Degree-Sum-Freedom Is Not EA Invariant: Exact Profiles in a 4-Uniform Permutation Family

Jingchuan Ma, Yanhua Liu and Qiaoyun Huang

Department of Computer Engineering, Fuzhou University Zhicheng College, Fuzhou, China

Abstract

Degree-sum-freedom is a local criterion for division-property propagation from affine input spaces. Immediately after defining this criterion, the published chapter asserts invariance under extended-affine (EA) equivalence. We show that this assertion does not hold beyond ordinary sum-freedom and quantify the resulting variation. First, the natural Gold APN pair x^3 and $x^3 + x$ has exact proper-flat values 3 and 2 on an infinite sequence of dimensions. We then study a known complete-mapping family of EA-equivalent, differentially 4-uniform permutations F_b, G_b on $2r$ bits. For every odd r and every $1 \le c \le \lfloor (r-3)/2 \rfloor$, we determine their exact codimension-c profiles: $\mu_c(F_b) = 2c$ and $\mu_c(G_b) = r + c - 1$, equivalently $\tau_{2r-c}(F_b) = 2r - 2c$ and $\tau_{2r-c}(G_b) = r - c + 1$. Thus the gap is $r - c - 1 \ge (r+1)/2$ simultaneously over a linear-size range of proper affine codimensions. The mate upper bound follows by specializing known generalized-degree duality with the exact source profile established here. The matching uniform lower bound is family-specific: after an associated-graded reduction, odd codimensions are detected by one classical consecutive Moore determinant, whereas even codimensions require a jointly nonvanishing family of replacement minors. A cyclic carry classification proves that the selected coefficients are complete reduced coefficients. These results concern local affine-input division-property behavior; they do not yield a multiround distinguisher or an attack on a concrete cipher.

Keywords: degree-sum-freedom, extended-affine equivalence, division property, generalized algebraic degree, Moore determinant, complete mapping

1 Introduction

Integral and division-property analyses follow low-degree monomials through the components of a primitive. Affine input spaces are especially natural test sets: their indicators are products of affine forms, and they are the canonical structured inputs behind many integral arguments [Tod15, BC16, HLU23]. A recent degree-sum-freedom criterion assigns to an S-box a threshold measuring how far the division property of every affine input space can propagate [Car26]. In contrast to ordinary higher-order sum-freedom, the criterion permits output monomials of degree larger than one and therefore gives a graded rather than all-or-nothing description.

Equivalence is consequential in such a description. Affine input and output permutations merely relabel affine spaces or coordinates, so a genuinely affine-invariant scalar can be evaluated on a convenient representative. Extended-affine (EA) equivalence also permits adding an input-dependent affine map to the output. Immediately after Definition 1, the

Emails: kiciot@qq.com (Jingchuan Ma), Lyhwa@fzu.edu.cn (Yanhua Liu), huangqy@fdzcxy.edu.cn (Qiaoyun Huang)

Date of this document: August 23, 2026.

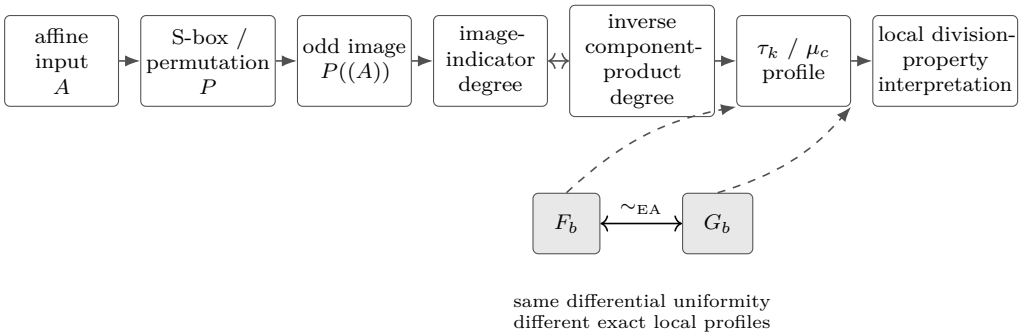

Figure 1: Conceptual route from an affine input to the scalar studied here. For a permutation, the image indicator is an affine-component product of P^{-1}. EA-equivalent representatives can retain the same differential uniformity while having different local profiles; the diagram makes no overall-security or multiround implication.

published chapter asserts invariance under this larger relation for all orders $k \geq 2$ and degree thresholds $t \geq 1$ [Car26, p. 226]. That conclusion would make the threshold a well-defined scalar of an EA class.

This assertion holds for ordinary sum-freedom ($t = 1$), but not for $t > 1$. The reason is structural: after an affine map is added to the output, products of output coordinates acquire mixed nonlinear–affine terms. The affine term alone sums to zero on a sufficiently large flat, whereas its products with components of the original function need not. A small counterexample establishes non-invariance, but by itself would leave open whether this is a pathology of an artificial truth table, a nonpermutation, or a single affine dimension.

This paper develops that correction into a structural profile theory. First, the standard Gold APN function x^3 and its EA mate $x^3 + x$ have exact values 3 and 2 on proper affine 3-flats over an infinite progression of dimensions. Second, a known complete-mapping construction gives EA-equivalent permutations F_b, G_b on $2r$ bits. Both are differentially 4-uniform, yet their exact profiles differ throughout a linear-size interval of proper affine codimensions. For odd r and

$$1 \leq c \leq \left\lfloor \frac{r-3}{2} \right\rfloor,$$

we prove

$$\mu_c(F_b) = 2c, \qquad \mu_c(G_b) = r + c - 1.$$

Here $\mu_c(P)$ is the minimum degree of an image indicator of an affine codimension-c space under a permutation P. Equivalently, the degree-sum-freedom values are

$$\tau_{2r-c}(F_b) = 2r - 2c, \qquad \tau_{2r-c}(G_b) = r - c + 1.$$

The exact gap $r - c - 1$ is at least $(r + 1)/2$ everywhere in the proved range. Figure 1 summarizes the objects linked by these identities.

Our contributions. The results are organized around four contributions.

1. We identify the mixed nonlinear–affine products that obstruct the stated EA invariance, derive a sufficient condition under which affine output addition is harmless, and give an infinite symbolic family attaining the elementary variation bound.
2. We prove a natural proper-flat separation inside the Gold APN EA class:

   $$\tau_3(x^3) = 3, \qquad \tau_3(x^3 + x) = 2$$

   for $n \geq 9$ and $n \equiv 3 \pmod 6$. This result retains APNness on both sides, although $x^3 + x$ is not a permutation.

Table 1: Prior framework and results established in this work. The right column records the role of the present analysis without attributing the underlying constructions or general tools to this paper.

Topic	Prior framework	Role of this work
Affine images and division property	Odd-image indicators, parity sets, generalized component degree	Indicator specialization defining μ_c and its relation to τ
Equivalence	Affine invariance; representation-sensitive propagation is known	Exact mixed-term obstruction and quantitative EA variation
Gold functions	APN and permutation properties	Proper-flat APN pair with exact values $\tau_3 = 3, 2$
Complete mappings	Construction and classification of the underlying family	Exact source and mate affine-profile analysis
Moore/Grassmannian tools	Consecutive Moore determinants, Moore exponent sets, Plücker coordinates	Cyclic coefficient classification and joint even-c detector for this family

3. In a known complete-mapping family, we determine exact profiles for two EA-equivalent, differentially 4-uniform permutations. The separation is simultaneous over $\Theta(r)$ proper affine codimensions, rather than a collection of isolated fixed-c examples.

4. We prove the mate lower bound by a uniform coefficient certificate. The known generalized-degree duality of Boura and Canteaut supplies the upper-bound mechanism [BC13]. The family-specific part is a complete cyclic carry classification followed by a parity-dependent Moore–Plücker argument: odd c uses one consecutive Moore determinant; even c uses c replacement minors whose simultaneous vanishing is impossible.

The general indicator formulation, generalized component degree, classical Moore nonvanishing, Plücker coordinates, and the complete-mapping construction are prior machinery. Table 1 distinguishes those inputs from the family-specific statements proved here.

Scope. The profile studied here is local to one S-box and affine input sets. A larger value of τ is not interpreted as more or less overall security. No statement in this paper supplies a multiround trail, a distinguisher, a key-recovery method, or an attack on a concrete cipher. Moreover, the mate formula is not claimed for $c > \lfloor (r-3)/2 \rfloor$; the large-c endpoint remains open.

Roadmap. Section 2 fixes the indicator and generalized-degree conventions and positions the prior work. Section 3 corrects the EA claim, and Section 4 gives the Gold example. Sections 5 and 6 introduce the permutation family and establish the source profile and the mate upper bound. The technical core, Section 7, proves the uniform lower certificate. Section 8 states the cryptographic interpretation and its limits before Section 9 concludes.

2 Preliminaries and Prior Framework

2.1 Boolean functions, flats, and odd images

All vector spaces are over $\mathbb{F}_2$. The algebraic degree of a Boolean function is the degree of its unique square-free algebraic normal form (ANF). For $X \subseteq \mathbb{F}_2^m$, write $\mathbf{1}_X$ for its Boolean

indicator. If $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is not injective, its relevant image of a set X is the *odd image*

$$F((X)) := \{y \in \mathbb{F}_2^m : |X \cap F^{-1}(y)| \text{ is odd}\}.$$

Thus

$$\sum_{x \in X} h(F(x)) = \sum_{y \in F((X))} h(y)$$

for every Boolean h, with sums in $\mathbb{F}_2$. This parity-set viewpoint is standard in the division-property literature [BC16, GRW16].

For an affine k-flat $A \subseteq \mathbb{F}_2^n$ with $1 \le k \le n$, define its local threshold

$$\tau(F, A) := \min\{t \ge 1 : \exists h : \mathbb{F}_2^m \to \mathbb{F}_2,\ 1 \le \deg h \le t,\ \sum_{x \in A} h(F(x)) = 1\},$$

whenever $F((A)) \neq \varnothing$. Reed–Muller duality gives the equivalent indicator formula

$$\tau(F, A) = m - \deg \mathbf{1}_{F((A))}. \tag{1}$$

The kth-order sum-free min-degree is the worst local threshold

$$\tau_k(F) := \max_{\substack{A \text{ affine} \\ \dim A = k}} \tau(F, A), \tag{2}$$

provided every such odd image is nonempty. Then F is kth-order t-degree-sum-free exactly when $\tau_k(F) \le t$ [Car26]. The field-power definition in that work is equivalent to (2), since powers of binary weight at most t span the Boolean functions of degree at most t.

2.2 Permutation fibers and the minimum indicator degree

Let P be a permutation of $V = \mathbb{F}_2^n$. Every affine codimension-c flat can be written

$$A_{L,\varepsilon} = \{x \in V : \ell_i(x) = \varepsilon_i,\ 1 \le i \le c\},$$

where $\ell_1, \dots, \ell_c \in V^*$ are independent and $\varepsilon \in \mathbb{F}_2^c$. Its indicator is

$$\mathbf{1}_{A_{L,\varepsilon}}(x) = \prod_{i=1}^{c} (1 + \varepsilon_i + \ell_i(x)).$$

Bijectivity gives the exact image-indicator identity

$$\mathbf{1}_{P(A_{L,\varepsilon})}(y) = \prod_{i=1}^{c} \big(1 + \varepsilon_i + \ell_i(P^{-1}(y))\big). \tag{3}$$

Definition 1 (Minimum affine-fiber indicator degree)**.** For $1 \le c \le n-1$, define

$$\mu_c(P) := \min_{\substack{\ell_1, \dots, \ell_c \text{ independent} \\ \varepsilon \in \mathbb{F}_2^c}} \deg \prod_{i=1}^{c} \big(1 + \varepsilon_i + \ell_i \circ P^{-1}\big). \tag{4}$$

Proposition 1 (Indicator characterization)**.** *For every n-bit permutation P and $1 \le c \le n-1$,*

$$\tau_{n-c}(P) = n - \mu_c(P), \qquad c \le \mu_c(P) \le n - 1.$$

Proof. The identity follows by minimizing the degree in (3) and using (1). Each indicator has weight 2^{n-c}. The minimum-distance bound for $\mathrm{RM}(d, n)$ gives $\deg \mathbf{1}_{P(A)} \ge c$. Its weight is even, so its full-degree ANF coefficient is zero and its degree is at most $n-1$. □

The proposition is an immediate specialization of established set-indicator and division-property machinery [GRW16, Car20]; it supplies the coordinate system for the family analysis below.

Table 2: Notation used throughout. In particular, δ_s is a maximum generalized degree, whereas μ_c is a minimum over affine-fiber indicators.

Symbol	Meaning
$\mathbb{F}_2$, K, q	binary field; $K = \mathbb{F}_{q^2}$; $q = 2^r$
r, c	half-dimension parameter; affine codimension
A, P	affine input flat; permutation or S-box
$\tau_k(P)$	worst local degree-sum threshold over affine k-flats
$\mu_c(P)$	minimum degree in (4)
$\delta_s(P)$	maximum generalized component-product degree in (5)
C_b, F_b, G_b, J_b, H_b	complete-mapping monomial and associated maps in (9); $H_b = x^{q+2} + bx$
R, L_λ, U_λ	normalized mate inverse; its linear and nonlinear trace components
$\Phi_{r,c}$	degree-$(r + c - 1)$ leading-symbol map in (14)
Tr, N	absolute trace to $\mathbb{F}_2$; norm $K \to \mathbb{F}_q$
P_I, E_I, p_I	detector row sum, target exponent, and K-valued Frobenius/Plücker minor indexed by I

2.3 Equivalences, components, and generalized degree

Maps $F, G : \mathbb{F}_2^n \to \mathbb{F}_2^m$ are *affine equivalent* if $G = A_{\text{out}} \circ F \circ A_{\text{in}}$ for affine permutations $A_{\text{in}}, A_{\text{out}}$. They are *EA equivalent* if additionally

$$G = A_{\text{out}} \circ F \circ A_{\text{in}} + A$$

for an affine map $A : \mathbb{F}_2^n \to \mathbb{F}_2^m$. Affine equivalence preserves τ_k and μ_c: the input map permutes affine flats and the output map preserves indicator degree. EA addition is the extra operation examined in Section 3.

For a vectorial Boolean function $H : \mathbb{F}_2^n \to \mathbb{F}_2^n$, let

$$\delta_s(H) := \max_{\substack{h:\mathbb{F}_2^n \to \mathbb{F}_2 \\ \deg h \le s}} \deg(h \circ H) \tag{5}$$

be its generalized algebraic degree [BC13]. Equivalently, after choosing output coordinates, it is the maximum degree of a product of at most s independent components. The maximum in δ_s and the minimum in μ_c point in opposite directions; an upper bound on the former does not provide the uniform lower bound required for the latter.

When $K = \mathbb{F}_{2^n}$, every binary component is uniquely

$$\ell_\lambda(x) = \mathrm{Tr}_{K/\mathbb{F}_2}(\lambda x),$$

because the trace pairing is nondegenerate. Components $\ell_{\lambda_1}, \dots, \ell_{\lambda_c}$ are independent exactly when the parameters $\lambda_1, \dots, \lambda_c$ are independent over $\mathbb{F}_2$.

2.4 Differential uniformity and notation

The differential uniformity of $F : V \to V$ is

$$\max_{a \neq 0, b} |\{x : F(x + a) + F(x) = b\}|.$$

Adding an affine map translates each derivative output and hence preserves this number. Inversion of a permutation transposes its difference distribution table and also preserves differential uniformity.

2.5 Prior-work boundary

Todo introduced the division property, and parity sets, set degree, inverse component products, and algebraic transition descriptions give several equivalent or compositional viewpoints [Tod15, BC16, GRW16, HLU23, BV23]. Broad representation dependence is also known: linearly equivalent S-box descriptions can lead to different propagation behavior in concrete analyses [LDF20]. Our claim is narrower and exact: the particular scalar τ_k is not EA invariant, and a family-specific codimension profile can be computed.

Higher-order sum-freedom and its Reed–Muller/Grassmannian formulations are active topics [Car25, Kas26, HKT26]. The recent degree-sum-freedom definition provides the immediate motivation [Car26]. Boura–Canteaut generalized degree and inverse duality are the source of our upper bound [BC13]; higher-order degree propagation predates the present setting [BCC11].

For scalar Boolean functions, restriction-degree stability and its indicator characterizations were developed by Carlet, Feukoua, and Sălăgean [CFS25b]. Their separate vectorial work is the closest coefficient-level framework to ours [CFS25a]: it multiplies affine trace indicators and uses consecutive or generalized Moore determinants to prevent degree drop for restrictions of power functions. Our object instead is a product of components of a nonmonomial inverse. Nonconsecutive Moore row sets require care [BZ20]; accordingly, the even-c argument uses its replacement minors only through a joint nonvanishing statement.

3 Degree-Sum-Freedom under EA Transformations

3.1 Mixed terms under EA addition

Let $F = (F_1, \dots, F_m)$ and let $L = (L_1, \dots, L_m)$ be affine. For an output-coordinate set S and an affine k-flat A, expansion gives

$$\sum_{x \in A} \prod_{j \in S} (F_j + L_j)(x) = \sum_{T \subseteq S} \sum_{x \in A} \left(\prod_{j \in T} F_j(x) \right) \left(\prod_{j \in S \setminus T} L_j(x) \right). \tag{6}$$

The $T = S$ term is the original moment. The $T = \varnothing$ term is an affine-coordinate product. The remaining terms are mixed products. The fact that a single affine function sums to zero on a k-flat controls neither these products nor their cancellation with the original moment. The published chapter states immediately after Definition 1 that the property is EA invariant for every $k \geq 2$ and $t \geq 1$ [Car26, p. 226]. Equation (6) exhibits mixed products not controlled by that assertion; the counterexamples below show that it is false when $t > 1$.

There is a useful positive boundary. Suppose every coordinate of F has degree at most d, and let $s = |S| \leq t$. A term in (6) indexed by $T \subsetneq S$ has input degree at most

$$d|T| + s - |T| \leq \max\{s, d(s-1)+1\} \leq \max\{t, d(t-1)+1\}.$$

This bound includes the all-affine term $T = \varnothing$, whose degree is at most $s \leq t$. Since a Boolean polynomial of degree less than k sums to zero on every affine k-flat, all additional terms vanish under the sufficient condition

$$\max\{t, d(t-1)+1\} < k. \tag{7}$$

Consequently, F and $F + L$ have identical moments for all output monomials of degree at most t, so t-degree-sum-freedom is preserved. This condition is not necessary, but it makes explicit why unconditional EA invariance is too strong.

3.2 Exact scalar variation

For $d \geq 3$, identify $\mathbb{F}_2^d$ with the integers $0, \ldots, 2^d - 1$ through a fixed basis. Let P_d be the permutation with the cycle $0 \mapsto 1 \mapsto 2 \mapsto 0$ and every other point fixed, and put $Q_d = P_d + \mathrm{id}$.

Theorem 1 (Sharp full-flat EA variation)**.** *The maps $P_d, Q_d : \mathbb{F}_2^d \to \mathbb{F}_2^d$ are EA equivalent and have defined full-flat values*

$$\tau_d(P_d) = d, \qquad \tau_d(Q_d) = 2.$$

Consequently, for every $t > 1$, t-degree-sum-freedom is not invariant under EA equivalence.

Proof. On the unique full-dimensional input flat, the odd image of the permutation P_d is the whole codomain. Its indicator is the constant one, so (1) gives $\tau_d(P_d) = d$. The values of Q_d on the three-cycle are $1, 3, 2$, while every fixed point maps to zero. Since $2^d - 3$ is odd, its odd image is $\{0, 1, 2, 3\} = \mathrm{span}(e_1, e_2)$, whose indicator has degree $d - 2$. Thus $\tau_d(Q_d) = 2$. Choosing $d = t + 1$ separates pass from fail at threshold t. □

Whenever two EA mates have defined τ_k, their values lie in $[1, \min(k, m)]$. Ordinary sum-freedom is EA invariant, so a value one cannot coexist with a larger value in one EA class. Therefore

$$|\tau_k(F) - \tau_k(G)| \leq \max\{0, \min(k, m) - 2\}.$$

Theorem 1 attains this bound for $n = m = k = d$. It shows that the failure is not a lone truth table, but its flat is not proper and the construction has no standard differential role. The next section supplies the natural proper-flat example.

4 A Natural Gold/APN Separation

Let $n \geq 9$ with $n \equiv 3 \pmod 6$, let $K = \mathbb{F}_{2^n}$, and define

$$F_n(x) = x^3, \qquad G_n(x) = x^3 + x.$$

These maps are EA equivalent through addition of the identity. For $a \neq 0$,

$$F_n(x + a) + F_n(x) = ax^2 + a^2x + a^3.$$

After $x = au$, a derivative equation reduces to $u^2 + u = \gamma$, which has kernel $\{0, 1\}$. Thus F_n is APN; adding x translates each derivative by a, so G_n is APN as well [Nyb94]. Since n is odd, $\gcd(3, 2^n - 1) = 1$ and F_n is a permutation. The mate is not: $G_n(0) = G_n(1) = 0$.

Theorem 2 (Gold proper-flat separation)**.** *For every $n \geq 9$ with $n \equiv 3 \pmod 6$,*

$$\tau_3(F_n) = 3, \qquad \tau_3(G_n) = 2.$$

Both values concern genuine proper affine 3-flats.

Proof. Let $A = a + U$ be any affine 3-flat. Its coset polynomial has the form

$$R_A(T) = \prod_{x \in A} (T + x) = T^8 + c_2T^4 + c_1T^2 + c_0T + d, \qquad c_0 = \prod_{u \in U \setminus \{0\}} u \neq 0.$$

Writing $p_j = \sum_{x \in A} x^j$, Newton identities in characteristic two give

$$p_1 = p_2 = p_3 = p_5 = p_9 = 0, \qquad p_7 = c_0.$$

Table 3: Exact families used in the paper. The Gold mate is APN but not a permutation; both complete-mapping representatives are permutations and differentially 4-uniform.

Family	Permutation?	Differential uniformity	EA relation	Exact result
x^3	yes	2	$G = F + \mathrm{id}$	$\tau_3 = 3$
$x^3 + x$	no	2	$G = F + \mathrm{id}$	$\tau_3 = 2$
$F_b = C_b^{-1}$	yes	4	$G_b = F_b + \mathrm{id}$	$\mu_c = 2c$ for $1 \le c \le r - 1$
G_b	yes	4	$G_b = F_b + \mathrm{id}$	$\mu_c = r + c - 1$ for $1 \le c \le \lfloor (r-3)/2 \rfloor$

Since $(x^3 + x)^3 = x^9 + x^7 + x^5 + x^3$,

$$\sum_{x \in A} G_n(x)^3 = c_0 \neq 0. \tag{8}$$

Nondegeneracy of the trace pairing gives $\lambda \in K^*$ with $\mathrm{Tr}(\lambda c_0) = 1$. Put $h(y) = \mathrm{Tr}(\lambda y^3)$. The exponents $3 \cdot 2^i \bmod (2^n - 1)$, $0 \le i < n$, are distinct because the 2-cyclotomic coset of 3 has size n; each is a cyclic shift of a binary word of weight two. Since every trace-expansion coefficient λ^{2^i} is nonzero, the unique reduced univariate representation of h has algebraic degree exactly two. Equation (8) gives $\sum_{x \in A} h(G_n(x)) = 1$. On the other hand, $\sum_{x \in A} G_n(x) = p_3 + p_1 = 0$, so every linear Boolean component has zero sum; a constant term also sums to zero because $|A| = 8$. Thus every affine 3-flat has exact local threshold two.

Because $3 \mid n$, the field K contains $\mathbb{F}_8$ as a 3-dimensional subspace. Cubing permutes $\mathbb{F}_8$, and hence the image of this flat under F_n is $\mathbb{F}_8$. Its indicator has degree $n - 3$, yielding local threshold three. Since F_n is a permutation, every odd image is nonempty, and the general upper bound $\tau_3 \le 3$ completes the proof. □

The theorem already rules out treating τ_3 as a scalar attached to an APN EA class. It is not an artificial high-codimension effect: (8) holds on every affine 3-flat. Conversely, it does not supply two permutations. Known classifications of Gold functions plus linearized perturbations show that permutation mates in this route collapse to affine translations [LW11]. The complete-mapping family in Section 5 addresses the permutation requirement.

5 EA-Equivalent Differentially 4-Uniform Permutations

5.1 The complete-mapping construction

Let $r \ge 3$ be odd, $q = 2^r$, and $K = \mathbb{F}_{q^2} = \mathbb{F}_{2^{2r}}$. Choose either nontrivial cube root $u \in K$, so $u^2 + u + 1 = 0$, and choose $b \in K^*$ with

$$b^{q-1} = u.$$

Such b exists because $u^{q+1} = 1$. Since $q \equiv 2 \pmod 3$, $u \notin \mathbb{F}_q$ and $u^q = u^2$. Define

$$C_b(x) = b^{-1} x^{q+2}, \qquad F_b = C_b^{-1}, \qquad J_b = C_b + \mathrm{id}, \qquad G_b = F_b + \mathrm{id}\,. \tag{9}$$

Complete mappings of finite fields are classical [NR82]. The parameter row used here is due to Bassalygo and Zinoviev [BZ15]; recent classification work places it in a broader four-term class [DXZ26]. Neither the existence of the family nor that classification is a contribution of this paper.

Proposition 2 (Consequences of the known complete-mapping construction)**.** *For the parameters above, F_b and G_b are EA-equivalent permutations, and both have differential uniformity exactly four.*

Proof. Put $H_b(x) = x^{q+2} + bx$. The complete-permutation theorem [BZ15] applies because $r > 1$ is odd, $b \notin \mathbb{F}_q$, and $b^{3(q-1)} = 1$. Hence both $C_b = b^{-1}x^{q+2}$ and $J_b = b^{-1}H_b = C_b + \mathrm{id}$ permute K. As

$$G_b = J_b \circ C_b^{-1} = F_b + \mathrm{id},$$

G_b is a permutation and the last equality is the explicit EA relation.

The exponent $q + 2 = 2(2^{r-1} + 1)$ is a Frobenius rotation of a Gold exponent. Its nonzero derivative has kernel of size $2^{\gcd(r-1,2r)} = 4$, so C_b is differentially 4-uniform. Inversion transposes the difference distribution table, giving the same uniformity for F_b. Finally, the identity $D_aG_b(x) = D_aF_b(x) + a$ translates derivative outputs and preserves their multiplicities. □

The permutation property is inherited from the complete-mapping construction; the displayed EA relation and differential consequences are the exact facts needed below. In particular, the two representatives have the same differential uniformity but, as we show below, different affine-input profiles.

5.2 The source profile

The source side is comparatively direct because $F_b^{-1} = C_b$ is a quadratic monomial. For $\lambda \in K$, its component is

$$Q_\lambda(x) = \mathrm{Tr}(\lambda b^{-1}x^{q+2}).$$

Theorem 3 (Exact source profile)**.** *For every odd $r \geq 3$, every admitted b, and $1 \leq c \leq r - 1$,*

$$\deg \prod_{i=1}^{c} (\varepsilon_i + Q_{\lambda_i}) = 2c$$

for every independent $\lambda_1, \ldots, \lambda_c$ and every $\varepsilon \in \mathbb{F}_2^c$. Consequently

$$\mu_c(F_b) = 2c, \qquad \tau_{2r-c}(F_b) = 2r - 2c.$$

Proof. Absorb the nonzero scalar b^{-1} into the component parameters. In the trace-product expansion, select Frobenius rows $0, 1, \ldots, c - 1$. The exponent

$$E = (q + 2)(1 + 2 + \cdots + 2^{c-1}) = (q + 2)(2^c - 1)$$

has two disjoint binary blocks because $c < r$, and hence binary weight $2c$. Its coefficient is the consecutive Moore determinant

$$\det\left(\lambda_i^{2^j}\right)_{0 \leq j < c,\ 1 \leq i \leq c},$$

which is nonzero precisely when the λ_i are independent [LN97].

For completeness of this coefficient, view a cyclic rotation of $q + 2$ as an edge with support $\{j + 1, j + r\}$ modulo $2r$. These edges form two r-cycles because $\gcd(r - 1, 2r) = 2$. The selected $c < r$ edges form a proper matching; a second maximum-weight contribution to the same exponent would be a second matching on the same proper path, which is impossible. Any carry lowers the binary weight. The product therefore has degree at least $2c$, and quadraticity gives the reverse inequality. Constants contribute only proper products, so they cannot cancel the degree-$2c$ layer. Apply Proposition 1. □

The mate side is harder: G_b^{-1} is nonmonomial, and μ_c requires a lower bound for every independent component space, not merely one product of high degree.

6 Generalized-Degree Duality and the Mate Upper Bound

The relation $G_b = J_b \circ C_b^{-1}$ gives

$$G_b^{-1} = C_b \circ J_b^{-1} = \mathrm{id} + J_b^{-1}. \tag{10}$$

This identity separates a linear part from the inverse of the quadratic permutation J_b.

6.1 Known duality mechanism

The exact source analysis in Theorem 3 shows that products of s independent components of C_b have degree $2s$ for $1 \le s \le r-1$. Adding the identity does not change their highest quadratic layer, so the same family-specific calculation gives

$$\delta_s(J_b) = 2s, \qquad 1 \le s \le r-1.$$

We now feed this exact profile into Boura–Canteaut inverse generalized-degree duality. In their notation [BC13, Definition 3.1 and Theorem 3.1, p. 693],

$$\delta_\ell(T^{-1}) < 2r - k \quad \Longleftrightarrow \quad \delta_k(T) < 2r - \ell.$$

This strict duality yields the specialization

$$\delta_s(J_b^{-1}) = r + \left\lfloor \frac{s}{2} \right\rfloor, \qquad 1 \le s \le 2r-3. \tag{11}$$

Indeed, put $k_- = \lfloor (2r-s-1)/2 \rfloor$. Then $\delta_{k_-}(J_b) = 2k_- < 2r - s$, so strict duality and integrality give

$$\delta_s(J_b^{-1}) \le 2r - k_- - 1 = r + \left\lfloor \frac{s}{2} \right\rfloor.$$

For $s \ge 2$, put $k_+ = \lceil (2r-s)/2 \rceil \le r-1$. Now $\delta_{k_+}(J_b) = 2k_+ \ge 2r - s$, so the right-hand strict inequality fails and duality gives $\delta_s(J_b^{-1}) \ge 2r - k_+ = r + \lfloor s/2 \rfloor$. For $s = 1$, the same calculation gives the upper bound r, which is all that Proposition 3 needs. The matching lower bound is the range-free $c = 1$ coefficient identity (20) proved in Section 7.3; the linear conjugacy in Section 6.2 transfers it from J_u^{-1} to every J_b^{-1}. Thus the duality principle is inherited, while equality for this J_b also uses the exact source information and coefficient calculation proved here.

Proposition 3 (Mate product upper bound)**.** *For $1 \le c \le r-1$, every product of c components of G_b^{-1} has degree at most $r + c - 1$. Every product of $j < c$ components has degree at most $r + j - 1$.*

Proof. Expand the product using (10). A term with $s \ge 1$ components from J_b^{-1} and $c - s$ linear components has degree at most

$$\delta_s(J_b^{-1}) + c - s = r + c - \left\lceil \frac{s}{2} \right\rceil \le r + c - 1$$

by (11). The all-linear term has degree at most c. The same calculation applies to every proper product. □

This proposition proves

$$\mu_c(G_b) \le r + c - 1,$$

but not equality: δ_c is a maximum, whereas μ_c is a minimum over every independent component tuple and every offset. The remaining task is to exhibit, uniformly for each tuple, at least one nonzero coefficient of weight $r + c - 1$.

6.2 Normalized inverse

The coefficient calculation can be normalized without losing any parameter. Since $u^{q-1} = u$, the relation $b^{q-1} = u$ implies $(b/u)^{q-1} = 1$. Hence write $b = u\alpha$ with $\alpha \in \mathbb{F}_q^*$, and choose the unique $t \in \mathbb{F}_q^*$ satisfying $t^2 = \alpha$. Since

$$H_b(tx) = t^3 H_u(x), \qquad H_b(x) = x^{q+2} + bx,$$

we also have $J_b(tx) = tJ_u(x)$. Thus J_b and J_u are linearly conjugate, so their generalized component degrees, and those of their inverses, agree. The input/output scalings are invertible $\mathbb{F}_2$-linear maps, and it suffices to analyze $b = u$.

For this normalization, let

$$R(y) := G_u^{-1}(y) = y + uH_u^{-1}(y), \qquad w = \mathrm{N}_{K/\mathbb{F}_q}(y).$$

Direct inversion of the norm map gives

$$R(y) = yS(w), \qquad S(w) = 1 + u\,\frac{\mathcal{A}(w)^2 + u^2\mathcal{A}(w) + u}{w}, \qquad \mathcal{A}(w) = (1+w)^{(2q-1)/3}. \tag{12}$$

The numerator in the quotient has zero constant term, and the quotient is taken before reduction modulo $w^q - w$. Formula (12) is used only to extract complete reduced coefficients; the finite validations are not premises of the proof.

For a direct substitution check, write $A = \mathcal{A}(w)$. Since cubing permutes $\mathbb{F}_q$, $A^3 = 1 + w$, and hence

$$w = (A+1)(A+u)(A+u^2), \qquad A^2 + u^2A + u = (A+1)(A+u).$$

For $w \neq 0$, the evaluated quotient in (12) equals $1/(A+u^2)$. At $w = 0$, the quotient polynomial takes its constant-coefficient value u^2 because $(2q-1)/3$ is odd; since $A = 1$ there, this is again $1/(A+u^2)$. Consequently $S(w) = (A+1)/(A+u^2)$. The denominator never vanishes because $A \in \mathbb{F}_q$ whereas $u^2 \notin \mathbb{F}_q$. If $x = y/(A+u^2)$, then

$$\mathrm{N}(x) = \frac{w}{(A+u)(A+u^2)} = A + 1, \qquad H_u(x) = x\big(\mathrm{N}(x) + u\big) = x(A+u^2) = y.$$

Finally $y + ux = yS(w)$, proving pointwise that the displayed R is G_u^{-1}.

For $\lambda \in K$, write

$$f_\lambda(y) = \mathrm{Tr}(\lambda R(y)) = L_\lambda(y) + U_\lambda(y), \quad L_\lambda(y) = \mathrm{Tr}(\lambda y), \quad U_\lambda(y) = \mathrm{Tr}(\lambda J_u^{-1}(y)).$$

The next section constructs the required coefficient of $\prod_i f_{\lambda_i}$.

7 The Linear-Range Moore–Plücker Hierarchy

Theorem 4 (Exact mate hierarchy)**.** *Let r be odd, choose either nontrivial cube root $u \in K$, and let b be any admitted parameter satisfying $b^{q-1} = u$. For*

$$1 \le c \le \left\lfloor \frac{r-3}{2} \right\rfloor,$$

every independent $\lambda_1, \ldots, \lambda_c \in K$ and every $\varepsilon \in \mathbb{F}_2^c$ satisfy

$$\deg \prod_{i=1}^{c} \big(\varepsilon_i + \mathrm{Tr}(\lambda_i G_b^{-1})\big) = r + c - 1. \tag{13}$$

Consequently, $\mu_c(G_b) = r + c - 1$.

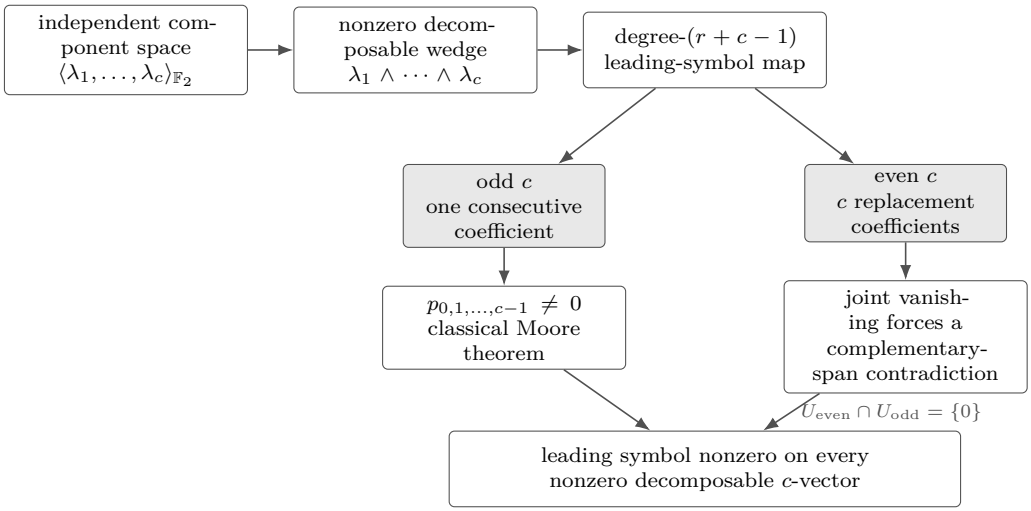

Figure 2: Architecture of the family-specific lower certificate. The only nonvanishing theorem used for a Moore determinant is the classical consecutive-row result. The nonconsecutive even-c minors are used jointly through complementary spans, not asserted individually to be Moore exponent sets. The conclusion is nonvanishing on decomposable wedges; injectivity of the full leading-symbol map is neither used nor claimed.

The interpretation is uniform: every affine codimension-c image indicator has the same degree throughout the stated range. The proof has six parts: the known upper bound in Proposition 3, an associated-graded reduction, a complete coefficient classification, separate odd/even detectors, joint nonvanishing, and transfer to offsets and all b. Figure 2 shows this architecture.

7.1 Associated-graded leading symbol

Let

$$\mathcal{B}_{2r} = \mathbb{F}_2[x_1, \ldots, x_{2r}]/(x_i^2 - x_i)$$

with the algebraic-degree filtration $F_d\mathcal{B}_{2r}$. Its associated graded algebra is

$$\mathrm{gr}(\mathcal{B}_{2r}) \cong \mathbb{F}_2[x_1, \ldots, x_{2r}]/(x_i^2).$$

Thus Boolean reduction may lower degree, but a lowered term cannot re-enter the target graded layer. In characteristic two this square-zero commutative algebra is the exterior algebra on its degree-one generators.

By (11), a product of s functions U_λ has degree at most $r + \lfloor s/2 \rfloor$. After multiplication by $c - s$ linear factors, the degree is at most

$$r + c - \left\lceil \frac{s}{2} \right\rceil.$$

Hence only the one-U and two-U blocks can reach degree $r + c - 1$:

$$\Phi_{r,c}(\lambda_1 \wedge \cdots \wedge \lambda_c) = \mathrm{Top}_{r+c-1}\Bigg(\sum_i U_{\lambda_i} \prod_{j \neq i} L_{\lambda_j} + \sum_{i<j} U_{\lambda_i} U_{\lambda_j} \prod_{k \neq i,j} L_{\lambda_k} \Bigg). \tag{14}$$

Here products are reduced in the Boolean algebra before the top symbol is taken. If two component parameters agree, idempotence reduces the full product to a proper product, whose degree is at most $r + c - 2$ by Proposition 3. Therefore (14) is alternating and defines

$$\Phi_{r,c} : \Lambda^{c}_{\mathbb{F}_2} K \longrightarrow F_{r+c-1}\mathcal{B}_{2r}/F_{r+c-2}\mathcal{B}_{2r}.$$

The desired lower bound is exactly that its kernel contains no nonzero decomposable c-vector.

7.2 Complete coefficient and carry classification

For a c-element row set $I \subseteq \{0, \dots, 2r-1\}$ containing 0, set

$$P_I = \sum_{i \in I} 2^i, \qquad E_I = 2^{2r-1} - 2^{r-1} + P_I - 1,$$

and define the Frobenius minor

$$p_I(\lambda_1, \dots, \lambda_c) = \det(\lambda_j^{2^i})_{i \in I,\ 1 \le j \le c}.$$

This is a K-valued Plücker linear form after scalar extension. For a polynomial function on K, the notation $[y^E]$ below refers to its unique reduced representative of degree below 2^{2r}. Thus a coefficient identity must account for every exponent alias modulo $2^{2r} - 1$ on K^*, as well as the value at zero; selecting one convenient unreduced term would not suffice.

Lemma 1 (Pure detector coefficients)**.** *Assume $c \ge 2$ and $r \ge 2c + 3$, and put $I_c^\circ = \{0, 1, \dots, c-1\}$.*

1. If c is odd, then

$$[y^{E_{I_c^\circ}}] \prod_{j=1}^{c} f_{\lambda_j}(y) = p_{I_c^\circ}(\lambda).$$

2. If c is even, then for every odd $i \in \{1, 3, \dots, c-1\}$ and $k \in \{c, c+1\}$,

$$[y^{E_{I_{i,k}}}] \prod_{j=1}^{c} f_{\lambda_j}(y) = p_{I_{i,k}}(\lambda), \quad I_{i,k} = (I_c^\circ \setminus \{i\}) \cup \{k\}.$$

Every equality is a complete coefficient identity modulo $2^{2r} - 1$, and the scalar is one for either choice of u.

Proof. We prove coefficient completeness, not merely the existence of one favorable term in the trace expansion.

Step 1: reduced Frobenius classes. Fix one of the row sets I in the statement and abbreviate $P = P_I$. A distinct Frobenius row class J in the trace expansion splits into a lower half and a conjugate upper half,

$$A = \sum_{\substack{j \in J \\ j < r}} 2^j, \qquad B = \sum_{r + j \in J} 2^j.$$

Its ordinary Frobenius exponent is $A + qB$. Since $q \equiv -1 \pmod{q+1}$ and $E_I \equiv P \pmod{q+1}$, a class can reach the target only if

$$A - B = P + \kappa(q+1). \tag{15}$$

The bounds $0 \le A, B \le q-1$ exclude all translates except $\kappa = 0, -1$. For the negative translate, write $B = q - t$. The selected row patterns satisfy $P < 2^{c+2}$, hence $1 \le t < 2^{c+2}$ and

$$\mathrm{wt}_2(B) = r - \mathrm{wt}_2(t-1), \qquad \mathrm{wt}_2(A) + \mathrm{wt}_2(B) \ge r - (c+2) > c,$$

so the negative translate requires more than the available c rows. Only $\kappa = 0$ remains. Consequently $A = P + B$, and the requirement that the class use exactly c rows is

$$\mathrm{wt}_2(B) + \mathrm{wt}_2(P + B) = c. \tag{16}$$

Step 2: complete norm-coefficient extraction. Passing the signed filter is only the first half of the reduction. The norm $w = y^{q+1}$ contributes exponents in multiples of $q+1$, so equality with E_I modulo $(q-1)(q+1)$ still requires reduction modulo $q-1$. Reverse coefficient extraction from (12) gives

$$\alpha = \langle 2P + 1 + 6B \rangle_{q-1}, \qquad D = 2P - 1,$$

where $\langle \cdot \rangle_{q-1}$ is the positive residue in $\{1, \dots, q-1\}$. The range ensures $D < q - 1$. Summing the entire Laurent class, rather than choosing one term, yields

$$\sum_{T \in u + \mathbb{F}_q} (T + u^2)^{\alpha} T^{-D} (T+1) = \binom{\alpha}{D-1} (u^2)^{\alpha - D + 1}. \tag{17}$$

Here positive powers below $q-1$ sum to zero over $\mathbb{F}_q$, reciprocal powers T^{-j} for $1 \le j \le D$ sum to one, and adjacent terms cancel. Lucas' theorem now turns the remaining binomial coefficient into the bitwise condition

$$M := 2P - 2 \quad \preceq_2 \quad \alpha. \tag{18}$$

This establishes the exact scalar attached to every class that survived Step 1.

Step 3: the cyclic carry system. It remains to solve (16) and (18) simultaneously. Write χ_j and b_j for the bits of $2P+1$ and B, respectively, g_j for the end-around carry, and α_j for the output bit. Because multiplication by 2 and 4 rotates bits modulo $2^r - 1$,

$$s_j = \chi_j + b_{j-1} + b_{j-2} + g_j, \quad \alpha_j = s_j \bmod 2, \quad g_{j+1} = \left\lfloor \frac{s_j}{2} \right\rfloor, \tag{19}$$

with $b_{-1} = b_{r-1}$, $b_{-2} = b_{r-2}$, and $g_r = g_0$. The condition $g_r = g_0$ is the end-around boundary condition; it cannot be replaced by an ordinary zero initial carry. The carry g_j lies in $\{0, 1, 2\}$. With $\sigma = \chi_j + b_{j-1} + b_{j-2}$, every local transition is listed in

σ	$g_j = 0 : (\alpha_j, g_{j+1})$	$g_j = 1 : (\alpha_j, g_{j+1})$	$g_j = 2 : (\alpha_j, g_{j+1})$
0	$(0,0)$	$(1,0)$	$(0,1)$
1	$(1,0)$	$(0,1)$	$(1,1)$
2	$(0,1)$	$(1,1)$	$(0,2)$
3	$(1,1)$	$(0,2)$	$(1,2)$

(T)

For example, the middle entry in the row $\sigma = 2$ reads: an incoming carry $g_j = 1$ gives $s_j = 3$, hence $(\alpha_j, g_{j+1}) = (1,1)$. At a position with $M_j = 1$, Lucas' condition keeps only entries with $\alpha_j = 1$.

In parallel, write p_j, a_j for the bits of P, A and e_j for the ordinary carry in $A = P + B$. Then

$$p_j + b_j + e_j = a_j + 2e_{j+1}, \qquad e_0 = e_r = 0.$$

Define $W_j := \sum_{\ell < j} (a_\ell + b_\ell)$. Then (16) requires the terminal cost $W_r = c$. The local state $(b_{j-2}, b_{j-1}, e_j, g_j, W_j)$ therefore defines a finite cyclic path problem with fixed initial/terminal ordinary carry, cyclic b-history and cyclic g-feedback.

Step 4: classification of surviving paths. The quantity being minimized is the row cost W_r; only paths of cost exactly c represent a distinct c-row class. We make the finite-state induction explicit. Put

$$\Delta_j = W_j - \sum_{\ell<j} p_\ell.$$

Every selected row set has $\mathrm{wt}_2(P) = c$, so the required terminal condition is $\Delta_r = 0$.

Tail invariant. On a zero column, the ordinary and cyclic tables determine the next state from $(b_{j-2}, b_{j-1}, e_j, g_j, \Delta_j)$ and the single choice b_j. Running this recurrence backward from $e_r = 0$ and $g_r = g_0$ gives

(b_{r-2}, b_{r-1}, g_0)	minimum possible terminal excess
$(0,0,0)$	0
any other feedback boundary	≥ 2

The base check substitutes the twelve triples $(b_{r-2}, b_{r-1}, g_0) \in \mathbb{F}_2^2 \times \{0,1,2\}$ into the displayed cyclic table and the binary-addition recurrence. Prepending one further zero column preserves the two bounds: the zero state maps only to itself at excess zero, whereas every other admissible predecessor either pays at least two units or remains in the second row. This is the backward-induction invariant. Since $r \geq 2c+3$ supplies a zero tail beyond all detector and Lucas bits, every nonzero-feedback path has $W_r \geq c+2$ and cannot contribute. Hence a cost-c path enters the low run with $(b_{r-2}, b_{r-1}, e_0, g_0, \Delta_0) = (0,0,0,0,0)$.

Run invariant. For the baseline pattern, $p_j = 1$ on $0 \leq j < c$, while the Lucas mask is mandatory on bits $2, \ldots, c$. Backward pruning from the terminal constraints leaves exactly the following forward continuation graph:

state $(b_{j-2}, b_{j-1}, e_j, g_j, \Delta_j)$	b_j	next state
$Z = (0,0,0,0,0)$	0	Z
Z	1	$A_{\mathrm{in}} = (0,1,1,0,0)$ $\quad (j=0 \text{ only})$
A_{in}	0	$A_- = (1,0,1,1,-1)$ $\quad (j=1 \text{ only})$
A_-	1	$A_+ = (0,1,1,1,0)$
A_+	0	A_-

The base of the backward pruning is the mandatory bit at position c. Each listed forward transition follows by direct substitution in the two recurrences; every omitted choice has no continuation to $\Delta_r = 0$. Thus the only branches are $B = 0$ and the alternating word $b_{2j} = 1, b_{2j+1} = 0$. Along the latter branch the prefix excess alternates between 0 and -1. It closes with $\Delta_r = 0$ exactly when c is even, in which case

$$B = 1 + 2^2 + \cdots + 2^{c-2} = \frac{2^c - 1}{3}.$$

For odd c, the terminal ordinary carry contributes one additional row, so $W_r = c+1$.

Defect and terminal. Now let $P = 2^c - 1 - 2^i + 2^k$, with i odd and $k \in \{c, c+1\}$. The zero branch remains admissible. The run graph leaves only the same alternating candidate. If $k = c+1$, its ordinary row cost is $c+1$. If $k = c$, the cost is also $c+1$ when $i = c-1$; for $i \leq c-3$ it has cost c, but the cyclic recurrence gives $\alpha_{c+1} = 0$ while $(2P-2)_{c+1} = 1$, contradicting Lucas' condition. Thus the alternating branch never survives a replacement detector. Since the run graph contains no third branch, $B = 0$ is the unique replacement survivor.

The complete survivor classification is therefore

P	surviving B
$2^c - 1$	0, and $(2^c-1)/3$ iff c is even
$2^c - 1 - 2^i + 2^k$, i odd, $k \in \{c, c+1\}$	0

For odd c, the baseline coefficient is therefore the sole minor $p_{I_c^\circ}$. For even c, the baseline has one additional minor and is deliberately not used. Each replacement pattern has only $B = 0$ and hence the pure minor in the statement. Repeated rows have zero target coefficient by alternation of (14). Steps 1–4 account for every alias modulo $(q-1)(q+1) = 2^{2r} - 1$ and prove the claimed scalar one for either cube root. □

Illustration at $c = 4$. At the smallest boundary instance $r = 11$, the low five bits already display the general even-c obstruction:

row set I	P_I	cost-four survivors B	coefficient consequence
$\{0,1,2,3\}$	$(01111)_2$	$(00000)_2, (00101)_2$	baseline plus one extra minor
$\{0,2,3,4\}$	$(11101)_2$	$(00000)_2$	pure replacement minor $p_{\{0,2,3,4\}}$

The alternating word $(00101)_2$ is the value $(2^4 - 1)/3$ from the run step. Omitting the odd row 1 and inserting row 4 creates the defect that destroys this path. This is an illustration only; the preceding state argument is valid for arbitrary admitted c and r. Purity also does not assert that this individual replacement minor is always nonzero—the even-c proof uses the full joint detector family.

7.3 Odd codimensions: one classical Moore detector

Assume c is odd. The selected exponent is

$$E_{I_c^\circ} = 2^{2r-1} - 2^{r-1} + 2^c - 2.$$

Its support is the disjoint union of $\{1, \dots, c-1\}$ and $\{r-1, \dots, 2r-2\}$, so its binary weight is $r + c - 1$. By Lemma 1, its complete coefficient is

$$p_{I_c^\circ}(\lambda) = \det \begin{pmatrix} \lambda_1 & \cdots & \lambda_c \\ \lambda_1^2 & \cdots & \lambda_c^2 \\ \vdots & & \vdots \\ \lambda_1^{2^{c-1}} & \cdots & \lambda_c^{2^{c-1}} \end{pmatrix}.$$

These are consecutive Frobenius rows. The classical Moore theorem says that the determinant is nonzero exactly when $\lambda_1, \dots, \lambda_c$ are independent over $\mathbb{F}_2$ [LN97]. No generalized or nonconsecutive Moore criterion is invoked.

The case $c = 1$ is separate from Lemma 1 and is valid for every odd $r \geq 3$. Here $I = \{0\}$ and $P = 1$. For a one-row Frobenius class, the signed filter leaves only $A = 1, B = 0$. The derivation of the Laurent-sum identity (17) remains valid here because $D = 1 < q - 1$; with $\alpha = 3$, its scalar is $\binom{3}{0}(u^2)^3 = 1$. Therefore

$$[y^{2^{2r-1}-2^{r-1}}] f_\lambda(y) = p_{\{0\}}(\lambda) = \lambda \qquad (r \geq 3 \text{ odd}). \tag{20}$$

The target exponent has binary weight r. Since L_λ is linear, this is also a degree-r coefficient of U_λ for every $\lambda \neq 0$, proving the $s = 1$ lower bound used in (11) without the assumptions $c \geq 2$ or $r \geq 2c + 3$.

7.4 Even codimensions: a joint detector family

Suppose c is even. One baseline detector does not suffice: the alternating carry path in the proof of Lemma 1 gives a genuine second minor. Instead, use the c replacement detectors

$$p_{(I_c^\circ \setminus \{i\}) \cup \{k\}}, \qquad i \in \{1, 3, \dots, c-1\}, \quad k \in \{c, c+1\}.$$

Each is a complete coefficient of weight $r + c - 1$ by the lemma.

Lemma 2 (Joint replacement-minor nonvanishing)**.** *For every independent $\lambda_1, \dots, \lambda_c$, at least one of the c replacement minors above is nonzero.*

Proof. Put

$$v_j = (\lambda_1^{2^j}, \dots, \lambda_c^{2^j}) \in K^c.$$

The consecutive Moore theorem makes $v_0, \dots, v_{c-1}$ a K-basis. Split that basis into the complementary spans

$$U_{\text{even}} = \operatorname{span}_K(v_0, v_2, \dots, v_{c-2}), \qquad U_{\text{odd}} = \operatorname{span}_K(v_1, v_3, \dots, v_{c-1}).$$

They have dimension $c/2$ and intersect only at zero.

Assume all replacement minors vanish. Write $v_c = \sum_{j=0}^{c-1} a_j v_j$. Replacing baseline row i by v_c gives $a_i p_{I_c^\circ}$. The contradiction can therefore be read as the following chain:

$$\begin{aligned} \text{all } k = c \text{ replacements vanish} &\implies v_c \in U_{\text{even}}, \\ \text{componentwise squaring} &\implies v_{c+1} = v_c^2 \in U_{\text{odd}}, \\ \text{all } k = c+1 \text{ replacements vanish} &\implies v_{c+1} \in U_{\text{even}}, \\ U_{\text{even}} \cap U_{\text{odd}} = \{0\} &\implies v_{c+1} = 0. \end{aligned}$$

The last conclusion forces every $\lambda_j = 0$ and contradicts their independence. Crucially, the conclusion comes from simultaneous vanishing of each detector family; no individual nonconsecutive replacement minor is asserted to be universally nonzero. □

The replacement minors are not claimed to be Moore exponent sets. Their role is joint and elementary once the consecutive baseline is known to be a basis.

7.5 Offsets, parameter transfer, and completion

The odd and even arguments prove that every homogeneous full c-product has a nonzero degree-$(r + c - 1)$ coefficient. Expanding affine offsets adds only products of $j < c$ components. By Proposition 3, each has degree at most $r + j - 1 \le r + c - 2$ and therefore cannot cancel the certified top layer.

Finally, write $b = u\alpha$ and $t^2 = \alpha$ as in Section 6. Direct substitution gives

$$G_b^{-1}(tu^2 z) = tu^2 R(z).$$

Both multipliers are invertible $\mathbb{F}_2$-linear maps. They preserve algebraic degree, component independence, and every affine offset. Thus the normalized proof covers both cube roots and every admitted b. Proposition 3 supplies the matching upper bound, proving Theorem 4.

Corollary 1 (Exact linear-range EA profile separation)**.** *For every parameter choice in (9), odd r, and $1 \le c \le \lfloor (r-3)/2 \rfloor$,*

$$\begin{aligned} \tau_{2r-c}(F_b) &= 2r - 2c, \\ \tau_{2r-c}(G_b) &= r - c + 1, \\ \Delta_{r,c} := \tau_{2r-c}(F_b) - \tau_{2r-c}(G_b) &= r - c - 1 \ge \frac{r+1}{2}. \end{aligned}$$

Proof. Combine Proposition 1 and Theorems 3 and 4. The last inequality follows from $c \le (r-3)/2$. □

The range condition $r \ge 2c + 3$ is used to keep the detector rows below the high target block, exclude the negative signed translate in (15), and bound nonzero cyclic feedback. Equality is valid. Beyond this range the low rows approach the conjugate Frobenius half; the proof does not extend, and no value is asserted for the mate.

Table 4: Exact complete-mapping profiles. The common linear range is $1 \le c \le \lfloor (r-3)/2 \rfloor$; the wider source range is shown only to separate what is known on the two sides. In the last row, $\mu_c(G_b) - \mu_c(F_b) = \tau_{2r-c}(F_b) - \tau_{2r-c}(G_b) = r - c - 1$.

Representative	μ_c	τ_{2r-c}	proved range
F_b	$2c$	$2r-2c$	$1 \le c \le r-1$
G_b	$r+c-1$	$r-c+1$	$1 \le c \le \lfloor (r-3)/2 \rfloor$
Gap magnitude	$r-c-1$	$r-c-1$	common range

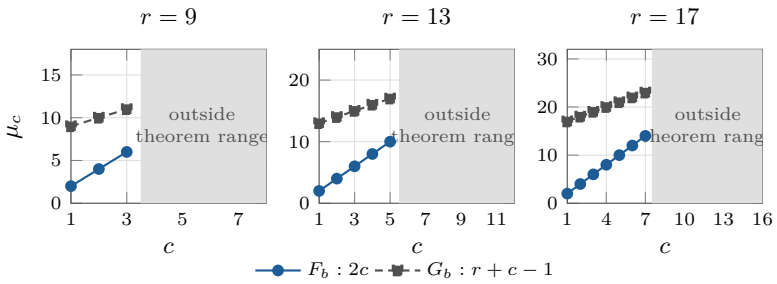

Figure 3: Exact profile separation for representative odd r. Only $1 \le c \le \lfloor (r-3)/2 \rfloor$ is plotted as a theorem. The shaded region is deliberately not extrapolated. The vertical gap is $\mu_c(G_b) - \mu_c(F_b) = r - c - 1$, equal to $\tau_{2r-c}(F_b) - \tau_{2r-c}(G_b)$.

8 Cryptographic Interpretation and Limitations

The exact profile in Corollary 1 has a deliberately local interpretation. If an affine input set has dimension $2r - c$, then its image under a permutation is described by an indicator of degree at least μ_c. Through (1), this degree determines the lowest degree at which a Boolean output test can have odd parity on that one image. The theorem therefore compares two descriptions of a single S-box transition under affine inputs. It does not compose these local numbers across rounds.

Three consequences are justified. First, degree-sum-freedom with output degree greater than one is not an invariant of an EA class: even natural APN maps and differentially 4-uniform permutations exhibit exact separations. Second, differential uniformity does not determine this affine-input profile; F_b and G_b share differential uniformity four while their values differ by $r - c - 1$. Third, the discrepancy is not confined to hyperplanes. It persists simultaneously for every codimension in a range of size $\lfloor (r-3)/2 \rfloor$, with a gap that remains linear in r.

These statements do not order the two representatives by security. A larger or smaller local threshold can interact with round functions, linear layers, key additions, and chosen integral distinguishers in ways not modeled here. In particular, the proof gives none of the following: a propagation rule for arbitrary multiround affine sets, a trail through a concrete design, a data or time complexity, or a key-recovery consequence. The family is used as a controlled separation theorem, not proposed as a cipher component.

The theorem also has a sharp proof boundary. It covers $1 \le c \le \lfloor (r-3)/2 \rfloor$ and no larger codimension. The carry argument uses $r \ge 2c + 3$ at three distinct points summarized at the end of Section 7; a pattern observed at a tested endpoint would not replace those inequalities. Determining the remaining profile of G_b, or finding a different uniform certificate there, is open. Likewise, the present coefficient method is family-specific. Generalized-degree duality explains the upper bound, but the matching lower bound relies on the normalized inverse (12), its cyclic carry system, and the joint replacement-minor cover.

From a design-analysis perspective, the practical lesson is methodological: when a division-property summary permits nonlinear output tests, an EA addition must be analyzed through all mixed products. Affine equivalence remains safe for the scalar because it only relabels affine input sets and output coordinates. EA equivalence is too coarse unless an additional condition rules out the mixed terms, as in (7).

9 Conclusion

We showed that the published EA-invariance assertion for degree-sum-freedom does not hold beyond ordinary sum-freedom and developed two exact, structured separations. The Gold pair x^3, x^3+x shows the phenomenon within an APN EA class on proper affine 3-flats. The complete-mapping pair F_b, G_b strengthens it to EA-equivalent, differentially 4-uniform permutations and to a linear range of codimensions. For odd r and $1 \le c \le \lfloor (r-3)/2 \rfloor$, their exact profiles are

$$\mu_c(F_b) = 2c, \qquad \mu_c(G_b) = r + c - 1,$$

or, equivalently,

$$\tau_{2r-c}(F_b) = 2r - 2c, \qquad \tau_{2r-c}(G_b) = r - c + 1.$$

The proof combines inherited machinery with a family-specific certificate. Generalized-degree duality supplies the mate upper bound, while the uniform lower bound reduces the leading layer to complete coefficients: odd codimensions use a consecutive Moore determinant, while even codimensions use a jointly nonvanishing family of replacement minors. A cyclic carry classification ensures that these are the complete reduced coefficients, not selected terms of an unreduced expansion.

The mate profile beyond $c = \lfloor (r-3)/2 \rfloor$ remains open. Whether a local profile distinction survives a specified round function with a useful trail and measurable complexity is a separate cryptographic question, not a consequence of this theorem. The precise methodological lesson is that an EA representative cannot in general stand in for another when a local division-property summary permits nonlinear output tests: the mixed terms must be analyzed explicitly.

References

[BC13] Christina Boura and Anne Canteaut. On the influence of the algebraic degree of F^{-1} on the algebraic degree of $G \circ F$. *IEEE Transactions on Information Theory*, 59(1):691–702, 2013. doi:10.1109/TIT.2012.2214203.

[BC16] Christina Boura and Anne Canteaut. Another view of the division property. In *Advances in Cryptology – CRYPTO 2016, Part I*, volume 9814 of *Lecture Notes in Computer Science*, pages 654–682. Springer, 2016. URL: https://eprint.iacr.org/2016/554, doi:10.1007/978-3-662-53018-4_24.

[BCC11] Christina Boura, Anne Canteaut, and Christophe De Cannière. Higher-order differential properties of Keccak and Luffa. In *Fast Software Encryption – FSE 2011*, volume 6733 of *Lecture Notes in Computer Science*, pages 252–269. Springer, 2011. doi:10.1007/978-3-642-21702-9_15.

[BV23] Tim Beyne and Michiel Verbauwhede. Integral cryptanalysis using algebraic transition matrices. *IACR Transactions on Symmetric Cryptology*, 2023(4):244–269, 2023. doi:10.46586/tosc.v2023.i4.244-269.

[BZ15] Leonid A. Bassalygo and Victor A. Zinoviev. Permutation and complete permutation polynomials. *Finite Fields and Their Applications*, 33:198–211, 2015. doi:10.1016/j.ffa.2014.11.010.

[BZ20] Daniele Bartoli and Yue Zhou. Asymptotics of Moore exponent sets. *Journal of Combinatorial Theory, Series A*, 175:105281, 2020. doi:10.1016/j.jcta.2020.105281.

[Car20] Claude Carlet. Handling vectorial functions by means of their graph indicators. *IEEE Transactions on Information Theory*, 66(10):6324–6339, 2020. doi:10.1109/TIT.2020.2981524.

[Car25] Claude Carlet. Two generalizations of almost perfect nonlinearity. *Journal of Cryptology*, 38(2):20, 2025. doi:10.1007/s00145-025-09538-5.

[Car26] Claude Carlet. A notion on S-boxes for a partial resistance to some integral attacks. In *Arithmetic of Finite Fields – WAIFI 2026*, volume 16611 of *Lecture Notes in Computer Science*, pages 221–238. Springer, 2026. doi:10.1007/978-3-032-27574-5_14.

[CFS25a] Claude Carlet, Serge Feukoua, and Ana Sălăgean. On the algebraic degree stability of vectorial Boolean functions when restricted to affine subspaces. arXiv:2504.03307v2, 2025. URL: https://arxiv.org/abs/2504.03307, doi:10.48550/arXiv.2504.03307.

[CFS25b] Claude Carlet, Serge Feukoua, and Ana Sălăgean. The stability of the algebraic degree of Boolean functions when restricted to affine spaces. *Designs, Codes and Cryptography*, 93(11):4799–4832, 2025. URL: https://link.springer.com/article/10.1007/s10623-025-01702-z, doi:10.1007/s10623-025-01702-z.

[DXZ26] Zhiguo Ding, Wei Xiong, and Michael E. Zieve. Determination of all complete mappings of $\mathbb{F}_{q^2}$ of the form $ax^{3q} + bx^{2q+1} + cx^{q+2} + dx^3$. *International Journal of Number Theory*, 22(1):175–193, 2026. doi:10.1142/S1793042126500119.

[GRW16] Faruk Göloğlu, Vincent Rijmen, and Qingju Wang. On the division property of S-boxes. Cryptology ePrint Archive, Paper 2016/188, 2016. URL: https://eprint.iacr.org/2016/188.

[HKT26] Philipp Heering, Christian Kaspers, and Vladislav Taranchuk. On Reed–Muller subcodes, Grassmannian partitions and sum-free functions. arXiv:2605.22958, 2026. URL: https://arxiv.org/abs/2605.22958.

[HLU23] Phil Hebborn, Gregor Leander, and Aleksei Udovenko. Mathematical aspects of division property. *Cryptography and Communications*, 15(4):731–774, 2023. doi:10.1007/s12095-022-00622-2.

[Kas26] Christian Kaspers. Nonvanishing k-flats of Boolean and vectorial functions. In *Fourteenth International Workshop on Coding and Cryptography (WCC 2026)*, 2026. Extended version: arXiv:2603.28266. URL: https://wcc2026.inria.fr/assets/final_versions/WCC2026_paper_49.pdf.

[LDF20] Baptiste Lambin, Patrick Derbez, and Pierre-Alain Fouque. Linearly equivalent S-boxes and the division property. *Designs, Codes and Cryptography*, 88(10):2207–2231, 2020. doi:10.1007/s10623-020-00773-4.

[LN97] Rudolf Lidl and Harald Niederreiter. *Finite Fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, 2 edition, 1997.

[LW11] Yongqiang Li and Mingsheng Wang. On EA-equivalence of certain permutations to power mappings. *Designs, Codes and Cryptography*, 58(3):259–269, 2011. doi:10.1007/s10623-010-9406-8.

[NR82] Harald Niederreiter and Karl H. Robinson. Complete mappings of finite fields. *Journal of the Australian Mathematical Society, Series A*, 33(2):197–212, 1982. doi:10.1017/S1446788700018346.

[Nyb94] Kaisa Nyberg. Differentially uniform mappings for cryptography. In *Advances in Cryptology – EUROCRYPT '93*, volume 765 of *Lecture Notes in Computer Science*, pages 55–64. Springer, 1994. doi:10.1007/3-540-48285-7_6.

[Tod15] Yosuke Todo. Structural evaluation by Generalized Integral Property. In *Advances in Cryptology – EUROCRYPT 2015, Part I*, volume 9056 of *Lecture Notes in Computer Science*, pages 287–314. Springer, 2015. doi:10.1007/978-3-662-46800-5_12.