Advances in Mathematics of Communications
Vol. 27, 2027, 101097 (November xx, 2026)
doi:10.3934/amc.2026.101097

NON-PERMUTATION PHENOMENA IN TRIVARIATE FAMILIES OVER $\mathbb{F}_{2^m}$ AND RESOLUTION OF A CONJECTURE

Daniele Bartoli[*1], Mohit Pal[2], Pantelimon Stănică[3] and Tommaso Toccotelli[1]

[1]Department of Mathematics and Computer Science, University of Perugia, Italy

[2]Department of Informatics, University of Bergen, Norway

[3]Applied Mathematics Department, Naval Postgraduate School, USA

(Communicated by Sihem Mesnager)

Abstract. Permutation polynomials over finite fields with simple multivariate expressions are of interest in cryptography and coding theory. Li and Kaleyski (IEEE Trans. Inf. Theory, 2024) generalized two sporadic quadratic APN permutations into infinite families of trivariate APN functions. Motivated by their constructions, we study the permutation property of a related trivariate family. We reduce its non-degenerate eight-parameter form to a four-parameter model and derive polynomial conditions that imply non-permutation. For two parameter subfamilies, we obtain exact root criteria when the odd extension degree is sufficiently large relative to the Frobenius exponent. We also give a complete computational classification over $\mathbb{F}_8^3$, with exactly 20 parameter choices yielding permutations for each of the two nontrivial Frobenius automorphisms of $\mathbb{F}_8$. As an application of elimination and algebraic geometry, we prove that the trivariate function C_u introduced by Beierle et al. (Finite Fields Appl., 2022) is not a permutation of $\mathbb{F}_{2^m}^3$ for every odd $m \geq 23$ and every $u \in \mathbb{F}_{2^m}^*$. This settles the remaining permutation part of their conjecture for all odd extension degrees at least 23.

1. **Introduction.** Let $Q = 2^m$ with $m \geq 1$, and let $F : \mathbb{F}_Q^n \to \mathbb{F}_Q^n$ be a vectorial function. When F is bijective, it is a permutation and is a natural S-box candidate in symmetric cryptography. For even characteristic, differential behavior is encoded by the equations

$$F(x+a) + F(x) = b, \qquad a \in \mathbb{F}_Q^n \setminus \{0\},\ b \in \mathbb{F}_Q^n.$$

Low differential uniformity is essential for the resistance to differential cryptanalysis [7]. The differential uniformity of F is $\delta_F = \max_{a \neq 0,\, b} \#\{x \in \mathbb{F}_Q^n : F(x+a) + F(x) = b\}$. In particular, APN functions (uniformity 2) are optimal in characteristic two.

2020 *Mathematics Subject Classification.* Primary: 12E20, 11T06; Secondary: 14G15.

Key words and phrases. Finite fields, permutation polynomials, vectorial Boolean functions, algebraic geometry, algebraic varieties.

The first author is supported by the Italian National Group for Algebraic and Geometric Structures and their Applications (INdAM - GNSAGA Project, CUP E53C24001950001).

*Corresponding author: Daniele Bartoli.

Two sporadic APN permutations over $\mathbb{F}_{2^9}$ discovered by Beierle and Leander [6] triggered several trivariate generalizations. Beierle, Carlet, Leander, and Perrin [5] investigated the maps $C_u : \mathbb{F}_{2^m}^3 \to \mathbb{F}_{2^m}^3$, with $u \in \mathbb{F}_{2^m}^*$, defined by

$$C_u(X, Y, Z) = \left(X^3 + uY^2Z,\ Y^3 + uXZ^2,\ Z^3 + uX^2Y\right),$$

and conjectured that, beyond the known small-dimensional cases, this form should not yield permutations/APN functions. The APN part was settled in [2], while the permutation part remained open. Li and Kaleyski introduced two infinite trivariate APN families [12]. Bartoli and Stănică generalized these constructions by allowing coefficients in $\mathbb{F}_{2^m}^*$ and established CCZ-inequivalence results both within and between the resulting families [3]. Subsequently, Göloğlu and Kölsch [4] introduced a broader triprojective family containing these constructions up to linear equivalence. They also established CCZ-inequivalence to Gold APN functions.

We study polynomial conditions that prevent these trivariate maps from being permutations. We then apply a related elimination argument to C_u.

Main contributions.

1. We start from an 8-parameter trivariate family and prove that every non-degenerate instance is affine-equivalent to a canonical 4-parameter model (Proposition 3.1).
2. For the normalized model, we give polynomial root conditions for failure of the permutation property and exact criteria for two subfamilies (Theorems 4.1, 4.4, and 4.5).
3. For $m = 3$, we obtain a complete characterization by exhaustive computation, with exactly 20 parameter choices yielding permutations, split into two structural families (Proposition 5.1 and Table 1).
4. We prove the remaining permutation part of the Beierle–Carlet–Leander–Perrin conjecture for sufficiently large odd extension degrees. Thus, for every odd $m \geq 23$ and every $u \in \mathbb{F}_{2^m}^*$, C_u is not a permutation (Theorem 6.3).

Section 2 states the point-count estimate and component lemma. Section 3 gives the normalization. Section 4 gives the polynomial criteria, and Section 5 gives the classification over $\mathbb{F}_8$. Section 6 proves the non-permutation result for C_u. Section 7 discusses the results and open problems.

2. Preliminaries and algebraic geometry tools.

Unless explicitly stated otherwise, we work over $\mathbb{F}_{2^m}$ with m odd and $m \geq 3$, and set $q = 2^i$ with $\gcd(i, m) = 1$. All parameters belong to $\mathbb{F}_{2^m}$, and any additional nonvanishing conditions are stated in the relevant results. For a map F, we write $D_aF(x) = F(x + a) + F(x)$ when $a \neq 0$.

We use the algebraic-geometric terminology of [10, 11]. Write $\overline{\mathbb{F}_Q}$ for the algebraic closure of $\mathbb{F}_Q$, and denote by $\mathbb{P}^r(\mathbb{F}_Q)$ and $\mathbb{A}^r(\mathbb{F}_Q)$ the projective and affine spaces of dimension r over $\mathbb{F}_Q$. For an $\mathbb{F}_q$-vector space W, $\mathrm{PG}(W, q)$ denotes the set of its one-dimensional $\mathbb{F}_q$-subspaces. The solution set of a polynomial system $\mathcal{S}$ consists of its common zeros in the specified affine space over the ground field.

A variety $\mathcal{V}$ is the common zero set of finitely many polynomials. An affine $\mathbb{F}_Q$-rational variety $\mathcal{V} \subset \mathbb{A}^r(\overline{\mathbb{F}_Q})$ is defined by polynomials $F_1, \ldots, F_s \in \mathbb{F}_Q[X_1, \ldots, X_r]$. The set $\mathcal{V}(\mathbb{F}_Q) = \mathcal{V} \cap \mathbb{A}^r(\mathbb{F}_Q)$ consists of $\mathbb{F}_Q$-rational points. A variety is absolutely irreducible if it cannot be written as a union of proper subvarieties over $\overline{\mathbb{F}_Q}$.

The dimension of a variety is the maximal length of a chain of distinct, nonempty, absolutely irreducible subvarieties. Varieties of dimensions 1 and 2 are called curves

and surfaces. A hypersurface in $\mathbb{A}^r$ or $\mathbb{P}^r$ is the zero set of one nonzero nonconstant polynomial. The degree of an s-dimensional projective variety is the number of intersection points with a general projective subspace of complementary dimension.

The Frobenius map $\Phi_Q : x \mapsto x^Q$ fixes $\mathbb{F}_Q$ pointwise. It acts on affine and projective points by raising their coordinates to the Qth power and on polynomials by raising their coefficients to that power. We find $\mathbb{F}_Q$-rational points on absolutely irreducible $\mathbb{F}_Q$-rational components by applying the following Lang-Weil estimate.

Theorem 2.1 (Strengthened Lang-Weil [9, Theorem 7.1])**.** *Let $\mathcal{V} \subseteq \mathbb{A}^n(\overline{\mathbb{F}_Q})$ be an absolutely irreducible $\mathbb{F}_Q$-rational variety of dimension $r > 0$ and degree δ. If $Q > 2(r+1)\delta^2$, then*

$$\left|\#\mathcal{V}(\mathbb{F}_Q) - Q^r\right| \leq (\delta-1)(\delta-2)Q^{r-1/2} + 5\delta^{13/3}Q^{r-1}.$$

Lemma 2.2 ([1, Lemma 2.1])**.** *Let $\mathcal{H}$ be a projective hypersurface and $\mathcal{X}$ an $\mathbb{F}_Q$-rational projective variety of dimension $n-1$ in $\mathbb{P}^n(\overline{\mathbb{F}_Q})$. If $\mathcal{X} \cap \mathcal{H}$ has a non-repeated absolutely irreducible $\mathbb{F}_Q$-rational component, then $\mathcal{X}$ has a non-repeated absolutely irreducible $\mathbb{F}_Q$-rational component.*

3. **The general trivariate family.** Motivated by the Li-Kaleyski construction [12], we study the general family

$$G(x,y,z) = (c_1x^{q+1} + c_2x^qz + c_3yz^q, c_4x^qz + c_5y^{q+1}, c_6xy^q + c_7y^qz + c_8z^{q+1})$$

over $\mathbb{F}_{2^m}^3$, where $q = 2^i$ with $1 \leq i < m$ and $\gcd(i,m) = 1$, and $c_1, \ldots, c_8 \in \mathbb{F}_{2^m}$. Here two maps are called affine-equivalent if one is obtained from the other by pre- and post-composition with invertible affine maps. In this section, non-degenerate means $c_1c_4c_5c_8 \neq 0$.

Proposition 3.1. *Assume throughout this statement that all parameters lie in $\mathbb{F}_{2^m}$ under the standing hypotheses from the preliminaries. Up to affine equivalence, any non-degenerate function G with $c_1, c_4, c_5, c_8 \neq 0$ is of the normalized form*

$$G_{norm}(x,y,z) = (x^{q+1} + a_1x^qz + a_2yz^q,\ x^qz + y^{q+1},\ a_3xy^q + a_4y^qz + z^{q+1}),$$

where $a_1, a_2, a_3, a_4 \in \mathbb{F}_{2^m}$ are free parameters.

Proof. Consider affine transformations consisting of input scaling

$$(x,y,z) \mapsto (\lambda_1x, \lambda_2y, \lambda_3z),$$

where $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{F}_{2^m}^*$, and output scaling by $\mu_1, \mu_2, \mu_3 \in \mathbb{F}_{2^m}^*$. Under these transformations, G becomes

$$\begin{aligned} G'(x,y,z) = \big(&\mu_1c_1\lambda_1^{q+1}x^{q+1} + \mu_1c_2\lambda_1^q\lambda_3x^qz + \mu_1c_3\lambda_2\lambda_3^qyz^q,\\ &\mu_2c_4\lambda_1^q\lambda_3x^qz + \mu_2c_5\lambda_2^{q+1}y^{q+1},\\ &\mu_3c_6\lambda_1\lambda_2^qxy^q + \mu_3c_7\lambda_2^q\lambda_3y^qz + \mu_3c_8\lambda_3^{q+1}z^{q+1}\big). \end{aligned}$$

We construct the normalization as follows. Choose $\lambda_1, \lambda_3 \in \mathbb{F}_{2^m}^*$ arbitrarily. Set

$$\mu_1 = \frac{1}{c_1\lambda_1^{q+1}}, \quad \mu_3 = \frac{1}{c_8\lambda_3^{q+1}}.$$

This normalizes the coefficients of x^{q+1} and z^{q+1} to 1.

For the second component, we require both the coefficient of y^{q+1} and the coefficient of x^qz to equal 1. Thus, we require

$$\mu_2c_5\lambda_2^{q+1} = 1, \quad \mu_2c_4\lambda_1^q\lambda_3 = 1.$$

From the second constraint, $\mu_2 = \frac{1}{c_4\lambda_1^q\lambda_3}$. Substitution into the first constraint gives

$$\frac{c_5\lambda_2^{q+1}}{c_4\lambda_1^q\lambda_3} = 1 \quad \Longrightarrow \quad \lambda_2^{q+1} = \frac{c_4\lambda_1^q\lambda_3}{c_5}.$$

Since $\gcd(q+1, 2^m-1) = 1$ when m is odd and $\gcd(i,m) = 1$, the map $t \mapsto t^{q+1}$ is a bijection on $\mathbb{F}_{2^m}^*$, so λ_2 is uniquely determined by

$$\lambda_2 = \left(\frac{c_4\lambda_1^q\lambda_3}{c_5}\right)^{1/(q+1)}.$$

Thus, λ_2 is well-defined and nonzero. With these choices, set $\mu_2 = \frac{1}{c_4\lambda_1^q\lambda_3}$.

The four remaining non-normalized coefficients become

$$a_1 = \mu_1 c_2 \lambda_1^q \lambda_3 = \frac{c_2\lambda_3}{c_1\lambda_1}, \quad a_2 = \mu_1 c_3 \lambda_2 \lambda_3^q = \frac{c_3\lambda_2\lambda_3^q}{c_1\lambda_1^{q+1}},$$
$$a_3 = \mu_3 c_6 \lambda_1 \lambda_2^q = \frac{c_6\lambda_1\lambda_2^q}{c_8\lambda_3^{q+1}}, \quad a_4 = \mu_3 c_7 \lambda_2^q \lambda_3 = \frac{c_7\lambda_2^q\lambda_3}{c_8\lambda_3^{q+1}} = \frac{c_7\lambda_2^q}{c_8\lambda_3^q}.$$

Since c_2, c_3, c_6, c_7 are free parameters, the parameters (a_1, a_2, a_3, a_4) can take any values in $\mathbb{F}_{2^m}^4$ by choosing appropriate c_2, c_3, c_6, c_7 (with λ_2 then determined as above). Conversely, any normalized form corresponds to several choices of the original parameters. The reduction preserves the permutation property since it is a composition of bijections. □

Remark 3.2. The choice $a_1 = a_2 = a_3 = a_4 = 1$ gives the Li–Kaleyski function F_1 from [12].

Henceforth we study

$$G(x,y,z) = (x^{q+1} + a_1x^qz + a_2yz^q,\ x^qz + y^{q+1},\ a_3xy^q + a_4y^qz + z^{q+1}). \tag{1}$$

We next express failure of the permutation property as solvability of a differential system.

4. Polynomial criteria for the permutation property.

The function G is a permutation if and only if for any nonzero $(\alpha,\beta,\gamma) \in \mathbb{F}_{2^m}^3 \setminus \{(0,0,0)\}$, the equation $G(x+\alpha, y+\beta, z+\gamma) + G(x,y,z) = (0,0,0)$ has no solution $(x,y,z) \in \mathbb{F}_{2^m}^3$. This leads to a system of polynomial equations.

Note that the solvability of the condition in the following theorems depends on the specific choice of i relative to the field extension degree m. More precisely, for each fixed i there exists $m_0(i)$ such that the statements below hold for every odd $m \geq m_0(i)$ with $\gcd(i,m) = 1$.

Theorem 4.1. *Let m be odd and sufficiently large, $\gcd(i,m) = 1$, and $q = 2^i$. Let*

$$G_{a_1,a_2,a_3,a_4}(x,y,z) = (x^{q+1} + a_1x^qz + a_2yz^q,\ x^qz + y^{q+1},\ a_3xy^q + a_4y^qz + z^{q+1})$$

with $a_1, a_2, a_3, a_4 \in \mathbb{F}_{2^m}$. If $a_2a_3 \neq 0$ and

$$a_2^{q+1}a_3^qT^{q^2+q+1} + a_2^qa_4^qT^{q^2+q} + 1 = 0$$

has a solution T in $\mathbb{F}_{2^m}$, then G_{a_1,a_2,a_3,a_4} is not a permutation on $\mathbb{F}_{2^m}^3$.

Proof. Consider the set

$$\Theta := \{\theta \in \overline{\mathbb{F}_2} : a_2^{q+1}a_3^q\theta^{q^2+q+1} + a_2^q a_4^q \theta^{q^2+q} + 1 = 0\}.$$

Note that $a_2a_3 \neq 0$ implies $\#\Theta = q^2+q+1$. Indeed, the derivative of the polynomial defining Θ is $a_2^{q+1}a_3^q T^{q^2+q}$, and hence all its roots are simple.

Let $\alpha, \beta, \gamma \in \mathbb{F}_{2^m}$ with $\alpha \neq 0$. Consider the system

$$\begin{cases} \alpha^q x + x^q\alpha + a_1\gamma x^q + a_2\gamma^q y + a_1\alpha^q z + a_2\beta z^q + \alpha^{q+1} + a_1\alpha^q\gamma + a_2\beta\gamma^q = 0, \\ \gamma x^q + \beta^q y + \beta y^q + \alpha^q z + \alpha^q\gamma + \beta^{q+1} = 0, \\ a_3\beta^q x + a_3\alpha y^q + a_4\gamma y^q + a_4\beta^q z + \gamma^q z + \gamma z^q + a_3\alpha\beta^q + a_4\beta^q\gamma + \gamma^{q+1} = 0. \end{cases} \tag{2}$$

This is precisely the system obtained from $G(x+\alpha, y+\beta, z+\gamma)+G(x,y,z) = (0,0,0)$.

We define

$$A = \alpha x^q + \alpha^q x + \alpha^{q+1}, \qquad C = \beta y^q + \beta^q y + \beta^{q+1}, \qquad E_0 = \beta^q x + \alpha y^q + \alpha\beta^q.$$

On $\alpha \neq 0$, the second equation gives $z = (\gamma(x^q + \alpha^q) + C)/\alpha^q$. After substituting this expression, the first equation is equivalent to $D\gamma^q = T$, where

$$D = \beta x^{q^2} + \alpha^{q^2} y, \qquad T = a_2^{-1}\alpha^{q^2}(A + a_1 C) + \beta C^q. \tag{3}$$

The third equation, multiplied by α^{q^2}, becomes $U\gamma^{q+1} + V\gamma^q + W\gamma + J = 0$, with

$$\begin{aligned} U &= x^{q^2} + \alpha^{q^2-q}x^q + \alpha^{q^2}, & V &= C\alpha^{q^2-q}, \\ W &= a_4\alpha^{q^2}y^q + a_4\beta^q x^q\alpha^{q^2-q} + C^q, & J &= a_3\alpha^{q^2}E_0 + a_4\beta^q C\alpha^{q^2-q}. \end{aligned} \tag{4}$$

Thus, on $\alpha D \neq 0$, the differential system is equivalent to

$$K = U^q T^{q+1} + V^q T^q D + W^q T D^q + J^q D^{q+1} = 0. \tag{5}$$

Indeed, choose the unique $\gamma \in \mathbb{F}_{2^m}$ with $\gamma^q = T/D$, and recover z from the second equation. Equation (5) is exactly the qth power of the remaining equation, multiplied by D^{q+1}, so it is equivalent to that equation over $\mathbb{F}_{2^m}$.

Set $\beta = 1$ and put $N = q^2+q+1$, $v = \alpha^{q-1}y$, and $B_0 = x^q + \alpha^{q-1}x + \alpha^q$. In the highest homogeneous part of K, the term V^qT^qD has smaller degree than the other three. Their sum gives

$$K^{(H)} = \frac{\alpha^{q^3+N}}{a_2^{q+1}}\left(B_0^N + a_2^q a_4^q v^{N-1}B_0 + a_2^{q+1}a_3^q v^N\right) = a_3^q\alpha^{q^3+N}\prod_{\theta\in\Theta}(v + \theta B_0).$$

The factors

$$H_\theta = \alpha^{q-1}y + \theta(x^q + \alpha^{q-1}x + \alpha^q)$$

are distinct and absolutely irreducible. Indeed, setting $\alpha = 1$ gives

$$y + \theta(x^q + x + 1),$$

which is absolutely irreducible since it has degree one in y, and H_θ is its homogenization.

By hypothesis, at least one θ belongs to $\mathbb{F}_{2^m}$, so one factor of $K^{(H)}$ is defined over $\mathbb{F}_{2^m}$ and absolutely irreducible. This factor extends to a factor of K that is absolutely irreducible and defined over $\mathbb{F}_{2^m}$. Indeed, H_θ occurs with multiplicity one in $K^{(H)}$. Hence there is a unique absolutely irreducible factor of K whose highest homogeneous part is divisible by H_θ. Since H_θ is defined over $\mathbb{F}_{2^m}$, this factor is fixed by $\mathrm{Gal}(\overline{\mathbb{F}_2}/\mathbb{F}_{2^m})$ and is therefore defined over $\mathbb{F}_{2^m}$.

For sufficiently large m, there exist solutions of $K(x,y,\alpha,1)=0$ in $\mathbb{F}_{2^m}$ with $\beta x^{q^2}+\alpha^{q^2}y\neq 0$ and $\alpha\neq 0$. Indeed, the absolutely irreducible component obtained above is not contained in either $\alpha=0$ or $\beta x^{q^2}+\alpha^{q^2}y=0$. The highest homogeneous part of $D(x,y,\alpha,1)$ is $\alpha^{q^2}y$. None of the factors H_θ divides α or y. Since H_θ divides the highest homogeneous part of the component polynomial, the component cannot be contained in $\alpha D=0$. Their intersections with the component have smaller dimension and bounded degree depending only on i, so they contribute only lower-order terms in the Lang–Weil estimate. Here β remains fixed at 1.

Thus, γ is uniquely determined by $\gamma^q=T/D$, with $\beta=1$, and z is recovered from

$$\gamma x^q+\beta^q y+\beta y^q+\alpha^q z+\alpha^q\gamma+\beta^{q+1}=0,$$

proving that G_{a_1,a_2,a_3,a_4} is not a permutation. □

Lemma 4.2. *Let $q=2^i$, and $N=q^2+q+1$. For $A,B\in\mathbb{F}_{2^m}$ with $B\neq 0$, put $P(T)=T^N+AT+B$ and $V=\ker(X^{q^3}+AX^q+BX)$ in $\overline{\mathbb{F}_2}$. If P has a root in $\mathbb{F}_{2^{2m}}$, then it has a root in $\mathbb{F}_{2^m}$. The same conclusion holds if a root $\theta\notin\mathbb{F}_{2^m}$ satisfies $\theta^{q+1}=r\theta+s$ for some $r,s\in\mathbb{F}_{2^m}$.*

Proof. The q-polynomial defining V is separable of degree q^3, so V has dimension 3 over $\mathbb{F}_q$. For $x\neq 0$,

$$x^{-1}(x^{q^3}+Ax^q+Bx)=P(x^{q-1}).$$

Thus, $\langle x\rangle_q\mapsto x^{q-1}$ is a bijection from $\mathrm{PG}(V,q)$ to the roots of P. It is well-defined because $\lambda^{q-1}=1$ for $\lambda\in\mathbb{F}_q^*$, and it is injective because $x^{q-1}=y^{q-1}$ implies $x/y\in\mathbb{F}_q^*$. Every root of P is obtained by choosing a $(q-1)$-st root in $\overline{\mathbb{F}_2}$. The Frobenius $\sigma: x\mapsto x^{2^m}$ preserves V. If it preserves a 2-dimensional $\mathbb{F}_q$-subspace $W\subset V$, choose $v\notin W$ and write $\sigma(v)=\delta v+w$ modulo W, where $\delta\in\mathbb{F}_q^*$ and $w\in W$. The additive map $u\mapsto\sigma(u)-\delta u$ on the finite space W either has a nonzero kernel, or is surjective. In the first case a point of $\mathrm{PG}(W,q)$ is fixed by σ. In the second case, choose $u\in W$ with $\sigma(u)-\delta u=w$, so $\langle v+u\rangle_q$ is fixed. Either fixed point corresponds to a root of P in $\mathbb{F}_{2^m}$.

If $\theta\in\mathbb{F}_{2^{2m}}\setminus\mathbb{F}_{2^m}$ is a root, its projective point P_0 satisfies $\sigma^2(P_0)=P_0$ and $\sigma(P_0)\neq P_0$. Thus, P_0 and $\sigma(P_0)$ span a σ-invariant line. The preceding argument gives a fixed point and therefore a root in $\mathbb{F}_{2^m}$, proving the first assertion. For the second, $s\neq 0$, since $s=0$ would imply $\theta^q=r\in\mathbb{F}_{2^m}$. Raising $\theta^{q+1}=r\theta+s$ to the qth power and multiplying by θ gives

$$\theta^N=(r^{q+1}+s^q)\theta+r^q s.$$

Since $\theta\notin\mathbb{F}_{2^m}$ and $P(\theta)=0$, we obtain $r^{q+1}+s^q=A$ and $r^q s=B$. Hence $T^{q+1}+rT+s$ divides $P(T)$. Indeed, if $D(T)=T^{q+1}+rT+s$ and $M(X)=X^{q^2}+rX^q+sX$, then

$$P(T)=TD(T)^q+r^qD(T),\qquad X^{q^3}+AX^q+BX=M(X)^q+r^qM(X).$$

These identities also show that the kernel of M is a 2-dimensional $\mathbb{F}_q$-subspace of V. It is σ-invariant because $r,s\in\mathbb{F}_{2^m}$. The preceding argument again gives a root of P in $\mathbb{F}_{2^m}$. □

Lemma 4.3. *Let $m\geq 3$ be odd, $q=2^i$, and $\gcd(i,m)=1$. If $a\in\mathbb{F}_{2^m}$, $c\in\mathbb{F}_{2^m}^*$, and $R(T)=T^{q^2+q+1}+a^qT+1/c$ has no root in $\mathbb{F}_{2^m}$, then $G_{a,1/c,c,ac}$ is a permutation of $\mathbb{F}_{2^m}^3$.*

Proof. Write $N = q^2 + q + 1$, and let Θ be the roots of R in $\overline{\mathbb{F}_2}$. These roots are distinct. In fact, a common root of R and R' would satisfy $\theta^{N-1} = a^q$, which gives $R(\theta) = 1/c \neq 0$. Put

$$A = \alpha x^q + \alpha^q x + \alpha^{q+1}, \quad B = \beta x^q + \alpha^q y + \alpha^q \beta, \quad C = \beta y^q + \beta^q y + \beta^{q+1}, \quad E = A + aC.$$

We first establish the polynomial identities needed on the open set $\alpha D \neq 0$. Define

$$\begin{aligned} \mathcal{N}(A,B,C) = {} & A^{q^2+q}E + a^q B^{q^2+q}E + c^{-1}B^{q^2}CE^q + c^{-q}C^{q^2}B^qE \\ & + c^{-(q+1)}C^N + c^{-1}BC^qA^{q^2} + c^{-1}B^N. \end{aligned} \tag{6}$$

Then

$$\mathcal{N}(A,B,C) = \prod_{\theta \in \Theta} \left(A + \theta B + (a + \theta^{q+1})C\right). \tag{7}$$

To prove this, regard A, B, C as independent indeterminates and set $S = CA^q + B^{q+1}$ and $V_0 = cB^qE + C^{q+1}$. Expansion using $(u+v)^q = u^q + v^q$ gives the identity

$$CV_0^{q+1} + c^q BV_0 S^q + c^{q+1} ES^{q+1} = c^{q+1}C^{q+1}\mathcal{N}(A,B,C).$$

On the hyperplane $E + \theta B + \theta^{q+1}C = 0$, raising its equation to the qth power, multiplying by θ, and using $R(\theta) = 0$ gives $A^q\theta + B^q\theta^{q+1} + C^q/c = 0$. Combining the two relations yields $S\theta + V_0/c = 0$. Substituting $V_0 = cS\theta$ in the preceding identity makes its left side zero. Since the linear polynomial $E + \theta B + \theta^{q+1}C$ does not divide C, it divides $\mathcal{N}$. These N linear factors are pairwise distinct, $\mathcal{N}$ has degree N, and its coefficient of A^N is 1. This proves (7).

For K from (5), specialized to $(a_1, a_2, a_3, a_4) = (a, 1/c, c, ac)$, we also have

$$K = c^{q+1}\alpha^{q^3}\mathcal{N}(A,B,C). \tag{8}$$

Here is an explicit way to check the cancellation. Set $\alpha = 1$. The definitions in (3) and (4) become

$$\begin{aligned} &D = B + \beta A^q, && C = \beta B^q + \beta^q D, && T = cE + \beta C^q, \\ &U = A^q, && V = C, && W = ac(B^q + \beta^q A^q) + C^q, \\ &J = cB^q + c\beta^q(A^q + E). \end{aligned}$$

Substitution in (5), followed by expansion of the qth powers, gives the seven terms $c^{q+1}\mathcal{N}$ in (6). Both sides of (8) are homogeneous of degree $q^3 + (q+1)N$ in x, y, α, β. Homogenizing this identity on $\alpha = 1$ therefore gives (8).

Let $\mathrm{Tr}(t) = \sum_{j=0}^{m-1} t^{2^j}$ be the absolute trace from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$. Since m is odd, $\mathrm{Tr}(t^q + t + 1) = 1$ for every $t \in \mathbb{F}_{2^m}$. In particular, $t^q + t + 1$ never vanishes in $\mathbb{F}_{2^m}$. Suppose that the differential system has a solution with $(\alpha, \beta, \gamma) \neq (0,0,0)$.

If $\alpha = \beta = 0$, then $\gamma \neq 0$, and the first two equations give $x = y = 0$. The third gives $(z/\gamma)^q + z/\gamma + 1 = 0$, contrary to the trace calculation. If $\alpha = 0$ and $\beta \neq 0$, homogeneity allows us to divide all six coordinates by β and assume $\beta = 1$. Put $u = y^q + y + 1$, $k_0 = ac + \gamma^q$, and $w = z + \gamma y$. The three equations respectively give

$$w^q = k_0 u, \qquad \gamma x^q = u, \qquad cx = k_0 w.$$

Since $u \neq 0$, both γ and x are nonzero, and therefore $k_0 \neq 0$. Raising the last equation to the qth power and using the first two gives $\gamma k_0^{q+1} = c^q$. Thus, $\theta = \gamma k_0/c \in \mathbb{F}_{2^m}^*$ satisfies $\theta^{q+1} = \gamma^q/c$ and $\theta = \gamma(a + \theta^{q+1})$. Raising the latter identity to the qth power and dividing by $c\theta^q$ gives $R(\theta) = 0$, a contradiction.

Next suppose $\alpha \neq 0$ and $D = 0$. Divide all coordinates by α and assume $\alpha = 1$. We have $y = \beta x^{q^2}$. Put $u = x^q + x + 1 \neq 0$. Then $A = u$, $C = \beta^{q+1} u^{q^2}$, and the first reduced equation is $T = 0$. Hence

$$cu + ca\beta^{q+1} u^{q^2} + \beta^N u^{q^3} = 0.$$

It follows that $\beta \neq 0$ and that $v = \beta u^{q-1} \in \mathbb{F}_{2^m}^*$ satisfies $v^N + cav^{q+1} + c = 0$. Since $\gcd(q-1, 2^m - 1) = 1$, choose $z_0 \in \mathbb{F}_{2^m}^*$ with $z_0^{q-1} = v$. The $\mathbb{F}_2$-linear map $M(z) = z^{q^3} + caz^{q^2} + cz$ then has z_0 in its kernel. The trace pairing $(r, s) \mapsto \mathrm{Tr}(rs)$ is nondegenerate, since $\mathrm{Tr}(1) = 1$ and for $r \neq 0$ one can take $s = r^{-1}$. The adjoint M^* is defined by $\mathrm{Tr}(M(r)s) = \mathrm{Tr}(rM^*(s))$ for all $r, s \in \mathbb{F}_{2^m}$. It is given by

$$M^*(z) = z^{q^{m-3}} + (caz)^{q^{m-2}} + cz.$$

This formula follows from $\mathrm{Tr}(rs^{q^j}) = \mathrm{Tr}(r^{q^{m-j}} s)$. In a basis, the matrix of M^* is conjugate to the transpose of the matrix of M. The two maps therefore have the same rank, so M^* has a nonzero kernel element z_1. Raising $M^*(z_1) = 0$ to the q^3-th power gives

$$0 = z_1 + c^q a^q z_1^q + c^{q^3} z_1^{q^3} = (cz_1)^{q^3} + a^q (cz_1)^q + (cz_1)/c.$$

Consequently, $R((cz_1)^{q-1}) = 0$, again a contradiction.

Finally suppose $\alpha D \neq 0$. The differential equations give $K = 0$, so (8) and (7) give $A + \theta B + (a + \theta^{q+1})C = 0$ for some $\theta \in \Theta$. The elements $1, \theta, a + \theta^{q+1}$ are linearly independent over $\mathbb{F}_{2^m}$. Otherwise $\theta \notin \mathbb{F}_{2^m}$ and a dependence would give $\theta^{q+1} = r\theta + s$ with $r, s \in \mathbb{F}_{2^m}$, and Lemma 4.2 would give a root of R in $\mathbb{F}_{2^m}$. Thus, $A = B = C = 0$. But $A = \alpha^{q+1}((x/\alpha)^q + x/\alpha + 1)$ cannot vanish when $\alpha \neq 0$. This last contradiction excludes all nonzero difference vectors and proves the lemma. □

Theorem 4.4. *Let m be odd and sufficiently large, $\gcd(i, m) = 1$, and $q = 2^i$. Let*

$$G_{a,1,1,a}(x, y, z) = (x^{q+1} + ax^q z + yz^q,\ x^q z + y^{q+1},\ xy^q + ay^q z + z^{q+1}),$$

where $a \in \mathbb{F}_{2^m}$. Then $G_{a,1,1,a}$ is a permutation of $\mathbb{F}_{2^m}^3$ if and only if

$$P_a(T) = T^{q^2+q+1} + a^q T^{q^2+q} + 1$$

has no roots in $\mathbb{F}_{2^{2m}}$.

Proof. We first show that if P_a has a root in $\mathbb{F}_{2^{2m}}$, then it has a root in $\mathbb{F}_{2^m}$. Consider the q-polynomial

$$\mathcal{L}_a(X) = X^{q^3} + a^q X^q + X$$

and let $V = \ker \mathcal{L}_a$. Since $\mathcal{L}_a'(X) = 1$, V is a 3-dimensional $\mathbb{F}_q$-vector space. Moreover,

$$P_a(x^{1-q}) = 0 \quad \Longleftrightarrow \quad x \in V \setminus \{0\},$$

and hence the roots of P_a are in bijection with the points of $\mathrm{PG}(V, q)$ via

$$\langle x \rangle_q \longmapsto x^{1-q}.$$

Indeed, for $x \neq 0$ in $\overline{\mathbb{F}_2}$, multiplication by x^{q^3-1} gives

$$x^{q^3-1} P_a(x^{1-q}) = 1 + a^q x^{q-1} + x^{q^3-1} = x^{-1} \mathcal{L}_a(x),$$

because $(q-1)(q^2+q+1) = q^3 - 1$. This also shows directly why the projective parametrization is well-defined.

The reciprocal polynomial $T^{q^2+q+1} + a^q T + 1$ has a root in $\mathbb{F}_{2^{2m}}$ exactly when P_a does. By Lemma 4.2, it then has a root in $\mathbb{F}_{2^m}$, and so does P_a. Hence, if P_a

has a root in $\mathbb{F}_{2^{2m}}$, it has a root in $\mathbb{F}_{2^m}$, and Theorem 4.1 implies that $G_{a,1,1,a}$ is not a permutation.

Conversely, suppose that P_a has no roots in $\mathbb{F}_{2^{2m}}$. Put $N = q^2 + q + 1$ and $\widetilde{R}(T) = T^N + a^q T + 1$. Since $\widetilde{R}(T) = T^N P_a(1/T)$ and both constant terms are nonzero, $\widetilde{R}$ also has no root in $\mathbb{F}_{2^{2m}}$. Let $\widetilde{\Theta}$ be its roots in $\overline{\mathbb{F}_2}$, and define

$$A = \alpha x^q + \alpha^q x + \alpha^{q+1}, \quad B = \beta x^q + \alpha^q y + \alpha^q \beta,$$
$$C = \beta y^q + \beta^q y + \beta^{q+1}, \quad D = \beta x^{q^2} + \alpha^{q^2} y.$$

For each $\theta \in \widetilde{\Theta}$, the elements $1, \theta, a + \theta^{q+1}$ are linearly independent over $\mathbb{F}_{2^m}$. Indeed, $\theta \notin \mathbb{F}_{2^m}$, and a dependence would yield $\theta^{q+1} = r\theta + s$ with $r, s \in \mathbb{F}_{2^m}$. Lemma 4.2 would then give a root of $\widetilde{R}$ in $\mathbb{F}_{2^m}$, a contradiction.

Suppose there were a solution of system (2) with a nonzero difference vector. If $\alpha D \neq 0$, the polynomial identities (7) and (8), with $c = 1$, give

$$0 = K = \alpha^{q^3} \prod_{\theta \in \widetilde{\Theta}} \left(A + \theta B + (a + \theta^{q+1}) C \right).$$

One factor therefore vanishes, and the linear independence forces $A = B = C = 0$. However, $\alpha \neq 0$ and $A = 0$ would give $(x/\alpha)^q + x/\alpha + 1 = 0$. The absolute trace of its left side is 1 when m is odd, so this is impossible.

The excluded cases must also be checked because the elimination uses division by αD. They are treated directly in Lemma 4.3, whose proof applies to all odd $m \geq 3$. With $c = 1$, the case $\alpha = \beta = 0$ gives the same impossible trace equation in z/γ. If $\alpha = 0$ and $\beta \neq 0$, normalization to $\beta = 1$ produces a root $\theta = \gamma(a + \gamma^q)$ of $\widetilde{R}$ in $\mathbb{F}_{2^m}$. If $\alpha \neq 0$ and $D = 0$, normalization to $\alpha = 1$ produces a nonzero kernel element of $M(z) = z^{q^3} + az^{q^2} + z$. Its trace adjoint has a nonzero kernel element z_1, and raising the adjoint equation to the q^3-th power gives $z_1^{q^3} + a^q z_1^q + z_1 = 0$. Thus, $\widetilde{R}(z_1^{q-1}) = 0$, again a contradiction. These cases exhaust all possible difference vectors, proving that $G_{a,1,1,a}$ is a permutation. □

Theorem 4.5. *Let m be odd and sufficiently large, $\gcd(i, m) = 1$, and $q = 2^i$. Let*

$$G_{a_1,1/a_3,a_3,a_1a_3}(x, y, z) = \left(x^{q+1} + a_1 x^q z + \frac{1}{a_3} y z^q,\ x^q z + y^{q+1},\ a_3 x y^q + a_1 a_3 y^q z + z^{q+1} \right),$$

where $a_1 \in \mathbb{F}_{2^m}$ and $a_3 \in \mathbb{F}_{2^m}^*$. Then $G_{a_1,1/a_3,a_3,a_1a_3}$ is a permutation of $\mathbb{F}_{2^m}^3$ if and only if

$$R_{a_1,a_3}(T) = T^{q^2+q+1} + a_1^q T + \frac{1}{a_3}$$

has no roots in $\mathbb{F}_{2^{2m}}$.

Proof. Write $k = \mathbb{F}_{2^m}$, $N = q^2 + q + 1$, and $R(T) = T^N + a_1^q T + 1/a_3$. We first explain why a root in $\mathbb{F}_{2^{2m}}$ implies a root in k. Consider the q-polynomial

$$\mathcal{L}(X) = X^{q^3} + a_1^q X^q + \frac{1}{a_3} X$$

and its kernel V in $\overline{\mathbb{F}_2}$. Its derivative is $1/a_3 \neq 0$, so it has q^3 distinct roots. These roots form a 3-dimensional $\mathbb{F}_q$-vector space. For $x \neq 0$, $x^{-1}\mathcal{L}(x) = R(x^{q-1})$, since $(q-1)N = q^3 - 1$. Thus, $\langle x \rangle_q \mapsto x^{q-1}$ is a bijection from $\mathrm{PG}(V, q)$ to the roots of R. Indeed, two nonzero vectors have the same image exactly when their quotient belongs to $\mathbb{F}_q^*$.

The Frobenius $\sigma : x \mapsto x^{2^m}$ preserves V and acts semilinearly over $\mathbb{F}_q$. If a root θ belongs to $\mathbb{F}_{2^{2m}} \setminus k$, its corresponding projective point P satisfies $\sigma^2(P) = P$ and $\sigma(P) \neq P$. The line joining P and $\sigma(P)$ is therefore σ-invariant. For completeness, an invariant line in this projective plane forces a fixed point. Let $W \subset V$ be its 2-dimensional vector space, choose $v \notin W$, and write $\sigma(v) = \delta v + w$ with $\delta \in \mathbb{F}_q^*$ and $w \in W$. The additive map $u \mapsto \sigma(u) - \delta u$ on W either has a nonzero kernel, which gives a fixed projective point in W, or is bijective. In the latter case choose u with $\sigma(u) - \delta u = w$. Characteristic 2 gives $\sigma(v + u) = \delta(v + u)$, again a fixed point. Under the root correspondence, a fixed point gives a root in k.

Let $\theta \in k$ be such a root. The constant term of R is nonzero, so $\theta \neq 0$, and $t = \theta^{-1}$ satisfies

$$\frac{1}{a_3} t^N + a_1^q t^{N-1} + 1 = 0.$$

For $a_2 = 1/a_3$ and $a_4 = a_1 a_3$, this is exactly the polynomial condition in Theorem 4.1, because $a_2^{q+1} a_3^q = 1/a_3$ and $a_2^q a_4^q = a_1^q$. That theorem proves non-permutation for sufficiently large odd m.

Conversely, suppose that R has no roots in $\mathbb{F}_{2^{2m}}$, and let Θ be its roots in $\overline{\mathbb{F}_2}$. We show first that $1, \theta, a_1 + \theta^{q+1}$ are linearly independent over k for every $\theta \in \Theta$. Since $\theta \notin k$, a dependence would give $\theta^{q+1} = r\theta + s$ with $r, s \in k$. Here $s \neq 0$, since otherwise $\theta^q = r \in k$ would imply $\theta \in k$. Raising the relation to the qth power and multiplying by θ gives

$$\theta^N = (r^{q+1} + s^q)\theta + r^q s.$$

Together with $R(\theta) = 0$ and $\theta \notin k$, this yields $r^{q+1} + s^q = a_1^q$ and $r^q s = 1/a_3$. Put $\mathcal{M}(X) = X^{q^2} + rX^q + sX$. Then

$$\mathcal{L}(X) = \mathcal{M}(X)^q + r^q \mathcal{M}(X).$$

Since $s \neq 0$, the kernel of $\mathcal{M}$ is a 2-dimensional $\mathbb{F}_q$-subspace of V. It is σ-invariant because $r, s \in k$. The invariant-line argument above would therefore give a root of R in k, a contradiction. This proves the linear independence.

Suppose now that system (2) has a solution with $(\alpha, \beta, \gamma) \neq (0, 0, 0)$ for the present parameters. Define

$$A = \alpha x^q + \alpha^q x + \alpha^{q+1}, \quad B = \beta x^q + \alpha^q y + \alpha^q \beta,$$
$$C = \beta y^q + \beta^q y + \beta^{q+1}, \quad D = \beta x^{q^2} + \alpha^{q^2} y.$$

On $\alpha D \neq 0$, the explicit identities (7) and (8), proved in Lemma 4.3, give

$$0 = K = a_3^{q+1} \alpha^{q^3} \prod_{\theta \in \Theta} \left(A + \theta B + (a_1 + \theta^{q+1}) C \right).$$

Thus, one factor vanishes. Since $A, B, C \in k$, the linear independence just proved implies $A = B = C = 0$. But $A = \alpha^{q+1}((x/\alpha)^q + x/\alpha + 1)$ cannot vanish. Indeed, the absolute trace satisfies $\mathrm{Tr}(t^q + t + 1) = 1$ for every $t \in k$, because m is odd.

It remains to treat the cases excluded by division in the elimination. If $\alpha = \beta = 0$, then $\gamma \neq 0$. The first and second differential equations give $y = 0$ and $x = 0$, respectively. The third then gives $(z/\gamma)^q + z/\gamma + 1 = 0$, contradicting the trace identity.

If $\alpha = 0$ and $\beta \neq 0$, the homogeneity of the differential equations allows us to divide all six coordinates by β and assume $\beta = 1$. Put $u = y^q + y + 1$, $k_0 = a_1 a_3 + \gamma^q$, and $w = z + \gamma y$. The three equations reduce to

$$w^q = k_0 u, \qquad \gamma x^q = u, \qquad a_3 x = k_0 w.$$

Since $u \neq 0$, we have $\gamma x \neq 0$ and $k_0 \neq 0$. Raising the last equation to the qth power gives $\gamma k_0^{q+1} = a_3^q$. Hence $\theta = \gamma k_0/a_3 \in k^*$ satisfies $\theta^{q+1} = \gamma^q/a_3$ and $\theta = \gamma(a_1 + \theta^{q+1})$. Raising the latter equation to the qth power and dividing by $a_3\theta^q$ yields $R(\theta) = 0$, a contradiction.

Finally, suppose $\alpha \neq 0$ and $D = 0$. Divide all coordinates by α and assume $\alpha = 1$. Then $y = \beta x^{q^2}$. With $u = x^q + x + 1 \neq 0$, the reduced first equation $T = 0$ becomes

$$a_3 u + a_3 a_1 \beta^{q+1} u^{q^2} + \beta^N u^{q^3} = 0.$$

It follows that $\beta \neq 0$, and $v = \beta u^{q-1}$ satisfies $v^N + a_3 a_1 v^{q+1} + a_3 = 0$. Since $\gcd(q-1, 2^m - 1) = 1$, choose $z_0 \in k^*$ with $z_0^{q-1} = v$. The $\mathbb{F}_2$-linear map $M(z) = z^{q^3} + a_3 a_1 z^{q^2} + a_3 z$ has z_0 in its kernel. Its adjoint for the nondegenerate trace pairing is

$$M^*(z) = z^{q^{m-3}} + (a_3 a_1 z)^{q^{m-2}} + a_3 z.$$

The adjoint has the same rank as M, so there is $z_1 \in k^*$ with $M^*(z_1) = 0$. Raising this equation to the q^3-th power gives

$$(a_3 z_1)^{q^3} + a_1^q (a_3 z_1)^q + \frac{a_3 z_1}{a_3} = 0.$$

Thus, $R((a_3 z_1)^{q-1}) = 0$, again a contradiction. All cases are excluded, so the differential system has no solution with a nonzero difference vector. The map is therefore a permutation. □

5. Complete characterization for $m = 3$.

Proposition 5.1. *Let* $\gcd(i, 3) = 1$ *and* $q = 2^i$. *The function*

$$G(x, y, z) = (x^{q+1} + a_1 x^q z + a_2 y z^q,\ x^q z + y^{q+1},\ a_3 x y^q + a_4 y^q z + z^{q+1})$$

is a permutation over $\mathbb{F}_{2^3}^3$ *if and only if one of the following conditions holds:*

(Type I) $(a_1, a_4) = (0, 0)$ *with* a_2, a_3 *as specified in Table 1 (*13 *cases for each* q*),*
or

(Type II) $(a_1, a_2, a_3, a_4) = (a, 1, 1, a)$ *for some* $a \in \mathbb{F}_{2^3}^*$ *(*7 *cases).*

Proof. We performed an exhaustive computational search over all $(2^3)^4 = 4096$ parameter tuples $(a_1, a_2, a_3, a_4) \in \mathbb{F}_{2^3}^4$. For each, we verified whether G defines a bijection on $\mathbb{F}_{2^3}^3$ by computing the image and checking $|\mathrm{Im}(G)| = |\mathbb{F}_{2^3}^3| = 512$. This identifies exactly 20 permutations for each of $i = 1$ and $i = 2$. The Type II tuples agree in both cases. For Type I, the tuples for $q = 4$ are obtained from those for $q = 2$ by interchanging a_2 and a_3, as recorded in Table 1. An independent exhaustive check is included in the accompanying file `verify_m3.py`. The project repository is cited in [13]. □

The classification in this section is computational. The proof of Proposition 6.1 also uses exact polynomial division, with the full verification program in Appendix B.

Remark 5.2. Type I tuples satisfy $a_1 = a_4 = 0$. Type II tuples satisfy $a_2 = a_3 = 1$ and $a_1 = a_4 \neq 0$. Among the 64 tuples satisfying both $a_1 = a_4$ and $a_2 = a_3$, exactly eight yield permutations for each value of q, namely the seven Type II tuples and $(0, 0, 0, 0)$. The symmetry conditions are therefore not sufficient for permutation and are not necessary for all permutations in the table.

TABLE 1. All permutations over $\mathbb{F}_8^3$. Let $\alpha^3+\alpha+1=0$. The Type I pairs (a_2,a_3) are listed separately for $q=2$ and $q=4$, with $a_1=a_4=0$. For both values of q, the seven Type II tuples are $(a,1,1,a)$ with $a\in\mathbb{F}_8^*$.

	$q=2$		$q=4$	
#	a_2	a_3	a_2	a_3
1	0	0	0	0
2	α	$\alpha+1$	$\alpha+1$	α
3	α	α^2+1	α^2+1	α
4	α^2	$\alpha^2+\alpha+1$	$\alpha^2+\alpha+1$	α^2
5	α^2	α^2+1	α^2+1	α^2
6	$\alpha+1$	α^2	α^2	$\alpha+1$
7	$\alpha+1$	$\alpha^2+\alpha$	$\alpha^2+\alpha$	$\alpha+1$
8	$\alpha^2+\alpha$	$\alpha+1$	$\alpha+1$	$\alpha^2+\alpha$
9	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$
10	$\alpha^2+\alpha+1$	α	α	$\alpha^2+\alpha+1$
11	$\alpha^2+\alpha+1$	α^2	α^2	$\alpha^2+\alpha+1$
12	α^2+1	α	α	α^2+1
13	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha$	α^2+1

6. **Resolution of a conjecture by Beierle et al. [5].** In this section, let $u\in\mathbb{F}_{2^m}^*$. We prove that $C_u(X,Y,Z)=(X^3+uY^2Z, Y^3+uXZ^2, Z^3+uX^2Y)$ is not a permutation for odd $m\geq 23$. This settles the remaining permutation part of the conjecture in [5] for these extension degrees. We construct a nonzero difference vector for which the differential equation has a solution.

Note that for even m, C_u fails to be a permutation, since $C_u(X,0,0)=(X^3,0,0)$ and the function $X\mapsto X^3$ is 3-to-1. In what follows we assume that m is odd.

We analyze when C_u fails to be a permutation by studying the differential equation

$$C_u(X+\alpha,Y+\beta,Z+\gamma)+C_u(X,Y,Z)=(0,0,0).$$

The function C_u is a permutation if and only if this equation has only trivial solutions $\{(X,Y,Z,0,0,0) : X,Y,Z\in\mathbb{F}_{2^m}\}$. Expanding in characteristic 2, where $(A+B)^3=A^3+A^2B+AB^2+B^3$, this condition becomes

$$\begin{cases} \alpha X^2+\alpha^2X+u\gamma Y^2+u\beta^2Z &= \alpha^3+u\beta^2\gamma \\ \beta Y^2+\beta^2Y+u\gamma^2X+u\alpha Z^2 &= \beta^3+u\gamma^2\alpha \\ \gamma Z^2+\gamma^2Z+u\beta X^2+u\alpha^2Y &= \gamma^3+u\alpha^2\beta. \end{cases} \tag{9}$$

Before we take our algebraic geometry approach, we make some observations. First, we assume that only one of α,β, and γ is nonzero. Without loss of generality (here because of the symmetric property of C_u), we may assume that $\alpha\neq 0$ and $\beta=\gamma=0$. Then system (9) becomes

$$\begin{cases} \alpha X^2+\alpha^2X+\alpha^3 &= 0 \\ u\alpha Z^2 &= 0 \\ u\alpha^2Y &= 0. \end{cases}$$

Dividing the first equation by α^3 and putting $t=X/\alpha$ gives $t^2+t+1=0$. Its roots belong to $\mathbb{F}_4\setminus\mathbb{F}_2$, which is disjoint from $\mathbb{F}_{2^m}$ when m is odd. Thus, this equation has no solution in $\mathbb{F}_{2^m}$.

Next, we assume that only one of α, β, and γ is zero. Again, we may assume that $\alpha, \beta \neq 0$ and $\gamma = 0$. Then system (9) becomes

$$\begin{cases} \alpha X^2 + \alpha^2 X + u\beta^2 Z &= \alpha^3 \\ \beta Y^2 + \beta^2 Y + u\alpha Z^2 &= \beta^3 \\ u\beta X^2 + u\alpha^2 Y &= u\alpha^2\beta, \end{cases} \tag{10}$$

which can be further simplified by making the substitutions $X \mapsto \alpha X$ and $Y \mapsto \beta Y$, so system (10) is equivalent to

$$\begin{cases} \alpha^3(X^2 + X + 1) + u\beta^2 Z &= 0 \\ \beta^3(Y^2 + Y + 1) + u\alpha Z^2 &= 0 \\ X^2 + Y + 1 &= 0. \end{cases} \tag{11}$$

Next, squaring the first equation and putting $X^2 = Y + 1$ into it, we have

$$\alpha^6(Y^2 + Y + 1) + u^2\beta^4 Z^2 = 0.$$

Multiplying the above equation by α and putting $u\alpha Z^2 = \beta^3(Y^2 + Y + 1)$, we have

$$(\alpha^7 + u\beta^7)(Y^2 + Y + 1) = 0.$$

Thus, system (11) is equivalent to

$$\begin{cases} (\alpha^7 + u\beta^7)(Y^2 + Y + 1) &= 0 \\ \beta^3(Y^2 + Y + 1) + u\alpha Z^2 &= 0 \\ X^2 + Y + 1 &= 0. \end{cases}$$

Notice that if $\alpha^7 + u\beta^7 = 0$, i.e., u is a 7th power, then the above system has nonzero solutions $(X, Y, Z) \in \mathbb{F}_{2^m}^3$ and consequently C_u is not a permutation. When u is not a 7th power, then the first equation of this system has no solution $\overline{y} \in \mathbb{F}_{2^m}$ for m odd. Thus, in what follows, we assume that u is not a 7th power and m is odd.

Let $f(\alpha, \beta, X, Y, Z)$, $g(\beta, X, Y, Z)$, $h(\beta, X, Y, Z)$, $a_i(\beta, Y, Z)$, $i = 0, \ldots, 21$, be defined as in the Appendix.

Proposition 6.1. *Define*

$$\Theta := \{(x, y, z, a, b, c) \in \mathbb{F}_{2^m}^6 : (b + y)h(b, x, y, z) \neq 0,\ c = f(a, b, x, y, z),$$
$$a = g(b, x, y, z)/h(b, x, y, z), \sum_{i=0}^{21} a_i(b, y, z)x^i = 0\}.$$

Each element of Θ *is a solution of system* (9).

Proof. We prove this implication by polynomial division in MAGMA [8]. From the first equation of system (9),

$$\alpha X^2 + \alpha^2 X + u\gamma Y^2 + u\beta^2 Z = \alpha^3 + u\beta^2\gamma,$$

assuming $\beta + Y \neq 0$, we solve for γ, obtaining

$$\gamma = f(\alpha, \beta, X, Y, Z) := \frac{\alpha^3 + \alpha^2 X + \alpha X^2 + \beta^2 Zu}{\beta^2 u + Y^2 u}.$$

Here $\beta^2 u + Y^2 u = u(\beta + Y)^2 \neq 0$.

Put $P(\beta, X, Y, Z) = \sum_{i=0}^{21} a_i(\beta, Y, Z)X^i$ and choose $\alpha = \frac{g(\beta,X,Y,Z)}{h(\beta,X,Y,Z)}$. With

$$d = u(\beta + Y)^2, \qquad n = g^3 + g^2 Xh + gX^2 h^2 + u\beta^2 Zh^3,$$

the first equation gives $\gamma = n/(dh^3)$. On substituting these expressions, the numerators of the second and third equations, after multiplication by d^2h^7 and d^3h^9, respectively, are

$$E_2 = d^2(\beta Y^2 + \beta^2 Y + \beta^3)h^7 + d^2ugZ^2h^6 + un^2(Xh + g),$$
$$H = nZ^2d^2h^6 + n^2Zdh^3 + u(\beta X^2h^2 + g^2(Y + \beta))d^3h^7 + n^3.$$

Exact division in $\mathbb{F}_2[u, \beta, X, Y, Z]$ gives $P \mid E_2$ and $H = PR$ for a polynomial R. The MAGMA program in Appendix B checks both identities using the displayed coefficients a_i. Hence $P = 0$ and $(\beta+Y)h \neq 0$ imply all three equations of system (9). The formulas for α and γ then determine the lift uniquely. This factorization alone gives no converse, because a solution may lie on $R = 0$ instead of $P = 0$. The explicit polynomials f, g, h, a_i are listed in Appendix A. □

To apply projective geometry techniques, we work in projective coordinates $(X_2 : X_4 : X_5 : X_6)$ corresponding to the affine coordinates (β, X, Y, Z) used in Proposition 6.1, with the identification $(X_2 : X_4 : X_5 : X_6) = (\beta : X : Y : Z)$ in affine charts.

Proposition 6.2. *Let $\mathcal{S} \subset \mathbb{P}^3(\overline{\mathbb{F}_Q})$ be the $\mathbb{F}_Q$-rational surface defined by*

$$\sum_{i=0}^{21} a_i(X_2, X_5, X_6)X_4^i = 0.$$

Then $\mathcal{S}$ contains an absolutely irreducible component defined over $\mathbb{F}_Q$, distinct from $X_2 = 0$, of degree at most 24, and not contained in $(X_2+X_5)h(X_2, X_4, X_5, X_6) = 0$.

Proof. First note that X_2 is not a factor of $\sum_{i=0}^{21} a_i(X_2, X_5, X_6)X_4^i$; otherwise $u \in \mathbb{F}_4^*$, a contradiction. To prove that the surface $\mathcal{S}$ contains a non-repeated, absolutely irreducible component defined over $\mathbb{F}_Q$, we analyze its defining polynomial $F(X_2, X_4, X_5, X_6) = \sum_{i=0}^{21} a_i(X_2, X_5, X_6)X_4^i$.

Consider the intersection of $\mathcal{S}$ with the plane $X_4 = 0$. The resulting curve is defined by $F(X_2, 0, X_5, X_6) = a_0(X_2, X_5, X_6)$. We observe that

$$X_2 \mid a_0(X_2, X_5, X_6) \quad \text{and} \quad X_2^2 \nmid a_0(X_2, X_5, X_6).$$

This indicates that X_2 is a simple (non-repeated) factor of a_0. Let the factorization of F into absolutely irreducible factors over $\overline{\mathbb{F}_Q}$ be

$$F(X_2, X_4, X_5, X_6) = H_1 \cdots H_r.$$

Setting $X_4 = 0$ yields the factorization $a_0 = H_1|_{X_4=0} \cdots H_r|_{X_4=0}$. Since X_2 is a simple factor of a_0, it must divide exactly one factor on the right-hand side, say $H_k|_{X_4=0}$.

We claim that the component H_k is defined over $\mathbb{F}_Q$. The Frobenius automorphism Φ_Q permutes the set of absolutely irreducible factors $\{H_1, \ldots, H_r\}$. Since $a_0 \in \mathbb{F}_Q[X_2, X_5, X_6]$, we have $\Phi_Q(a_0) = a_0$, and since $X_2 \in \mathbb{F}_Q$, $\Phi_Q(X_2) = X_2$. Suppose, for the sake of contradiction, that H_k is not defined over $\mathbb{F}_Q$. Then $\Phi_Q(H_k) = H_j$ for some index $j \neq k$. Applying Φ_Q to the relation $X_2 \mid H_k|_{X_4=0}$ yields

$$X_2 = \Phi_Q(X_2) \mid \Phi_Q(H_k|_{X_4=0}) = H_j|_{X_4=0}.$$

This implies that X_2 divides at least two distinct factors of a_0, namely $H_k|_{X_4=0}$ and $H_j|_{X_4=0}$. Consequently, X_2^2 must divide their product, which divides a_0. This

contradicts the fact that $X_2^2 \nmid a_0$. Thus, $\Phi_Q(H_k) = H_k$, establishing that the absolutely irreducible component H_k is defined over $\mathbb{F}_Q$. Let us denote this component by $\mathcal{S}'$.

Finally, we check that $\mathcal{S}'$ is not contained in the degenerate locus given by $(X_2 + X_5)h(X_2, X_4, X_5, X_6) = 0$. The intersection of this locus with $X_4 = 0$ is

$$u^5X_6^2(X_2+X_5)^3((u^2+u^5)X_2^3X_5^4+(u^2+u^5)X_2^2X_5^5+(u^2+u^5)X_2X_5^6+u^5X_5^7+X_6^7) = 0.$$

Since X_2 is not a factor of this polynomial (as the term X_6^7 prevents it), the component $\mathcal{S}'$ (which intersects $X_4 = 0$ at $X_2 = 0$) cannot be contained in $(X_2 + X_5)h = 0$. □

Theorem 6.3. *Assume throughout this statement that all parameters lie in $\mathbb{F}_{2^m}$ under the standing hypotheses from the preliminaries. If $m \geq 23$ is odd and $u \in \mathbb{F}_{2^m}^*$, then the function $C_u : \mathbb{F}_{2^m}^3 \to \mathbb{F}_{2^m}^3$ given by*

$$(X, Y, Z) \mapsto (X^3 + uY^2Z, Y^3 + uXZ^2, Z^3 + uX^2Y)$$

is not a permutation. This resolves the remaining permutation part of the conjecture posed by Beierle, Carlet, Leander, and Perrin [5] for odd extension degrees $m \geq 23$.

Proof. For C_u to be a permutation, the system of equations in (9) must only have trivial solutions. We show that for $m \geq 23$, there always exists a nontrivial solution $(\alpha, \beta, \gamma) \neq (0, 0, 0)$ and a corresponding (X, Y, Z) that satisfies the system. This existence is guaranteed by finding an $\mathbb{F}_{2^m}$-rational point on a specific algebraic variety derived from the system.

We analyze the system by algebraic elimination. A solution exists if there is a point $(X, Y, Z, \alpha, \beta, \gamma)$ satisfying the system for some nonzero (α, β, γ). It is sufficient to find a rational point on the component considered below outside the degenerate locus. Proposition 6.1 then lifts such a point to a solution of system (9).

The case where u is a seventh power was handled above. Assume now that it is not. By Proposition 6.2, $\mathcal{S}$ has an absolutely irreducible $\mathbb{F}_Q$-rational component $\mathcal{S}'$ of degree $\delta \leq 24$, distinct from the plane $X_2 = 0$. We work in the affine chart $X_2 = 1$. Its part $V = \mathcal{S}' \cap \{X_2 = 1\}$ is an absolutely irreducible affine surface of degree δ. Theorem 2.1 applies because $Q = 2^m \geq 2^{23} > 2(2 + 1)24^2 = 3456$, and gives

$$\#V(\mathbb{F}_Q) \geq Q^2 - 506Q^{3/2} - 5 \cdot 24^{13/3}Q.$$

On this chart the inadmissible points satisfy $(1 + X_5)h(1, X_4, X_5, X_6) = 0$. This polynomial has degree at most 12. Proposition 6.2 shows that V is not contained in its zero set. Thus, their intersection has dimension at most one and, by Bézout, degree at most $24 \cdot 12 = 288$. The affine degree bound gives at most dQ rational points for a set of dimension at most one and total degree d. Applying it to the components of the intersection excludes at most $288Q$ points. Consequently, the number of admissible points is at least

$$Q^2 - 506Q^{3/2} - (5 \cdot 24^{13/3} + 288)Q.$$

This is positive for $Q \geq 2^{23}$. After division by Q, the expression is $f(Q) = Q - 506\sqrt{Q} - 5 \cdot 24^{13/3} - 288$. Its derivative is $f'(Q) = 1 - 253/\sqrt{Q} > 0$ for $Q \geq 2^{23}$, and $f(2^{23}) > 2{,}137{,}749$. Hence the lower bound is positive for every $Q \geq 2^{23}$. An admissible point has $\beta = X_2 = 1$, so its lift through Proposition 6.1 has a nonzero difference vector (α, β, γ). It therefore proves that C_u is not a permutation. □

Remark 6.4. The threshold comes from positivity of the lower bound after inadmissible points are excluded. The hypothesis $Q > 3456$ permits application of the point-count theorem, but does not by itself guarantee an admissible rational point. At $Q = 2^{23}$, the lower bound divided by Q is greater than 2,137,749. The threshold need not be optimal.

7. Conclusion and open problems.

We give a polynomial root condition that forces non-permutation in the normalized trivariate family and exact root criteria for the two subfamilies in Theorems 4.4 and 4.5. The classification over $\mathbb{F}_8$ gives 20 permutations for each of $q = 2$ and $q = 4$, with the Type I parameter pairs interchanged. For the family C_u, the admissible component and the point-count estimate prove non-permutation for every odd $m \geq 23$ and every nonzero u.

Problem. *For which odd extension degrees m do Type I tuples $(0, a_2, a_3, 0)$ with $a_2a_3 \neq 0$ give permutations? Can such tuples be specified for infinitely many m?*

The exclusion of $a_2a_3 = 0$ removes the tuple $(0, 0, 0, 0)$, which gives a product of three Gold permutations for every odd m with $\gcd(i, m) = 1$. Theorem 4.1 does apply when $a_1 = a_4 = 0$ and $a_2a_3 \neq 0$, and then rules out a permutation for sufficiently large m whenever $a_2^{q+1}a_3^q T^{q^2+q+1} + 1$ has a root in $\mathbb{F}_{2^m}$.

Problem. *Are there parameter families beyond Types I and II that yield permutations for infinitely many odd extension degrees?*

Theorem 4.5 concerns only the subfamily $a_2 = 1/a_3$ and $a_4 = a_1a_3$. It does not rule out generic parameter choices in the full four-parameter family.

Problem. *Determine the permutation behavior of C_u for the remaining odd extension degrees $m < 23$, with particular attention to parameters u that are not seventh powers. Can the admissible point-count bound be improved to lower the threshold?*

If $3 \nmid m$, then $\gcd(7, 2^m - 1) = 1$, so every nonzero u is a seventh power and the elementary argument in Section 6 already proves non-permutation. Under the standing assumption $m \geq 3$, the extension degrees not covered by that argument or Theorem 6.3 are therefore $m = 3, 9, 15, 21$.

Use of Generative-AI tools declaration. The authors acknowledge the use of OpenAI (GPT-6.1 Sol) for independent Python computational programs developed during the revision, which double-checked our initial Magma, SageMath, and Python implementation. The authors are responsible for the mathematical statements, proofs, and code.

Acknowledgments. The authors express their deep appreciation to the editor, as well as to the anonymous referees, whose thorough reading and constructive comments have greatly improved the paper. The third-named author (PS) thanks the first-named author (DB) for the invitation to Università degli Studi di Perugia and the excellent working conditions.

Appendix A. Polynomial definitions.

We list below the functions $f(\alpha, \beta, X, Y, Z)$, $g(\beta, X, Y, Z)$, $h(\beta, X, Y, Z)$, $a_i(\beta, Y, Z)$, $i = 0, \ldots, 21$, needed in Proposition 6.1.

$$f(\alpha, \beta, X, Y, Z) := \frac{\alpha^3 + \alpha^2 X + \alpha X^2 + \beta^2 Zu}{\beta^2 u + Y^2 u},$$

$$\begin{aligned} g(\beta, X, Y, Z) := {} & \beta^{12}u^9 + \beta^{12}u^6 + \beta^{12}u^3 + \beta^{12} + \beta^9 XZ^2u^{10} + \beta^9 XZ^2u^4 + \beta^9 Y^3u^9 + \beta^9 Y^3u^3 \\ & + \beta^8 XYZ^2u^{10} + \beta^8 XYZ^2u^4 + \beta^8 Y^4u^6 + \beta^8 Y^4 + \beta^6 X^2Z^4u^8 + \beta^6 X^2Z^4u^5 \end{aligned}$$

$$
\begin{aligned}
&+\beta^6Y^6u^6+\beta^6Y^6u^3+\beta^5X^7u^8+\beta^5X^7u^5+\beta^5XY^4Z^2u^{10}+\beta^5XY^4Z^2u^7\\
&+\beta^4X^7Yu^8+\beta^4X^7Yu^5+\beta^4X^2Y^2Z^4u^8+\beta^4X^2Y^2Z^4u^5+\beta^4XY^5Z^2u^{10}\\
&+\beta^4XY^5Z^2u^7+\beta^4Y^8u^9+\beta^4Y^8+\beta^3X^7Y^2u^5+\beta^3X^4Y^4Zu^6+\beta^3X^3Z^6u^6\\
&+\beta^3X^3Z^6u^3+\beta^3X^2Y^3Z^4u^5+\beta^3XY^6Z^2u^4+\beta^3Y^9u^3+\beta^3Y^2Z^7u^4\\
&+\beta^2X^8Z^2u^6+\beta^2X^7Y^3u^8+\beta^2X^5Y^2Z^3u^7+\beta^2X^4Y^5Zu^6+\beta^2X^3YZ^6u^3\\
&+\beta^2XY^7Z^2u^7+\beta^2XY^7Z^2u^4+\beta^2XZ^9u^5+\beta^2Y^{10}u^6+\beta^2Y^3Z^7u^4\\
&+\beta X^7Y^4u^8+\beta X^4Y^6Zu^6+\beta X^3Y^2Z^6u^6+\beta X^3Y^2Z^6u^3+\beta X^2Y^5Z^4u^5\\
&+\beta XY^8Z^2u^7+\beta Y^{11}u^9+\beta Y^4Z^7u^4,\\
h(\beta,X,Y,Z):=\;&u^5(\beta+Y)^2(\beta^3X^6u^3+\beta^3X^6+\beta^3Y^4Z^2u^5+\beta^3Y^4Z^2u^2+\beta^2X^6Yu^3+\beta^2X^6Y\\
&+\beta^2Y^5Z^2u^5+\beta^2Y^5Z^2u^2+\beta X^6Y^2u^3+\beta X^6Y^2+\beta Y^6Z^2u^5+\beta Y^6Z^2u^2\\
&+X^7Z^2u+X^4Y^2Z^3u^2+X^2YZ^6u+XY^4Z^4u^3+Y^7Z^2u^5+Z^9),\\
a_0(\beta,Y,Z):=\;&\beta^{24}u^{21}+\beta^{24}u^{18}+\beta^{24}u^{15}+\beta^{24}u^{12}+\beta^{24}u^9+\beta^{24}u^6+\beta^{24}u^3+\beta^{24}\\
&+\beta^{21}Y^3u^{21}+\beta^{21}Y^3u^{15}+\beta^{21}Y^3u^9+\beta^{21}Y^3u^3+\beta^{20}Y^4u^{21}+\beta^{20}Y^4u^{15}\\
&+\beta^{20}Y^4u^9+\beta^{20}Y^4u^3+\beta^{18}Y^6u^{18}+\beta^{18}Y^6u^{15}+\beta^{18}Y^6u^6+\beta^{18}Y^6u^3\\
&+\beta^{17}Y^7u^{21}+\beta^{17}Y^7u^{15}+\beta^{17}Y^7u^9+\beta^{17}Y^7u^3+\beta^{16}Y^8u^{15}+\beta^{16}Y^8u^{12}\\
&+\beta^{16}Y^8u^3+\beta^{16}Y^8+\beta^{15}Y^9u^{15}+\beta^{15}Y^9u^3+\beta^{15}Y^2Z^7u^{16}+\beta^{15}Y^2Z^7u^4\\
&+\beta^{14}Y^{10}u^{15}+\beta^{14}Y^{10}u^3+\beta^{14}Y^3Z^7u^{16}+\beta^{14}Y^3Z^7u^4+\beta^{13}Y^{11}u^{15}\\
&+\beta^{13}Y^{11}u^3+\beta^{13}Y^4Z^7u^{16}+\beta^{13}Y^4Z^7u^4+\beta^{12}Y^{12}u^{15}+\beta^{12}Y^{12}u^{12}\\
&+\beta^{12}Y^{12}u^9+\beta^{12}Y^{12}u^6+\beta^{11}Y^{13}u^{15}+\beta^{11}Y^{13}u^3+\beta^{11}Y^6Z^7u^{16}\\
&+\beta^{11}Y^6Z^7u^4+\beta^{10}Y^{14}u^{15}+\beta^{10}Y^{14}u^3+\beta^{10}Y^7Z^7u^{16}+\beta^{10}Y^7Z^7u^4\\
&+\beta^9Y^{15}u^{15}+\beta^9Y^{15}u^9+\beta^9Y^8Z^7u^{22}+\beta^9Y^8Z^7u^4+\beta^8Y^{16}u^{21}+\beta^8Y^{16}u^{18}\\
&+\beta^8Y^{16}u^9+\beta^8Y^{16}+\beta^8Y^9Z^7u^{22}+\beta^8Y^9Z^7u^{16}+\beta^7Y^{17}u^{15}+\beta^7Y^{17}u^3\\
&+\beta^7Y^{10}Z^7u^{16}+\beta^7Y^{10}Z^7u^4+\beta^6Y^{18}u^{15}+\beta^6Y^{18}u^6+\beta^6Y^{11}Z^7u^{22}\\
&+\beta^6Y^{11}Z^7u^4+\beta^6Y^4Z^{14}u^{11}+\beta^6Y^4Z^{14}u^8+\beta^5Y^{19}u^{21}+\beta^5Y^{19}u^9\\
&+\beta^5Y^{12}Z^7u^{16}+\beta^5Y^{12}Z^7u^4+\beta^4Y^{20}u^{21}+\beta^4Y^{20}u^{12}+\beta^4Y^{13}Z^7u^{22}\\
&+\beta^4Y^{13}Z^7u^{16}+\beta^4Y^6Z^{14}u^{11}+\beta^4Y^6Z^{14}u^8+\beta^3Y^{21}u^{15}+\beta^3Y^{14}Z^7u^{16}\\
&+\beta^3Y^7Z^{14}u^{11}+\beta^3Z^{21}u^{12}+\beta^2Y^{22}u^{18}+\beta^2Y^{15}Z^7u^{22}+\beta^2Y^8Z^{14}u^8\\
&+\beta^2YZ^{21}u^{12}+\beta Y^{23}u^{21}+\beta Y^{16}Z^7u^{22}+\beta Y^9Z^{14}u^{11}+\beta Y^2Z^{21}u^{12},\\
a_1(\beta,Y,Z):=\;&\beta^{21}Z^2u^{19}+\beta^{21}Z^2u^{13}+\beta^{21}Z^2u^7+\beta^{21}Z^2u+\beta^{20}YZ^2u^{19}+\beta^{20}YZ^2u^{13}\\
&+\beta^{20}YZ^2u^7+\beta^{20}YZ^2u+\beta^{18}Y^3Z^2u^{19}+\beta^{18}Y^3Z^2u^{13}+\beta^{18}Y^3Z^2u^7\\
&+\beta^{18}Y^3Z^2u+\beta^{17}Y^4Z^2u^{19}+\beta^{17}Y^4Z^2u^{13}+\beta^{17}Y^4Z^2u^7+\beta^{17}Y^4Z^2u\\
&+\beta^{15}Y^6Z^2u^{13}+\beta^{15}Y^6Z^2u+\beta^{14}Y^7Z^2u^{13}+\beta^{14}Y^7Z^2u+\beta^{13}Y^8Z^2u^{13}\\
&+\beta^{13}Y^8Z^2u+\beta^{11}Y^{10}Z^2u^{13}+\beta^{11}Y^{10}Z^2u+\beta^{10}Y^{11}Z^2u^{13}+\beta^{10}Y^{11}Z^2u\\
&+\beta^9Y^{12}Z^2u^{13}+\beta^9Y^{12}Z^2u^7+\beta^8Y^{13}Z^2u^7+\beta^8Y^{13}Z^2u+\beta^7Y^{14}Z^2u^{13}\\
&+\beta^7Y^{14}Z^2u+\beta^6Y^{15}Z^2u^{13}+\beta^6Y^{15}Z^2u^7+\beta^5Y^{16}Z^2u^{19}+\beta^5Y^{16}Z^2u^7\\
&+\beta^4Y^{17}Z^2u^{19}+\beta^4Y^{17}Z^2u^{13}+\beta^3Y^{18}Z^2u^{13}+\beta^3Y^4Z^{16}u^9+\beta^2Y^{19}Z^2u^{19}\\
&+\beta^2Y^5Z^{16}u^9+\beta Y^{20}Z^2u^{19}+\beta Y^6Z^{16}u^9,\\
a_2(\beta,Y,Z):=\;&\beta^{18}Z^4u^{23}+\beta^{18}Z^4u^{20}+\beta^{18}Z^4u^{11}+\beta^{18}Z^4u^8+\beta^{16}Y^2Z^4u^{23}\\
&+\beta^{16}Y^2Z^4u^{20}+\beta^{16}Y^2Z^4u^{11}+\beta^{16}Y^2Z^4u^8+\beta^{15}Y^3Z^4u^{23}+\beta^{15}Y^3Z^4u^{11}\\
&+\beta^{14}Y^4Z^4u^{23}+\beta^{14}Y^4Z^4u^{11}+\beta^{13}Y^5Z^4u^{23}+\beta^{13}Y^5Z^4u^{11}+\beta^{11}Y^7Z^4u^{23}\\
&+\beta^{11}Y^7Z^4u^{11}+\beta^{10}Y^8Z^4u^{23}+\beta^{10}Y^8Z^4u^{11}+\beta^9Y^9Z^4u^{23}+\beta^9Y^9Z^4u^{17}\\
&+\beta^9Y^2Z^{11}u^{18}+\beta^9Y^2Z^{11}u^6+\beta^8Y^{10}Z^4u^{17}+\beta^8Y^{10}Z^4u^{11}+\beta^8Y^3Z^{11}u^{18}\\
&+\beta^8Y^3Z^{11}u^6+\beta^7Y^{11}Z^4u^{23}+\beta^7Y^{11}Z^4u^{11}+\beta^6Y^{12}Z^4u^{23}+\beta^6Y^{12}Z^4u^{17}\\
&+\beta^6Y^{12}Z^4u^{11}+\beta^6Y^{12}Z^4u^8+\beta^6Y^5Z^{11}u^{18}+\beta^6Y^5Z^{11}u^6+\beta^5Y^{13}Z^4u^{23}\\
&+\beta^5Y^{13}Z^4u^{11}+\beta^4Y^{14}Z^4u^{17}+\beta^4Y^{14}Z^4u^8+\beta^4Y^7Z^{11}u^{18}+\beta^4Y^7Z^{11}u^6\\
&+\beta^3Y^{15}Z^4u^{23}+\beta^3Y^{15}Z^4u^{11}+\beta^3Y^8Z^{11}u^6+\beta^3YZ^{18}u^{13}+\beta^2Y^{16}Z^4u^{20}
\end{aligned}
$$

$$
\begin{aligned}
&+\beta^2Y^{16}Z^4u^{17}+\beta^2Y^9Z^{11}u^{18}+\beta^2Y^2Z^{18}u^{13}+\beta Y^{17}Z^4u^{23}+\beta Y^{17}Z^4u^{17}\\
&+\beta Y^{10}Z^{11}u^{18}+\beta Y^3Z^{18}u^{13}+Y^{18}Z^4u^{23}+Y^{18}Z^4u^{20}+Y^4Z^{18}u^{13}+Y^4Z^{18}u^{10},\\
a_3(\beta,Y,Z):=&\beta^{15}Z^6u^{21}+\beta^{15}Z^6u^{15}+\beta^{15}Z^6u^9+\beta^{15}Z^6u^3+\beta^{14}YZ^6u^{21}+\beta^{14}YZ^6u^{15}\\
&+\beta^{14}YZ^6u^9+\beta^{14}YZ^6u^3+\beta^{13}Y^2Z^6u^{21}+\beta^{13}Y^2Z^6u^{15}+\beta^{13}Y^2Z^6u^9\\
&+\beta^{13}Y^2Z^6u^3+\beta^{11}Y^4Z^6u^{21}+\beta^{11}Y^4Z^6u^{15}+\beta^{11}Y^4Z^6u^9+\beta^{11}Y^4Z^6u^3\\
&+\beta^{10}Y^5Z^6u^{21}+\beta^{10}Y^5Z^6u^{15}+\beta^{10}Y^5Z^6u^9+\beta^{10}Y^5Z^6u^3+\beta^9Y^6Z^6u^{15}\\
&+\beta^9Y^6Z^6u^3+\beta^8Y^7Z^6u^{21}+\beta^8Y^7Z^6u^9+\beta^7Y^8Z^6u^{21}+\beta^7Y^8Z^6u^{15}+\beta^7Y^8Z^6u^9\\
&+\beta^7Y^8Z^6u^3+\beta^6Y^9Z^6u^{15}+\beta^6Y^9Z^6u^3+\beta^5Y^{10}Z^6u^{21}+\beta^5Y^{10}Z^6u^{15}\\
&+\beta^5Y^{10}Z^6u^9+\beta^5Y^{10}Z^6u^3+\beta^4Y^{11}Z^6u^{21}+\beta^4Y^{11}Z^6u^9+\beta^3Y^{12}Z^6u^{21}\\
&+\beta^3Y^{12}Z^6u^{15}+\beta^3Y^{12}Z^6u^9+\beta^2Y^{13}Z^6u^{15}+\beta Y^{14}Z^6u^{15},\\
a_4(\beta,Y,Z):=&\beta^{15}Y^4Zu^{18}+\beta^{15}Y^4Zu^6+\beta^{14}Y^5Zu^{18}+\beta^{14}Y^5Zu^6+\beta^{13}Y^6Zu^{18}\\
&+\beta^{13}Y^6Zu^6+\beta^{12}Z^8u^{19}+\beta^{12}Z^8u^{16}+\beta^{12}Z^8u^{13}+\beta^{12}Z^8u^{10}\\
&+\beta^{11}Y^8Zu^{18}+\beta^{11}Y^8Zu^6+\beta^{10}Y^9Zu^{18}+\beta^{10}Y^9Zu^6+\beta^9Y^{10}Zu^{18}\\
&+\beta^9Y^{10}Zu^6+\beta^9Y^3Z^8u^{19}+\beta^9Y^3Z^8u^{13}+\beta^8Y^4Z^8u^{16}+\beta^8Y^4Z^8u^{10}\\
&+\beta^7Y^{12}Zu^{18}+\beta^7Y^{12}Zu^6+\beta^6Y^{13}Zu^{18}+\beta^6Y^{13}Zu^6+\beta^6Y^6Z^8u^{19}\\
&+\beta^6Y^6Z^8u^{10}+\beta^5Y^{14}Zu^{18}+\beta^5Y^{14}Zu^6+\beta^4Y^8Z^8u^{16}+\beta^4Y^8Z^8u^{13}\\
&+\beta^3Y^{16}Zu^{18}+\beta^3Y^2Z^{15}u^{14}+\beta^3Y^2Z^{15}u^8+\beta^2Y^{17}Zu^{18}+\beta^2Y^{10}Z^8u^{19}\\
&+\beta^2Y^{10}Z^8u^{10}+\beta^2Y^3Z^{15}u^{14}+\beta^2Y^3Z^{15}u^8+\beta Y^{18}Zu^{18}+\beta Y^{11}Z^8u^{19}\\
&+\beta Y^{11}Z^8u^{13}+\beta Y^4Z^{15}u^{14}+\beta Y^4Z^{15}u^8+Y^{12}Z^8u^{19}+Y^{12}Z^8u^{16},\\
a_5(\beta,Y,Z):=&\beta^9Z^{10}u^{11}+\beta^9Z^{10}u^5+\beta^8YZ^{10}u^{11}+\beta^8YZ^{10}u^5+\beta^6Y^3Z^{10}u^{11}\\
&+\beta^6Y^3Z^{10}u^5+\beta^4Y^5Z^{10}u^{11}+\beta^4Y^5Z^{10}u^5+\beta^3Y^6Z^{10}u^5+\beta^2Y^7Z^{10}u^{11}\\
&+\beta Y^8Z^{10}u^{11},\\
a_6(\beta,Y,Z):=&\beta^9Y^4Z^5u^{20}+\beta^9Y^4Z^5u^8+\beta^8Y^5Z^5u^{20}+\beta^8Y^5Z^5u^8+\beta^6Y^7Z^5u^{20}\\
&+\beta^6Y^7Z^5u^8+\beta^6Z^{12}u^{15}+\beta^6Z^{12}u^{12}+\beta^6Z^{12}u^9+\beta^6Z^{12}u^6+\beta^4Y^9Z^5u^{20}\\
&+\beta^4Y^9Z^5u^8+\beta^4Y^2Z^{12}u^{15}+\beta^4Y^2Z^{12}u^{12}+\beta^4Y^2Z^{12}u^9+\beta^4Y^2Z^{12}u^6\\
&+\beta^3Y^{10}Z^5u^8+\beta^3Y^3Z^{12}u^9+\beta^2Y^{11}Z^5u^{20}+\beta^2Y^4Z^{12}u^{15}+\beta^2Y^4Z^{12}u^{12}\\
&+\beta^2Y^4Z^{12}u^6+\beta Y^{12}Z^5u^{20}+\beta Y^5Z^{12}u^9+Y^6Z^{12}u^{15}+Y^6Z^{12}u^{12},\\
a_7(\beta,Y,Z):=&\beta^{15}Y^2u^{17}+\beta^{15}Y^2u^5+\beta^{14}Y^3u^{17}+\beta^{14}Y^3u^5+\beta^{13}Y^4u^{17}+\beta^{13}Y^4u^5\\
&+\beta^{11}Y^6u^{17}+\beta^{11}Y^6u^5+\beta^{10}Y^7u^{17}+\beta^{10}Y^7u^5+\beta^9Y^8u^{17}+\beta^9Y^8u^5\\
&+\beta^7Y^{10}u^{17}+\beta^7Y^{10}u^5+\beta^6Y^{11}u^{17}+\beta^6Y^{11}u^5+\beta^5Y^{12}u^{17}+\beta^5Y^{12}u^5\\
&+\beta^3Y^{14}u^{17}+\beta^3Z^{14}u^{13}+\beta^2Y^{15}u^{17}+\beta^2YZ^{14}u^{13}+\beta Y^{16}u^{17}\\
&+\beta Y^2Z^{14}u^{13},\\
a_8(\beta,Y,Z):=&\beta^6Y^8Z^2u^{15}+\beta^6Y^8Z^2u^{12}+\beta^4Y^{10}Z^2u^{15}+\beta^4Y^{10}Z^2u^{12}+\beta^3Y^{11}Z^2u^{15}\\
&+\beta^3Y^4Z^9u^{16}+\beta^3Y^4Z^9u^{10}+\beta^2Y^{12}Z^2u^{12}+\beta^2Y^5Z^9u^{16}+\beta^2Y^5Z^9u^{10}\\
&+\beta Y^{13}Z^2u^{15}+\beta Y^6Z^9u^{16}+\beta Y^6Z^9u^{10},\\
a_9(\beta,Y,Z):=&\beta^9Y^2Z^4u^{19}+\beta^9Y^2Z^4u^7+\beta^8Y^3Z^4u^{19}+\beta^8Y^3Z^4u^7+\beta^6Y^5Z^4u^{19}\\
&+\beta^6Y^5Z^4u^7+\beta^4Y^7Z^4u^{19}+\beta^4Y^7Z^4u^7+\beta^3Y^8Z^4u^{13}+\beta^3Y^8Z^4u^7\\
&+\beta^2Y^9Z^4u^{19}+\beta^2Y^9Z^4u^{13}+\beta Y^{10}Z^4u^{19}+\beta Y^{10}Z^4u^{13},\\
a_{10}(\beta,Y,Z):=&\beta^3Y^5Z^6u^{17}+\beta^2Y^6Z^6u^{17}+\beta Y^7Z^6u^{17}+Y^8Z^6u^{17}+Y^8Z^6u^{14},\\
a_{11}(\beta,Y,Z):=&\beta^3Y^2Z^8u^9+\beta^2Y^3Z^8u^9+\beta Y^4Z^8u^9,\\
a_{12}(\beta,Y,Z):=&\beta^9Z^3u^{18}+\beta^9Z^3u^{12}+\beta^8YZ^3u^{18}+\beta^8YZ^3u^{12}+\beta^6Y^3Z^3u^{18}+\beta^6Y^3Z^3u^{12}\\
&+\beta^4Y^5Z^3u^{18}+\beta^4Y^5Z^3u^{12}+\beta^3Y^6Z^3u^{18}+\beta^2Y^7Z^3u^{12}+\beta Y^8Z^3u^{12},\\
a_{13}(\beta,Y,Z):=&0,\\
a_{14}(\beta,Y,Z):=&\beta^9Yu^{19}+\beta^9Yu^{13}+\beta^8Y^2u^{19}+\beta^8Y^2u^{13}+\beta^6Y^4u^{19}+\beta^6Y^4u^{10}\\
&+\beta^4Y^6u^{19}+\beta^4Y^6u^{10}+\beta^3Y^7u^{13}+\beta^3Z^7u^{14}+\beta^2Y^8u^{19}+\beta^2Y^8u^{13}\\
&+\beta^2Y^8u^{10}+\beta^2YZ^7u^{14}+\beta Y^9u^{19}+\beta Y^2Z^7u^{14},
\end{aligned}
$$

$$a_{15}(\beta,Y,Z) := \beta^3Y^4Z^2u^{17} + \beta^3Y^4Z^2u^{11} + \beta^2Y^5Z^2u^{17} + \beta^2Y^5Z^2u^{11} + \beta Y^6Z^2u^{17} + \beta Y^6Z^2u^{11},$$
$$a_{16}(\beta,Y,Z) := \beta^3YZ^4u^{15} + \beta^2Y^2Z^4u^{15} + \beta Y^3Z^4u^{15} + Y^4Z^4u^{15} + Y^4Z^4u^{12},$$
$$a_{17}(\beta,Y,Z) := 0,$$
$$a_{18}(\beta,Y,Z) := \beta^3Y^2Zu^{16} + \beta^2Y^3Zu^{16} + \beta Y^4Zu^{16},$$
$$a_{19}(\beta,Y,Z) := 0,$$
$$a_{20}(\beta,Y,Z) := 0,$$
$$a_{21}(\beta,Y,Z) := \beta^3u^{15} + \beta^2Yu^{15} + \beta Y^2u^{15}.$$

Appendix B. **Verification code for Proposition 6.1.** The following MAGMA program checks $P \mid E_2$ and $H = PR$ over $\mathbb{F}_2[u,\beta,X,Y,Z]$ from the coefficients printed above. It is also written to `verify_factorization_H.m` when this source is compiled. The test uses exact polynomial arithmetic and prints `Verification passed` only if both divisions succeed.

```
F2 := GF(2);
R<u,b,X,Y,Z> := PolynomialRing(F2,5);
g := b^12*u^9+b^12*u^6+b^12*u^3+b^12+b^9*X*Z^2*u^10+b^9*X*Z^2*u^4+b^9*Y^3*u^9
     +b^9*Y^3*u^3+b^8*X*Y*Z^2*u^10+b^8*X*Y*Z^2*u^4+b^8*Y^4*u^6+b^8*Y^4+b^6*X^2*Z^4*u^8
     +b^6*X^2*Z^4*u^5+b^6*Y^6*u^6+b^6*Y^6*u^3+b^5*X^7*u^8+b^5*X^7*u^5+b^5*X*Y^4*Z^2*u^10
     +b^5*X*Y^4*Z^2*u^7+b^4*X^7*Y*u^8+b^4*X^7*Y*u^5+b^4*X^2*Y^2*Z^4*u^8
     +b^4*X^2*Y^2*Z^4*u^5+b^4*X*Y^5*Z^2*u^10+b^4*X*Y^5*Z^2*u^7+b^4*Y^8*u^9+b^4*Y^8
     +b^3*X^7*Y^2*u^5+b^3*X^4*Y^4*Z*u^6+b^3*X^3*Z^6*u^6+b^3*X^3*Z^6*u^3
     +b^3*X^2*Y^3*Z^4*u^5+b^3*X*Y^6*Z^2*u^4+b^3*Y^9*u^3+b^3*Y^2*Z^7*u^4+b^2*X^8*Z^2*u^6
     +b^2*X^7*Y^3*u^8+b^2*X^5*Y^2*Z^3*u^7+b^2*X^4*Y^5*Z*u^6+b^2*X^3*Y*Z^6*u^3
     +b^2*X*Y^7*Z^2*u^7+b^2*X*Y^7*Z^2*u^4+b^2*X*Z^9*u^5+b^2*Y^10*u^6+b^2*Y^3*Z^7*u^4
     +b*X^7*Y^4*u^8+b*X^4*Y^6*Z*u^6+b*X^3*Y^2*Z^6*u^6+b*X^3*Y^2*Z^6*u^3
     +b*X^2*Y^5*Z^4*u^5+b*X*Y^8*Z^2*u^7+b*Y^11*u^9+b*Y^4*Z^7*u^4;
h := u^5*(b+Y)^2*(b^3*X^6*u^3+b^3*X^6+b^3*Y^4*Z^2*u^5+b^3*Y^4*Z^2*u^2+b^2*X^6*Y*u^3
     +b^2*X^6*Y+b^2*Y^5*Z^2*u^5+b^2*Y^5*Z^2*u^2+b*X^6*Y^2*u^3+b*X^6*Y^2+b*Y^6*Z^2*u^5
     +b*Y^6*Z^2*u^2+X^7*Z^2*u+X^4*Y^2*Z^3*u^2+X^2*Y*Z^6*u+X*Y^4*Z^4*u^3+Y^7*Z^2*u^5
     +Z^9);
a0 := b^24*u^21+b^24*u^18+b^24*u^15+b^24*u^12+b^24*u^9+b^24*u^6+b^24*u^3+b^24
      +b^21*Y^3*u^21+b^21*Y^3*u^15+b^21*Y^3*u^9+b^21*Y^3*u^3+b^20*Y^4*u^21+b^20*Y^4*u^15
      +b^20*Y^4*u^9+b^20*Y^4*u^3+b^18*Y^6*u^18+b^18*Y^6*u^15+b^18*Y^6*u^6+b^18*Y^6*u^3
      +b^17*Y^7*u^21+b^17*Y^7*u^15+b^17*Y^7*u^9+b^17*Y^7*u^3+b^16*Y^8*u^15+b^16*Y^8*u^12
      +b^16*Y^8*u^3+b^16*Y^8+b^15*Y^9*u^15+b^15*Y^9*u^3+b^15*Y^2*Z^7*u^16
      +b^15*Y^2*Z^7*u^4+b^14*Y^10*u^15+b^14*Y^10*u^3+b^14*Y^3*Z^7*u^16+b^14*Y^3*Z^7*u^4
      +b^13*Y^11*u^15+b^13*Y^11*u^3+b^13*Y^4*Z^7*u^16+b^13*Y^4*Z^7*u^4+b^12*Y^12*u^15
      +b^12*Y^12*u^12+b^12*Y^12*u^9+b^12*Y^12*u^6+b^11*Y^13*u^15+b^11*Y^13*u^3
      +b^11*Y^6*Z^7*u^16+b^11*Y^6*Z^7*u^4+b^10*Y^14*u^15+b^10*Y^14*u^3+b^10*Y^7*Z^7*u^16
      +b^10*Y^7*Z^7*u^4+b^9*Y^15*u^15+b^9*Y^15*u^9+b^9*Y^8*Z^7*u^22+b^9*Y^8*Z^7*u^4
      +b^8*Y^16*u^21+b^8*Y^16*u^18+b^8*Y^16*u^9+b^8*Y^16+b^8*Y^9*Z^7*u^22
      +b^8*Y^9*Z^7*u^16+b^7*Y^17*u^15+b^7*Y^17*u^3+b^7*Y^10*Z^7*u^16+b^7*Y^10*Z^7*u^4
      +b^6*Y^18*u^15+b^6*Y^18*u^6+b^6*Y^11*Z^7*u^22+b^6*Y^11*Z^7*u^4+b^6*Y^4*Z^14*u^11
      +b^6*Y^4*Z^14*u^8+b^5*Y^19*u^21+b^5*Y^19*u^9+b^5*Y^12*Z^7*u^16+b^5*Y^12*Z^7*u^4
      +b^4*Y^20*u^21+b^4*Y^20*u^12+b^4*Y^13*Z^7*u^22+b^4*Y^13*Z^7*u^16+b^4*Y^6*Z^14*u^11
      +b^4*Y^6*Z^14*u^8+b^3*Y^21*u^15+b^3*Y^14*Z^7*u^16+b^3*Y^7*Z^14*u^11+b^3*Z^21*u^12
      +b^2*Y^22*u^18+b^2*Y^15*Z^7*u^22+b^2*Y^8*Z^14*u^8+b^2*Y*Z^21*u^12+b*Y^23*u^21
      +b*Y^16*Z^7*u^22+b*Y^9*Z^14*u^11+b*Y^2*Z^21*u^12;
a1 := b^21*Z^2*u^19+b^21*Z^2*u^13+b^21*Z^2*u^7+b^21*Z^2*u+b^20*Y*Z^2*u^19
      +b^20*Y*Z^2*u^13+b^20*Y*Z^2*u^7+b^20*Y*Z^2*u+b^18*Y^3*Z^2*u^19+b^18*Y^3*Z^2*u^13
      +b^18*Y^3*Z^2*u^7+b^18*Y^3*Z^2*u+b^17*Y^4*Z^2*u^19+b^17*Y^4*Z^2*u^13
      +b^17*Y^4*Z^2*u^7+b^17*Y^4*Z^2*u+b^15*Y^6*Z^2*u^13+b^15*Y^6*Z^2*u+b^14*Y^7*Z^2*u^13
      +b^14*Y^7*Z^2*u+b^13*Y^8*Z^2*u^13+b^13*Y^8*Z^2*u+b^11*Y^10*Z^2*u^13+b^11*Y^10*Z^2*u
      +b^10*Y^11*Z^2*u^13+b^10*Y^11*Z^2*u+b^9*Y^12*Z^2*u^13+b^9*Y^12*Z^2*u^7
      +b^8*Y^13*Z^2*u^7+b^8*Y^13*Z^2*u+b^7*Y^14*Z^2*u^13+b^7*Y^14*Z^2*u+b^6*Y^15*Z^2*u^13
      +b^6*Y^15*Z^2*u^7+b^5*Y^16*Z^2*u^19+b^5*Y^16*Z^2*u^7+b^4*Y^17*Z^2*u^19
      +b^4*Y^17*Z^2*u^13+b^3*Y^18*Z^2*u^13+b^3*Y^4*Z^16*u^9+b^2*Y^19*Z^2*u^19
      +b^2*Y^5*Z^16*u^9+b*Y^20*Z^2*u^19+b*Y^6*Z^16*u^9;
a2 := b^18*Z^4*u^23+b^18*Z^4*u^20+b^18*Z^4*u^11+b^18*Z^4*u^8+b^16*Y^2*Z^4*u^23
      +b^16*Y^2*Z^4*u^20+b^16*Y^2*Z^4*u^11+b^16*Y^2*Z^4*u^8+b^15*Y^3*Z^4*u^23
      +b^15*Y^3*Z^4*u^11+b^14*Y^4*Z^4*u^23+b^14*Y^4*Z^4*u^11+b^13*Y^5*Z^4*u^23
      +b^13*Y^5*Z^4*u^11+b^11*Y^7*Z^4*u^23+b^11*Y^7*Z^4*u^11+b^10*Y^8*Z^4*u^23
      +b^10*Y^8*Z^4*u^11+b^9*Y^9*Z^4*u^23+b^9*Y^9*Z^4*u^17+b^9*Y^2*Z^11*u^18
      +b^9*Y^2*Z^11*u^6+b^8*Y^10*Z^4*u^17+b^8*Y^10*Z^4*u^11+b^8*Y^3*Z^11*u^18
      +b^8*Y^3*Z^11*u^6+b^7*Y^11*Z^4*u^23+b^7*Y^11*Z^4*u^11+b^6*Y^12*Z^4*u^23
      +b^6*Y^12*Z^4*u^17+b^6*Y^12*Z^4*u^11+b^6*Y^12*Z^4*u^8+b^6*Y^5*Z^11*u^18
      +b^6*Y^5*Z^11*u^6+b^5*Y^13*Z^4*u^23+b^5*Y^13*Z^4*u^11+b^4*Y^14*Z^4*u^17
      +b^4*Y^14*Z^4*u^8+b^4*Y^7*Z^11*u^18+b^4*Y^7*Z^11*u^6+b^3*Y^15*Z^4*u^23
```

```
      +b^3*Y^15*Z^4*u^11+b^3*Y^8*Z^11*u^6+b^3*Y*Z^18*u^13+b^2*Y^16*Z^4*u^20
      +b^2*Y^16*Z^4*u^17+b^2*Y^9*Z^11*u^18+b^2*Y^2*Z^18*u^13+b*Y^17*Z^4*u^23
      +b*Y^17*Z^4*u^17+b*Y^10*Z^11*u^18+b*Y^3*Z^18*u^13+Y^18*Z^4*u^23+Y^18*Z^4*u^20
      +Y^4*Z^18*u^13+Y^4*Z^18*u^10;
a3 := b^15*Z^6*u^21+b^15*Z^6*u^15+b^15*Z^6*u^9+b^15*Z^6*u^3+b^14*Y*Z^6*u^21
      +b^14*Y*Z^6*u^15+b^14*Y*Z^6*u^9+b^14*Y*Z^6*u^3+b^13*Y^2*Z^6*u^21+b^13*Y^2*Z^6*u^15
      +b^13*Y^2*Z^6*u^9+b^13*Y^2*Z^6*u^3+b^11*Y^4*Z^6*u^21+b^11*Y^4*Z^6*u^15
      +b^11*Y^4*Z^6*u^9+b^11*Y^4*Z^6*u^3+b^10*Y^5*Z^6*u^21+b^10*Y^5*Z^6*u^15
      +b^10*Y^5*Z^6*u^9+b^10*Y^5*Z^6*u^3+b^9*Y^6*Z^6*u^15+b^9*Y^6*Z^6*u^3
      +b^8*Y^7*Z^6*u^21+b^8*Y^7*Z^6*u^9+b^7*Y^8*Z^6*u^21+b^7*Y^8*Z^6*u^15+b^7*Y^8*Z^6*u^9
      +b^7*Y^8*Z^6*u^3+b^6*Y^9*Z^6*u^15+b^6*Y^9*Z^6*u^3+b^5*Y^10*Z^6*u^21
      +b^5*Y^10*Z^6*u^15+b^5*Y^10*Z^6*u^9+b^5*Y^10*Z^6*u^3+b^4*Y^11*Z^6*u^21
      +b^4*Y^11*Z^6*u^9+b^3*Y^12*Z^6*u^21+b^3*Y^12*Z^6*u^15+b^3*Y^12*Z^6*u^9
      +b^2*Y^13*Z^6*u^15+b*Y^14*Z^6*u^15;
a4 := b^15*Y^4*Z*u^18+b^15*Y^4*Z*u^6+b^14*Y^5*Z*u^18+b^14*Y^5*Z*u^6+b^13*Y^6*Z*u^18
      +b^13*Y^6*Z*u^6+b^12*Z^8*u^19+b^12*Z^8*u^16+b^12*Z^8*u^13+b^12*Z^8*u^10
      +b^11*Y^8*Z*u^18+b^11*Y^8*Z*u^6+b^10*Y^9*Z*u^18+b^10*Y^9*Z*u^6+b^9*Y^10*Z*u^18
      +b^9*Y^10*Z*u^6+b^9*Y^3*Z^8*u^19+b^9*Y^3*Z^8*u^13+b^8*Y^4*Z^8*u^16+b^8*Y^4*Z^8*u^10
      +b^7*Y^12*Z*u^18+b^7*Y^12*Z*u^6+b^6*Y^13*Z*u^18+b^6*Y^13*Z*u^6+b^6*Y^6*Z^8*u^19
      +b^6*Y^6*Z^8*u^10+b^5*Y^14*Z*u^18+b^5*Y^14*Z*u^6+b^4*Y^8*Z^8*u^16+b^4*Y^8*Z^8*u^13
      +b^3*Y^16*Z*u^18+b^3*Y^2*Z^15*u^14+b^3*Y^2*Z^15*u^8+b^2*Y^17*Z*u^18
      +b^2*Y^10*Z^8*u^19+b^2*Y^10*Z^8*u^10+b^2*Y^3*Z^15*u^14+b^2*Y^3*Z^15*u^8
      +b*Y^18*Z*u^18+b*Y^11*Z^8*u^19+b*Y^11*Z^8*u^13+b*Y^4*Z^15*u^14+b*Y^4*Z^15*u^8
      +Y^12*Z^8*u^19+Y^12*Z^8*u^16;
a5 := b^9*Z^10*u^11+b^9*Z^10*u^5+b^8*Y*Z^10*u^11+b^8*Y*Z^10*u^5+b^6*Y^3*Z^10*u^11
      +b^6*Y^3*Z^10*u^5+b^4*Y^5*Z^10*u^11+b^4*Y^5*Z^10*u^5+b^3*Y^6*Z^10*u^5
      +b^2*Y^7*Z^10*u^11+b*Y^8*Z^10*u^11;
a6 := b^9*Y^4*Z^5*u^20+b^9*Y^4*Z^5*u^8+b^8*Y^5*Z^5*u^20+b^8*Y^5*Z^5*u^8
      +b^6*Y^7*Z^5*u^20+b^6*Y^7*Z^5*u^8+b^6*Z^12*u^15+b^6*Z^12*u^12+b^6*Z^12*u^9
      +b^6*Z^12*u^6+b^4*Y^9*Z^5*u^20+b^4*Y^9*Z^5*u^8+b^4*Y^2*Z^12*u^15+b^4*Y^2*Z^12*u^12
      +b^4*Y^2*Z^12*u^9+b^4*Y^2*Z^12*u^6+b^3*Y^10*Z^5*u^8+b^3*Y^3*Z^12*u^9
      +b^2*Y^11*Z^5*u^20+b^2*Y^4*Z^12*u^15+b^2*Y^4*Z^12*u^12+b^2*Y^4*Z^12*u^6
      +b*Y^12*Z^5*u^20+b*Y^5*Z^12*u^9+Y^6*Z^12*u^15+Y^6*Z^12*u^12;
a7 := b^15*Y^2*u^17+b^15*Y^2*u^5+b^14*Y^3*u^17+b^14*Y^3*u^5+b^13*Y^4*u^17
      +b^13*Y^4*u^5+b^11*Y^6*u^17+b^11*Y^6*u^5+b^10*Y^7*u^17+b^10*Y^7*u^5+b^9*Y^8*u^17
      +b^9*Y^8*u^5+b^7*Y^10*u^17+b^7*Y^10*u^5+b^6*Y^11*u^17+b^6*Y^11*u^5+b^5*Y^12*u^17
      +b^5*Y^12*u^5+b^3*Y^14*u^17+b^3*Z^14*u^13+b^2*Y^15*u^17+b^2*Y*Z^14*u^13+b*Y^16*u^17
      +b*Y^2*Z^14*u^13;
a8 := b^6*Y^8*Z^2*u^15+b^6*Y^8*Z^2*u^12+b^4*Y^10*Z^2*u^15+b^4*Y^10*Z^2*u^12
      +b^3*Y^11*Z^2*u^15+b^3*Y^4*Z^9*u^16+b^3*Y^4*Z^9*u^10+b^2*Y^12*Z^2*u^12
      +b^2*Y^5*Z^9*u^16+b^2*Y^5*Z^9*u^10+b*Y^13*Z^2*u^15+b*Y^6*Z^9*u^16+b*Y^6*Z^9*u^10;
a9 := b^9*Y^2*Z^4*u^19+b^9*Y^2*Z^4*u^7+b^8*Y^3*Z^4*u^19+b^8*Y^3*Z^4*u^7
      +b^6*Y^5*Z^4*u^19+b^6*Y^5*Z^4*u^7+b^4*Y^7*Z^4*u^19+b^4*Y^7*Z^4*u^7+b^3*Y^8*Z^4*u^13
      +b^3*Y^8*Z^4*u^7+b^2*Y^9*Z^4*u^19+b^2*Y^9*Z^4*u^13+b*Y^10*Z^4*u^19+b*Y^10*Z^4*u^13;
a10 := b^3*Y^5*Z^6*u^17+b^2*Y^6*Z^6*u^17+b*Y^7*Z^6*u^17+Y^8*Z^6*u^17+Y^8*Z^6*u^14;
a11 := b^3*Y^2*Z^8*u^9+b^2*Y^3*Z^8*u^9+b*Y^4*Z^8*u^9;
a12 := b^9*Z^3*u^18+b^9*Z^3*u^12+b^8*Y*Z^3*u^18+b^8*Y*Z^3*u^12+b^6*Y^3*Z^3*u^18
       +b^6*Y^3*Z^3*u^12+b^4*Y^5*Z^3*u^18+b^4*Y^5*Z^3*u^12+b^3*Y^6*Z^3*u^18
       +b^2*Y^7*Z^3*u^12+b*Y^8*Z^3*u^12;
a13 := 0;
a14 := b^9*Y*u^19+b^9*Y*u^13+b^8*Y^2*u^19+b^8*Y^2*u^13+b^6*Y^4*u^19+b^6*Y^4*u^10
       +b^4*Y^6*u^19+b^4*Y^6*u^10+b^3*Y^7*u^13+b^3*Z^7*u^14+b^2*Y^8*u^19+b^2*Y^8*u^13
       +b^2*Y^8*u^10+b^2*Y*Z^7*u^14+b*Y^9*u^19+b*Y^2*Z^7*u^14;
a15 := b^3*Y^4*Z^2*u^17+b^3*Y^4*Z^2*u^11+b^2*Y^5*Z^2*u^17+b^2*Y^5*Z^2*u^11
       +b*Y^6*Z^2*u^17+b*Y^6*Z^2*u^11;
a16 := b^3*Y*Z^4*u^15+b^2*Y^2*Z^4*u^15+b*Y^3*Z^4*u^15+Y^4*Z^4*u^15+Y^4*Z^4*u^12;
a17 := 0;
a18 := b^3*Y^2*Z*u^16+b^2*Y^3*Z*u^16+b*Y^4*Z*u^16;
a19 := 0;
a20 := 0;
a21 := b^3*u^15+b^2*Y*u^15+b*Y^2*u^15;
P := a0 + a1*X^1 + a2*X^2 + a3*X^3 + a4*X^4 + a5*X^5 + a6*X^6 + a7*X^7 + a8*X^8
     + a9*X^9 + a10*X^10 + a11*X^11 + a12*X^12 + a13*X^13 + a14*X^14 + a15*X^15
     + a16*X^16 + a17*X^17 + a18*X^18 + a19*X^19 + a20*X^20 + a21*X^21;
d := u*(b+Y)^2;
n := g^3 + g^2*X*h + g*X^2*h^2 + b^2*Z*u*h^3;
E2 := d^2*(b*Y^2+b^2*Y+b^3)*h^7 + d^2*u*g*Z^2*h^6 + u*n^2*(X*h+g);
H := n*Z^2*d^2*h^6 + n^2*Z*d*h^3 + u*(b*X^2*h^2+g^2*(Y+b))*d^3*h^7 + n^3;
ok2, Q2 := IsDivisibleBy(E2,P);
assert ok2;
assert E2 eq P*Q2;
ok3, Rfac := IsDivisibleBy(H,P);
assert ok3;
```

```
assert H eq P*Rfac;
print "Verification passed".
```

REFERENCES

[1] Y. Aubry, G. McGuire and F. Rodier, A few more functions that are not APN infinitely often, *Finite Fields: Theory and Applications, Contemp. Math.*, American Mathematical Society, Providence, RI, **518** (2010), 23-31.

[2] D. Bartoli and M. Timpanella, On a conjecture on APN permutations, *Cryptogr. Commun.*, **14** (2022), 925-931.

[3] D. Bartoli and P. Stănică, Infinite families of APN permutations in constrained trivariate classes over $\mathbb{F}_{2^m}$, 2026. arXiv:2603.15146.

[4] F. Göloğlu and L. Kölsch, Triprojective almost perfect nonlinear permutations and functions, 2026. arXiv:2605.17545.

[5] C. Beierle, C. Carlet, G. Leander and L. Perrin, A further study of quadratic APN permutations in dimension nine, *Finite Fields Appl.*, **81** (2022), 102049.

[6] C. Beierle and G. Leander, New instances of quadratic APN functions, *IEEE Trans. Inf. Theory*, **68** (2022), 670-678.

[7] E. Biham and A. Shamir, Differential cryptanalysis of DES-like cryptosystems, *J. Cryptol.*, **4** (1991), 3-72.

[8] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system. I. The user language, *J. Symbolic Comput.*, **24** (1997), 235-265.

[9] A. Cafure and G. Matera, Improved explicit estimates on the number of solutions of equations over a finite field, *Finite Fields Appl.*, **12** (2006), 155-185.

[10] R. Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics, 52, Springer-Verlag, 1977.

[11] J. W. P. Hirschfeld, G. Korchmáros and F. Torres, *Algebraic Curves over a Finite Field*, Princeton University Press, 2013.

[12] K. Li and N. Kaleyski, Two new infinite families of APN functions in trivariate form, *IEEE Trans. Inf. Theory*, **70** (2024), 1436-1452.

[13] P. Stănică, Trivariate permutation project, Source Code, 2025. Available from: https://github.com/pstanica/trivariatePP-APN.

Received February 19, 2026; 1st revision August 19, 2026; 2nd revision October 16, 2026.