International Journal of Mathematics Trends and Technology
ISSN: 2231-5373/ https://doi.org/10.14445/22315373/IJMTT-V72I10P109

Volume 72 Issue 10, 106-115, October 2026
© 2026 Seventh Sense Research Group®

Original Article

Orthomorphisms of Finite Fields from the Polynomial Viewpoint: Classification by Degree, Extremal Theory, Applications and Computational Checks

Rasmi M[1], Girish K. P[2]

[1]*Department of Mathematics, N.S.S. College, Ottapalam, University of Calicut, Kerala, India.*
[2]*Department of Mathematics, MES Kalladi College(Autonomous), Mannarkkad, University of Calicut, Kerala, India.*

[2]*Corresponding Author : girikalam@gmail.com*

Received: 28 August 2026 Revised: 01 October 2026 Accepted: 18 October 2026 Published: 29 October 2026

Abstract - *Orthomorphism polynomials over finite fields are permutation polynomials f for which $f(x)-x$ is again a permutation polynomial, and they underlie orthogonal Latin squares and cryptographic constructions. Their classification has advanced one degree at a time, each step resting on a classification of permutation polynomials of the same degree, and the classification for degree eight has been missing. This paper determines all orthomorphism polynomials of degree eight over fields of odd order. Translation and scaling symmetries reduce the problem to Fan's list of normalised degree-eight permutation polynomials, and the resulting finite search is carried out by two independent exhaustive enumerations that agree. Such polynomials exist over exactly two odd fields, of orders 11 and 29, and over the field of order 29 every canonical one is a binomial $cx(x^7+a)$ parametrised by an ordered pair of distinct elements of a four-element set. The paper also reviews the classification by degree, the extremal theory of maximal degree and minimal Hamming distance, cyclotomic orthomorphisms and applications, and it rechecks by computation the finite statements of Allsop and Wanless, of Kousik and Basnet, and of Eberhard, Manners and Mrazović; every recomputed value agrees with the literature. The degree-eight result extends the classification of orthomorphism polynomials from degree seven to degree eight in odd characteristic, and it leaves the even-characteristic case and the degrees above eight as the main open problems.*

Keywords *- Complete Mappings, Cyclotomic Maps, Hamming Distances, Latin Squares, Transversals.*

1. Introduction

Let $\mathbb{F}_q$ denote the finite field with $q=p^n$ elements, p prime. A polynomial $f\in\mathbb{F}_q[x]$ is a Permutation Polynomial (PP) if the map $c\mapsto f(c)$ is a bijection of $\mathbb{F}_q$. Permutation Polynomials go back to Hermite and Dickson [1], are treated in standard texts [2, 3] and are used in coding theory, combinatorial design and cryptography [4]. A PP f is an orthomorphism polynomial if $f(x)-x$ is also a PP; equivalently, f induces an orthomorphism of the additive group of $\mathbb{F}_q$, that is, a permutation θ for which $x\mapsto\theta(x)-x$ is again a permutation. Up to a change of sign, orthomorphisms are the same objects as complete mappings [5]. They originate in the construction of orthogonal Latin squares by Mann [6] and in the work of Paige [7] and of Hall and Paige [8] on finite groups, and the orthomorphisms of $(\mathbb{F}_q,+)$ correspond to the transversals of the Cayley table of the additive group [9, 10].

Orthomorphism polynomials of small degree have been classified one degree at a time, and each classification rests on a classification of permutation polynomials of the same degree: degrees up to five by Niederreiter and Robinson [11], degree six by Shallue and Wanless [12] and degree seven by Kousik and Basnet [5]. Fan classified the permutation polynomials of degree eight over fields of odd order [13] and of even order [14]. The corresponding orthomorphism classification is not a formal consequence of Fan's results, because linear equivalence preserves the permutation property but not the orthomorphism property, and it has not been reported. The research gap is therefore twofold. The classification of orthomorphism polynomials of degree eight is missing, and the finite statements that connect the existing results (the degree bound, the extremal degree, the minimal Hamming distance) are spread over several papers and have not been checked independently of their authors.

This paper closes the first gap for fields of odd order and addresses the second. Its novelty is as follows. Fan classifies permutation polynomials of degree eight up to linear equivalence, and Kousik and Basnet classify orthomorphism polynomials of degree seven, whereas the present result classifies orthomorphism polynomials of degree eight. It does so by proving two

This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)

reduction lemmas that translate Fan's list into a finite search, by carrying out that search with two independent exhaustive computations, and by giving a closed description of the answer over the field of order 29. The paper also reviews the classification by degree, the extremal theory and the applications, and it recomputes finite statements of the literature, so that the new result is set beside what is known. Table 2 distinguishes the types of evidence behind each result.

Section 2 describes the literature base, proves the reduction lemmas and describes the algorithms. Section 3 presents the review, the degree-eight classification, the recomputed statements, a discussion and the open problems, and Section 4 concludes.

2. Materials and Methods

2.1. Literature Base and Selection

2.1.1. Scope

The paper is a research article whose original part is the degree-eight classification and the recomputation of finite statements (Sections 3.5 and 3.6); its literature base covers orthomorphism and complete mapping polynomials over finite fields from 1942 to 2026 and places the new results among the known ones. Results on complete mappings of arbitrary groups are mentioned only for context.

2.1.2. Sources and Selection

The literature base was assembled in two steps. First, a logged search was carried out on 3 October 2026 with a general academic web-search tool and the five queries: *orthomorphism polynomials over finite fields*, *complete mapping polynomials finite fields classification of degree*, *orthomorphism Hamming distance Latin bitrades transversals Cayley table*, *cyclotomic orthomorphisms finite fields existence* and *orthomorphisms complete mappings cryptography block cipher applications*, which returned 9, 9, 10, 9 and 9 results. Together with four seed papers (Shallue and Wanless [12], Allsop and Wanless [15], Kousik and Basnet [5], and Li, Zha and Tu [16]), this gave 50 records; after removal of 30 duplicates, exclusion of 6 records at title and abstract screening and of 4 at full-text eligibility, 10 records remained. Second, backward citation from the reference lists of the seeds, of Hou's survey [4] and of Evans's monograph [9] added further works, giving a corpus of 34 primary studies on orthomorphisms and complete mappings. The works cited here are those of that corpus that concern polynomials over finite fields, supplemented by foundational and background sources (Dickson, Paige, Hall and Paige, the texts of Lidl and Niederreiter and of Mullen and Panario, and Wanless's survey of transversals). A work was included if (i) it concerns orthomorphisms, complete mappings or complete permutation polynomials of finite fields, or the permutation-polynomial classification on which these rest; (ii) it proves, constructs, enumerates or applies them; and (iii) its authorship and publication details could be confirmed from the record itself or from a repository. Works on other algebraic structures, expository notes without new results, and records whose authorship could not be confirmed were excluded.

2.1.3. Synthesis

Each included work was classified by the type of claim (theorem proved analytically, theorem proved with computer assistance, conjecture, computation) and by the degree or parameter range it covers. Unresolved problems in Section 3.8 are those that the sources themselves state as open and that remain open after the computations reported here.

2.1.4. Limits

Screening was done by the authors alone; the search used a single general-purpose web-search tool and not several bibliographic databases, and the review can miss work outside the citation networks of the seed papers.

2.2. Preliminaries and Reduction Lemmas

Two polynomials are *linearly related* if $g(x) = \alpha f(\beta x + \gamma) + \delta$ with $\alpha, \beta \in \mathbb{F}_q^*$ and $\gamma, \delta \in \mathbb{F}_q$; then f is a PP if and only if g is [12, 15]. Linear equivalence does not preserve the orthomorphism property: $f(x) = 2x$ is an orthomorphism polynomial over $\mathbb{F}_q$ for odd q, whereas $f(x) = x$ is not [17]. Every map $\mathbb{F}_q \to \mathbb{F}_q$ is represented by a unique polynomial of degree less than q, and the degree of an orthomorphism polynomial is the degree of this reduced form. A polynomial with $f(0) = 0$ is called *canonical*. Two symmetries do preserve the orthomorphism property, and they are the basis of every enumeration below.

Lemma 1 (translation and constants). For $\gamma, \delta \in \mathbb{F}_q$ and a polynomial f put $(\gamma, \delta) \cdot f = f(x + \gamma) + \delta$. This operation maps orthomorphism polynomials of degree d to orthomorphism polynomials of degree d. If $p \nmid d$, let S_0 be the set of orthomorphism polynomials of degree d that are canonical and have vanishing coefficient of x^{d-1}, and let $N_0 = |S_0|$. Then $(\gamma, \delta, f_0) \mapsto (\gamma, \delta) \cdot f_0$ is a bijection from $\mathbb{F}_q \times \mathbb{F}_q \times S_0$ onto the set of all orthomorphism polynomials of degree d. Consequently, the number of orthomorphism polynomials of degree d is $q^2 N_0$ and the number of canonical ones is $q N_0$.

Proof. Let $g = (\gamma, \delta) \cdot f$ with f an orthomorphism polynomial. Then g is a PP because f is, and $g(x) - x = \big(f(x+\gamma) - (x+\gamma)\big) + \gamma + \delta$ is a PP because $f(y) - y$ is a PP; the reduced degree is unchanged. *Injectivity.* Let $f_0 \in S_0$ have leading coefficient c and put $g = (\gamma, \delta) \cdot f_0$. The coefficient of x^{d-1} in g is $dc\gamma$, because that coefficient of f_0 is 0; as $p \nmid d$ and $c \neq 0$, γ is determined by g. Then $g(-\gamma) = f_0(0) + \delta = \delta$ determines δ, and $f_0(x) = g(x - \gamma) - \delta$ is determined too. *Surjectivity.* Let g be an orthomorphism polynomial of degree d with leading coefficient c and coefficient a_{d-1} of x^{d-1}. Put $\gamma = a_{d-1}/(dc)$, $\delta = g(-\gamma)$ and $f_0(x) = g(x - \gamma) - \delta$. The coefficient of x^{d-1} in f_0 is $a_{d-1} - dc\gamma = 0$ and $f_0(0) = g(-\gamma) - \delta = 0$, f_0 is an orthomorphism polynomial by the first paragraph (applied with $(-\gamma, -\delta)$), so $f_0 \in S_0$ and $(\gamma, \delta) \cdot f_0 = g$. The image $(\gamma, \delta) \cdot f_0$ is canonical exactly when $f_0(\gamma) + \delta = 0$, which fixes δ for each γ; hence there are q canonical images of each f_0, which gives qN_0 canonical polynomials. ▫ □

Lemma 2 (reduction to normalised permutation polynomials). Let $p \nmid d$ and let $\mathcal{N}_d(q)$ be the set of monic polynomials $g = x^d + \sum_{i=1}^{d-2} a_i x^i$ that are PPs of $\mathbb{F}_q$. Then the orthomorphism polynomials of degree d that are canonical and have vanishing coefficient of x^{d-1} are exactly the polynomials cg with $g \in \mathcal{N}_d(q)$, $c \in \mathbb{F}_q^*$ and $cg(x) - x$ a PP. The representation $f = cg$ is unique (c is the leading coefficient of f), so no polynomial is counted twice. Hence $N_0 = \#\{(c, g) : g \in \mathcal{N}_d(q),\ c \in \mathbb{F}_q^*,\ cg(x) - x \text{ is a PP}\}$.

Proof. If f is canonical with $a_{d-1} = 0$ and leading coefficient c, then $g = c^{-1}f$ is monic, $g(0) = 0$, has vanishing coefficient of x^{d-1}, and is a PP because multiplication by c^{-1} permutes $\mathbb{F}_q$; so $g \in \mathcal{N}_d(q)$ and $f = cg$. Conversely, for $g \in \mathcal{N}_d(q)$ and $c \in \mathbb{F}_q^*$ the polynomial cg is a canonical PP with $a_{d-1} = 0$, and it is an orthomorphism polynomial exactly when $cg(x) - x$ is a PP. Uniqueness is clear. ▫ □

A third symmetry is used only to speed up the enumerations. For $\lambda \in \mathbb{F}_q^*$ the map $f(x) \mapsto \lambda f(x/\lambda)$ preserves the orthomorphism property, because $\lambda f(x/\lambda) - x = \lambda(f(y) - y)$ with $y = x/\lambda$. It sends the coefficient a_i to $\lambda^{1-i}a_i$, hence the leading coefficient c of a polynomial of degree d to $c\lambda^{1-d}$, and it preserves the conditions $f(0) = 0$ and $a_{d-1} = 0$. Therefore, the number of canonical orthomorphism polynomials with $a_{d-1} = 0$ and leading coefficient c depends only on the coset of c modulo the subgroup of $(d-1)$-th powers of $\mathbb{F}_q^*$.

Theorem 3 (degree bound; Niederreiter and Robinson [11] for odd characteristic, Wan [18] for characteristic 2). For $q > 3$, every orthomorphism polynomial over $\mathbb{F}_q$ has reduced degree at most $q - 3$.

Theorem 3 implies that an orthomorphism polynomial of degree d can exist only if $q \geq d + 3$; for $d = 8$ it requires $q \geq 11$.

2.3. Algorithms, finite fields and computing environment

Fields. Prime fields are $\mathbb{Z}/p\mathbb{Z}$ with elements $0, \ldots, p-1$. A field $\mathbb{F}_{p^k}$ is built as $\mathbb{F}_p[x]/\big(m(x)\big)$ with the modulus of Table 1; an element $a_0 + a_1 x + \cdots + a_{k-1}x^{k-1}$ is coded by the integer $\sum a_i p^i$. Addition and multiplication tables are generated from these data and checked for the field axioms and for cyclicity of the multiplicative group before use.

Table 1. Moduli used to construct the non-prime fields of Sections 3.5 and 3.6

Field	Modulus	Coding of elements
$\mathbb{F}_9$	$x^2 + 1$	$a_0 + 3a_1$
$\mathbb{F}_{16}$	$x^4 + x + 1$	$a_0 + 2a_1 + 4a_2 + 8a_3$
$\mathbb{F}_{25}$	$x^2 + x + 2$	$a_0 + 5a_1$
$\mathbb{F}_{27}$	$x^3 + 2x + 1$	$a_0 + 3a_1 + 9a_2$
$\mathbb{F}_{32}$	$x^5 + x^2 + 1$	$\sum a_i 2^i$

Method A (via permutation polynomials). (1) Enumerate all monic polynomials $g = x^8 + a_6 x^6 + \cdots + a_1 x$ over $\mathbb{F}_q$; for each choice of $(a_6, \ldots, a_2)$ the coefficient a_1 is swept over $\mathbb{F}_q$ Moreover, g is tested for the permutation property by evaluation at all points, with early exit at the first repeated value. This produces the set. $\mathcal{N}_8(q)$ of Lemma 2. (2) For every $g \in \mathcal{N}_8(q)$ and every $c \in \mathbb{F}_q^*$, test whether $cg(x) - x$ is a PP; the number of successes is $N_0(q)$ by Lemma 2. For $q \geq 37$ (used only to confirm Theorem 5), the scaling symmetry $g \mapsto t^{-8}g(tx)$, which multiplies a_6 by t^{-2}, reduces step (1) to one value of a_6 per coset of the squares; this shortcut was validated against the full enumeration in ten fields.

Method B (direct enumeration). All canonical polynomials $f = cx^8 + a_6x^6 + \cdots + a_1x$ with $a_7 = 0$ and prescribed leading coefficient c are enumerated, and the coefficient a_1 is swept so that f and $f - x$ are tested together, again with early exit. By the third symmetry of Section 2.2 (degree $d = 8$, so cosets modulo the subgroup H of 7th powers), one leading coefficient per coset of H suffices, and $N_0(q) = |H| \sum_c n(c)$ with $n(c)$ the count for the representative c. This method does not use $\mathcal{N}_8(q)$ Moreover, is independent of Fan's theorem.

Implementation and environment. Both methods are implemented in C (enumerator, compiled with gcc -O2) with Python 3.12 scripts for field construction and bookkeeping, on a Linux x86-64 machine with one core. The running time of any single field is below two minutes. All source code, field tables, lists of normalised polynomials and outputs, with SHA-256 checksums, are in Online Resource 1.

3. Results and Discussion

3.1. Classification of Orthomorphism Polynomials by Degree

Degree at most five. All orthomorphism polynomials of degree less than 6 over every $\mathbb{F}_q$, and those of degree 6 when $\gcd(6, q) = 1$, were classified by Niederreiter and Robinson [11].

Degree six. Dickson's classification of degree-six PPs over fields of odd characteristic [1] was cited as complete only for $\gcd(6, q) = 1$ by Niederreiter and Robinson [11] and by Mullen [19], while others called it a partial list. Shallue and Wanless traced this to Dickson's characteristic-3 case, which was complete up to linear equivalence but not in normalised form; they repeated the calculations and restated the classification in normalised form [12]. Together with the characteristic-2 classification of Li, Chandler and Xiang [20], this yields a complete classification of degree-six PPs. Shallue and Wanless then proved that no degree-six orthomorphism polynomial exists in characteristic 2 and that in characteristic 3 they exist exactly over $\mathbb{F}_9$ [12].

Degree seven. Fan proved that every non-exceptional PP of degree 7 over $\mathbb{F}_q$, $q > 7$, $q \notin \{9,11,13,17,19,23,25,27,31,49\}$, is linearly related to the Dickson polynomial $D_7(x, a) = x^7 - 7ax^5 + 14a^2x^3 - 7a^3x$ with $a = 0$ and $q \not\equiv 1 \pmod 7$, or $a \neq 0$ and $q^2 \not\equiv 1 \pmod 7$, and listed coefficient tuples for the finitely many exceptional fields [21]. Kousik and Basnet combined this with the characteristic-2 result [20]:

Theorem 4 (Kousik and Basnet [5]). For $q > 7$, a non-exceptional degree-seven orthomorphism polynomial over $\mathbb{F}_q$ exists if and only if $q \in \{11,13,17,19,25\}$. Every orthomorphism polynomial over $\mathbb{F}_{7^t}$, $t \geq 2$, is exceptional; none of degree seven exists in characteristic 2, over $\mathbb{F}_{23}$ or over $\mathbb{F}_{31}$; and for $q \equiv 6 \pmod 7$, $q \neq 13$, none exists at all.

Degree eight. Fan classified the PPs of degree 8 over fields of odd order [13] and of even order [14]:

Theorem 5 (Fan [13]). For an odd prime power $q > 8$, a permutation polynomial of degree 8 exists over. $\mathbb{F}_q$ if and only if $q \in \{11,13,19,23,27,29,31\}$.

The orthomorphism classification for degree 8 is the subject of Section 3.5. Beyond degree 8, no classification of PPs exists so that none can be derived for orthomorphism polynomials.

Table 2. Classification of orthomorphism polynomials by degree, with the type of evidence behind each statement

Degree	Result	Source	Type of evidence
≤ 5	complete for all q	Niederreiter, Robinson [11]	analytic proof
6	complete for all q	[11, 12, 20]	analytic proof, built on re-derived classification of PPs
7	non-exceptional ones exist iff $q \in \{11,13,17,19,25\}$	Kousik, Basnet [5]	analytic proof with case analysis of Fan's tuples; counts by computer
8, q odd	exist iff $q \in \{11,29\}$	this paper, Section 3.5	computer-assisted proof using Fan's theorem [13]; independent enumeration
8, q even	open	—	PP classification available [14]; orthomorphism step not done
≥ 9	open	—	no PP classification

3.2. Extremal Theory: Maximum Degree and Hamming Distance

The degree bound of Theorem 3 raises the question of how large the degree of an orthomorphism polynomial can be.

Theorem 6 (Allsop and Wanless [15]). For every prime power $q \notin \{2,3,5,8\}$, there is an orthomorphism polynomial over $\mathbb{F}_q$ of degree exactly $q-3$.

Distinct permutations of $\mathbb{F}_q$ agree on at most $q-2$ points, so the Hamming distance $H(f,g) = |\{a: f(a) \neq g(a)\}|$ between distinct orthomorphisms is at least 2; if $f(a) = f(b)$ for $a \neq b$ then $f(a) - b = f(b) - a$ would contradict the injectivity of $x \mapsto f(x) - x$ when $H = 2$, so $H(f,g) \geq 3$.

Lemma 7 ([15]). If f, g are distinct reduced orthomorphism polynomials with $H(f,g) = 3$, then $\max(\deg f, \deg g) = q - 3$.

Allsop and Wanless give four constructions valid in different regimes (odd characteristic other than 5; $q \equiv 1 \pmod 3$; large odd q, using a result of Cavenagh, Hämäläinen and Nelson on orthomorphisms with three prescribed values [22]; and $q = 2^r$ with $r \geq 5$ odd), which together cover all $q \notin \{2,5,8\}$:

Theorem 8 ([15]). Orthomorphism polynomials f, g with $H(f,g) = 3$ exist if and only if $q \notin \{2,5,8\}$; for $q = 5$ and $q = 8$ the minimum Hamming distance is 4.

Theorem 6 follows from Theorem 8 and Lemma 7. The case of prime q was proved earlier by Cavenagh and Wanless [23], who used the correspondence between orthomorphisms and transversals of the Cayley table.

Typical degree and enumeration. Konyagin and Pappalardi proved that asymptotically almost all PPs over. $\mathbb{F}_q$ have reduced degree $q-2$ [24]. Allsop and Wanless observed that the data for $q \leq 17$ are consistent with an analogue for orthomorphisms:

Conjecture 9 (Allsop and Wanless [15], Conjecture 13). Asymptotically almost all orthomorphism polynomials over $\mathbb{F}_q$ have reduced degree $q-3$.

The number of orthomorphisms of $\mathbb{F}_q$ equals the number of complete mappings of the elementary abelian group of order q. For a group of order q satisfying the Hall–Paige condition, Eberhard, Manners and Mrazović proved that this number is $\left(e^{-1/2} + o(1)\right) q!^2/q^{q-1}$ [25]; Allsop and Wanless use this to show that almost all orthomorphisms are irregular in the sense of Section 3.3.

3.3. Cyclotomic Orthomorphisms and Complete Mappings of Groups

Let $q - 1 = nk$ and let γ generate $\mathbb{F}_q^*$. The cosets $C_{j,n} = \{\gamma^{ni+j}: 0 \leq i < k\}$ of the index-n subgroup partition $\mathbb{F}_q^*$. A *cyclotomic map* of index n is $\psi(x) = a_i x$ for $x \in C_{i,n}$, $\psi(0) = 0$, with $a_0, \ldots, a_{n-1} \in \mathbb{F}_q$. Niederreiter and Winterhof proved the existence of several classes of cyclotomic orthomorphisms and of their generalisation to R-orthomorphisms [26]. Fear and Wanless determined which pairs (q,k) admit an orthomorphism that is cyclotomic of least index k (Evans's Problem 28), and gave a partial answer, for sufficiently large q, to the question of which orthomorphisms are orthogonal to a given non-linear cyclotomic orthomorphism (Problem 27) [9, 27].

An orthomorphism is *irregular* if none of its translates $x \mapsto \theta(x+g) - \theta(g)$ is cyclotomic of index smaller than $q-1$. Allsop and Wanless proved that irregular orthomorphisms exist for all even $q > 4$ and for $q \equiv 1 \pmod 3$ with $q > 7$, and that asymptotically almost all orthomorphisms are irregular [15].

The field case is a special case of the theory of complete mappings of a finite group G. Hall and Paige conjectured that G has a complete mapping if and only if its Sylow 2-subgroups are trivial or non-cyclic [8]; the conjecture was completed with the classification of finite simple groups [28], and a quantitative proof was given by Eberhard, Manners and Mrazović [25]. Bors and Wang studied parities of complete mappings and orthomorphisms [29], and Evans's survey collects applications [30].

3.4. Complete permutation polynomials and applications

Complete permutation polynomials. In characteristic 2, $f(x) - x = f(x) + x$ and the two notions coincide; Theorem 3 applies verbatim to complete mappings. The Akbary–Ghioca–Wang criterion [31], which reduces the permutation property of

f to that of an induced map on a smaller set, underlies many constructions, including monomial and trinomial classes over $\mathbb{F}_{2^n}$ [32]. Li, Zha and Tu study $xh(x^{q-1})$ over $\mathbb{F}_{q^2}$ Moreover, reduce the property, through the unit circle and Dickson polynomials, to non-vanishing conditions on two auxiliary functions [16].

Latin squares and design. Complete mappings of a group give orthogonal mates of its Cayley table, and orthomorphisms correspond to transversals [6, 9]. Orthogonal cyclotomic orthomorphisms yield large sets of mutually orthogonal Latin squares [9], and the distance-3 pairs of Theorem 8 are used to construct 3-homogeneous Latin bitrades [15, 23].

Cryptography and coding. Mittenthal proposed orthomorphic mappings for nonlinear substitution devices [33]. Bors and Wang describe constructions that place an orthomorphism in the round function, namely the Lai–Massey scheme, the block cipher FOX and the stream cipher Loiss [29]. Schulz's anti-symmetric mappings [34] and the permutations of Shaheen and Winterhof [35] serve as check-digit systems.

3.5. Degree-Eight Orthomorphism Polynomials Over Odd Fields

Statement and status of the result.

Theorem 10. Let q be an odd prime power. An orthomorphism polynomial of degree 8 exists over. $\mathbb{F}_q$ if and only if $q \in \{11,29\}$. Over $\mathbb{F}_{11}$ there are 2 640 canonical ones, 29 040 in all; over $\mathbb{F}_{29}$ there are 348 canonical ones, 10 092 in all.

The evidence is of two kinds, which are kept apart. *Analytic part.* Theorem 3, Theorem 5 (Fan, proved in [13]) and Lemmas 1 and 2 (proved in Section 2.2) reduce the statement to a finite problem: by Theorem 3, $q \geq 11$; by Theorem 5, a degree-8 orthomorphism polynomial is a degree-8 PP, so $q \in \{11,13,19,23,27,29,31\}$; by the two lemmas it remains to compute $N_0(q)$ for these seven fields. *Computational part.* The seven values of $N_0(q)$ are obtained by exhaustive finite computation, by two methods that share no code and no intermediate data. The theorem is therefore a computer-assisted theorem: it is exactly as reliable as Fan's theorem and the correctness of the enumeration programs. Fan's theorem is used for odd $q > 31$ only; for odd $q \leq 61$ the non-existence of degree-8 PPs outside the list was also confirmed by the exhaustive count of the paragraph on the confirmation of Fan's theorem below.

Table 3. Degree-eight orthomorphism polynomials over odd fields: intermediate data and results (all counts computed)

q	$\lvert\mathcal{N}_8(q)\rvert$	pairs tested	N_0 (A)	N_0 (B)	canonical qN_0	all q^2N_0
11	2 754	27 540	240	240	2 640	29 040
13	1 380	16 560	0	0	0	0
19	864	15 552	0	0	0	0
23	154	3 388	0	0	0	0
27	364	9 464	0	0	0	0
29	32	896	12	12	348	10 092
31	30	900	0	0	0	0

Counting and completeness. By Lemma 2 the pairs (c, g) are in bijection with the polynomials counted, so no polynomial is omitted or duplicated once $\mathcal{N}_8(q)$ is complete. Completeness of $\mathcal{N}_8(q)$ was validated in three ways: (i) the enumerated sets are closed under the scaling $g \mapsto t^{-8}g(tx)$ (checked for every element); (ii) the numbers of orbits under this scaling, namely 277, 117 and 48 for $q = 11,13,19$, coincide with the numbers of linearly related classes reported by Fan [13], and the orbit counts for $q = 23,27,29,31$ are 7, 14, 2 and 1; (iii) method B, which does not use $\mathcal{N}_8(q)$, returns the same value of N_0 in every field (Table 3, columns A and B). The 240 and 12 polynomials counted over $\mathbb{F}_{11}$ and $\mathbb{F}_{29}$ were re-tested with plain integer arithmetic modulo p for the properties that f and $f - x$ permute the field.

Independent check over $\mathbb{F}_{11}$. The degree distribution of all 3 441 canonical orthomorphisms of $\mathbb{F}_{11}$, obtained by exhaustive backtracking over all orthomorphisms and interpolation of each, is $\{1: 9,\ 6: 132,\ 7: 660,\ 8: 2\,640\}$. The count of degree 8 agrees with the table, and the counts of degrees 6 and 7 agree with Section 3.6.

*Confirmation of Fan's theorem.*The sets $\mathcal{N}_8(q)$ were computed for all 18 odd prime powers q with $9 \leq q \leq 61$. They are non-empty exactly for $q \in \{11,13,19,23,27,29,31\}$, in agreement with Theorem 5.

Proposition 11. Let $A = \{4,10,19,25\} \subset \mathbb{F}_{29}$. The canonical degree-eight orthomorphism polynomials over $\mathbb{F}_{29}$ with vanishing coefficient of x^7 are exactly the twelve polynomials

$$f_{a,a'}(x) = c\,x\,(x^7 + a), \qquad c = (a - a')^{-1}, \quad a, a' \in A,\ a \neq a',$$

and for these $f_{a,a'}(x) - x = c\,x\,(x^7 + a')$. Explicitly, $f = cx^8 + bx$ with $(c, b) \in \{(2,9), (2,21), (5,9), (5,21), (24,9), (24,21), (27,9), (27,21), (11,15), (13,15), (16,15), (18,15)\}$.

Proof. Sufficiency. Multiplication by $c \neq 0$ permutes $\mathbb{F}_{29}$, so $cx(x^7 + a)$ is a PP if and only if $x(x^7 + a)$ is. Since $28 = 4 \cdot 7$, Zieve's criterion [36] applies to $x(x^7 + a) = x\,h(x^7)$ with $h(y) = y + a$, $d = 4$, $r = 1$ and $(q - 1)/d = 7$: it is a PP of $\mathbb{F}_{29}$ if and only if $\gcd(1,7) = 1$ (true) and $x(x + a)^7$ permutes the group $\mu_4 = \{1,12,17,28\}$ of fourth roots of unity. Direct evaluation gives, for $a = 4,10,19,25$, the values of $x(x + a)^7$ at $x = 1,12,17,28$ as $(28,12,1,17)$, $(12,17,28,1)$, $(1,28,17,12)$ and $(17,1,12,28)$ respectively; each is a permutation of μ_4. For all other $a \in \mathbb{F}_{29}^*$ the criterion fails, so A is exactly the set of a for which $x(x^7 + a)$ permutes $\mathbb{F}_{29}$. If $a, a' \in A$ are distinct and $c = (a - a')^{-1}$, then $f = cx(x^7 + a)$ is a PP, and $f(x) - x = cx(x^7 + a - (c)^{-1}) = cx(x^7 + a')$ is a PP as well. The twelve ordered pairs give the twelve pairs. $(c, b = ca)$ listed. *Necessity.* By Lemma 2, Table 3 (methods A and B) shows. $N_0(29) = 12$; since the twelve polynomials above are distinct orthomorphism polynomials of the required type, they are all of them. ▫ □

Proposition 11 gives a short, hand-checkable description of the answer over $\mathbb{F}_{29}$, whose sufficiency part is a check on four elements: the orthomorphisms arise from pairs of permutation binomials $x(x^7 + a)$ and $x(x^7 + a')$ with $a, a' \in A$ whose parameters differ by the reciprocal of the leading coefficient. Over $\mathbb{F}_{11}$ the 240 polynomials fall into 24 orbits of size 10 under $f(x) \mapsto \lambda f(x/\lambda)$.

3.6. Recomputation of Finite Statements of the Literature

Purpose and status. The computations of this section recheck statements proved elsewhere. They do not prove those statements; they exclude transcription or reading errors and supply intermediate data. Methods are those of Section 3.5 (direct enumeration, with the number of canonical polynomials multiplied by q and by q^2 according to (Lemma 1), together with exhaustive enumeration of all permutations of $\mathbb{F}_q$ for $q \leq 9$ and backtracking for $q \geq 11$.

Small fields. Over $\mathbb{F}_5$ every orthomorphism is linear, $f(x) = ax + b$ with $a \in \{2,3,4\}$, giving 15 orthomorphisms. Over $\mathbb{F}_7$ there are 133, of which 19 are canonical: five linear maps ax $(a = 2, \ldots, 6)$ and fourteen of degree $4 = q - 3$. Table 4 lists the fourteen as full coefficient tuples. (a_4, a_3, a_2, a_1); they are pairwise distinct.

Table 4. The fourteen canonical orthomorphism polynomials of degree 4 over $\mathbb{F}_7$, $f(x) = a_4x^4 + a_3x^3 + a_2x^2 + a_1x$, as tuples (a_4, a_3, a_2, a_1)

(1,6,3,0)	**(1,5,5,0)**	**(1,4,6,1)**	**(1,3,6,0)**	**(1,2,5,1)**	**(1,1,3,1)**	**(1,0,0,4)**
(6,6,4,0)	(6,5,2,0)	(6,4,1,1)	(6,3,1,0)	(6,2,2,1)	(6,1,4,1)	(6,0,0,4)

Degrees 6 and 7. Table 5 gives the counts. Degree-six orthomorphism polynomials exist over $\mathbb{F}_9$ and $\mathbb{F}_{11}$ and over no other field of order at most 32; in particular, none exists in characteristic 2 and, in characteristic 3, only $\mathbb{F}_9$ among $\mathbb{F}_9, \mathbb{F}_{27}$, as stated by Shallue and Wanless [12]. Degree-seven ones exist exactly over. $\mathbb{F}_{11}, \mathbb{F}_{13}, \mathbb{F}_{17}, \mathbb{F}_{19}, \mathbb{F}_{25}$ among the fields of order 9 to 32, in agreement with Theorem 4; over $\mathbb{F}_{11}$ there are 660 canonical ones, hence $660 \times 11 = 7\,260$, the count of [5]. The exact counts for the other fields are omitted here because they are the principal subject of separate work.

Table 5. Canonical orthomorphism polynomials of degree 6 and 7 (computed). For $p \mid 6$, no normalisation of a_5 is possible and canonical polynomials are counted directly; "yes" means that they exist

q	degree 6	degree 7		q	degree 6	degree 7
9	168	0		23	0	0
11	132	660		25	0	yes
13	0	yes		27	0	0
16	0	0		29	0	0
17	0	yes		31	0	0
19	0	yes		32	0	0

Extremal facts. Exhaustive enumeration of all orthomorphisms of $\mathbb{F}_q$ for $q \leq 11$ gives **Table 6**. Degrees were obtained by interpolation (the coefficient of x^k is $-\sum_c f(c)c^{q-1-k}$), and the minimum distance from every canonical orthomorphism to all orthomorphisms, which suffices by translation invariance. The table confirms Theorem 3 (no degree above $q-3$), Theorem 6 (degree $q-3$ occurs for $q = 4,7,9,11$ and not for $q = 3,5,8$) and Theorem 8 (minimum distance 3 except 4 for $q = 5,8$). Lemma 7 holds for all 12 272 pairs at distance 3 found for $q = 7,9,11$ (none exists for $q = 8$). The proportion of canonical orthomorphisms of degree $q-3$ is 0.737, 0.675 and 0.767 for $q = 7,9,11$; this is consistent with Conjecture 13 but gives no evidence for the asymptotic statement. The numbers of canonical orthomorphisms, $1,2,3,19,48,249,3\,441$ for $q = 3,4,5,7,8,9,11$, equal the totals of Table 3.2 of [12], which provides an independent validation of the enumeration. For $q = 13,16,17$ the counts, computed by backtracking over transversals of the Cayley table, divided by q are 79 259, 15 296 512 and 94 471 089, again the totals of that table. The last column of Table 6 is the ratio of $\kappa(q)$ to the estimate $e^{-1/2}q!^2/q^{q-1}$ of [25]; it is within 2.1% of 1 for $q = 7,11,13,17$, and it illustrates the asymptotic formula in this range without proving anything about it.

Table 6. Orthomorphisms of $(\mathbb{F}_q, +)$: number $\kappa(q)$, maximum reduced degree, minimum Hamming distance and ratio of $\kappa(q)$ to the Hall–Paige estimate (computed)

q	$\kappa(q)$	max. degree	$q-3$ attained	min. distance	ratio
3	3	1	no	3	1.237
4	8	1	yes	3	1.466
5	15	1	no	4	1.073
7	133	4	yes	3	1.016
8	384	4	no	4	0.817
9	2 241	6	yes	3	1.208
11	37 851	8	yes	3	1.016
13	1 030 367	—	—	—	1.021
16	244 744 192	—	—	—	1.063
17	1 606 008 513	—	—	—	1.018

3.7. Discussion

*Why the degree-eight classification could be completed: e*arlier classifications (degrees 6 and 7) proceeded by working through the explicit lists of permutation polynomials family by family and solving for the scalars that make a member an orthomorphism [5, 12]. For degree 8, the same strategy is possible in principle, but the list of Fan has far more members for small fields (2 754 normalised polynomials over $\mathbb{F}_{11}$). Three ingredients make a uniform computational treatment possible: the free action of Lemma 1, which removes the translation and constant parameters; Lemma 2, which turns the problem into a test of at most $q-1$ scalars per normalised polynomial; and the fact, from Theorem 5, that only seven odd fields carry degree-8 PPs at all. The cost of the entire classification is below two minutes per field.

Comparison with the state of the art. Table 2 summarises the position. The result is not a better value of a known quantity; it extends the classification of orthomorphism polynomials by one degree in odd characteristic, from 7 to 8, and the extension is of the same logical type as its predecessors (a finite problem on top of a permutation-polynomial classification), with the difference that the finite problem is solved by exhaustive search with an independent cross-check rather than by case analysis. Proposition 11 adds a structural explanation for the second field, which no earlier classification supplies at degree 8.

Limits. The result does not cover even q, where $p \mid 8$ and translation cannot remove the coefficient of x^7, so that the search space is larger by a factor q; it does not cover degree 9 or higher, for which no PP classification exists; and the claim of completeness for odd $q > 61$ rests on Fan's theorem.

3.8. Open Problems

(1) **Degree eight in characteristic 2.** The odd case is settled; the even case, using [14], is open, as is any classification beyond degree 8.
(2) **Asymptotic degree.** Conjecture 13 of Allsop and Wanless [15].
(3) **Irregularity.** Irregular orthomorphisms are known for even $q > 4$ and for $q \equiv 1 \pmod 3$, $q > 7$; whether this residue condition can be removed is open [15].

(4) **Evans's Problem 27, general case.** The partial answer of Fear and Wanless holds for sufficiently large q [27].
(5) **Cryptographic parameters.** Differential uniformity and nonlinearity of the explicit families produced by classification and construction papers are largely undetermined [16].

4. Conclusion

The classification of orthomorphism polynomials by degree is complete through degree seven in all characteristics, and the present paper extends it to degree eight in odd characteristic: such polynomials exist only over the fields of order 11 and 29, the first with 2 640 canonical polynomials and the second with twelve explicit binomials up to translation. The proof is analytic in its reduction (Lemmas 1 and 2, Fan's theorem) and computational in its finite part, which two independent enumerations confirm. The extremal theory shows that the bound $q - 3$ is reached for all but four small fields, and the recomputed finite statements agree with the literature. The remaining problems are the even-characteristic degree-eight case, the typical-degree conjecture and the cryptographic evaluation of the explicit families.

Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

Funding Statement

The authors received no financial support for the research, authorship and publication of this paper.

Author Contribution Statement

RM and GKP designed the study and wrote the manuscript. GKP carried out the computations. Both authors read and approved the manuscript.

Data Availability Statement

The programs, field tables, lists of normalised polynomials and outputs of all computations are provided as Online Resource 1.

Use of Generative AI

During the preparation of this manuscript, the authors used Claude (Anthropic) to draft and revise the text and to write and run the programs described in Sections 2.3 and 3.6. The authors reviewed, edited and verified all AI-assisted content and take full responsibility for its accuracy and originality.

Acknowledgments

The authors thank the Department of Mathematics, N.S.S. College, Ottapalam, and the Research & Post Graduate Department of Mathematics, MES Kalladi College, Mannarkkad, both affiliated to the University of Calicut, Kerala, India, for institutional support.

References

[1] Leonard Eugene Dickson, "The Analytic Representation of Substitutions on a Power of a Prime Number of Letters with a Discussion of the Linear Group, Part II," *Annals of Mathematics*, vol. 11, no. 1-6, pp. 65-120, 1896. [CrossRef] [Google Scholar] [Publisher Link]
[2] Rudolf Lidl, and Harald Niederreiter, *Finite Fields*, 2nd ed., Cambridge University Press, 1997. [Google Scholar] [Publisher Link]
[3] Gary L. Mullen, and Daniel Panario, *Handbook of Finite Fields*, 1st ed., CRC Press, 2013. [CrossRef] [Google Scholar] [Publisher Link]
[4] Xiang-Dong Hou, "Permutation Polynomials over Finite Fields — A Survey of Recent Advances," *Finite Fields and Their Applications*, vol. 32, pp. 82-119, 2015. [CrossRef] [Google Scholar] [Publisher Link]
[5] Bhitali Kousik, and Dhiren Kumar Basnet, "Orthomorphism Polynomials of Degree 7 Over Finite Fields," *arXiv*, pp. 1-14, 2026. [CrossRef] [Google Scholar] [Publisher Link]
[6] Henry B. Mann, "The Construction of Orthogonal Latin Squares," *The Annals of Mathematical Statistics*, vol. 13, pp. 418-423, 1942. [Google Scholar] [Publisher Link]
[7] Lowell J. Paige, "A Note on Finite Abelian Groups," *Bulletin of the American Mathematical Society*, vol. 53, pp. 590-593, 1947. [CrossRef] [Google Scholar] [Publisher Link]
[8] Marshall Hall, and Lowell J. Paige, "Complete Mappings of Finite Groups," *Pacific Journal of Mathematics*, vol. 5, no. 4, pp. 541-549, 1955. [CrossRef] [Google Scholar] [Publisher Link]
[9] Anthony B. Evans, *Orthogonal Latin Squares Based on Groups*, 1st ed., Springer International Publishing, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[10] Ian M. Wanless, "Transversals in Latin Squares: A Survey," *London Mathematical Society Lecture Note Series. Cambridge University Press*, vol. 392, pp. 403-437, 2011. [CrossRef] [Google Scholar] [Publisher Link]

[11] Harald Niederreiter, and Karl H. Robinson, "Complete Mappings of Finite Fields," *Journal of the Australian Mathematical Society Series A Pure Mathematics and Statistics*, vol. 33, no. 2, pp. 197-212, 1982. [CrossRef] [Google Scholar] [Publisher Link]

[12] Christopher J. Shallue, and Ian M. Wanless, "Permutation Polynomials and Orthomorphism Polynomials of Degree Six," *Finite Fields and Their Applications*, vol. 20, pp. 84-92, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[13] Xiang Fan, "Permutation Polynomials of Degree 8 Over Finite Fields of Odd Characteristic," *Bulletin of the Australian Mathematical Society*, vol. 101, no. 1, pp. 40-55, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[14] Xiang Fan, "Permutation Polynomials of Degree 8 Over Finite Fields of Characteristic 2," *Finite Fields and Their Applications*, vol. 64, pp. 1-20, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[15] Jack Allsop, and Ian M. Wanless, "Degree of Orthomorphism Polynomials over Finite Fields," *Finite Fields and Their Applications*, vol. 75, pp. 1-9, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[16] Jian Li, Zhengbang Zha, and Ziran Tu, "New Constructions of Complete Permutation Polynomials Over Finite Fields of Even Characteristic," *Mathematics*, vol. 14, no. 9, pp. 1-17, 2026. [CrossRef] [Google Scholar] [Publisher Link]

[17] Christopher J. Shallue, "Permutation Polynomials of Finite Fields," *arXiv*, pp. 1-64, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[18] Daqing Wan, "On a Problem of Niederreiter and Robinson about Finite Fields," *Journal of the Australian Mathematical Society Series A*, vol. 41, no. 3, pp. 336-338, 1986. [Google Scholar]

[19] Gary L. Mullen, "Finite Fields, Coding Theory, and Advances in Communications and Computing," *Lecture Notes in Pure and Applied Mathematics*, 1993. [Google Scholar]

[20] Jiyou Li, David B. Chandler, and Qing Xiang, "Permutation Polynomials of Degree 6 or 7 Over Finite Fields of Characteristic 2," *Finite Fields and Their Applications*, vol. 16, no. 6, pp. 406-419, 2010. [CrossRef] [Google Scholar] [Publisher Link]

[21] Xiang Fan, "A Classification of Permutation Polynomials of Degree 7 Over Finite Fields," *Finite Fields and Their Applications*, vol. 59, pp. 1-21, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[22] Nicholas J. Cavenagh, Carlo Hämäläinen, and Adrian M. Nelson, "On Completing Three Cyclically Generated Transversals to a Latin Square," *Finite Fields and Their Applications*, vol. 15, no. 3, pp. 294-303, 2009. [CrossRef] [Google Scholar] [Publisher Link]

[23] Nicholas J. Cavenagh, and Ian M. Wanless, "On the Number of Transversals in Cayley Tables of Cyclic Groups," *Discrete Applied Mathematics*, vol. 158, no. 2, pp. 136-146, 2010. [CrossRef] [Google Scholar] [Publisher Link]

[24] Sergei Konyagin, and Francesco Pappalardi, "Enumerating Permutation Polynomials Over Finite Fields by Degree II," *Finite Fields and Their Applications*, vol. 12, no. 1, pp. 26-37, 2006. [CrossRef] [Google Scholar] [Publisher Link]

[25] Sean Eberhard, Freddie Manners, and Rudi Mrazović, "An Asymptotic for the Hall–Paige Conjecture," *Advances in Mathematics*, vol. 404, pp. 1-73, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[26] Harald Niederreiter, and Arne Winterhof, "Cyclotomic *R*-Orthomorphisms of Finite Fields," *Discrete Mathematics*, vol. 295, no. 1-3, pp. 161-171, 2005. [CrossRef] [Google Scholar] [Publisher Link]

[27] David Fear, and Ian M. Wanless, "Existence Results for Cyclotomic Orthomorphisms," *Journal of Algebraic Combinatorics*, vol. 46, no. 1, pp. 1-14, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[28] Stewart Wilcox, "Reduction of the Hall–Paige Conjecture to Sporadic Simple Groups," *Journal of Algebra*, vol. 321, no. 5, pp. 1407-1428, 2009. [CrossRef] [Google Scholar] [Publisher Link]

[29] Alexander Bors, and Qiang Wang, "Compositions and Parities of Complete Mappings and of Orthomorphisms," *Journal of Combinatorial Theory, Series A*, vol. 196, pp. 1-50, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[30] Anthony B. Evans, "Applications of Complete Mappings and Orthomorphisms of Finite Groups," *Quasigroups Related Systems*, vol. 33, no. 1, pp. 5-30, 2015. [Google Scholar] [Publisher Link]

[31] Amir Akbary, Dragos Ghioca, and Qiang Wang, "On Constructing Permutations of Finite Fields," *Finite Fields and Their Applications*, vol. 17, no. 1, pp. 51-67, 2011. [CrossRef] [Google Scholar] [Publisher Link]

[32] Ziran Tu, Xiangyong Zeng, and Lei Hu, "Several Classes of Complete Permutation Polynomials," *Finite Fields and Their Applications*, vol. 25, pp. 182-193, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[33] Lothrop Mittenthal, "Block Substitutions using Orthomorphic Mappings," *Advances in Applied Mathematics*, vol. 16, no. 1, pp. 59-71, 1995. [CrossRef] [Google Scholar] [Publisher Link]

[34] Ralph-Hardo Schulz, *On Check Digit Systems using Anti-Symmetric Mappings*, Springer, pp. 295-310, 2000. [CrossRef] [Google Scholar] [Publisher Link]

[35] Rasha Shaheen, and Arne Winterhof, "Permutations of Finite Fields for Check Digit Systems," *Designs, Codes & Cryptography*, vol. 57, no. 3, pp. 361-371, 2010. [CrossRef] [Google Scholar] [Publisher Link]

[36] Michael E. Zieve, "On Some Permutation Polynomials Over F_q of the Form $xrh(x(q-1)/d)$," *Proceedings of the American Mathematical Society*, vol. 137, pp. 2209-2216, 2009. [CrossRef] [Google Scholar] [Publisher Link]