

Basis Rigidity of the AES S-box and Generic Rigidity of Inversion under Affine Transformations

Zheng Zhang *Na Zhang †

Abstract

The AES S-box is constructed from finite field inversion followed by a fixed affine transformation. Since inversion possesses intrinsic Frobenius symmetries among its coordinate realizations, we study how these basis symmetries are altered by outer affine transformations.

We first develop a deterministic rigidity criterion for transformed inversion and apply it to the AES S-box. This shows that the linear part of the AES S-box affine transformation alone makes the transformed inversion map basis rigid. We then investigate the corresponding generic problem when the outer invertible linear transformation varies. The existence of a nontrivial linear stabilizer is reduced to a conjugacy problem for semilinear candidates arising from two sided linear equivalences of inversion, which we characterize in terms of relative norms and Frobenius orbits. We also determine the dimensions of the associated centralizer algebras exactly. These structural results imply that, for a uniformly chosen outer linear transformation, the probability that the linear stabilizer is nontrivial is bounded by $2^{-\Omega(n^2)}$, with sharper finite dimensional bounds obtained from the exact conjugacy condition. Computational experiments independently verify the AES rigidity result, the conjugacy and centralizer formulas, and the finite dimensional estimates in small dimensions.

Keywords: AES S-box, finite field inversion, linear stabilizers, semilinear conjugacy.

1 Introduction

The AES S-box [6] is one of the most important nonlinear components in modern symmetric-key cryptography. Its construction is algebraic. Over $\mathbb{F}_{2^8}$, it is obtained from finite field inversion followed by a fixed affine transformation. This description makes the AES S-box a natural object for studying the interaction between finite field structure and coordinate realization.

A finite field map is represented as a vectorial function only after a basis over $\mathbb{F}_2$ is chosen. Different ordered bases generally lead to different coordinate realizations, but distinct bases can sometimes produce the same coordinate realization. Finite field inversion is a basic example. Because inversion commutes with Frobenius automorphisms, its coordinate realizations possess an intrinsic basis redundancy. In our previous work [12], we showed that these Frobenius symmetries account for all such collisions among ordered basis representations.

The AES S-box is obtained by placing a fixed affine layer on top of this highly symmetric inversion map. This makes AES a natural first case for asking how an outer transformation changes the basis rigidity of inversion. The same question can then be posed more generally. When inversion is followed by an arbitrary invertible linear map, when can the resulting map have a nontrivial linear stabilizer, and is this behavior typical or exceptional?

We study this question under linear changes of coordinates induced by finite field basis transformations. We consider both the behavior for a fixed outer linear map, with the AES S-box linear layer as a distinguished case, and the generic behavior when the outer linear map varies over $\text{GL}_n(\mathbb{F}_2)$.

*Corresponding author. Department of Mathematics, Towson University, 7800 York Rd, Towson, MD 21204, USA. Email: zhengzhang@towson.edu.

†Department of Mathematics, Towson University, 7800 York Rd, Towson, MD 21204, USA. Email: nzhang@towson.edu.

1.1 Related Work and Scope

The AES S-box has been studied extensively from the viewpoint of linear and affine equivalence. Biryukov et al. [1] developed algorithms for these equivalence problems and exhibited 2040 self-equivalence relations for the Rijndael S-box. Ranea and Preneel [7] further investigated self-equivalence encodings and centralizer structures arising in white-box implementations.

General two sided affine self-equivalences are broader than the common linear symmetry considered here, since the input and output transformations may differ and affine translations may also be allowed. A finite field basis change is more restrictive, since the same linear coordinate transformation acts simultaneously on both sides. Thus a function may possess many general self-equivalences while still being rigid under basis changes.

Different finite field representations of the AES S-box have also been studied through polynomial, matrix, and basis-dependent descriptions [8, 5]. These works describe how the algebraic form of the S-box changes with the chosen representation. Our question is different. We ask when two distinct ordered bases induce exactly the same coordinate realization.

The main algebraic input to our analysis is the classification of inversion equivalence pairs due to Yuan et al. [11]. In characteristic two and for $n \geq 4$, their result identifies the possible semilinear transformations associated with finite field inversion. This classification determines the semilinear candidates arising from two sided linear equivalences of inversion, but it does not determine which of them are compatible with a fixed outer linear transformation, nor how frequently such compatibility occurs when the outer transformation varies. These compatibility and counting questions are central to the present work.

Broader equivalence classes of inversion have also been considered. For $n \geq 5$, Kölsch [3] showed that every function CCZ-equivalent to inversion is EA-equivalent to it, and that every permutation in its CCZ class is affine equivalent to inversion. Such results concern membership in equivalence classes. By contrast, we fix an individual transformed inversion map and study its stabilizer under linear conjugation.

A separate line of work concerns generic stabilizer triviality. Ishizuka [2] investigates this question for extended-affine stabilizers of vectorial functions over finite fields. Our setting involves a different symmetry and a different probability space. We fix the nonlinear core as finite field inversion and vary only the outer invertible linear transformation. Genericity in the full function space therefore does not directly determine the exceptional proportion within this structured family. Our rigidity bounds are established independently.

In summary, the present paper lies between the theory of self-equivalences of cryptographic functions and the algebraic structure of finite field inversion. Our contribution is to determine how the semilinear equivalence structure of inversion interacts with a fixed or varying outer linear transformation, with the AES S-box providing the principal motivating example.

1.2 Our Contributions

Our contributions are as follows:

1. We derive a deterministic coefficient criterion for basis rigidity of transformed inversion. Applying it to the AES S-box linear layer shows that the AES S-box is basis rigid. No nonidentity linear change of basis preserves its coordinate realization. Moreover, this linear layer alone enforces the rigidity and the affine constant is not needed.
2. We characterize exactly which semilinear candidates arising from two sided linear equivalences of inversion can occur as linear symmetries of $A \circ J_n$ for some invertible outer linear map A . The resulting conjugacy criterion is expressed in terms of relative norms and Frobenius orbits. We also determine exactly the dimensions of the corresponding centralizer algebras.
3. Using the conjugacy criterion and the centralizer dimensions, we obtain a generic rigidity theorem for transformed inversion. For a uniformly chosen invertible outer linear transformation, the probability that the linear stabilizer is nontrivial is bounded by $2^{-\Omega(n^2)}$. We further derive computable finite dimensional refinements by retaining the exact conjugacy condition and grouping the admissible norm values according to their degrees over $\mathbb{F}_2$.

4. We provide independent computational verification of the theoretical results. A closure search on complete truth tables confirms the AES rigidity result without using the semilinear reduction. Exact enumeration determines the exceptional probabilities for $n = 3, 4, 5$, while direct matrix computations verify the conjugacy criterion, the centralizer dimension formula, and the grouped refined bound for all 3,537 nonidentity semilinear candidates in dimensions $3 \leq n \leq 8$. Monte Carlo sampling provides additional finite dimensional comparisons in dimensions $5 \leq n \leq 8$.

2 Deterministic Rigidity of Transformed Inversion

This section develops the deterministic framework needed to analyze basis rigidity for transformed inversion maps. We first relate basis collisions to linear stabilizers, then use the two sided linear equivalences of finite field inversion to identify the possible semilinear stabilizer candidates. We next derive coefficient compatibility conditions for a fixed outer linear transformation and apply them to the AES S-box. The resulting AES rigidity theorem serves as a concrete motivating case for the broader generic theory developed in Section 3.

2.1 Basis Representations and Linear Stabilizers

Let $\mathbb{F} = \mathbb{F}_{2^n}$, and fix an ordered reference basis $E = (e_1, \dots, e_n)$. For an ordered $\mathbb{F}_2$ -basis $B = (b_1, \dots, b_n)$, let $P_B \in \text{GL}_n(\mathbb{F}_2)$ be defined by

$$[x]_E = P_B[x]_B.$$

Let $F : \mathbb{F} \rightarrow \mathbb{F}$ be a map. We identify F with its coordinate realization in the reference basis E . Its realization in the basis B is

$$F_B = P_B^{-1} F P_B.$$

Definition 1. Two ordered $\mathbb{F}_2$ -bases B and B' are said to be *equivalent with respect to F* , written

$$B \sim_F B',$$

if

$$F_B = F_{B'}.$$

The *linear stabilizer* of F is

$$\text{Stab}(F) = \{T \in \text{GL}_n(\mathbb{F}_2) : TF = FT\}.$$

A direct conjugation argument gives

$$F_B = F_{B'} \iff P_{B'} P_B^{-1} \in \text{Stab}(F). \tag{1}$$

Definition 2. The map F is called *basis rigid* if

$$F_B = F_{B'} \implies B = B'$$

for all ordered $\mathbb{F}_2$ -bases B, B' of $\mathbb{F}$.

By (1),

$$F \text{ is basis rigid} \iff \text{Stab}(F) = \{I\}.$$

Moreover, the equivalence classes of ordered bases are precisely the cosets of $\text{Stab}(F)$ in $\text{GL}_n(\mathbb{F}_2)$. Since ordered $\mathbb{F}_2$ -bases of $\mathbb{F}$ are in bijection with $\text{GL}_n(\mathbb{F}_2)$, the number of distinct basis representations is

$$N_{\text{rep}}(F) = \frac{|\text{GL}_n(\mathbb{F}_2)|}{|\text{Stab}(F)|}.$$

2.2 Stabilizer Reduction for Affine Transformations of Inversion

Let $\mathbb{F} = \mathbb{F}_{2^n}$ and define the inversion map

$$J_n(x) = \begin{cases} x^{-1}, & x \neq 0, \\ 0, & x = 0. \end{cases}$$

Definition 3. For $A \in \text{GL}_n(\mathbb{F}_2)$ and $c \in \mathbb{F}$, define

$$F_{A,c}(x) = A(J_n(x)) + c.$$

We refer to $F_{A,c}$ as a transformed inversion map with an affine outer layer.

Let $\sigma(x) = x^2$ denote the Frobenius automorphism, and for $a \in \mathbb{F}^\times$ let

$$M_a(x) = ax.$$

Although $F_{A,c}$ contains an affine outer layer, a change of basis still acts through a single linear map on the input and output coordinate spaces. Hence its basis symmetries are governed by the linear stabilizer introduced in subsection 2.1.

For pure inversion, the linear stabilizer is the Frobenius group

$$\text{Stab}(J_n) = \langle \sigma \rangle = \{\sigma^r : 0 \leq r < n\}.$$

Thus inversion has an exact n -fold redundancy among ordered basis representations. After composition with an outer affine transformation, the resulting linear stabilizer need not be a subgroup of $\text{Stab}(J_n)$. We therefore use the classification of two sided linear equivalences of inversion. This yields semilinear candidates of the form $M_a\sigma^r$, which become linear symmetries of the transformed map precisely when they satisfy the compatibility conditions derived below.

Theorem 4 (Yuan et al. [11]). *Let $n \geq 4$ and $T, U \in \text{GL}_n(\mathbb{F}_2)$. Then*

$$J_n T = U J_n$$

if and only if there exist $a \in \mathbb{F}^\times$ and $0 \leq r < n$ such that

$$T = M_a \sigma^r, \quad U = M_{a^{-1}} \sigma^r.$$

This is the $p = 2$ case of Theorem 1 of Yuan et al. [11], rewritten in our notation and composition convention.

We now reduce the stabilizer of $F_{A,c}$ to this classification.

Lemma 5. *For $T \in \text{GL}_n(\mathbb{F}_2)$,*

$$T \in \text{Stab}(F_{A,c})$$

if and only if

$$T(c) = c \quad \text{and} \quad J_n T = (A^{-1} T A) J_n.$$

Proof. The relation $T F_{A,c} = F_{A,c} T$ is equivalent to

$$T A J_n(x) + T(c) = A J_n(Tx) + c.$$

Setting $x = 0$ gives $T(c) = c$, and substitution then yields

$$T A J_n = A J_n T,$$

or equivalently

$$J_n T = (A^{-1} T A) J_n.$$

The converse follows by reversing the argument. □

Theorem 6. *Let $n \geq 4$. Then*

$$\text{Stab}(F_{A,c}) = \{M_a \sigma^r : A^{-1} M_a \sigma^r A = M_{a^{-1}} \sigma^r, M_a \sigma^r(c) = c\},$$

where $a \in \mathbb{F}^\times$ and $0 \leq r < n$.

Proof. By Lemma 5, any $T \in \text{Stab}(F_{A,c})$ satisfies

$$T(c) = c, \quad J_n T = (A^{-1} T A) J_n.$$

Theorem 4 therefore gives $T = M_a \sigma^r$ and

$$A^{-1} M_a \sigma^r A = M_{a^{-1}} \sigma^r.$$

The converse follows from the same two results. $\square$

Thus, for a fixed outer linear map A , every linear symmetry must be one of the semilinear candidates $M_a \sigma^r$ and satisfy a specific compatibility relation with A . In the next subsection, we translate this relation into explicit coefficient conditions using the linearized polynomial representation of A . For later use, we write

$$T_{a,r} := M_a \sigma^r, \quad a \in \mathbb{F}^\times, \quad 0 \leq r < n.$$

2.3 Coefficient Compatibility and Deterministic Rigidity

The stabilizer reduction above restricts every linear symmetry of $A \circ J_n$ to a semilinear map of the form $M_a \sigma^r$. We now translate the remaining compatibility condition into constraints on the linearized polynomial coefficients of A .

Let

$$A(x) = \sum_{i=0}^{n-1} \lambda_i x^{2^i}, \quad \lambda_i \in \mathbb{F},$$

be the unique linearized polynomial representation of $A \in \text{GL}_n(\mathbb{F}_2)$, and write

$$S_A = \{i : \lambda_i \neq 0\}.$$

Proposition 7. *Let $n \geq 4$, and suppose*

$$T_{a,r} = M_a \sigma^r \in \text{Stab}(A \circ J_n),$$

where $a \in \mathbb{F}^\times$ and $0 \leq r < n$. Then, for every $i \in S_A$,

$$a^{2^i+1} = \lambda_i^{1-2^r}.$$

Consequently, for every $i, j \in S_A$,

$$\left(\frac{\lambda_j^{2^i+1}}{\lambda_i^{2^j+1}} \right)^{1-2^r} = 1.$$

Proof. By Theorem 6, with $c = 0$, the stabilizing condition is

$$M_a \sigma^r A = A M_{a^{-1}} \sigma^r.$$

Applying both sides to $x \in \mathbb{F}$ gives

$$a A(x)^{2^r} = A(a^{-1} x^{2^r}).$$

Using the linearized polynomial representation of A ,

$$\sum_{i=0}^{n-1} a \lambda_i^{2^r} x^{2^{i+r}} = \sum_{i=0}^{n-1} \lambda_i a^{-2^i} x^{2^{i+r}}.$$

Since $\sigma^n = I$, the Frobenius exponents are understood modulo n . Uniqueness of the linearized polynomial representation therefore gives

$$a\lambda_i^{2^r} = \lambda_i a^{-2^i}$$

for every i . Hence, whenever $\lambda_i \neq 0$,

$$a^{2^i+1} = \lambda_i^{1-2^r}.$$

For $i, j \in S_A$, raising the relation for i to the power $2^j + 1$ and the relation for j to the power $2^i + 1$ eliminates a and gives

$$\lambda_i^{(2^j+1)(1-2^r)} = \lambda_j^{(2^i+1)(1-2^r)}.$$

Rearranging yields

$$\left(\frac{\lambda_j^{2^i+1}}{\lambda_i^{2^j+1}} \right)^{1-2^r} = 1.$$

□

For $i, j \in S_A$, define

$$\Gamma_{ij} = \frac{\lambda_j^{2^i+1}}{\lambda_i^{2^j+1}} \in \mathbb{F}^\times.$$

Theorem 8. *Let $n \geq 4$. Suppose that the linearized polynomial coefficients of $A \in \text{GL}_n(\mathbb{F}_2)$ satisfy the following two conditions:*

1.

$$\gcd(2^n - 1, \{2^i + 1 : i \in S_A\}) = 1;$$

2. *for every $1 \leq r < n$, there exist $i, j \in S_A$ such that*

$$\text{ord}(\Gamma_{ij}) \nmid 2^r - 1.$$

Then

$$\text{Stab}(A \circ J_n) = \{I\}.$$

Proof. Let $M_a \sigma^r \in \text{Stab}(A \circ J_n)$.

If $r = 0$, Proposition 7 gives

$$a^{2^i+1} = 1$$

for every $i \in S_A$. Since the order of a also divides $2^n - 1$, the first condition forces $a = 1$.

Now suppose $1 \leq r < n$. Proposition 7 implies

$$\text{ord}(\Gamma_{ij}) \mid 2^r - 1$$

for every $i, j \in S_A$, contradicting the second condition. Hence no stabilizing map with $r \neq 0$ exists.

Therefore the identity is the only element of $\text{Stab}(A \circ J_n)$. □

Remark 1. *If $\lambda_0 \neq 0$, the first condition of Theorem 8 is automatic, since $2^0 + 1 = 2$ whereas $2^n - 1$ is odd.*

The criterion isolates the coefficient obstruction responsible for deterministic rigidity. We now apply it to the AES S-box linear layer, where a single pair of coefficients is sufficient to exclude every candidate with nonzero Frobenius exponent.

2.4 AES Basis Rigidity

We now apply Theorem 8 to the linear part of the AES S-box affine transformation. Following FIPS 197 [6], we use the field representation

$$\mathbb{F}_{2^8} = \mathbb{F}_2[t]/(t^8 + t^4 + t^3 + t + 1)$$

with the ordered polynomial basis

$$E = (1, t, \dots, t^7).$$

We identify a byte $\sum_{i=0}^7 b_i 2^i$ with the field element $\sum_{i=0}^7 b_i t^i$, where $b_i \in \mathbb{F}_2$. All byte values below are written in hexadecimal.

In this representation, the AES S-box is

$$S_{\text{AES}}(x) = A_{\text{AES}}(J_8(x)) + 63,$$

where A_{AES} is the invertible $\mathbb{F}_2$ -linear map defined by

$$A_{\text{AES}} \left(\sum_{i=0}^7 b_i t^i \right) = \sum_{i=0}^7 (b_i + b_{i+4} + b_{i+5} + b_{i+6} + b_{i+7}) t^i.$$

Here the bit indices are taken modulo 8, and the coefficients are added in $\mathbb{F}_2$.

The linearized polynomial representation of this map is

$$A_{\text{AES}}(x) = \sum_{i=0}^7 \lambda_i x^{2^i},$$

with

$$(\lambda_0, \dots, \lambda_7) = (05, 09, F9, 25, F4, 01, B5, 8F).$$

These coefficients can be verified by evaluating both representations on the basis elements $1, t, \dots, t^7$.

Theorem 9. *The linear part A_{AES} of the AES S-box affine transformation satisfies*

$$\text{Stab}(A_{\text{AES}} \circ J_8) = \{I\}.$$

In particular, $A_{\text{AES}} \circ J_8$ is basis rigid.

Proof. Since $\lambda_0 \neq 0$, the first condition of Theorem 8 holds by Remark 1.

For the second condition, consider the pair $(i, j) = (0, 1)$. The coefficients above give

$$\Gamma_{01} = \frac{\lambda_1^2}{\lambda_0^3} = E7.$$

Computation in the specified field gives

$$E7^{15} = 35, \quad E7^{51} = 50, \quad E7^{85} = BC.$$

The order of Γ_{01} divides $|\mathbb{F}_{2^8}^\times| = 255$. Since $255 = 3 \cdot 5 \cdot 17$ and none of these powers equals 1, we obtain

$$\text{ord}(\Gamma_{01}) = 255.$$

Consequently, for every $1 \leq r \leq 7$,

$$\text{ord}(\Gamma_{01}) \nmid 2^r - 1,$$

because $0 < 2^r - 1 < 255$.

Both conditions of Theorem 8 are therefore satisfied, yielding

$$\text{Stab}(A_{\text{AES}} \circ J_8) = \{I\}.$$

□

Thus the linear layer alone makes transformed inversion basis rigid. The same conclusion holds for the full AES S-box.

Corollary 10.

$$\text{Stab}(S_{\text{AES}}) = \{I\}.$$

Proof. Let $T \in \text{Stab}(S_{\text{AES}})$. Then

$$T(A_{\text{AES}}(J_8(x)) + 63) = A_{\text{AES}}(J_8(Tx)) + 63$$

for every $x \in \mathbb{F}_{2^8}$. Setting $x = 0$ gives $T(63) = 63$. By linearity of T , the constant terms therefore cancel, leaving

$$TA_{\text{AES}}J_8 = A_{\text{AES}}J_8T.$$

Hence

$$T \in \text{Stab}(A_{\text{AES}} \circ J_8),$$

and Theorem 9 implies $T = I$. □

Corollary 11. *For ordered $\mathbb{F}_2$ -bases B, B' of $\mathbb{F}_{2^8}$,*

$$S_{\text{AES}, B} = S_{\text{AES}, B'} \iff B = B'.$$

Proof. By the basis-equivalence criterion,

$$S_{\text{AES}, B} = S_{\text{AES}, B'} \iff P_{B'}P_B^{-1} \in \text{Stab}(S_{\text{AES}}).$$

Since $\text{Stab}(S_{\text{AES}}) = \{I\}$, we obtain $P_{B'} = P_B$, hence $B = B'$. The converse is immediate. □

The AES result shows that the AES S-box linear layer completely eliminates the Frobenius redundancy of inversion. This motivates the broader question addressed in the next section. How often does such rigidity occur when the outer linear transformation varies?

3 Generic Rigidity

The AES result shows that a fixed outer linear transformation can make transformed inversion basis rigid. In this section, we show that such rigidity is generic when the outer invertible linear transformation varies. Our argument reduces the existence of a nontrivial linear symmetry to a conjugacy problem for the semilinear candidates arising from two sided linear equivalences of inversion. This leads to an asymptotic rigidity theorem and sharper finite dimensional bounds.

3.1 Stabilizer Events as Conjugacy Conditions

Recall the notation of Section 2, and let

$$G = \text{GL}_n(\mathbb{F}_2), \quad F_A := F_{A,0} = A \circ J_n, \quad A \in G.$$

For the semilinear candidates $T_{a,r} = M_a\sigma^r$, define

$$U_{a,r} := M_{a^{-1}}\sigma^r.$$

By Theorem 6, applied with $c = 0$, we have

$$\text{Stab}(F_A) = \{T_{a,r} : A^{-1}T_{a,r}A = U_{a,r}\}.$$

Since $T_{1,0} = I$, the stabilizer is nontrivial precisely when

$$A^{-1}T_{a,r}A = U_{a,r}$$

for some $(a, r) \neq (1, 0)$.

For $T, U \in G$, define the conjugator set

$$\mathcal{C}(T, U) = \{A \in G : A^{-1}TA = U\},$$

and write

$$C_G(T) = \{C \in G : CT = TC\}$$

for the group centralizer of T in G .

Lemma 12. *Let $T, U \in G$. If T and U are not conjugate in G , then*

$$\mathcal{C}(T, U) = \emptyset.$$

Otherwise, for any $A_0 \in \mathcal{C}(T, U)$,

$$\mathcal{C}(T, U) = A_0 C_G(U) = C_G(T) A_0.$$

In particular,

$$|\mathcal{C}(T, U)| = |C_G(T)| = |C_G(U)|.$$

Proof. Suppose $A_0^{-1}TA_0 = U$ and write $A = A_0C$. Then

$$A^{-1}TA = U \iff C^{-1}UC = U,$$

so

$$\mathcal{C}(T, U) = A_0 C_G(U).$$

The second coset description follows similarly, and conjugation by A_0 identifies $C_G(T)$ with $C_G(U)$. $\square$

Consequently, if A is chosen uniformly from G , then

$$\Pr_A(A^{-1}TA = U) = \begin{cases} \frac{|C_G(T)|}{|G|}, & T \sim U, \\ 0, & T \not\sim U, \end{cases}$$

where $\sim$ denotes conjugacy in G .

Let

$$p_n = \Pr_A(\text{Stab}(F_A) \neq \{I\}).$$

Applying the union bound over all nonidentity semilinear candidates gives

$$p_n \leq \frac{1}{|G|} \sum_{\substack{a \in \mathbb{F}^\times, 0 \leq r < n \\ (a, r) \neq (1, 0)}} \mathbf{1}_{\{T_{a, r} \sim U_{a, r}\}} |C_G(T_{a, r})|. \quad (2)$$

Thus the generic rigidity problem reduces to determining when $T_{a, r}$ and $U_{a, r}$ are conjugate and controlling the size of their centralizers. We first address the conjugacy condition.

3.2 Conjugacy of Semilinear Candidates

Equation (2) shows that a semilinear candidate contributes to the exceptional probability only when $T_{a, r}$ and $U_{a, r}$ are conjugate in G . We now characterize exactly when this occurs. We use standard facts about finite fields, Frobenius automorphisms, and relative norms [4].

For $0 \leq r < n$, define

$$d_r = \gcd(n, r), \quad K_r = \mathbb{F}_{2^{d_r}},$$

where $\gcd(n, 0) = n$, and let

$$z_{a, r} = N_{\mathbb{F}/K_r}(a)$$

denote the norm of a from the extension $\mathbb{F}/K_r$. For $r = 0$, the norm is the identity, so $z_{a, 0} = a$. We first have two elementary observations.

Lemma 13. For every $a \in \mathbb{F}^\times$ and $0 \leq r < n$,

$$T_{a,r}^{n/d_r} = M_{z_{a,r}}, \quad U_{a,r}^{n/d_r} = M_{z_{a,r}}^{-1}.$$

Proof. Let $m = n/d_r$. Since σ^r generates $\text{Gal}(\mathbb{F}/K_r)$,

$$T_{a,r}^m = M_{a a^{2^r} \dots a^{2^{(m-1)r}}} = M_{N_{\mathbb{F}/K_r}(a)} = M_{z_{a,r}}.$$

The second identity follows by replacing a with a^{-1} . □

Lemma 14. Let $z, w \in K_r^\times$. Then the multiplication maps M_z and M_w are conjugate in $\text{GL}_n(\mathbb{F}_2)$ if and only if

$$w = z^{2^k}$$

for some $0 \leq k < d_r$.

Proof. Let

$$e_z = [\mathbb{F}_2(z) : \mathbb{F}_2].$$

As an $\mathbb{F}_2$ -linear transformation, M_z has minimal polynomial equal to the minimal polynomial of z over $\mathbb{F}_2$, with each corresponding rational canonical block occurring n/e_z times. Consequently, M_z and M_w are conjugate if and only if z and w have the same minimal polynomial over $\mathbb{F}_2$.

Over a finite field, this is equivalent to z and w belonging to the same Frobenius orbit. Since $z, w \in K_r = \mathbb{F}_{2^{d_r}}$, this means

$$w = z^{2^k}$$

for some $0 \leq k < d_r$. □

We can now determine the conjugacy condition appearing in (2).

Theorem 15. Let $a \in \mathbb{F}^\times$ and $0 \leq r < n$. Then

$$T_{a,r} \sim U_{a,r} \iff z_{a,r}^{-1} = z_{a,r}^{2^k} \text{ for some } 0 \leq k < d_r \iff z_{a,r}^{2^k+1} = 1 \text{ for some } 0 \leq k < d_r.$$

Proof. Suppose first that

$$T_{a,r} \sim U_{a,r}.$$

Taking the (n/d_r) th power preserves conjugacy, so Lemma 13 gives

$$M_{z_{a,r}} \sim M_{z_{a,r}}^{-1}.$$

Lemma 14 therefore implies

$$z_{a,r}^{-1} = z_{a,r}^{2^k}$$

for some $0 \leq k < d_r$.

Conversely, suppose

$$z_{a,r}^{-1} = z_{a,r}^{2^k}$$

for some $0 \leq k < d_r$.

If $r = 0$, then $z_{a,0} = a$, and

$$a^{-1} = a^{2^k}.$$

Since

$$\sigma^k M_a \sigma^{-k} = M_{a^{2^k}},$$

we immediately obtain

$$M_a \sim M_{a^{-1}}.$$

Now assume $1 \leq r < n$. Since Frobenius powers commute,

$$\sigma^k T_{a,r} \sigma^{-k} = M_{a^{2^k}} \sigma^r.$$

Moreover,

$$N_{\mathbb{F}/K_r}(a^{2^k}) = z_{a,r}^{2^k} = z_{a,r}^{-1} = N_{\mathbb{F}/K_r}(a^{-1}).$$

Hence

$$N_{\mathbb{F}/K_r}\left(\frac{a^{-1}}{a^{2^k}}\right) = 1.$$

By the finite field form of Hilbert's Theorem 90, there exists $b \in \mathbb{F}^\times$ such that

$$b^{2^r-1} = \frac{a^{-1}}{a^{2^k}}.$$

Therefore

$$M_b^{-1}(M_{a^{2^k}}\sigma^r)M_b = M_{a^{2^k}b^{2^r-1}}\sigma^r = M_{a^{-1}}\sigma^r = U_{a,r}.$$

Thus $T_{a,r}$ and $U_{a,r}$ are conjugate. □

The theorem gives an explicit criterion for deciding which semilinear candidates can contribute to the exceptional set. In particular, the conjugacy indicator in (2) can now be written entirely in terms of the relative norm $z_{a,r}$.

Corollary 16. *The conjugacy indicator in (2) is given explicitly by*

$$\mathbf{1}_{\{T_{a,r} \sim U_{a,r}\}} = \mathbf{1}_{\{z_{a,r}^{-1} = z_{a,r}^{2^k} \text{ for some } 0 \leq k < d_r\}}.$$

Equivalently, a candidate contributes only if

$$\text{ord}(z_{a,r}) \mid 2^k + 1$$

for some $0 \leq k < d_r$.

Theorem 15 makes the conjugacy condition in (2) explicit in terms of the relative norm $z_{a,r}$. It characterizes exactly which semilinear candidates can stabilize $A \circ J_n$ for some invertible outer linear map A . To bound the contributions of the admissible candidates, we next estimate the sizes of their group centralizers.

3.3 Centralizers of Semilinear Maps

The conjugacy criterion determines which semilinear candidates can contribute to the exceptional set. To count the outer linear maps that realize each admissible conjugacy, we now study their centralizers. For classical work on centralizers of semilinear transformations, see [9]. Here we require an explicit dimension formula for the specific semilinear maps

$$T_{a,r} = M_a \sigma^r$$

arising from inversion. The maps $T_{a,r}(x) = ax^{2^r}$ are semilinear with respect to the Frobenius automorphism σ^r of $\mathbb{F}$, while they are linear over $\mathbb{F}_2$.

Definition 17. For $T \in G$, define

$$Z(T) = \{L \in \text{End}_{\mathbb{F}_2}(\mathbb{F}) : LT = TL\}.$$

We call $Z(T)$ the *centralizer algebra* of T . Its invertible elements form the group centralizer

$$C_G(T) = Z(T) \cap G.$$

Thus

$$|C_G(T)| \leq |Z(T)| = 2^{\dim_{\mathbb{F}_2} Z(T)}.$$

We next determine the dimension of $Z(T_{a,r})$.

Lemma 18. Let $a \in \mathbb{F}^\times$, and put

$$e_a = [\mathbb{F}_2(a) : \mathbb{F}_2].$$

Then

$$Z(M_a) = \text{End}_{\mathbb{F}_{2^{e_a}}}(\mathbb{F}),$$

and hence

$$\dim_{\mathbb{F}_2} Z(M_a) = \frac{n^2}{e_a}.$$

Proof. An $\mathbb{F}_2$ -linear map L commutes with M_a if and only if it commutes with multiplication by every element of

$$\mathbb{F}_2[a] = \mathbb{F}_2(a) = \mathbb{F}_{2^{e_a}}.$$

Equivalently, L is $\mathbb{F}_{2^{e_a}}$ -linear. Hence

$$Z(M_a) = \text{End}_{\mathbb{F}_{2^{e_a}}}(\mathbb{F}).$$

Since $\mathbb{F}$ has dimension n/e_a over $\mathbb{F}_{2^{e_a}}$, the endomorphism algebra has dimension $(n/e_a)^2$ over $\mathbb{F}_{2^{e_a}}$. Therefore its dimension over $\mathbb{F}_2$ is

$$e_a \left(\frac{n}{e_a} \right)^2 = \frac{n^2}{e_a}.$$

□

The case $r \neq 0$ is controlled by the relative norm introduced in subsection 3.2.

Lemma 19. Let $a \in \mathbb{F}^\times$ and $1 \leq r < n$. Write

$$d_r = \gcd(n, r), \quad z_{a,r} = N_{\mathbb{F}/\mathbb{F}_{2^{d_r}}}(a),$$

and let

$$e_{a,r} = [\mathbb{F}_2(z_{a,r}) : \mathbb{F}_2].$$

Then

$$\dim_{\mathbb{F}_2} Z(T_{a,r}) = \frac{nd_r}{e_{a,r}}.$$

Proof. Every $\mathbb{F}_2$ -linear map $L : \mathbb{F} \rightarrow \mathbb{F}$ has a unique linearized polynomial representation

$$L(x) = \sum_{i=0}^{n-1} \ell_i x^{2^i}, \quad \ell_i \in \mathbb{F}.$$

Then

$$LT_{a,r}(x) = \sum_{i=0}^{n-1} \ell_i a^{2^i} x^{2^{i+r}},$$

whereas

$$T_{a,r}L(x) = \sum_{i=0}^{n-1} a\ell_i^{2^r} x^{2^{i+r}}.$$

Since the Frobenius exponents are taken modulo n , addition by r permutes the indices. Uniqueness of the linearized polynomial representation therefore gives

$$LT_{a,r} = T_{a,r}L \iff \ell_i^{2^r} = a^{2^i-1} \ell_i \quad (0 \leq i < n). \quad (3)$$

Consider more generally

$$u^{2^r} = \eta u, \quad \eta \in \mathbb{F}^\times.$$

If a nonzero solution u_0 exists, then every nonzero solution has the form

$$u_0 v, \quad v \in \mathbb{F}_{2^{d_r}}^\times,$$

because

$$\left(\frac{u}{u_0}\right)^{2^r} = \frac{u}{u_0}.$$

Hence the solution space has dimension d_r over $\mathbb{F}_2$.

By the finite field form of Hilbert's Theorem 90, a nonzero solution exists if and only if

$$N_{\mathbb{F}/\mathbb{F}_{2^{d_r}}}(\eta) = 1.$$

Applying this to the i th equation in (3), with

$$\eta = a^{2^i-1},$$

gives

$$N_{\mathbb{F}/\mathbb{F}_{2^{d_r}}}(a^{2^i-1}) = z_{a,r}^{2^i-1} = 1.$$

Equivalently,

$$z_{a,r}^{2^i} = z_{a,r}.$$

Since

$$e_{a,r} = [\mathbb{F}_2(z_{a,r}) : \mathbb{F}_2],$$

this holds exactly when

$$e_{a,r} \mid i.$$

Moreover,

$$z_{a,r} \in \mathbb{F}_{2^{d_r}},$$

so

$$e_{a,r} \mid d_r \mid n.$$

Therefore exactly

$$\frac{n}{e_{a,r}}$$

indices in $\{0, \dots, n-1\}$ satisfy this condition.

Each admissible coefficient ℓ_i contributes a d_r -dimensional solution space, and the coefficient equations are independent. Hence

$$\dim_{\mathbb{F}_2} Z(T_{a,r}) = \frac{n}{e_{a,r}} d_r = \frac{nd_r}{e_{a,r}}.$$

□

For $r = 0$, we use the convention

$$d_0 = n, \quad z_{a,0} = a, \quad e_{a,0} = [\mathbb{F}_2(a) : \mathbb{F}_2].$$

Lemmas 18 and 19 therefore give the unified formula

$$\dim_{\mathbb{F}_2} Z(T_{a,r}) = \frac{nd_r}{e_{a,r}}$$

for every $a \in \mathbb{F}^\times$ and $0 \leq r < n$.

3.4 Probability of Nontrivial Stabilizers

We now combine the conjugacy criterion of subsection 3.2 with the centralizer formulas of subsection 3.3. Let A be chosen uniformly from

$$G = \mathrm{GL}_n(\mathbb{F}_2),$$

and define

$$p_n = \Pr_A(\mathrm{Stab}(A \circ J_n) \neq \{I\}).$$

Recall from subsection 3.1,

$$p_n \leq \frac{1}{|G|} \sum_{\substack{a \in \mathbb{F}_2^\times, \ 0 \leq r < n \\ (a,r) \neq (1,0)}} \mathbf{1}_{\{T_{a,r} \sim U_{a,r}\}} |C_G(T_{a,r})|.$$

The conjugacy criterion of subsection 3.2 gives

$$T_{a,r} \sim U_{a,r} \iff z_{a,r}^{2^k+1} = 1 \text{ for some } 0 \leq k < d_r,$$

while subsection 3.3 gives

$$|C_G(T_{a,r})| \leq 2^{nd_r/e_{a,r}}.$$

Hence

$$p_n \leq \frac{1}{|G|} \sum_{\substack{a \in \mathbb{F}_2^\times, \ 0 \leq r < n \\ (a,r) \neq (1,0)}} \mathbf{1}_{\{z_{a,r}^{2^k+1}=1 \text{ for some } 0 \leq k < d_r\}} 2^{nd_r/e_{a,r}}.$$

The preceding structural results now yield the main probabilistic rigidity theorem of this section.

Theorem 20. *For $n \geq 4$,*

$$p_n \leq \frac{n}{c_0} 2^{-n^2/2+n},$$

where

$$c_0 = \prod_{j=1}^{\infty} (1 - 2^{-j}) > 0.$$

In particular,

$$p_n \leq 2^{-\Omega(n^2)}.$$

Proof. We first obtain a uniform bound on the centralizers of all nonidentity semilinear candidates. Recall from subsection 3.3 that

$$\dim_{\mathbb{F}_2} Z(T_{a,r}) = \frac{nd_r}{e_{a,r}}.$$

Suppose first that $r = 0$. Then $d_0 = n$ and

$$e_{a,0} = [\mathbb{F}_2(a) : \mathbb{F}_2].$$

Since $(a, 0) \neq (1, 0)$, we have $a \neq 1$. As $\mathbb{F}_2^\times = \{1\}$, this implies $e_{a,0} \geq 2$. Hence

$$\dim_{\mathbb{F}_2} Z(T_{a,0}) = \frac{n^2}{e_{a,0}} \leq \frac{n^2}{2}.$$

Now suppose that $1 \leq r < n$. Then $d_r = \gcd(n, r)$ is a proper divisor of n , and therefore

$$d_r \leq \frac{n}{2}.$$

Since $e_{a,r} \geq 1$, we obtain

$$\dim_{\mathbb{F}_2} Z(T_{a,r}) = \frac{nd_r}{e_{a,r}} \leq nd_r \leq \frac{n^2}{2}.$$

Thus every nonidentity candidate satisfies

$$|C_G(T_{a,r})| \leq |Z(T_{a,r})| \leq 2^{n^2/2}. \quad (4)$$

There are

$$n(2^n - 1) - 1 < n2^n$$

nonidentity pairs (a, r) . Dropping the conjugacy indicator from the union bound in subsection 3.1 and applying (4) therefore gives

$$p_n \leq \frac{n(2^n - 1) - 1}{|G|} 2^{n^2/2} < \frac{n2^n}{|G|} 2^{n^2/2}.$$

Finally,

$$|G| = |\mathrm{GL}_n(\mathbb{F}_2)| = 2^{n^2} \prod_{j=1}^n (1 - 2^{-j}).$$

Since

$$\prod_{j=1}^n (1 - 2^{-j}) \geq c_0, \quad c_0 = \prod_{j=1}^{\infty} (1 - 2^{-j}) > 0,$$

we conclude that

$$p_n < \frac{n2^n 2^{n^2/2}}{c_0 2^{n^2}} = \frac{n}{c_0} 2^{-n^2/2+n}.$$

In particular, p_n is bounded by $2^{-\Omega(n^2)}$. □

Remark 2. For a fixed $c \in \mathbb{F}_{2^n}$, Theorem 6 gives

$$\mathrm{Stab}(F_{A,c}) = \{T \in \mathrm{Stab}(A \circ J_n) : T(c) = c\} \subseteq \mathrm{Stab}(A \circ J_n).$$

Consequently, if A is chosen uniformly from $\mathrm{GL}_n(\mathbb{F}_2)$, then

$$\Pr_A(\mathrm{Stab}(F_{A,c}) \neq \{I\}) \leq p_n \leq \frac{n}{c_0} 2^{-n^2/2+n}, \quad n \geq 4.$$

The refined upper bounds for p_n derived below therefore also apply to $F_{A,c}$.

3.5 Refined Finite Dimensional Bounds

The uniform estimate in the preceding subsection discards the exact conjugacy condition. Retaining this condition together with the exact centralizer dimensions gives the sharper bound

$$B_n^{\mathrm{conj}} = \frac{1}{|G|} \sum_{\substack{a \in \mathbb{F}^\times, 0 \leq r < n \\ (a,r) \neq (1,0)}} \mathbf{1}_{\{z_{a,r}^{2^k+1} = 1 \text{ for some } 0 \leq k < d_r\}} 2^{nd_r/e_{a,r}}.$$

By subsection 3.4,

$$p_n \leq B_n^{\mathrm{conj}}.$$

For comparison, omitting the conjugacy condition gives

$$B_n = \frac{1}{|G|} \sum_{\substack{a \in \mathbb{F}^\times, 0 \leq r < n \\ (a,r) \neq (1,0)}} 2^{nd_r/e_{a,r}},$$

and therefore

$$p_n \leq B_n^{\mathrm{conj}} \leq B_n.$$

To evaluate the refined bound more explicitly, we first characterize which norm values can satisfy the conjugacy condition.

Lemma 21. *Let $z \in \mathbb{F}_{2^d}^\times$, and let*

$$e_z = [\mathbb{F}_2(z) : \mathbb{F}_2].$$

If $e_z > 1$, then

$$z^{-1} = z^{2^k}$$

for some integer $0 \leq k < e_z$ if and only if e_z is even and

$$z^{-1} = z^{2^{e_z/2}}.$$

Equivalently,

$$z^{2^{e_z/2}+1} = 1.$$

Proof. Suppose that

$$z^{-1} = z^{2^k}.$$

Applying the same Frobenius power again gives

$$z^{2^{2k}} = z.$$

Since the Frobenius orbit of z has length e_z , it follows that

$$e_z \mid 2k.$$

On the other hand, $e_z \nmid k$, since otherwise $z^{2^k} = z$ and hence $z = z^{-1}$, which forces $z = 1$ in characteristic two, contradicting $e_z > 1$.

Thus e_z is even and

$$k \equiv \frac{e_z}{2} \pmod{e_z}.$$

Hence

$$z^{-1} = z^{2^{e_z/2}}.$$

The converse is immediate, and the last equality is equivalent to

$$z^{2^{e_z/2}+1} = 1.$$

□

For $e \geq 1$, let Q_e denote the number of nonzero elements $z \in \mathbb{F}_{2^e}$ of exact degree e over $\mathbb{F}_2$ whose multiplicative inverse belongs to the same Frobenius orbit as z . Then

$$Q_1 = 1,$$

and Lemma 21 gives

$$Q_e = 0 \quad \text{for odd } e > 1.$$

For even e ,

$$Q_e = \# \left\{ z \in \mathbb{F}_{2^e}^\times : [\mathbb{F}_2(z) : \mathbb{F}_2] = e, z^{2^{e/2}+1} = 1 \right\}.$$

We can now group the refined bound according to the degree of the norm value.

Proposition 22. *For every n ,*

$$B_n^{\text{conj}} = \frac{1}{|G|} \left[\sum_{r=0}^{n-1} \frac{2^n - 1}{2^{d_r} - 1} \sum_{e \mid d_r} Q_e 2^{nd_r/e} - 2^{n^2} \right].$$

Proof. Fix r . The norm map

$$N_{\mathbb{F}/\mathbb{F}_{2^{d_r}}} : \mathbb{F}^\times \longrightarrow \mathbb{F}_{2^{d_r}}^\times$$

is surjective, and each norm value has

$$\frac{2^n - 1}{2^{d_r} - 1}$$

preimages.

If a norm value z has exact degree e over $\mathbb{F}_2$, then $e \mid d_r$ and the corresponding centralizer contribution is

$$2^{nd_r/e}.$$

Among the elements of exact degree e , precisely Q_e satisfy the conjugacy condition. Hence the total contribution for fixed r is

$$\frac{2^n - 1}{2^{d_r} - 1} \sum_{e \mid d_r} Q_e 2^{nd_r/e}.$$

Summing over r also includes the identity candidate $(a, r) = (1, 0)$, whose contribution is 2^{n^2} . Removing this term gives the stated formula. $\square$

This grouped expression gives a computable finite dimensional refinement of the generic rigidity bound.

4 Computational Verification

We complement the theoretical results with three computations. First, we independently determine the linear stabilizers of the AES S-box and two related maps from their complete truth tables. Second, we enumerate all invertible linear maps in small dimensions to obtain exact probabilities of nontrivial stabilizers. Third, we sample uniformly random invertible linear maps in larger dimensions and compare the observed frequencies with the theoretical bounds.

The computations were performed in Ubuntu 22.04 using Python 3.10.12. Binary vectors are represented by integers, with vector addition implemented by bitwise XOR. Linear maps are represented by their images on the standard basis. The computational routines use only the Python standard library, plotting uses Matplotlib.

For finite field arithmetic, we use

$$\mathbb{F} = \mathbb{F}_2[x]/(m_n(x)),$$

with the following irreducible polynomials:

n	$m_n(x)$
3	$x^3 + x + 1$
4	$x^4 + x + 1$
5	$x^5 + x^2 + 1$
6	$x^6 + x + 1$
7	$x^7 + x + 1$
8	$x^8 + x^4 + x^3 + x + 1.$

For $n = 8$, this is the standard AES field representation. All nonzero inverses are checked by multiplication.

All computations were performed on a single CPU thread on an HP desktop computer with an Intel Core i7-13700F processor and 32 GB of RAM.

4.1 Independent Verification of AES Rigidity

We search for all invertible $\mathbb{F}_2$ -linear maps T satisfying

$$T \circ F = F \circ T$$

directly from the complete truth table of F . This search does not use the semilinear characterization of stabilizers or restrict the candidates to maps of the form $M_a \sigma^r$.

Table 1: Independent exhaustive closure search. Times measure the stabilizer search for each map.

Map	Stabilizer order	Time (s)
S_{AES}	1	0.00031
J_8	8	0.00402
$A_{\text{AES}} \circ J_8$	1	0.00250

The algorithm maintains an injective linear map on a subspace of $\mathbb{F}_2^n$. Assigning $T(x) = y$ for a vector outside the current domain extends the map to the enlarged span by linearity. Every assigned pair (x, y) also forces

$$T(F(x)) = F(y).$$

These consequences are propagated until no further assignments are forced or a conflict occurs. Branches with inconsistent assignments or a failure of injectivity are discarded.

If the domain remains a proper subspace, the algorithm chooses the first unassigned standard basis vector and considers every image outside the current image subspace. Consequently, every invertible linear map satisfying the commuting relation occurs in the search. Each completed map is additionally checked on the entire truth table.

The initial assignment $T(0) = 0$ forces $T(F(0)) = F(0)$. For the full AES S-box, closure from this constraint already determines the identity map. For the other two maps, branching is required.

We apply this procedure to the literal 256-entry AES S-box table, the pure inversion map J_8 , and $A_{\text{AES}} \circ J_8$. The AES table is also checked against its field-inversion and affine representation. The results are shown in Table 1.

For both AES maps, the unique solution is the identity. For J_8 , the eight recovered matrices are compared individually with

$$I, \sigma, \dots, \sigma^7,$$

and the two sets agree exactly. Thus the pure inversion case provides a nontrivial control for the search, while the AES computations independently confirm the rigidity results of subsection 2.4.

4.2 Exact Probabilities and Refined Bounds

We compute the exact exceptional probabilities in small dimensions and evaluate the bounds obtained in Section 3. We also check the conjugacy criterion and the centralizer dimension formula directly from the binary matrices of the semilinear candidates.

For each $n \in \{3, 4, 5\}$, we enumerate all $A \in \text{GL}_n(\mathbb{F}_2)$ by constructing ordered linearly independent column tuples. Each invertible matrix appears exactly once. We count

$$N_n = \# \{A \in \text{GL}_n(\mathbb{F}_2) : \text{Stab}(A \circ J_n) \neq \{I\}\}, \quad p_n = \frac{N_n}{|\text{GL}_n(\mathbb{F}_2)|}.$$

For $n = 3, 4$, every map $A \circ J_n$ is tested by the independent closure search of the preceding subsection. The resulting decision is also compared with the semilinear candidate test for every A , with no disagreements. In particular, the exact computation for $n = 3$ does not require extending the inversion-equivalence theorem beyond its stated range.

For $n = 5$, we use the stabilizer characterization and test

$$T_{a,r}A = AU_{a,r}$$

for nonidentity pairs (a, r) . Since both sides are linear, equality is checked on the standard basis. The enumeration covers all 9,999,360 invertible matrices and takes approximately 96 seconds. The exact results are given in Table 2.

We next verify the structural formulas for every nonidentity semilinear candidate in dimensions $n = 3, \dots, 8$. For each pair (a, r) , we construct the binary matrices of $T_{a,r}$ and $U_{a,r}$ and determine whether they are conjugate by comparing their elementary divisors. These are recovered from the characteristic

Table 2: Exact probabilities of nontrivial stabilizers. Times for $n = 3, 4$ include both closure search and the semilinear test.

n	$ \mathrm{GL}_n(\mathbb{F}_2) $	N_n	p_n	Time (s)
3	168	21	1/8	0.005
4	20,160	600	5/168	1.35
5	9,999,360	465	1/21504	96.38

Table 3: Theoretical upper bounds and exact probabilities. A dash indicates that the exact probability was not computed.

n	b_n	B_n	B_n^{conj}	Exact p_n
4	8.65687×10^{-1}	1.30159×10^{-1}	1.23810×10^{-1}	2.97619×10^{-2}
5	9.56458×10^{-2}	4.92832×10^{-4}	3.96825×10^{-4}	4.65030×10^{-5}
6	5.07238×10^{-3}	1.53807×10^{-4}	1.52264×10^{-4}	—
7	1.30766×10^{-4}	6.93708×10^{-10}	5.95276×10^{-10}	—
8	1.65117×10^{-6}	1.52614×10^{-8}	1.52613×10^{-8}	—

polynomials and the nullities of powers of their irreducible factors evaluated at the matrices. This direct test does not use the norm criterion.

For all 3,537 candidates, the direct conjugacy test agrees with

$$z_{a,r}^{2^k+1} = 1 \quad \text{for some } 0 \leq k < d_r.$$

We compute the nullity of the binary linear system independently

$$LT_{a,r} - T_{a,r}L = 0.$$

Every computed dimension agrees with $nd_r/e_{a,r}$. Finally, evaluating B_n^{conj} by its candidate sum and by the grouped expression in Proposition 22 gives exactly the same rational value in each dimension.

For comparison, write

$$b_n = \frac{n}{c_0} 2^{-n^2/2+n}$$

for the uniform bound, and retain the notation B_n and B_n^{conj} from subsection 3.5. Table 3 reports these bounds for $n = 4, \dots, 8$, along with the available exact probabilities. The exact $n = 3$ result is reported separately because the probability theorem is stated for $n \geq 4$.

The conjugacy condition improves the bound in every displayed dimension, but the improvement varies with n . For example, relative to B_n , the reduction is approximately 19.48% for $n = 5$ and 14.19% for $n = 7$, whereas it is only 0.000755% for $n = 8$.

For $n = 4, 5$, the exact probabilities lie strictly below B_n^{conj} . The remaining gap reflects two sources of overcounting: the replacement of group centralizers by their full centralizer algebras, and the overlap among the stabilizer events in the union bound. The finite dimensional bounds B_n and B_n^{conj} depend on the divisor structure of n and on the degrees of the norm values, so they need not decrease monotonically with n . Figure 1 illustrates this behavior on a logarithmic scale.

4.3 Monte Carlo Estimates

For each $n \in \{5, 6, 7, 8\}$, we independently sample 100,000 matrices from $\mathrm{GL}_n(\mathbb{F}_2)$. Each successive column is chosen uniformly outside the span of the preceding columns. Thus every ordered basis has probability

$$\prod_{k=0}^{n-1} (2^n - 2^k)^{-1} = |\mathrm{GL}_n(\mathbb{F}_2)|^{-1},$$

so the resulting matrices are uniformly distributed. Sampling is with replacement across trials, and the pseudorandom generator uses seed 20260906 + n in dimension n .

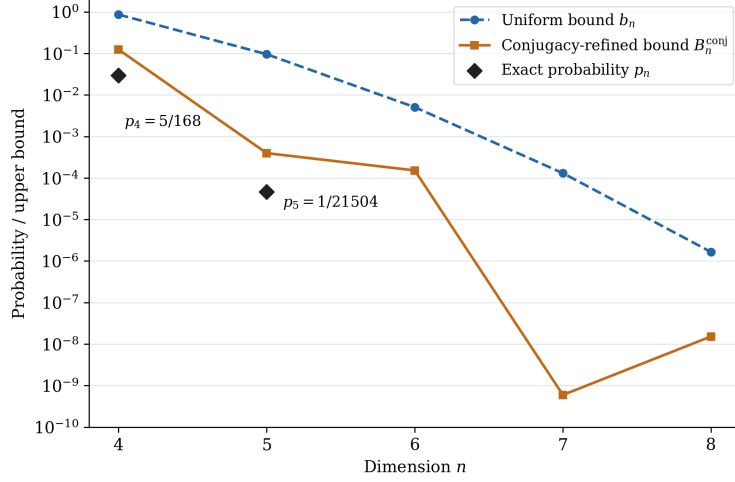


Figure 1: Uniform and conjugacy-refined upper bounds for the exceptional probability with the exact values of p_n for $n = 4, 5$ on a logarithmic scale.

Table 4: Monte Carlo estimates from 100,000 samples per dimension, with pointwise 95% Wilson score intervals.

n	k_n	$\hat{p}_n (\times 10^{-5})$	95% CI ($\times 10^{-5}$)	Time (s)
5	3	3.0	[1.02, 8.82]	1.12
6	6	6.0	[2.75, 13.09]	2.07
7	0	0.0	[0, 3.84]	4.02
8	0	0.0	[0, 3.84]	8.27

Each sampled matrix A is tested for a nontrivial stabilizer using the condition

$$T_{a,r}A = AU_{a,r}, \quad (a, r) \neq (1, 0).$$

As an additional consistency check, we compare the semilinear test with independent closure search on random matrices and prescribed examples with nontrivial stabilizers, with no disagreements.

Let $m = 100,000$, let k_n denote the number of samples with a nontrivial stabilizer, and put

$$\hat{p}_n = \frac{k_n}{m}.$$

Table 4 reports the observed frequencies and pointwise 95% Wilson score confidence intervals [10]. With $z = 1.959964$, the interval endpoints are

$$\frac{\hat{p}_n + \frac{z^2}{2m} \pm z \sqrt{\frac{\hat{p}_n(1 - \hat{p}_n)}{m} + \frac{z^2}{4m^2}}}{1 + \frac{z^2}{m}}.$$

These intervals are computed separately for each dimension and are not simultaneous confidence bands.

For $n = 5$, the exact probability

$$p_5 = \frac{1}{21504} \approx 4.65030 \times 10^{-5}$$

lies within the reported interval. For $n = 6$, the observed frequency

$$\hat{p}_6 = 6 \times 10^{-5}$$

is below the refined upper bound

$$B_6^{\text{conj}} \approx 1.52264 \times 10^{-4}.$$

For $n = 7, 8$, no nontrivial stabilizers are observed. This does not imply that the true probabilities are zero. In these dimensions, the theoretical bounds are smaller than the upper endpoints of the sampling intervals. Let $\mathbb{E}[k_n]$ denote the expected number of samples with a nontrivial stabilizer. Indeed,

$$\mathbb{E}[k_n] = mp_n \leq mB_n^{\text{conj}},$$

and therefore

$$\mathbb{E}[k_7] \leq 5.95276 \times 10^{-5}, \quad \mathbb{E}[k_8] \leq 1.52613 \times 10^{-3}.$$

The absence of observed events is therefore expected at this sample size.

5 Conclusion

We studied basis rigidity for finite field inversion under outer affine transformations, with the AES S-box as the main motivating example. For AES, we proved that no nontrivial linear change of basis preserves the coordinate realization. In fact, the AES S-box linear layer already removes the basis redundancy of pure inversion.

For the general family $A \circ J_n$, we characterized which semilinear candidates can occur as linear symmetries, determined the corresponding centralizer dimensions, and derived both finite dimensional bounds and an asymptotic rigidity result. In particular, for a uniformly random invertible linear map A , the probability that the linear stabilizer is nontrivial is bounded by $2^{-\Omega(n^2)}$.

The computations independently confirm the AES result, the structural formulas, and the finite dimensional bounds. Overall, the results show that the basis redundancy of inversion can be completely destroyed by an outer linear layer and is generically absent in the family considered here.

References

- [1] Alex Biryukov, Christophe De Cannière, An Braeken, and Bart Preneel. A toolbox for cryptanalysis: Linear and affine equivalence algorithms. In *Advances in Cryptology – EUROCRYPT 2003*, volume 2656 of *Lecture Notes in Computer Science*, pages 33–50. Springer, 2003.
- [2] Keita Ishizuka. Almost all vectorial functions have trivial extended-affine stabilizers, 2026. arXiv:2602.06668. <https://arxiv.org/abs/2602.06668>.
- [3] Lukas Kölsch. On CCZ-equivalence of the inverse function. *IEEE Transactions on Information Theory*, 67(7):4856–4862, 2021.
- [4] Rudolf Lidl and Harald Niederreiter. *Finite Fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, 2nd edition, 1997.
- [5] Jingmei Liu, Baodian Wei, Xiangguo Cheng, and Xinmei Wang. Cryptanalysis of Rijndael S-box and improvement. *Applied Mathematics and Computation*, 170(2):958–975, 2005.
- [6] National Institute of Standards and Technology. Advanced encryption standard (AES). Federal Information Processing Standards Publication 197, National Institute of Standards and Technology, 2023. Updated May 9, 2023.
- [7] Adrian Ranea and Bart Preneel. On self-equivalence encodings in white-box implementations. In *Selected Areas in Cryptography – SAC 2020*, volume 12804 of *Lecture Notes in Computer Science*, pages 639–669. Springer, 2021.
- [8] Joachim Rosenthal. A polynomial description of the Rijndael advanced encryption standard. *Journal of Algebra and Its Applications*, 2(2):223–236, 2003.

- [9] Kirby C. Smith. The centralizer of a semi-linear transformation. *Linear Algebra and its Applications*, 14(1):21–27, 1976.
- [10] Edwin B. Wilson. Probable inference, the law of succession, and statistical inference. *Journal of the American Statistical Association*, 22(158):209–212, 1927.
- [11] Feng Yuan, Ji-Jun Jiang, Yang Yang, Hai-Wen Ou, and Min-Juan Wang. Enumeration of cryptographic functions affine equivalent to the inverse function over F_{p^n} . *Chinese Journal of Computers*, 42(5):1126–1136, 2019.
- [12] Zheng Zhang and Na Zhang. Representation redundancy and structural complexity in finite-field inversion, 2026. arXiv:2609.04583. <https://arxiv.org/abs/2609.04583>.