = n^3, \qquad (L3_5)\quad \textstyle\sum_t y_t\, y_{s+t} = n(1-p),\\ &(L4_5)\quad \textstyle\sum_t (-1)^t y_t\, y_{2s-t} = \big(y_s + y_{s+n/2}\big)S, \qquad S := \sum_t (-1)^t y_t. \end{aligned} \tag{7}$$

Proof. By [10, Proposition 1.2], p is prime and H is a $(p, n+1, 1)$ difference set, that is, an nth-cyclotomic difference set in the sense of [10]. 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 χ_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 [10, 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 σ_5 is odd for every choice of ϖ_5 ([10, Lemma 3.5] holds for every primitive ϖ_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 $2 \in H$ [10, 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 [9, p. 175]). Apply [10, 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 (7), 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 $R(-s) = R(s)$, ($\mathrm{L3}_5$) gives $R(s) = n(1-p)$ for $s \not\equiv m$, and ($\mathrm{L2}_5$) gives $R(m) = n \cdot n^3 = n^4$. The *norm-free system in characteristic* 5 is ($\mathrm{L1}_5$), ($\mathrm{L3}_5$), $R(m) = n^4$, ($\mathrm{L4}_5$) 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 $\kappa^2 = p^2 = -1$.

6.2. **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

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

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

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

Theorem 6.2. *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 μ_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 $(\mathbb{Z}/2^e)^\times = \{\pm 1\} \times \langle 5 \rangle$ 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 μ_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 θ' 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, $j = e - 1, \ldots, 1$). 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 ξ 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 (L4$_5$) requires. (F4$_5$) at ± 1 is an identity; (F3$_5$) at 1 gives $\widehat{y}(1) = \pm n$, and at -1 it gives $S^2 = \kappa$; (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 (F1$_5$) and (F3$_5$), each layer of Step 3 by (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 ι_5) and Step 3, where $S^4 = -1$ is equivalent to $p^2 \equiv -1 \pmod 5$, the same fact that makes σ_5 odd in Proposition 6.1. The proof uses only that $p \equiv \pm 2 \pmod 5$ and $n = 2^e \geq 8$.

Corollary 6.3. *A sequence $y \in \mathbb{F}_{5^n}^n$ satisfies* (7) *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. (L1$_5$) gives $y_{n/2} = y_0^{5^{n/2}}$, so (L2$_5$) at $s = 0$ is $\mathrm{N}_5(y_0) = n^3$. If (7) holds, (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 (L2$_5$) holds at $s = 0$, and applying (L1$_5$) gives it for every s, as $n^3 \in \mathbb{F}_5$. □

So for $r = 5$, deciding whether (7) has a solution comes down to one norm condition on y_0, compared with two conditions for $r = 3$ (Section 2).

6.4. **The norm-free system in characteristic r.** Let $n = 2^a n_{\mathrm{odd}}$ with $a \geq 3$ and n_{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 6.4 below, n, p and the integer σ_r are parameters: no plane is assumed. If a non-Desarguesian flag-transitive plane of order n exists, let χ_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 ϖ_r. Then [10, Theorem 3.4(b)] with $\chi_r(2) = 1$ gives, exactly as in the proof of Proposition 6.1, elements $y_0, \ldots, y_{n-1}$ 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 (7). As for $r = 5$, (L2$_r$) gives $R(m) = n^4$. For any integer σ_r and $g = \gcd(\sigma_r, n)$, the *norm-free system in characteristic r* is (L1$_r$), (L3$_r$), $R(m) = n^4$, (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 (F1$_r$) $\widehat{y}(\xi^r) = \xi^{r\sigma_r}\widehat{y}(\xi)^r$, (F3$_r$) $\widehat{y}(\xi)\widehat{y}(\xi^{-1}) = \kappa\xi^m$ ($\xi \neq 1$), $\widehat{y}(1)^2 = n^2$, and (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 σ_r). (F3$_r$) at -1 gives $S^2 = \kappa$.

Theorem 6.4. *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 σ_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 σ_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 σ); 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 6.2.

Corollary 6.5. *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 σ_r satisfies $(-1)^{\sigma_r} = \big((-1)^{n/2}p/r\big) = (p/r)$ by* [10, Lemma 3.5]. *The argument before Theorem C shows that this needs only that p is prime. Thus the sign condition of Theorem 6.4(ii) and of Proposition 6.6 holds. Hence the norm-free system in characteristic r is solvable for every $r \not\equiv -1 \pmod{2^a}$, and, by Proposition 6.6, 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 6.4. 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, (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; (F3$_r$) defines $\widehat{y}$ on O^{-1}, and (F1$_r$) holds there as $\kappa^r = \kappa$.

Step 3. For ξ 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, (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 (F3$_r$). This proves (i). (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 $\prod_{\zeta \in \Xi_a} \widehat{y}(\zeta) = (-\kappa)^{2^{a-2}} = S^{2^{a-1}}$; (F1$_r$) at -1 is again $(-1)^{\sigma_r} S^{r-1} = 1$, which is, in Fourier form, the argument by which Xia proves [10, 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; κ 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 σ_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 6.6 ($r \equiv -1 \pmod{2^a}$)**.** *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 σ_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 ρ and (F3$_r$) give $\widehat{y}(\rho)^{1+r} = \kappa\rho^{m-r\sigma_r}$, with $r+1$ roots, and (F1$_r$) at ρ^{-1} (the wrap) follows as $\rho^{m(r-1)} = 1$. Step 3 of the proof of Theorem 6.4 does not use Step 1, so the first claim follows as in that proof. In the second case layers $a-1, \ldots, 1$ 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 $n_{\text{odd}} > 1$ we make no claim.

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. W. Feit, *Finite projective planes and a question about primes*, Proc. Amer. Math. Soc. **108** (1990), 561–564.
2. D. Goel, *Xia's equations for the Higman–McLaughlin (1961) conjecture: exact solution counts when the norm equation is replaced by its sum, and other miscellanea*, Zenodo, 2026, https://doi.org/10.5281/zenodo.23609692.
3. B. Gordon, W. H. Mills, and L. R. Welch, *Some new difference sets*, Canad. J. Math. **14** (1962), 614–625.
4. D. G. Higman and J. E. McLaughlin, *Geometric ABA-groups*, Illinois J. Math. **5** (1961), 382–397.
5. 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.

6. D. Jungnickel and K. Vedder, *On the geometry of planar difference sets*, European J. Combin. **5** (1984), 143–148.
7. W. M. Kantor, *Primitive permutation groups of odd degree, and an application to finite projective planes*, J. Algebra **106** (1987), 15–45.
8. K. Thas, *Finite flag-transitive projective planes: a survey and some remarks*, Discrete Math. **266** (2003), 417–429.
9. K. Thas and D. Zagier, *Finite projective planes, Fermat curves, and Gaussian periods*, J. Eur. Math. Soc. (JEMS) **10** (2008), 173–190.
10. B. 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.