Related Differentials of 4×4 MDS Matrices: A Complete Characterization

Kamil Otal[1], Ali Mert Sülçe[2], and Oğuz Yayla[2]

[1] TÜBİTAK BİLGEM National Research Institute of Electronics and Cryptology, Gebze, Kocaeli, Türkiye kamil.otal@gmail.com

[2] Institute of Applied Mathematics, Middle East Technical University, Çankaya, Ankara, Türkiye mert.sulce@metu.edu.tr, oguz@metu.edu.tr

Abstract. A pair of differences (x, y) is a *related differential* for a linear layer M if, for every coordinate at both the input and the output, at least one of the two values vanishes or the two values coincide. Related differentials underlie the zero-difference attack on AES of Bardeh and Rijmen, and the question of which maximum distance separable (MDS) matrices admit them was raised by Daemen and Rijmen, who showed that every 4×4 circulant MDS matrix does while some Hadamard ones do not. In earlier work the 3×3 MDS matrices over $\mathbb{F}_{2^r}$ admitting related differentials were characterized by fifteen explicit equations. In this paper we settle the 4×4 case completely: an MDS matrix $M = DNE$ over $\mathbb{F}_{2^r}$ admits a related differential if and only if at least one of 280 explicit polynomial equations in the nine free entries of its reduced form N holds. The equations, 70 quadratic and 210 cubic, are pairwise distinct, irreducible and pairwise coprime, and fall into 27 orbits under the natural symmetries. We further determine the structure of the equation set: the fifteen equations of the 3×3 case are exactly the points of $\mathrm{PG}(3, 2)$, while the 280 equations span a 14-dimensional $\mathbb{F}_2$-space, satisfy exactly 560 additive relations, and contain exactly 840 pairs that can never hold simultaneously on an MDS matrix. The discarded zero patterns split into 525 whose determinant condition is equivalent to the failure of MDS-ness and 289 vacuous cases. Over $\mathbb{F}_8$, the smallest field carrying 4×4 MDS matrices, exhaustive enumeration shows that there are exactly 720 reduced MDS matrices; each satisfying exactly 28 of the equations and each equation being satisfied by exactly 72 matrices; in particular every 4×4 MDS matrix over $\mathbb{F}_8$ admits a related differential. Over $\mathbb{F}_{2^{10}}$ we exhibit an explicit MDS matrix admitting none. All results are verified by exact computation against an independent exhaustive search.

Keywords: Maximum distance separable (MDS) matrices · Related differentials · Zero-difference attack · Branch number · Finite fields.

1 Introduction

MDS matrices are the standard tool for building diffusion layers of block ciphers and hash functions: an $n \times n$ matrix M over a finite field $\mathbb{F}_q$ is *maximum distance separable* (MDS) if every square submatrix of M is nonsingular, which is

equivalent to the optimal diffusion property that $\mathrm{wt}(v) + \mathrm{wt}(Mv) \geq n + 1$ for every nonzero v. The MixColumns matrix of the AES [8] is the best-known example, and the construction and classification of MDS matrices is a rich subject in its own right; see, e.g., the survey [4] and the recent complete construction [6]. Optimal diffusion is the designer's first line of defence against differential cryptanalysis [2], but it does not exclude finer structural properties of the linear layer that an attacker can exploit.

One such property is the existence of *related differentials*. Informally, a pair of differences (x, y) is related for M if in every coordinate at both the input and the output, at least one of the two values vanishes or the two values agree (Definition 1). Bardeh and Rijmen's zero-difference attack on reduced-round AES [1] exploits exactly such pairs for the AES MixColumns matrix. Much earlier, Daemen and Rijmen [3] had shown that related differentials exist for *every* 4×4 circulant MDS matrix, and they exhibited a 4×4 Hadamard MDS matrix admitting none so that, in this specific sense, some Hadamard matrices are more resilient than every circulant one. Jha, Li and Gligoroski [5] recently gave a systematic construction of 4×4 Hadamard MDS matrices resistant to related-differential cryptanalysis. Otal et al. [9] settled the problem completely in small dimensions: no 2×2 MDS matrix admits a related differential, all 3×3 circulant (and, over fields of even size, all involutory) MDS matrices do, and the 3×3 MDS matrices over $\mathbb{F}_{2^r}$ admitting related differentials are exactly those whose reduced form satisfies one of fifteen explicit equations. Kumar et al. [7] showed the existence of related differential for circulant MDS matrices of order n with $n \not\equiv \pm 2 \pmod{12}$ and non-MDS matrices.

The present paper completes this programme for the cryptographically most relevant dimension, $n = 4$, over fields of even size. Our main result (Theorem 5) states that a 4×4 MDS matrix $M = DNE$ over $\mathbb{F}_{2^r}$ admits a related differential if and only if at least one of 280 explicit polynomial equations in the nine free entries $a, b, c, d, e, f, g, h, i$ of the reduced form N vanishes. The equations, which are 70 quadratic and 210 cubic, are all multilinear and irreducible, and they arise as determinants of *punctured* copies of N, indexed by the admissible zero patterns of a related differential, and they collapse into 27 orbits under the natural symmetries (simultaneous row/column permutations and transposition); Table 1 lists one representative per orbit. The proof proceeds in two steps: a zero-pattern lemma (Lemma 1) showing that for an MDS matrix the zero positions of x, y and $z = x + y$ partition the input coordinates, and the output positions likewise, with weight budgets that form a permutation of $(3, 3, 2)$; and a linearization lemma (Lemma 2) translating the existence of a related differential with a prescribed pattern into the vanishing of one punctured determinant. The method re-proves the known results for $n = 2, 3$ uniformly.

We then analyze the structure of the equation set itself, answering two natural questions: which equations are related to one another, and which candidate equations are incompatible with MDS-ness. For $n = 3$ we observe a fact that seems to have gone unnoticed: the fifteen equations of [9] are exactly the fifteen nonzero vectors of a four-dimensional $\mathbb{F}_2$-space, a copy of $\mathrm{PG}(3, 2)$, so the sum

of any two of them is again one of the fifteen. For $n = 4$ the 280 equations span a 14-dimensional space, admit exactly 560 additive relations $f + g + h = 0$ (Proposition 1), and contain exactly 840 pairs whose sum is a product of minors of N, hence pairs of equations that can never hold simultaneously on an MDS matrix (Corollary 2). Dropping the admissibility constraint, the 1094 conceivable zero patterns split into a clean result (Proposition 2): the 280 admissible ones, 525 patterns whose punctured determinant factors into minors of N, so that the candidate equation is *equivalent* to the failure of MDS-ness (mirroring the eliminated branches in the proof of the 3×3 characterization) ,and 289 patterns whose punctured determinant vanishes identically.

Finally, we examine small fields. Since an $[8, 4, 5]$ MDS code requires $q \geq 8$ in characteristic two, $\mathbb{F}_8$ is the smallest admissible field, and there exhaustive enumeration is possible: $\mathbb{F}_8$ carries exactly 720 reduced 4×4 MDS matrices; each satisfies exactly 28 of the 280 equations, and each equation is satisfied by exactly 72 matrices (Theorem 6); in particular *every* 4×4 MDS matrix over $\mathbb{F}_8$ admits a related differential. In the opposite direction we exhibit an explicit MDS matrix over $\mathbb{F}_{2^{10}}$ admitting no related differentials (Example 1), and we report sampled densities over intermediate fields, which match a simple heuristic. All computational claims were verified in exact arithmetic against an independent exhaustive search implemented directly from the definition (Remark 6).

The paper is organized as follows. Section 2 fixes notation and recalls the required results from [1,3,6,9]. Sections 3–6 develop the zero-pattern and linearization lemmas and prove the main theorem, including the table of the 27 orbits, the duality corollary and a worked case. Section 7 studies the relations among the equations and the discarded cases. Section 8 contains the $\mathbb{F}_8$ census, the $\mathbb{F}_{2^{10}}$ example and the verification summary, and Section 9 concludes with open problems. The complete list of the 280 equations, grouped by the 27 orbits, is reproduced in Appendix A.

2 Preliminaries

Throughout, $q = 2^r$ and $\mathbb{F}_q$ denotes the finite field with q elements; all vectors are column vectors, $\mathrm{wt}(v)$ is the Hamming weight of v, and indices of coordinates run from 1 to n. A square matrix over $\mathbb{F}_q$ is *MDS* if all of its minors, of every order, are nonzero; equivalently, $[\, I \mid M^{\mathsf{T}}]$ generates an MDS code of parameters $[2n, n, n + 1]$ (see, e.g., [4,10]).

Definition 1 ([3]; see also [1]). *Let M be an $n \times n$ matrix over $\mathbb{F}_q$. A pair of vectors (x, y) over $\mathbb{F}_q$ is called a* related differential *for M if*

$$x_k\, y_k\, (x_k - y_k) = 0 \qquad \text{and} \qquad (Mx)_j\, (My)_j \left((Mx)_j - (My)_j \right) = 0$$

for all coordinates $k, j \in \{1, \ldots, n\}$.

Originally the four-tuple (x, y, Mx, My) was called a related differential in [1]. Following [9], we write $(x, y)_M$, or simply (x, y) when M is clear from the context. The pair is *trivial* if $x = 0$, $y = 0$ or $x = y$; trivial pairs are related differentials

for every matrix, so we consider only nontrivial ones throughout. We will use the following results.

Theorem 1 ([9, Theorem 1]). *There are no related differentials for any* 2×2 *MDS matrices.*

Theorem 2 ([6]; see also [9, Theorem 4]). *Let* M *be a square MDS matrix over* $\mathbb{F}_q$*. Then* $M = DNE$ *for invertible diagonal matrices* D, E *and a unique MDS matrix* N *whose first row and first column consist of* 1*s. We call* N *the* reduced form *of* M*.*

Theorem 3 ([9, Theorem 5]). *With* $M = DNE$ *as in Theorem 2, there exists a related differential for* M *if and only if there exists one for* N*.*

Theorem 4 ([9, Theorem 6]). *Let* M *be a* 3×3 *MDS matrix over* $\mathbb{F}_{2^r}$ *with reduced form*

$$N_3 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & a & b \\ 1 & c & d \end{pmatrix}.$$

Then M *has a related differential if and only if at least one of the following fifteen equations holds:*

(i) $a + d = 0$,	(ii) $b + c = 0$,	(iii) $ad + b = 0$,
(iv) $ad + c = 0$,	(v) $bc + a = 0$,	(vi) $bc + d = 0$,
(vii) $a + b + c + d = 0$,	(viii) $ad + bc + a + b = 0$,	(ix) $ad + bc + a + c = 0$,
(x) $ad + bc + b + d = 0$,	(xi) $ad + bc + c + d = 0$,	(xii) $ad + a + b + d = 0$,
(xiii) $ad + a + c + d = 0$,	(xiv) $bc + a + b + c = 0$,	(xv) $bc + b + c + d = 0$.

Setup and conventions

Throughout the rest of the paper let $q = 2^r$ and let

$$N = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & a & b & c \\ 1 & d & e & f \\ 1 & g & h & i \end{pmatrix}$$

be a 4×4 MDS matrix over $\mathbb{F}_{2^r}$ in the reduced form of Theorem 2; by Theorem 3 an arbitrary 4×4 MDS matrix M has a related differential if and only if its reduced form N does. For a related differential (x, y), we always assume the nontriviality conditions $x \neq 0$, $y \neq 0$, $x \neq y$, and we write

$$z = x + y, \qquad x' = Nx, \qquad y' = Ny, \qquad z' = Nz = x' + y'.$$

Note that $x + y + z = 0$ and $x' + y' + z' = 0$. In each coordinate k the related difference condition $x_k\, y_k\, (x_k + y_k) = 0$ says that at least one of x_k, y_k, z_k vanishes, and if two of them vanish then all three do; the same holds at the output for x'_j, y'_j, z'_j.

Recall that an $n \times n$ MDS matrix has (differential) branch number $n+1$: for every $v \neq 0$,

$$\mathrm{wt}(v) + \mathrm{wt}(Nv) \;\geq\; n+1, \tag{1}$$

equivalently, writing $\mathrm{z_{in}}(v) = \#\{k : \; v_k = 0\}$ and $\mathrm{z_{out}}(v) = \#\{j : \; (Nv)_j = 0\}$,

$$\mathrm{z_{in}}(v) + \mathrm{z_{out}}(v) \;\leq\; n-1.$$

The bound is standard: if $\mathrm{z_{in}}(v) + \mathrm{z_{out}}(v) \geq n$ for some $v \neq 0$, let $S = \mathrm{supp}(v)$ and let T be a set of $|S|$ rows in which Nv vanishes, which exists since $|T|$ may be chosen of size $n - \mathrm{z_{in}}(v) \leq \mathrm{z_{out}}(v)$; then the square submatrix $N[T, S]$ annihilates the totally nonzero vector $v|_S$, contradicting MDS-ness.

3 The Structure of Related Differentials

We first pin down the possible zero patterns of a related differential of an MDS matrix.

Lemma 1. *Let M be an $n \times n$ MDS matrix over $\mathbb{F}_{2^r}$ with $n \in \{2, 3, 4\}$ and let (x, y) be a related differential for M with $x, y \neq 0$ and $x \neq y$. Put $z = x + y \neq 0$. Then:*

1. *In every input coordinate* exactly one *of x_k, y_k, z_k is 0; and in every output coordinate exactly one of $(Mx)_j, (My)_j, (Mz)_j$ is 0. In particular $n = 2$ is impossible.*
2. *The zero positions define partitions*
   $$\{1, \ldots, n\} = I_x \sqcup I_y \sqcup I_z \quad \textit{(inputs)}, \qquad \{1, \ldots, n\} = O_x \sqcup O_y \sqcup O_z \quad \textit{(outputs)},$$
   where $I_v = \{k : \; v_k = 0\}$ and $O_v = \{j : \; (Mv)_j = 0\}$, satisfying
   $$|I_v| + |O_v| \;\leq\; n-1 \qquad (v \in \{x, y, z\}). \tag{2}$$
3. *For $n = 3$ one has $|I_v| + |O_v| = 2$ for all v; for $n = 4$ the triple $\big(|I_v| + |O_v|\big)_{v \in \{x,y,z\}}$ is a permutation of $(3, 3, 2)$. In particular, for $n = 4$ exactly two of the three codewords (v, Mv), $v \in \{x, y, z\}$, are minimum-weight codewords of the associated $[8, 4, 5]$ MDS code, and the third has weight 6.*

Proof. Since $x, y, z \neq 0$, inequality (1) applies to each of them, so $\sum_v \big(\mathrm{z_{in}}(v) + \mathrm{z_{out}}(v)\big) \leq 3(n-1)$. On the other hand, every one of the $2n$ coordinates (input and output) contributes at least 1 to this sum, and a coordinate in which two of the three quantities vanish contributes 3, because $x+y+z = 0$ and $x'+y'+z' = 0$ force the third to vanish as well. If T denotes the number of coordinates in which all three vanish, then

$$2n + 2T \;\leq\; \sum_v \big(\mathrm{z_{in}}(v) + \mathrm{z_{out}}(v)\big) \;\leq\; 3(n-1).$$

For $n = 2$ this reads $4 + 2T \leq 3$, a contradiction, proving Theorem 1 again. For $n = 3$ and $n = 4$ it forces $T = 0$, i.e. exactly one of the three vanishes in every coordinate, which is item (1); item (2) is then immediate. Moreover, $\sum_v \big(|I_v| + |O_v|\big) = 2n$ with every summand at most $n-1$, which for $n = 3$ forces $(2, 2, 2)$ and for $n = 4$ forces a permutation of $(3, 3, 2)$, proving item (3) since $\mathrm{wt}(v) + \mathrm{wt}(Mv) = 2n - \big(|I_v| + |O_v|\big)$.

Remark 1. Definition 1 requires *both* the pair (x, y) and its image (Mx, My) to satisfy the coordinate conditions the object is the four-tuple (x, y, Mx, My) of [1], abbreviated $(x, y)_M$ so relatedness of the input pair alone is a matrix-free property, and the matrix enters only through the output condition. It is through that condition that MDS-ness constrains the *input* zero sets. Note first that over $\mathbb{F}_{2^r}$ a coordinate can never have *exactly two* of x_k, y_k, z_k equal to 0: since $x_k + y_k + z_k = 0$, two zeros force the third. All three may, however, vanish simultaneously, and then the zero sets overlap instead of partitioning. For instance,

$$x = (0, a, b, 0)^{\mathsf{T}}, \qquad y = (0, a, 0, 0)^{\mathsf{T}}, \qquad z = x + y = (0, 0, b, 0)^{\mathsf{T}} \qquad (ab \neq 0)$$

satisfies the input conditions $x_k y_k (x_k + y_k) = 0$ with $I_x = \{1, 4\}$, $I_y = \{1, 3, 4\}$, $I_z = \{1, 2, 4\}$, the coordinates 1 and 4 being triply zero; it is in fact a related differential of the (invertible, non-MDS) identity matrix. Lemma 1 excludes such configurations when M is MDS: here $T \geq 2$ from the inputs alone, so $2n + 2T \geq 12 > 9 = 3(n - 1)$. The contradiction is also visible directly: $My = a\, Me_2$ and $Mz = b\, Me_3$ are nonzero multiples of columns of M, hence totally nonzero (every entry of an MDS matrix is nonzero; alternatively $\mathrm{wt}(y) = \mathrm{wt}(z) = 1$ and (1)), so the output condition $(Mx)_j (My)_j (Mz)_j = 0$ forces $Mx = 0$, i.e. $x = 0$. Thus, this (x, y) is never a related differential $(x, y)_M$ of an MDS M indeed of any matrix without zero entries. The discarded patterns of Proposition 2 are the determinant-level trace of these eliminated configurations.

4 Algebraic Characterization via Punctured Matrices

Lemma 1 establishes that the zero coordinates of any related differential strictly partition the input and output indices. We now demonstrate that fixing this combinatorial data, which we formalize as an *admissible pattern*, completely linearizes the related differential conditions. By masking specific entries of the matrix N according to a given pattern, we construct a *punctured matrix* N_P whose kernel explicitly captures the associated related differentials. This algebraic reduction translates the nonlinear existence problem into the vanishing of a single determinant, forming the core engine of our characterization.

Definition 2 (Admissible pattern, punctured matrix). *A* pattern *is a pair* $P = (\mathcal{I}, \mathcal{O})$ *of ordered partitions* $\mathcal{I} = (I_1, I_2, I_3)$ *of the column indices* $\{1, 2, 3, 4\}$ *and* $\mathcal{O} = (O_1, O_2, O_3)$ *of the row indices* $\{1, 2, 3, 4\}$ *into possibly empty parts. The pattern is* admissible *if* $|I_t| + |O_t| \leq 3$ *for* $t = 1, 2, 3$. *The* punctured matrix N_P *is obtained from* N *by replacing the entry* $N_{j,k}$ *by* 0 *whenever* $j \in O_t$ *and* $k \in I_t$ *for the same index* t.

Two patterns that differ by a permutation of the index set $\{1, 2, 3\}$ applied simultaneously to $\mathcal{I}$ and $\mathcal{O}$ give the same punctured matrix. Note that if (x, y) is a related differential, then so are (y, x), (x, z), (z, x), (y, z) and (z, y), where $z = x + y$; this is the source of that identification.

Lemma 2. *Let N be a 4×4 MDS matrix in reduced form over $\mathbb{F}_{2^r}$, and let $P = (\mathcal{I}, \mathcal{O})$ be an admissible pattern. Then there exists a related differential whose zero positions are given by P as in Lemma 1 if and only if $\det N_P = 0$. More precisely, the related differentials with pattern P correspond to the nonzero vectors $u \in \ker N_P$ via the relations*

$$x_k = \begin{cases} u_k, & k \notin I_1 \\ 0, & k \in I_1 \end{cases} \qquad y_k = \begin{cases} u_k, & k \notin I_2 \\ 0, & k \in I_2 \end{cases},$$

and every nonzero vector of $\ker N_P$ has all four coordinates nonzero.

Proof. Let (x, y) be a related differential with zero pattern P, where the parts are indexed so that $I_1 = I_x$, $O_1 = O_x$, etc. Fix an input coordinate k and let v be the (unique, by Lemma 1) vector among x, y, z with $v_k = 0$. Since $x_k + y_k + z_k = 0$, the other two coordinates are equal; call their common value u_k, and note that $u_k \neq 0$ because otherwise all three would vanish at k, contradicting Lemma 1(1). Thus, for every $v \in \{x, y, z\}$ and every k,

$$v_k = \begin{cases} u_k, & k \notin I_v, \\ 0, & k \in I_v. \end{cases}$$

Now fix an output coordinate j and let v be the vector with $j \in O_v$, i.e. $(Nv)_j = 0$. Then

$$0 = (Nv)_j = \sum_{k \notin I_v} N_{j,k}\, u_k = \big(N_P\, u\big)_j,$$

because the entries $N_{j,k}$ with $k \in I_v$, $j \in O_v$ are exactly the punctured ones in row j. Hence $u \in \ker N_P$, $u \neq 0$, and $\det N_P = 0$.

Conversely, let $u \in \ker N_P$, $u \neq 0$, and define x, y (and $z = x + y$) from u as in the statement. At every input coordinate the vector labelled by the part containing k vanishes, so the input condition of Definition 1 holds; at every output coordinate $j \in O_t$, the same computation as above gives $(Nv)_j = (N_P u)_j = 0$ for the vector v labelled t, so the output condition holds as well. It remains to verify nontriviality. Suppose $x = 0$; then $u_k = 0$ for all $k \notin I_1$, i.e. $\mathrm{supp}(u) \subseteq I_1$. If $I_1 = \emptyset$ then $u = 0$, a contradiction. Otherwise consider the rows $j \notin O_1$ of the relation $N_P u = 0$: for such j and $k \in I_1$ the entry of N_P is the original $N_{j,k}$, hence

$$\sum_{k \in I_1} N_{j,k}\, u_k = 0 \qquad \text{for all } j \notin O_1.$$

This is a homogeneous system whose coefficient matrix is the $(4 - |O_1|) \times |I_1|$ submatrix of N on rows $\{1, \ldots, 4\} \setminus O_1$ and columns I_1. By admissibility $4 - |O_1| \geq |I_1| + 1$, so this submatrix of the MDS matrix N contains a nonsingular $|I_1| \times |I_1|$ minor, forcing $u|_{I_1} = 0$ and hence $u = 0$, a contradiction. Thus, $x \neq 0$, and by the same argument applied to I_2 and I_3 also $y \neq 0$ and $z \neq 0$, i.e. $x \neq y$. Finally, a nonzero $u \in \ker N_P$ with some coordinate $u_k = 0$ would produce, by the construction just given, a nontrivial related differential in which all three of x_k, y_k, z_k vanish, contradicting Lemma 1(1); hence every nonzero kernel vector is totally nonzero.

5 The Complete Characterization in Dimension Four

With the linearization machinery in place, we now establish the central result of this paper. By enumerating the admissible zero patterns constrained by Lemma 1 and evaluating the corresponding punctured determinants introduced in Lemma 2, we obtain a complete, explicit algebraic condition for the existence of related differentials in 4×4 MDS matrices.

Theorem 5. *Let N be a 4×4 MDS matrix over $\mathbb{F}_{2^r}$ in the reduced form. Then N admits a related differential if and only if $\det N_P = 0$ for at least one admissible pattern P. In addition, there are exactly 280 admissible patterns, and the 280 polynomials $\det N_P \in \mathbb{F}_2[a, \ldots, i]$ are pairwise distinct and irreducible over $\mathbb{F}_2$. Hence N admits a related differential if and only if at least one of 280 explicit polynomial equations in the entries $a, b, \ldots, i$ holds.*

Proof. The equivalence comes from Lemma 1 together with Lemma 2. For the count, note that by (2) and $\sum_t(|I_t| + |O_t|) = 8$ the multiset $\{|I_t| + |O_t|\}$ equals $\{3, 3, 2\}$; distributing the labels over the $4+4$ coordinates gives $3 \cdot \binom{8}{3,3,2} = 1680$ ordered patterns, and the identification by the symmetric group S_3 acting on the labels (which is free, the parts having pairwise distinct zero sets) leaves $1680/6 = 280$ patterns. Distinctness and irreducibility of the 280 determinants is verified by a direct computation; the complete list is reproduced in Appendix A.

The 280 cases organize themselves by the shape of the punctured entry set $\bigcup_t O_t \times I_t$, which is determined by the part profile $\{(|I_t|, |O_t|)\}_t$:

shape	punctured entries of N	#cases
A	one entry	16
B	two entries in one row	24
C	two entries in one column	24
D	two rows with two entries each, the column pairs disjoint	36
E	two columns with two entries each, the row pairs disjoint	36
F	two in one column, two in one row, and one more entry, all in pairwise distinct rows and pairwise distinct columns	144

This geometric classification of the punctured entry sets directly dictates the algebraic structure of the corresponding determinants. Rather than treating these 280 conditions as an unstructured list, this shape-based partition naturally suggests the presence of underlying symmetries. As we detail in the subsequent section, acting on these shapes via the natural symmetries of the reduced matrix collapses the entire set of equations into a compact collection of distinct orbits, significantly simplifying the algebraic landscape.

6 The Explicit Equations

Permuting rows 2–4 of N and, independently, columns 2–4 preserves the reduced form, the MDS property and the existence of related differentials, and acts on

the entries $a, \ldots, i$ by the corresponding row/column permutation of the lower-right 3×3 block. Under this group of order 36, the 280 equations fall into 27 orbits. Table 1 lists one representative per orbit: the equation $\det N_P = 0$, the punctured positions of the representative and the orbit length. The full list of all 280 equations is given in Appendix A.

Corollary 1. *A 4×4 MDS matrix M over $\mathbb{F}_{2^r}$ admits a related differential if and only if M^T does.*

Proof. Transposing a pattern, $(\mathcal{I}, \mathcal{O}) \mapsto (\mathcal{O}, \mathcal{I})$, preserves admissibility and

$$\det\big(N_{(\mathcal{I},\mathcal{O})}\big) = \det\big((N^\mathsf{T})_{(\mathcal{O},\mathcal{I})}\big),$$

so the criterion of Theorem 5 is invariant under transposition of the reduced form. If $M = DNE$ as in Theorem 2 then $M^\mathsf{T} = EN^\mathsf{T}D$, so the reduced form of M^T is N^T, and the claim follows from Theorem 3.

Remark 2. Lemmas 1 and 2 apply verbatim for $n = 2$ and $n = 3$. For $n = 2$ there is no admissible pattern, which is Theorem 1. For $n = 3$ admissibility reads $|I_t| + |O_t| \leq 2$, forcing $|I_t| + |O_t| = 2$ for all t; the possible puncture sets are a single entry (9 cases) or three entries forming a transversal, i.e. one in each row and each column (6 cases), and the resulting 15 punctured determinants are exactly the fifteen equations of Theorem 4:

(vii) $\leftrightarrow$ puncture $(1,1)$,	(ix) $\leftrightarrow (1,2)$,
(x) $\leftrightarrow (1,3)$,	(viii) $\leftrightarrow (2,1)$,
(xv) $\leftrightarrow (2,2)$,	(xiii) $\leftrightarrow (2,3)$,
(xi) $\leftrightarrow (3,1)$,	(xii) $\leftrightarrow (3,2)$,
(xiv) $\leftrightarrow (3,3)$,	(ii) $\leftrightarrow \{(1,1),(2,2),(3,3)\}$,
(i) $\leftrightarrow \{(1,1),(2,3),(3,2)\}$,	(v) $\leftrightarrow \{(1,2),(2,1),(3,3)\}$,
(iv) $\leftrightarrow \{(1,2),(2,3),(3,1)\}$,	(iii) $\leftrightarrow \{(1,3),(2,1),(3,2)\}$,
(vi) $\leftrightarrow \{(1,3),(2,2),(3,1)\}$.	

This gives an alternative, uniform proof of Theorems 1 and 4.

Remark 3. We illustrate how one of the 280 cases reduces to a punctured determinant, in the notation of the proof of Theorem 4. Consider

$$x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}, \qquad y = \begin{pmatrix} 0 \\ 0 \\ x_3 \\ x_4 \end{pmatrix},$$

with all x_k nonzero (so $z = x + y = (x_1, x_2, 0, 0)^\mathsf{T}$), and require at the output that $(Ny)_1 = 0$, $(Nx)_2 = (Ny)_2$ (i.e. $(Nz)_2 = 0$) and $(Nx)_3 = (Nx)_4 = 0$. The four conditions are

$$x_3 + x_4 = 0, \qquad x_1 + ax_2 = 0,$$
$$x_1 + dx_2 + ex_3 + fx_4 = 0, \qquad x_1 + gx_2 + hx_3 + ix_4 = 0,$$

Table 1. The 27 orbit representatives. N has a related differential iff at least one of the 280 equations obtained from these by simultaneous permutations of rows 2–4 and columns 2–4 of N is satisfied.

#	punctures	orbit	equation (= 0)
A1	$(1,1)$	1	$ae+af+ah+ai+bd+bf+bg+bi+cd+ce+cg+ch+dh+di+eg+ei+fg+fh$
A2	$(1,2)$	3	$aei+afh+bdi+bfg+cdh+ceg+ae+af+ah+ai+bd+bg+cd+cg+dh+di+eg+fg$
A3	$(2,1)$	3	$aei+afh+bdi+bfg+cdh+ceg+ae+af+ah+ai+bd+bf+bg+bi+cd+ce+cg+ch$
A4	$(2,2)$	9	$bdi+bfg+cdh+ceg+bd+bf+bg+bi+cd+ce+cg+ch+dh+di+eg+ei+fg+fh$
B1	$(1,1),(1,2)$	3	$ae+af+ah+ai+bd+bg+cd+cg+dh+di+eg+fg$
B2	$(1,2),(1,3)$	3	$aei+afh+bdi+bfg+cdh+ceg+ae+ah+bd+bg+dh+eg$
B3	$(2,1),(2,2)$	9	$bdi+bfg+cdh+ceg+bd+bf+bg+bi+cd+ce+cg+ch$
B4	$(2,2),(2,3)$	9	$cdh+ceg+cd+ce+cg+ch+dh+di+eg+ei+fg+fh$
C1	$(1,1),(2,1)$	3	$ae+af+ah+ai+bd+bf+bg+bi+cd+ce+cg+ch$
C2	$(1,2),(2,2)$	9	$bdi+bfg+cdh+ceg+bd+bg+cd+cg+dh+di+eg+fg$
C3	$(2,1),(3,1)$	3	$aei+afh+bdi+bfg+cdh+ceg+ae+af+bd+bf+cd+ce$
C4	$(2,2),(3,2)$	9	$bfg+ceg+bf+bg+bi+ce+cg+ch+eg+ei+fg+fh$
D1	$(1,1),(1,2),(2,3),(2,4)$	9	$ae+af+ah+ai+dh+di+eg+fg$
D2	$(1,2),(1,3),(2,1),(2,4)$	9	$aei+afh+bdi+bfg+ae+ah+bd+bg$
D3	$(2,1),(2,2),(3,3),(3,4)$	18	$bdi+cdh+bd+bg+bi+cd+cg+ch$
E1	$(1,1),(2,1),(3,2),(4,2)$	9	$ae+af+ah+ai+bf+bi+ce+ch$
E2	$(1,2),(2,1),(3,1),(4,2)$	9	$aei+afh+bdi+cdh+ae+af+bd+cd$
E3	$(1,2),(2,2),(3,3),(4,3)$	18	$bdi+bfg+bd+bg+cd+cg+di+fg$
F1	$(1,1),(1,2),(2,3),(3,3),(4,4)$	18	$af+ah+cd+cg+dh+fg$
F2	$(1,1),(2,1),(3,2),(3,3),(4,4)$	18	$af+ah+bf+bg+cg+ch$
F3	$(1,1),(2,2),(2,3),(3,4),(4,4)$	9	$cd+ce+cg+ch+dh+eg$
F4	$(1,2),(1,3),(2,1),(3,1),(4,4)$	9	$afh+bfg+cdh+ceg+ae+bd$
F5	$(1,2),(1,3),(2,1),(3,4),(4,4)$	9	$cdh+ceg+ae+ah+bd+bg$
F6	$(1,2),(2,1),(2,3),(3,2),(4,4)$	36	$afh+ceg+ae+af+ah+cg$
F7	$(1,2),(2,1),(2,3),(3,4),(4,4)$	18	$cdh+ceg+ae+ah+cd+cg$
F8	$(1,2),(2,1),(3,1),(4,3),(4,4)$	9	$bfg+ceg+ae+af+bd+cd$
F9	$(1,2),(2,1),(3,2),(4,3),(4,4)$	18	$bfg+ceg+ae+af+bg+cg$

i.e. $u = (x_1, x_2, x_3, x_4)^\mathsf{T}$ lies in the kernel of

$$N_P = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 1 & a & 0 & 0 \\ 1 & d & e & f \\ 1 & g & h & i \end{pmatrix},$$

which is N punctured at $(1,1),(1,2),(2,3),(2,4)$ — the representative of orbit D1. Eliminating ($x_4 = x_3$, $x_1 = ax_2$) leaves $(a+d)x_2 + (e+f)x_3 = 0$ and $(a+g)x_2 + (h+i)x_3 = 0$, with a nonzero solution if and only if

$$(a+d)(h+i) + (e+f)(a+g) = ae + af + ah + ai + dh + di + eg + fg = 0,$$

the equation D1 of Table 1. All remaining cases are handled mechanically in the same way.

7 Relations Among the Equations and the Discarded Cases

Having established the explicit equations governing related differentials, two structural questions naturally arise: First, how do the 280 equations algebraically relate to one another? Second, what are the algebraic implications of the zero patterns that were discarded by Lemma 1? As we will show, understanding the discarded patterns not only clarifies the necessity of the MDS property but also reveals which pairs of equations are mutually exclusive.

Proposition 1. *The algebraic structure of the polynomials* $\det N_P$ *exhibits the following properties:*

1. ***Distinctness and Irreducibility:*** *The* 280 *polynomials of Theorem 5 are pairwise distinct, irreducible, and pairwise coprime. No polynomial equals, divides, or is divisible by a minor of* N*. The mapping from admissible patterns to equations is uniquely determined up to the symmetries of simultaneous row/column permutations and transposition yielding the* 27 *orbits of Table 1.*
2. ***The*** 3×3 ***Case:*** *For* $n = 3$*, the fifteen equations of Theorem 4 constitute exactly the fifteen nonzero elements of the four-dimensional* $\mathbb{F}_2$*-vector space*

   $$\operatorname{span}_{\mathbb{F}_2}\{\, a+d,\ b+c,\ ad+b,\ bc+a \,\} = \operatorname{span}_{\mathbb{F}_2}\{(\mathrm{i}), (\mathrm{ii}), (\mathrm{iii}), (\mathrm{v})\}.$$

   The sum of any two distinct equations yields another equation in the set, making the fifteen equations isomorphic to the point set of the projective space $\mathrm{PG}(3,2)$*.*
3. ***The*** 4×4 ***Case:*** *For* $n = 4$*, the picture is more complex. The* 280 *polynomials span a* 14*-dimensional* $\mathbb{F}_2$*-vector space. Within this space, there exist exactly* 560 *additive relations of the form* $f + g + h = 0$ *for distinct polynomials* f, g, h*. Grouped by the puncture shapes defined in Table 1, these triples distribute as follows:*

   $$\mathrm{AAB}: 24, \quad \mathrm{AAC}: 24, \quad \mathrm{BBB}: 16, \quad \mathrm{CCC}: 16, \quad \mathrm{DDD}: 24, \quad \mathrm{EEE}: 24,$$

$$\text{BFF}: 72, \quad \text{CFF}: 72, \quad \text{DFF}: 144, \quad \text{EFF}: 144.$$

Thus, if any two equations from a triple are satisfied, the third holds automatically. Furthermore, there is no translation vector $v \neq 0$ that preserves the set of 280 *equations $\mathcal{E}$ (i.e., $v + \mathcal{E} \neq \mathcal{E}$).*

Proof. While all enumerative claims have been rigorously verified via exact symbolic computation, the additive relations stem directly from the structural properties of the matrices:

Row Additivity: The determinant is linear with respect to each row. Suppose three admissible patterns puncture entries strictly within a single common row j. Let S_1, S_2, S_3 be their respective punctured column sets. If every column index appears in an *odd* number of these sets, the three punctured copies of row j will sum to the zero vector. Because all other rows remain identical, the three resulting determinants sum to 0. Given the admissibility constraint $|S_i| \in \{1, 2\}$, this odd-coverage condition is satisfied exactly when:

- $\{S_1, S_2, S_3\}$ partitions the four columns into sizes $1, 1, 2$, producing the $4 \cdot \binom{4}{2} = 24$ relations of type AAB.
- $|S_i| = 2$ for all i and they share a single common column (coverage $3, 1, 1, 1$), producing the $4 \cdot 4 = 16$ relations of type BBB.

By applying transposition, we symmetrically obtain the AAC and CCC relations. For example:

$$\det N_{\{(2,1)\}} + \det N_{\{(2,3)\}} + \det N_{\{(2,2),(2,4)\}} = 0.$$

Laplace Expansion: The remaining families emerge from Laplace expansions along two lines. For the DDD family, fix the punctures $(1, 1)$ and $(1, 4)$, and let the second punctured row r range over $\{2, 3, 4\}$ while strictly puncturing columns $\{2, 3\}$. If we expand $\det N_P$ along columns 2 and 3, the only surviving terms are $T_s = \det N[\{1, s\}, \{2, 3\}] \cdot \det N[\{2, 3, 4\} \setminus \{s\}, \{1, 4\}]$ for $s \in \{2, 3, 4\} \setminus \{r\}$. (Terms whose complementary block contains row 1 vanish because row 1 has no remaining support in columns 1 and 4, and terms involving row r similarly vanish). Summing these expansions over all possible r counts every T_s exactly twice, meaning the three determinants sum to 0 over $\mathbb{F}_2$.

The mixed families BFF, CFF, DFF, and EFF are derived via analogous two-line expansions. The complete set of 560 relations has been algebraically cross-checked to ensure no extraneous relations exist.

The discarded patterns explain both the cases eliminated in earlier proofs and a second, complementary phenomenon: the existence of equation pairs that can never hold simultaneously on an MDS matrix.

Proposition 2. *Drop the admissibility requirement and consider all ordered partitions $(\mathcal{I}, \mathcal{O})$ of $\{1, 2, 3, 4\}$ into three possibly empty blocks. Let $b_t = |I_t| + |O_t|$ denote the total number of punctured coordinates for part t, and let N_P be the corresponding punctured matrix. Then, exactly one of the following structural conditions holds:*

1. ***Admissible*** *(*$\max_t b_t \leq 3$*): The determinant* $\det N_P$ *is irreducible, and each equation* $\det N_P = 0$ *is satisfiable by MDS matrices over* $\mathbb{F}_{2^3}$*. In particular,* no single equation from Theorem 5 contradicts the MDS property.
2. ***Boundary*** *(*$\max_t b_t = 4$*): The determinant* $\det N_P$ *is a nonzero product of minors of* N *(comprising* 35 *distinct products). Consequently,* $\det N_P = 0$ *if and only if a minor of* N *vanishes. These candidate equations intrinsically* contradict *the MDS assumption and correspond exactly to the discarded branches. Representative factorizations include:*
   - Trivial pair ($x = 0$, splits $(4,0),(0,2),(0,2)$): $\det N_P = \det N$.
   - Single unpunctured cell in a row (punctures $(1,1)$, $(1,2)$, $(1,3)$, $(2,4)$, $(3,4)$):
   $$\det N_P = N_{1,4} \cdot \det N[\{2,3,4\},\{1,2,3\}] = ae + ah + bd + bg + dh + eg.$$
   - Block puncture (2×2 block at rows $\{1,2\}$, columns $\{1,2\}$):
   $$\det N_P = \det N[\{1,2\},\{3,4\}] \cdot \det N[\{3,4\},\{1,2\}] = (b+c)(d+g).$$
3. ***Degenerate*** *(*$\max_t b_t \geq 5$*): The determinant vanishes identically. If* $|I_t| = 4$ *or* $|O_t| = 4$*, the punctured matrix contains a zero row or column. Otherwise, the* $|O_t|$ *punctured rows form a* $(4 - |I_t|)$*-dimensional coordinate subspace. The candidate equation is vacuous and every kernel vector of* N_P *is degenerate and is excluded by the MDS minors.*

This result is the algebraic shadow of the weight count underlying Lemma 1: having b_t zeros among the eight coordinates of the codeword (v_t, Nv_t) leaves a weight of at most $8 - b_t$. Because the branch number of a 4×4 MDS matrix is 5, the boundary condition $b_t = 4$ represents the exact point where a theoretically possible weight transitions into a condition that only holds for non-MDS matrices. Correspondingly, the determinant degenerates into a product of minors. An analogous trichotomy accurately governs the $n = 3$ case, mapping perfectly to the eliminated branches in the proof of Theorem 4.

Corollary 2. *Among the* $\binom{280}{2} = 39060$ *possible pairs of the equations identified in Theorem 5, exactly* 840 *pairs* $\{f, g\}$ *sum to a polynomial* $f+g$ *that factors into a product of minors of* N*. These* 840 *pairs of equations are mutually exclusive and can never hold simultaneously for an MDS matrix.*

For any such exclusive pair $\{f, g\}$, the condition $f = g = 0$ implies $f + g = 0$, forcing a minor of N to vanish. Since N is MDS, this yields an immediate contradiction. As an example, if $f = \det N_{\{(1,4),(2,4)\}}$ and $g = \det N_{\{(2,4)\}}$, their sum evaluates directly to a minor: $f + g = \det N[\{2,3,4\},\{1,2,3\}]$. More broadly, every pairwise sum is governed by the multilinearity identity $\det N_P + \det N_Q = \det N_R$ established in the proof of Proposition 1. This identity completely classifies the pair sums:

- If the resulting pattern R is admissible, we obtain one of the 560 valid triples (1680 pairs where two equations imply a third).
- If R corresponds to a discarded boundary pattern ($b_t = 4$), we obtain the 840 mutually exclusive pairs.

– The remaining 36540 sums are generic polynomials that do not simply factor into minors.

This structured behavior contrasts sharply with the $n = 3$ case. As established in Proposition 1 (2), every pair sum in dimension three yields another equation from the set of fifteen. Consequently, no pair is excluded by minor factorization, and any two equations merely imply a third.

8 Examples and Computations over Small Fields

Since a 4×4 MDS matrix generates an $[8, 4, 5]$ MDS code, and an $[n, k]$ MDS code with $k \geq 2$ satisfies $n \leq q + k - 1$ (see, e.g., [10]), the smallest field of characteristic two carrying 4×4 MDS matrices is $\mathbb{F}_8$. Over this extremal field the situation can be settled exhaustively.

Theorem 6. *There are exactly* 720 *reduced* 4×4 *MDS matrices over* $\mathbb{F}_8$*. Every one of them satisfies at least one of the* 280 *equations of Theorem 5; in fact, with perfect regularity, each matrix satisfies exactly* 28 *of the* 280 *equations, and each equation is satisfied by exactly* 72 *of the* 720 *matrices. Consequently,* every 4×4 *MDS matrix over* $\mathbb{F}_8$ *admits a related differential.*

Proof. By exhaustive computation: the reduced matrices were enumerated by a levelwise search with minor pruning, the count 720 being consistent with independent rejection sampling, and the 280 equations were evaluated on each matrix. A sample of the resulting related differentials was checked directly against Definition 1 by the independent search of Remark 6. The final claim follows from Theorem 3.

Remark 4. The incidence structure of Theorem 6 is a tactical configuration: $720 \cdot 28 = 280 \cdot 72 = 20160$. We do not currently have a structural explanation for this double regularity (note also the suggestive count $720 = 6!$); see Section 9.

For larger fields, related-differential-free MDS matrices exist, as the following explicit example shows.

Example 1. Let $\mathbb{F}_{2^{10}} = \mathbb{F}_2[\alpha]$ with $\alpha^{10} + \alpha^3 + 1 = 0$ (then α is primitive), and let

$$N = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 & \alpha^4 \\ 1 & \alpha^8 & \alpha^{16} & \alpha^{32} \\ 1 & \alpha^{64} & \alpha^{128} & \alpha^{256} \end{pmatrix},$$

i.e. the entry in block position (j, k) is $\alpha^{2^{3(j-1)+(k-1)}}$. Then N is MDS and none of the 280 equations of Theorem 5 is satisfied, so DNE has no related differentials for any invertible diagonal D and E. Both facts were verified by exhaustive computation; we note that, in contrast to Example 2 of [9], the analogous matrix over $\mathbb{F}_{2^9}$ *does* satisfy one of the 280 equations, so the field must be checked individually.

Remark 5. Sampling suggests that related-differential-free MDS matrices are rare for small q and increasingly common as q grows. Among uniformly sampled reduced MDS matrices, the observed fractions admitting related differentials were 60/60 over $\mathbb{F}_{2^4}$, 40/40 over $\mathbb{F}_{2^5}$, 39/40 over $\mathbb{F}_{2^6}$, 54/80 over $\mathbb{F}_{2^8}$ and 1/12 over $\mathbb{F}_{2^{10}}$. This is in good agreement with the naive heuristic obtained by treating the 280 equations as independent events of probability $1/q$ each, namely $1-(1-1/q)^{280} \approx 1-e^{-280/q}$, which predicts ≈ 0.99, 0.66 and 0.24 for $r = 6, 8, 10$ respectively. We stress that this is a heuristic only; by Theorem 6 the true value is exactly 1 for $r = 3$.

Remark 6. All computational claims were verified independently in exact arithmetic: (i) for $n = 3$ the same procedure outputs exactly the fifteen equations of Theorem 4; (ii) for each of the 280 equations, MDS matrices satisfying it were sampled over $\mathbb{F}_{2^6}$ and the related differential predicted by Lemma 2 was constructed and checked directly against Definition 1; (iii) for several hundred random MDS matrices over $\mathbb{F}_{2^r}$, $r \in \{3, 4, 5, 6, 8, 10\}$, the criterion of Theorem 5 was compared with an independent exhaustive search for related differentials, enumerating all input zero types, including degenerate ones, and all output choices, with full agreement; and (iv) the criterion holds for every sampled 4×4 circulant MDS matrix, in accordance with [3], while sampled 4×4 Hadamard MDS matrices over $\mathbb{F}_{2^8}$ fall into both classes, in accordance with [3] and [5]. Finally, (v) Theorem 6 rests on an exhaustive enumeration of all reduced MDS matrices over $\mathbb{F}_{2^3}$, a sample of which was cross-checked against the independent search of (iii); moreover all 27 orbits of equations, and hence all 280 equations, by symmetry are realized by MDS matrices over each of $\mathbb{F}_{2^3}, \mathbb{F}_{2^4}, \mathbb{F}_{2^5}, \mathbb{F}_{2^7}$ by direct search, and over $\mathbb{F}_{2^6}$ equation by equation as in (ii).

9 Conclusion and Open Problems

In this paper, we gave a complete algebraic characterization of 4×4 MDS matrices over finite fields of even characteristic that admit related differentials. We showed that the existence of a related differential is equivalent to the vanishing of 280 explicit multilinear polynomials. This connects the combinatorial structure of zero-difference patterns directly to algebraic conditions on the matrix entries. We also studied the relationships among these equations and completely analyzed the special case of $\mathbb{F}_8$. As a result, checking whether a 4×4 MDS matrix is resistant to related differentials reduces to evaluating 280 low-degree polynomials. This provides a practical and precise tool for studying optimal diffusion layers.

Our results also suggest several directions for future work:

1. The classification over $\mathbb{F}_8$ (Theorem 6) shows a remarkable regularity. There are exactly 720 (= 6!) reduced MDS matrices. Each matrix satisfies exactly 28 equations, and each equation is satisfied by exactly 72 matrices. This highly symmetric structure suggests that a deeper algebraic or group-theoretic explanation exists. Known symmetries, such as simultaneous row

and column permutations, transposition, and Frobenius automorphisms, do not fully explain why the numbers 28 and 72 appear.

2. We constructed explicit related-differential-free MDS matrices over $\mathbb{F}2^{10}$ (Example 1) and proved that none exist over $\mathbb{F}8$. However, the cases of $\mathbb{F}16$ and $\mathbb{F}32$ remain open. The heuristic in Remark 5 predicts that the proportion of such matrices is approximately $e^{-280/q}$. For $q = 16$, this probability is about 2.5×10^{-8}. Since this density is extremely small, random search is unlikely to succeed. More structured algebraic methods that exploit symmetry may be needed.
3. Extending our approach to dimensions $n \geq 5$ is challenging. The main difficulty comes from Lemma 1, which is a key part of our linearization method. For $n \leq 4$, this lemma forces a clean separation of zero coordinates among the input vectors. This property no longer holds when $n \geq 5$. For example, when $n = 5$, a coordinate may exist where x, y, and z are all zero at the same time. Such cases make the weight constraints overlap and significantly increase the number of possible patterns that must be considered. As a result, the combinatorial complexity grows rapidly.

References

1. Bardeh, N.G., Rijmen, V.: New key-recovery attack on reduced-round AES. IACR Trans. Symmetric Cryptol. **2022**(2), 43–62 (2022)
2. Biham, E., Shamir, A.: Differential cryptanalysis of DES-like cryptosystems. J. Cryptol. **4**(1), 3–72 (1991)
3. Daemen, J., Rijmen, V.: New criteria for linear maps in AES-like ciphers. Cryptogr. Commun. **1**(1), 47–69 (2009)
4. Gupta, K.C., Pandey, S.K., Ray, I.G., Samanta, S.: Cryptographically significant MDS matrices over finite fields: a brief survey and some generalized results. Adv. Math. Commun. **13**(4), 779–843 (2019)
5. Jha, S., Li, S., Gligoroski, D.: Construction of Hadamard-based MixColumns matrices resistant to related-differential cryptanalysis. IACR Commun. Cryptol. **2**(1), 37 (2025)
6. Kumar, Y., Mishra, P.R., Samanta, S., Gupta, K.C., Gaur, A.: Construction of all MDS and involutory MDS matrices. Adv. Math. Commun. **18**(6), 1547–1566 (2024)
7. Kumar, Y., Yadav, A.A., Samanta, S.: Analyzing linear layers in related-differential cryptanalysis. arXiv:2605.27535 (2026)
8. National Institute of Standards and Technology: Advanced Encryption Standard (AES). FIPS PUB 197, U.S. Department of Commerce (2001)
9. Otal, K., Sülçe, A.M., Yayla, O.: On the cryptographic resilience of MDS matrices. Cryptology ePrint Archive, Paper 2025/2240 (2025), https://eprint.iacr.org/2025/2240
10. Roth, R.M.: Introduction to Coding Theory. Cambridge University Press, Cambridge (2006)

A The 280 equations

This appendix lists all 280 equations of Theorem 5, grouped by the 27 orbits of Table 1: orbit code and length in parentheses, representative first. Each entry gives the punctured positions of the pattern P as concatenated row column pairs e.g. (12)(21) means punctures at $(1,2)$ and $(2,1)$, followed by the expanded determinant $\det N_P$; the corresponding equation is $\det N_P = 0$. By Theorem 5, N admits a related differential if and only if at least one of these 280 polynomials vanishes.

A1 *(1)*
(11): $ae+af+ah+ai+bd+bf+bg+bi+cd+ce+cg+ch+dh+di+eg+ei+fg+fh$

A2 *(3)*
(12): $aei+afh+bdi+bfg+cdh+ceg+ae+af+ah+ai+bd+bg+cd+cg+dh+di+eg+fg$
(13): $aei+afh+bdi+bfg+cdh+ceg+ae+ah+bd+bf+bg+bi+ce+ch+dh+eg+ei+fh$
(14): $aei+afh+bdi+bfg+cdh+ceg+af+ai+bf+bi+cd+ce+cg+ch+di+ei+fg+fh$

A3 *(3)*
(21): $aei+afh+bdi+bfg+cdh+ceg+ae+af+ah+ai+bd+bf+bg+bi+cd+ce+cg+ch$
(31): $aei+afh+bdi+bfg+cdh+ceg+ae+af+bd+bf+cd+ce+dh+di+eg+ei+fg+fh$
(41): $aei+afh+bdi+bfg+cdh+ceg+ah+ai+bg+bi+cg+ch+dh+di+eg+ei+fg+fh$

A4 *(9)*
(22): $bdi+bfg+cdh+ceg+bd+bf+bg+bi+cd+ce+cg+ch+dh+di+eg+ei+fg+fh$
(23): $aei+afh+cdh+ceg+ae+af+ah+ai+cd+ce+cg+ch+dh+di+eg+ei+fg+fh$
(24): $aei+afh+bdi+bfg+ae+af+ah+ai+bd+bf+bg+bi+dh+di+eg+ei+fg+fh$
(32): $aei+afh+bfg+ceg+ae+af+ah+ai+bf+bg+bi+ce+cg+ch+eg+ei+fg+fh$
(33): $afh+bdi+bfg+cdh+af+ah+ai+bd+bf+bg+bi+cd+cg+ch+dh+di+fg+fh$
(34): $aei+bdi+cdh+ceg+ae+ah+ai+bd+bg+bi+cd+ce+cg+ch+dh+di+eg+ei$
(42): $aei+afh+bdi+cdh+ae+af+ah+ai+bd+bf+bi+cd+ce+ch+dh+di+ei+fh$
(43): $aei+bdi+bfg+ceg+ae+af+ai+bd+bf+bg+bi+cd+ce+cg+di+eg+ei+fg$
(44): $afh+bfg+cdh+ceg+ae+af+ah+bd+bf+bg+cd+ce+cg+ch+dh+eg+fg+fh$

B1 *(3)*
(11)(12): $ae+af+ah+ai+bd+bg+cd+cg+dh+di+eg+fg$
(11)(13): $ae+ah+bd+bf+bg+bi+ce+ch+dh+eg+ei+fh$
(11)(14): $af+ai+bf+bi+cd+ce+cg+ch+di+ei+fg+fh$

B2 *(3)*
(12)(13): $aei+afh+bdi+bfg+cdh+ceg+ae+ah+bd+bg+dh+eg$
(12)(14): $aei+afh+bdi+bfg+cdh+ceg+af+ai+cd+cg+di+fg$
(13)(14): $aei+afh+bdi+bfg+cdh+ceg+bf+bi+ce+ch+ei+fh$

B3 *(9)*
(21)(22): $bdi+bfg+cdh+ceg+bd+bf+bg+bi+cd+ce+cg+ch$
(21)(23): $aei+afh+cdh+ceg+ae+af+ah+ai+cd+ce+cg+ch$
(21)(24): $aei+afh+bdi+bfg+ae+af+ah+ai+bd+bf+bg+bi$
(31)(32): $aei+afh+bfg+ceg+ae+af+bf+ce+eg+ei+fg+fh$
(31)(33): $afh+bdi+bfg+cdh+af+bd+bf+cd+dh+di+fg+fh$
(31)(34): $aei+bdi+cdh+ceg+ae+bd+cd+ce+dh+di+eg+ei$
(41)(42): $aei+afh+bdi+cdh+ah+ai+bi+ch+dh+di+ei+fh$
(41)(43): $aei+bdi+bfg+ceg+ai+bg+bi+cg+di+eg+ei+fg$
(41)(44): $afh+bfg+cdh+ceg+ah+bg+cg+ch+dh+eg+fg+fh$

B4 *(9)*
(22)(23): $cdh+ceg+cd+ce+cg+ch+dh+di+eg+ei+fg+fh$
(22)(24): $bdi+bfg+bd+bf+bg+bi+dh+di+eg+ei+fg+fh$
(23)(24): $aei+afh+ae+af+ah+ai+dh+di+eg+ei+fg+fh$
(32)(33): $afh+bfg+af+ah+ai+bf+bg+bi+cg+ch+fg+fh$
(32)(34): $aei+ceg+ae+ah+ai+bg+bi+ce+cg+ch+eg+ei$
(33)(34): $bdi+cdh+ah+ai+bd+bg+bi+cd+cg+ch+dh+di$
(42)(43): $aei+bdi+ae+af+ai+bd+bf+bi+cd+ce+di+ei$
(42)(44): $afh+cdh+ae+af+ah+bd+bf+cd+ce+ch+dh+fh$
(43)(44): $bfg+ceg+ae+af+bd+bf+bg+cd+ce+cg+eg+fg$

C1 *(3)*
(11)(21): $ae+af+ah+ai+bd+bf+bg+bi+cd+ce+cg+ch$
(11)(31): $ae+af+bd+bf+cd+ce+dh+di+eg+ei+fg+fh$
(11)(41): $ah+ai+bg+bi+cg+ch+dh+di+eg+ei+fg+fh$

C2 *(9)*
(12)(22): $bdi+bfg+cdh+ceg+bd+bg+cd+cg+dh+di+eg+fg$
(12)(32): $aei+afh+bfg+ceg+ae+af+ah+ai+bg+cg+eg+fg$
(12)(42): $aei+afh+bdi+cdh+ae+af+ah+ai+bd+cd+dh+di$
(13)(23): $aei+afh+cdh+ceg+ae+ah+ce+ch+dh+eg+ei+fh$
(13)(33): $afh+bdi+bfg+cdh+ah+bd+bf+bg+bi+ch+dh+fh$
(13)(43): $aei+bdi+bfg+ceg+ae+bd+bf+bg+bi+ce+eg+ei$
(14)(24): $aei+afh+bdi+bfg+af+ai+bf+bi+di+ei+fg+fh$

(14)(34): $aei+bdi+cdh+ceg+ai+bi+cd+ce+cg+ch+di+ei$
(14)(44): $afh+bfg+cdh+ceg+af+bf+cd+ce+cg+ch+fg+fh$

C3 *(3)*
(21)(31): $aei+afh+bdi+bfg+cdh+ceg+ae+af+bd+bf+cd+ce$
(21)(41): $aei+afh+bdi+bfg+cdh+ceg+ah+ai+bg+bi+cg+ch$
(31)(41): $aei+afh+bdi+bfg+cdh+ceg+dh+di+eg+ei+fg+fh$

C4 *(9)*
(22)(32): $bfg+ceg+bf+bg+bi+ce+cg+ch+eg+ei+fg+fh$
(22)(42): $bdi+cdh+bd+bf+bi+cd+ce+ch+dh+di+ei+fh$
(23)(33): $afh+cdh+af+ah+ai+cd+cg+ch+dh+di+fg+fh$
(23)(43): $aei+ceg+ae+af+ai+cd+ce+cg+di+eg+ei+fg$
(24)(34): $aei+bdi+ae+ah+ai+bd+bg+bi+dh+di+eg+ei$
(24)(44): $afh+bfg+ae+af+ah+bd+bf+bg+dh+eg+fg+fh$
(32)(42): $aei+afh+ae+af+ah+ai+bf+bi+ce+ch+ei+fh$
(33)(43): $bdi+bfg+af+ai+bd+bf+bg+bi+cd+cg+di+fg$
(34)(44): $cdh+ceg+ae+ah+bd+bg+cd+ce+cg+ch+dh+eg$

D1 *(9)*
(11)(12)(23)(24): $ae+af+ah+ai+dh+di+eg+fg$
(11)(12)(33)(34): $ah+ai+bd+bg+cd+cg+dh+di$
(11)(12)(43)(44): $ae+af+bd+bg+cd+cg+eg+fg$
(11)(13)(22)(24): $bd+bf+bg+bi+dh+eg+ei+fh$
(11)(13)(32)(34): $ae+ah+bg+bi+ce+ch+eg+ei$
(11)(13)(42)(44): $ae+ah+bd+bf+ce+ch+dh+fh$
(11)(14)(22)(23): $cd+ce+cg+ch+di+ei+fg+fh$
(11)(14)(32)(33): $af+ai+bf+bi+cg+ch+fg+fh$
(11)(14)(42)(43): $af+ai+bf+bi+cd+ce+di+ei$

D2 *(9)*
(12)(13)(21)(24): $aei+afh+bdi+bfg+ae+ah+bd+bg$
(12)(13)(31)(34): $aei+bdi+cdh+ceg+ae+bd+dh+eg$
(12)(13)(41)(44): $afh+bfg+cdh+ceg+ah+bg+dh+eg$
(12)(14)(21)(23): $aei+afh+cdh+ceg+af+ai+cd+cg$
(12)(14)(31)(33): $afh+bdi+bfg+cdh+af+cd+di+fg$
(12)(14)(41)(43): $aei+bdi+bfg+ceg+ai+cg+di+fg$
(13)(14)(21)(22): $bdi+bfg+cdh+ceg+bf+bi+ce+ch$
(13)(14)(31)(32): $aei+afh+bfg+ceg+bf+ce+ei+fh$
(13)(14)(41)(42): $aei+afh+bdi+cdh+bi+ch+ei+fh$

D3 *(18)*
(21)(22)(33)(34): $bdi+cdh+bd+bg+bi+cd+cg+ch$
(21)(22)(43)(44): $bfg+ceg+bd+bf+bg+cd+ce+cg$
(21)(23)(32)(34): $aei+ceg+ae+ah+ai+ce+cg+ch$
(21)(23)(42)(44): $afh+cdh+ae+af+ah+cd+ce+ch$
(21)(24)(32)(33): $afh+bfg+af+ah+ai+bf+bg+bi$
(21)(24)(42)(43): $aei+bdi+ae+af+ai+bd+bf+bi$
(22)(23)(31)(34): $cdh+ceg+cd+ce+dh+di+eg+ei$
(22)(23)(41)(44): $cdh+ceg+cg+ch+dh+eg+fg+fh$
(22)(24)(31)(33): $bdi+bfg+bd+bf+dh+di+fg+fh$
(22)(24)(41)(43): $bdi+bfg+bg+bi+di+eg+ei+fg$
(23)(24)(31)(32): $aei+afh+ae+af+eg+ei+fg+fh$
(23)(24)(41)(42): $aei+afh+ah+ai+dh+di+ei+fh$
(31)(32)(43)(44): $bfg+ceg+ae+af+bf+ce+eg+fg$
(31)(33)(42)(44): $afh+cdh+af+bd+bf+cd+dh+fh$
(31)(34)(42)(43): $aei+bdi+ae+bd+cd+ce+di+ei$
(32)(33)(41)(44): $afh+bfg+ah+bg+cg+ch+fg+fh$
(32)(34)(41)(43): $aei+ceg+ai+bg+bi+cg+eg+ei$
(33)(34)(41)(42): $bdi+cdh+ah+ai+bi+ch+dh+di$

E1 *(9)*
(11)(21)(32)(42): $ae+af+ah+ai+bf+bi+ce+ch$
(11)(21)(33)(43): $af+ai+bd+bf+bg+bi+cd+cg$
(11)(21)(34)(44): $ae+ah+bd+bg+cd+ce+cg+ch$
(11)(22)(31)(42): $bd+bf+cd+ce+dh+di+ei+fh$
(11)(22)(32)(41): $bg+bi+cg+ch+eg+ei+fg+fh$
(11)(23)(31)(43): $ae+af+cd+ce+di+eg+ei+fg$
(11)(23)(33)(41): $ah+ai+cg+ch+dh+di+fg+fh$
(11)(24)(31)(44): $ae+af+bd+bf+dh+eg+fg+fh$
(11)(24)(34)(41): $ah+ai+bg+bi+dh+di+eg+ei$

E2 *(9)*
(12)(21)(31)(42): $aei+afh+bdi+cdh+ae+af+bd+cd$
(12)(21)(32)(41): $aei+afh+bfg+ceg+ah+ai+bg+cg$
(12)(22)(31)(41): $bdi+bfg+cdh+ceg+dh+di+eg+fg$
(13)(21)(31)(43): $aei+bdi+bfg+ceg+ae+bd+bf+ce$
(13)(21)(33)(41): $afh+bdi+bfg+cdh+ah+bg+bi+ch$
(13)(23)(31)(41): $aei+afh+cdh+ceg+dh+eg+ei+fh$
(14)(21)(31)(44): $afh+bfg+cdh+ceg+af+bf+cd+ce$
(14)(21)(34)(41): $aei+bdi+cdh+ceg+ai+bi+cg+ch$
(14)(24)(31)(41): $aei+afh+bdi+bfg+di+ei+fg+fh$

E3 *(18)*
(12)(22)(33)(43): $bdi+bfg+bd+bg+cd+cg+di+fg$
(12)(22)(34)(44): $cdh+ceg+bd+bg+cd+cg+dh+eg$
(12)(23)(32)(43): $aei+ceg+ae+af+ai+cg+eg+fg$
(12)(23)(33)(42): $afh+cdh+af+ah+ai+cd+dh+di$
(12)(24)(32)(44): $afh+bfg+ae+af+ah+bg+eg+fg$
(12)(24)(34)(42): $aei+bdi+ae+ah+ai+bd+dh+di$
(13)(22)(32)(43): $bfg+ceg+bf+bg+bi+ce+eg+ei$
(13)(22)(33)(42): $bdi+cdh+bd+bf+bi+ch+dh+fh$
(13)(23)(32)(42): $aei+afh+ae+ah+ce+ch+ei+fh$
(13)(23)(34)(44): $cdh+ceg+ae+ah+ce+ch+dh+eg$
(13)(24)(33)(44): $afh+bfg+ah+bd+bf+bg+dh+fh$
(13)(24)(34)(43): $aei+bdi+ae+bd+bg+bi+eg+ei$
(14)(22)(32)(44): $bfg+ceg+bf+ce+cg+ch+fg+fh$
(14)(22)(34)(42): $bdi+cdh+bi+cd+ce+ch+di+ei$
(14)(23)(33)(44): $afh+cdh+af+cd+cg+ch+fg+fh$
(14)(23)(34)(43): $aei+ceg+ai+cd+ce+cg+di+ei$
(14)(24)(32)(42): $aei+afh+af+ai+bf+bi+ei+fh$
(14)(24)(33)(43): $bdi+bfg+af+ai+bf+bi+di+fg$

F1 *(18)*
(11)(12)(23)(33)(44): $af+ah+cd+cg+dh+fg$
(11)(12)(23)(34)(43): $ae+ai+cd+cg+di+eg$
(11)(12)(23)(34)(44): $ae+ah+cd+cg+dh+eg$
(11)(12)(24)(33)(43): $af+ai+bd+bg+di+fg$
(11)(12)(24)(33)(44): $af+ah+bd+bg+dh+fg$
(11)(12)(24)(34)(43): $ae+ai+bd+bg+di+eg$
(11)(13)(22)(32)(44): $bf+bg+ce+ch+eg+fh$
(11)(13)(22)(34)(42): $bd+bi+ce+ch+dh+ei$
(11)(13)(22)(34)(44): $bd+bg+ce+ch+dh+eg$
(11)(13)(24)(32)(42): $ae+ah+bf+bi+ei+fh$
(11)(13)(24)(32)(44): $ae+ah+bf+bg+eg+fh$
(11)(13)(24)(34)(42): $ae+ah+bd+bi+dh+ei$
(11)(14)(22)(32)(43): $bf+bi+ce+cg+ei+fg$
(11)(14)(22)(33)(42): $bf+bi+cd+ch+di+fh$
(11)(14)(22)(33)(43): $bf+bi+cd+cg+di+fg$
(11)(14)(23)(32)(42): $af+ai+ce+ch+ei+fh$
(11)(14)(23)(32)(43): $af+ai+ce+cg+ei+fg$
(11)(14)(23)(33)(42): $af+ai+cd+ch+di+fh$

F2 *(18)*
(11)(21)(32)(33)(44): $af+ah+bf+bg+cg+ch$
(11)(21)(32)(34)(43): $ae+ai+bg+bi+ce+cg$
(11)(21)(32)(43)(44): $ae+af+bf+bg+ce+cg$
(11)(21)(33)(34)(42): $ah+ai+bd+bi+cd+ch$
(11)(21)(33)(42)(44): $af+ah+bd+bf+cd+ch$
(11)(21)(34)(42)(43): $ae+ai+bd+bi+cd+ce$
(11)(22)(23)(31)(44): $cd+ce+dh+eg+fg+fh$
(11)(22)(23)(34)(41): $cg+ch+dh+di+eg+ei$
(11)(22)(24)(31)(43): $bd+bf+di+eg+ei+fg$
(11)(22)(24)(33)(41): $bg+bi+dh+di+fg+fh$
(11)(22)(31)(43)(44): $bd+bf+cd+ce+eg+fg$
(11)(22)(33)(34)(41): $bg+bi+cg+ch+dh+di$
(11)(23)(24)(31)(42): $ae+af+dh+di+ei+fh$
(11)(23)(24)(32)(41): $ah+ai+eg+ei+fg+fh$
(11)(23)(31)(42)(44): $ae+af+cd+ce+dh+fh$
(11)(23)(32)(34)(41): $ah+ai+cg+ch+eg+ei$
(11)(24)(31)(42)(43): $ae+af+bd+bf+di+ei$
(11)(24)(32)(33)(41): $ah+ai+bg+bi+fg+fh$

F3 *(9)*
(11)(22)(23)(34)(44): $cd+ce+cg+ch+dh+eg$
(11)(22)(24)(33)(43): $bd+bf+bg+bi+di+fg$
(11)(22)(32)(43)(44): $bf+bg+ce+cg+eg+fg$
(11)(22)(33)(34)(42): $bd+bi+cd+ch+dh+di$
(11)(23)(24)(32)(42): $ae+af+ah+ai+ei+fh$
(11)(23)(32)(34)(43): $ae+ai+ce+cg+eg+ei$
(11)(23)(33)(42)(44): $af+ah+cd+ch+dh+fh$
(11)(24)(32)(33)(44): $af+ah+bf+bg+fg+fh$
(11)(24)(34)(42)(43): $ae+ai+bd+bi+di+ei$

F4 *(9)*
(12)(13)(21)(31)(44): $afh+bfg+cdh+ceg+ae+bd$
(12)(13)(21)(34)(41): $aei+bdi+cdh+ceg+ah+bg$
(12)(13)(24)(31)(41): $aei+afh+bdi+bfg+dh+eg$
(12)(14)(21)(31)(43): $aei+bdi+bfg+ceg+af+cd$
(12)(14)(21)(33)(41): $afh+bdi+bfg+cdh+ai+cg$
(12)(14)(23)(31)(41): $aei+afh+cdh+ceg+di+fg$
(13)(14)(21)(31)(42): $aei+afh+bdi+cdh+bf+ce$
(13)(14)(21)(32)(41): $aei+afh+bfg+ceg+bi+ch$
(13)(14)(22)(31)(41): $bdi+bfg+cdh+ceg+ei+fh$

F5 *(9)*
(12)(13)(21)(34)(44): $cdh+ceg+ae+ah+bd+bg$
(12)(13)(24)(31)(44): $afh+bfg+ae+bd+dh+eg$
(12)(13)(24)(34)(41): $aei+bdi+ah+bg+dh+eg$
(12)(14)(21)(33)(43): $bdi+bfg+af+ai+cd+cg$
(12)(14)(23)(31)(43): $aei+ceg+af+cd+di+fg$
(12)(14)(23)(33)(41): $afh+cdh+ai+cg+di+fg$
(13)(14)(21)(32)(42): $aei+afh+bf+bi+ce+ch$
(13)(14)(22)(31)(42): $bdi+cdh+bf+ce+ei+fh$
(13)(14)(22)(32)(41): $bfg+ceg+bi+ch+ei+fh$

F6 *(36)*
(12)(21)(23)(32)(44): $afh+ceg+ae+af+ah+cg$
(12)(21)(23)(34)(42): $aei+cdh+ae+ah+ai+cd$
(12)(21)(24)(32)(43): $aei+bfg+ae+af+ai+bg$
(12)(21)(24)(33)(42): $afh+bdi+af+ah+ai+bd$
(12)(22)(31)(33)(44): $bfg+cdh+bd+cd+dh+fg$
(12)(22)(31)(34)(43): $bdi+ceg+bd+cd+di+eg$
(12)(22)(33)(41)(44): $bfg+cdh+bg+cg+dh+fg$
(12)(22)(34)(41)(43): $bdi+ceg+bg+cg+di+eg$
(12)(23)(31)(34)(42): $aei+cdh+ae+cd+dh+di$
(12)(23)(32)(41)(44): $afh+ceg+ah+cg+eg+fg$
(12)(24)(31)(33)(42): $afh+bdi+af+bd+dh+di$
(12)(24)(32)(41)(43): $aei+bfg+ai+bg+eg+fg$
(13)(21)(22)(33)(44): $bfg+cdh+bd+bf+bg+ch$
(13)(21)(22)(34)(43): $bdi+ceg+bd+bg+bi+ce$
(13)(21)(24)(32)(43): $aei+bfg+ae+bf+bg+bi$
(13)(21)(24)(33)(42): $afh+bdi+ah+bd+bf+bi$
(13)(22)(31)(34)(43): $bdi+ceg+bd+ce+eg+ei$
(13)(22)(33)(41)(44): $bfg+cdh+bg+ch+dh+fh$
(13)(23)(31)(32)(44): $afh+ceg+ae+ce+eg+fh$
(13)(23)(31)(34)(42): $aei+cdh+ae+ce+dh+ei$
(13)(23)(32)(41)(44): $afh+ceg+ah+ch+eg+fh$
(13)(23)(34)(41)(42): $aei+cdh+ah+ch+dh+ei$
(13)(24)(31)(32)(43): $aei+bfg+ae+bf+eg+ei$
(13)(24)(33)(41)(42): $afh+bdi+ah+bi+dh+fh$
(14)(21)(22)(33)(44): $bfg+cdh+bf+cd+cg+ch$
(14)(21)(22)(34)(43): $bdi+ceg+bi+cd+ce+cg$
(14)(21)(23)(32)(44): $afh+ceg+af+ce+cg+ch$
(14)(21)(23)(34)(42): $aei+cdh+ai+cd+ce+ch$
(14)(22)(31)(33)(44): $bfg+cdh+bf+cd+fg+fh$
(14)(22)(34)(41)(43): $bdi+ceg+bi+cg+di+ei$
(14)(23)(31)(32)(44): $afh+ceg+af+ce+fg+fh$
(14)(23)(34)(41)(42): $aei+cdh+ai+ch+di+ei$
(14)(24)(31)(32)(43): $aei+bfg+af+bf+ei+fg$
(14)(24)(31)(33)(42): $afh+bdi+af+bf+di+fh$
(14)(24)(32)(41)(43): $aei+bfg+ai+bi+ei+fg$
(14)(24)(33)(41)(42): $afh+bdi+ai+bi+di+fh$

F7 *(18)*
(12)(21)(23)(34)(44): $cdh+ceg+ae+ah+cd+cg$
(12)(21)(24)(33)(43): $bdi+bfg+af+ai+bd+bg$
(12)(23)(31)(34)(43): $aei+ceg+ae+cd+di+eg$
(12)(23)(33)(41)(44): $afh+cdh+ah+cg+dh+fg$
(12)(24)(31)(33)(44): $afh+bfg+af+bd+dh+fg$
(12)(24)(34)(41)(43): $aei+bdi+ai+bg+di+eg$
(13)(21)(22)(34)(44): $cdh+ceg+bd+bg+ce+ch$
(13)(21)(24)(32)(42): $aei+afh+ae+ah+bf+bi$
(13)(22)(31)(34)(42): $bdi+cdh+bd+ce+dh+ei$
(13)(22)(32)(41)(44): $bfg+ceg+bg+ch+eg+fh$
(13)(24)(31)(32)(44): $afh+bfg+ae+bf+eg+fh$
(13)(24)(34)(41)(42): $aei+bdi+ah+bi+dh+ei$
(14)(21)(22)(33)(43): $bdi+bfg+bf+bi+cd+cg$
(14)(21)(23)(32)(42): $aei+afh+af+ai+ce+ch$
(14)(22)(31)(33)(42): $bdi+cdh+bf+cd+di+fh$
(14)(22)(32)(41)(43): $bfg+ceg+bi+cg+ei+fg$
(14)(23)(31)(32)(43): $aei+ceg+af+ce+ei+fg$
(14)(23)(33)(41)(42): $afh+cdh+ai+ch+di+fh$

F8 *(9)*
(12)(21)(31)(43)(44): $bfg+ceg+ae+af+bd+cd$
(12)(21)(33)(34)(41): $bdi+cdh+ah+ai+bg+cg$
(12)(23)(24)(31)(41): $aei+afh+dh+di+eg+fg$
(13)(21)(31)(42)(44): $afh+cdh+ae+bd+bf+ce$
(13)(21)(32)(34)(41): $aei+ceg+ah+bg+bi+ch$
(13)(22)(24)(31)(41): $bdi+bfg+dh+eg+ei+fh$
(14)(21)(31)(42)(43): $aei+bdi+af+bf+cd+ce$
(14)(21)(32)(33)(41): $afh+bfg+ai+bi+cg+ch$
(14)(22)(23)(31)(41): $cdh+ceg+di+ei+fg+fh$

F9 *(18)*
(12)(21)(32)(43)(44): $bfg+ceg+ae+af+bg+cg$
(12)(21)(33)(34)(42): $bdi+cdh+ah+ai+bd+cd$
(12)(22)(31)(43)(44): $bfg+ceg+bd+cd+eg+fg$
(12)(22)(33)(34)(41): $bdi+cdh+bg+cg+dh+di$
(12)(23)(24)(31)(42): $aei+afh+ae+af+dh+di$
(12)(23)(24)(32)(41): $aei+afh+ah+ai+eg+fg$

(13)(21)(32)(34)(43): $aei+ceg+ae+bg+bi+ce$
(13)(21)(33)(42)(44): $afh+cdh+ah+bd+bf+ch$
(13)(22)(24)(31)(43): $bdi+bfg+bd+bf+eg+ei$
(13)(22)(24)(33)(41): $bdi+bfg+bg+bi+dh+fh$
(13)(23)(31)(42)(44): $afh+cdh+ae+ce+dh+fh$
(13)(23)(32)(34)(41): $aei+ceg+ah+ch+eg+ei$
(14)(21)(32)(33)(44): $afh+bfg+af+bf+cg+ch$
(14)(21)(34)(42)(43): $aei+bdi+ai+bi+cd+ce$
(14)(22)(23)(31)(44): $cdh+ceg+cd+ce+fg+fh$
(14)(22)(23)(34)(41): $cdh+ceg+cg+ch+di+ei$
(14)(24)(31)(42)(43): $aei+bdi+af+bf+di+ei$
(14)(24)(32)(33)(41): $afh+bfg+ai+bi+fg+fh$