CORRELATION IMMUNITY OF THE BOOLEAN FUNCTIONS BUILT FROM MUTUALLY ORTHOGONAL CELLULAR AUTOMATA: THE EXHAUSTIVE CLASSIFICATION FOR LOCAL RULES OF DIAMETER AT MOST SIX

KOREA SUPERINTELLIGENCE LABS

Abstract. A bipermutive local rule of diameter d over $\mathbb{F}_2$ induces a Latin square of order 2^{d-1}; k rules whose squares are pairwise orthogonal form a set of k mutually orthogonal cellular automata (k-MOCA), and Mariot and Manzoni (arXiv:2207.08280; AUTOMATA 2023) proved that the $2^{2(d-1)} \times k(d-1)$ binary array obtained by juxtaposing the k output tables is the support of a Boolean function that is correlation immune of order at least 2. Their exhaustive search for $k = 3$ and $d \in \{4, 5\}$ found only orders 3 and 4, and they ask whether the bound 2 is ever attained. We classify the construction completely for $d \leq 5$ and every k: there are 16 sets of 3-MOCA at $d = 4$, and 264, 224 and 96 sets of 3-, 4- and 5-MOCA at $d = 5$, with no larger family at either diameter; the correlation immunity order is exactly 3 for every one of them except 72 of the 264, whose order is exactly 4. At $d = 6$ we compute the whole table (65 536 rules, 266 740 orthogonal pairs, 5 808 sets of 3-MOCA of orders 3, 4, 5 in 4 576, 960, 272 cases, families of every size up to 8 and none of size 9) and certify named families of orders 5, 4 and 3, a 4-MOCA of order 4, and an 8-MOCA giving a 40-variable function of weight 1 024 and order 3. Hence, in all 48 984 families with $k \geq 3$ and $d \leq 6$, the order is never 2; the largest order is $3, 4, 5$ at $d = 4, 5, 6$ and collapses to exactly 3 once $k \geq 5$. Under the counting convention of the source's own reference (families divided by 8), which its $d = 4$ entry obeys exactly, its Table 1 at $d = 5$ should read $33 = 24 + 9$ rather than $36 = 27 + 9$ (the arXiv version prints $27 + 6$), and its minimum-weight entry 24 at $(n, t) = (12, 4)$ contradicts the published value 128 of Kiss and Nagy. The maximum family sizes $3, 5, 8$ coincide with the maxima for linear rules proved by Mariot, Gadouleau, Formenti and Leporati; no family of general bipermutive rules exceeds them for $d \leq 6$. Every statement about $d \leq 5$ and every named $d = 6$ family is verified in Lean 4 by compiled evaluation from the source's definitions.

1. Introduction

The objects. Fix a diameter $d \geq 3$ and put $b = d - 1$. A local rule $f : \mathbb{F}_2^d \to \mathbb{F}_2$ is *bipermutive* if

$$f(x_1, \ldots, x_d) = x_1 \oplus \varphi(x_2, \ldots, x_{d-1}) \oplus x_d$$

for an arbitrary function $\varphi : \mathbb{F}_2^{d-2} \to \mathbb{F}_2$ of the $d - 2$ central variables, so there are exactly $2^{2^{d-2}}$ bipermutive rules of diameter d: $4, 16, 256, 65\,536$ for $d = 3, 4, 5, 6$. The *no-boundary cellular automaton* with rule f on $2b$ cells is the map $F : \mathbb{F}_2^{2b} \to \mathbb{F}_2^b$, $F(x)_i = f(x_i, \ldots, x_{i+d-1})$ for $1 \leq i \leq b$. Indexing rows by the left half $(x_1, \ldots, x_b)$ and columns by the right half $(x_{b+1}, \ldots, x_{2b})$ of the input, the values of F fill a Latin square L_F of order 2^b. Two bipermutive rules are *orthogonal* when the superposition of their Latin squares realises every ordered pair of symbols exactly once, and k pairwise orthogonal bipermutive automata $F_1, \ldots, F_k$ are a set of *k-MOCA* (mutually orthogonal cellular automata). Given k-MOCA, the array

$$A = \big(F_1(x), F_2(x), \ldots, F_k(x)\big)_{x \in \mathbb{F}_2^{2b}}$$

has $N = 2^{2b}$ rows and $n = kb$ binary columns; the rows of A are the support of a Boolean function f_A on n variables. Mariot and Manzoni [1, 2] prove (their Lemma 3 and Theorem 1) that A is a binary orthogonal array of strength at least 2, hence, by the characterisation of Camion, Carlet, Charpin and Sendrier [11], that f_A is *correlation immune of order at least* 2, and that its Hamming weight is $N = 2^{2b}$ whatever k is. Low-weight functions of high correlation immunity order are what masking countermeasures against side-channel attacks ask for; this is the motivation stated in the source, and it is not revisited here.

The source and its open question. The source (arXiv:2207.08280v1 [1], published as [2]; both versions were read, see the bibliography for what was read and how the numbering was resolved) reports an exhaustive search for $k = 3$ and $d \in \{4, 5\}$: "we performed an exhaustive search of all k-MOCA for $k = 3$ and $d = 4, 5$. In particular, we discarded $d = 3$ since there are no families of 3-MOCA in that case. On the other hand, going for higher values of k and d makes the search space too huge to be exhaustively visited in a limited time." Its Table 1 lists, per diameter, the number of 3-MOCA found, the parameters (n, w_H), the correlation immunity orders that occur with their multiplicities, and a column of minimum weights; the published version reads, in its own column order (d, #3-MOCA, n, w_H, CI, #CI, Min w_H),

d	#3-MOCA	n	w_H	CI	#CI	Min w_H
4	2	9	64	3	2	20
5	36	12	256	3	27	24
5	36	12	256	4	9	24

with the caption "Classification of correlation immune functions generated by 3-MOCA of diameter $d \in \{4, 5\}$". The arXiv version differs in exactly two places: the last row has #CI = 6, so that its two $d = 5$ rows sum to $27 + 6 = 33$ against the printed total 36, and the caption promises "diameter $d \in \{4, 5, 6\}$" although the body has no $d = 6$ row. The source draws from this table the observation that "all generated functions actually have a correlation immunity order higher than 2", and closes with (Section 5, identical in both versions):

> "The most natural open question remains whether our Theorem 1 is really a tight lower bound on the correlation immunity of the Boolean functions constructed through k-MOCA. If further experiments show that the lowest correlation immunity order is always at least 3, then it would be interesting to try refining Lemma 3, and prove that the binary OA obtained from a set of k-MOCA has always at least strength 3."

and, in Section 4, "Further experiments on larger diameters should be performed to see if this hypothesis holds, or if there exist functions constructed through our methods that are effectively second-order correlation immune." The 2025 survey by Manzoni, Mariot and Menara [5] restates the construction and still reports only "a binary OA of strength at least 2".

What is settled here. Everything below is an exact statement about finite objects defined verbatim from the source, established by exhaustive computation and, for $d \leq 5$ and for the named $d = 6$ families, machine-checked (Section 8).

- **The complete classification for $d \leq 5$, every k** (Theorems 3.2, 3.3, 4.1, 4.2, 4.4). Table 1 gives the numbers of k-MOCA and Table 2 the correlation immunity orders. At $d = 4$ there are 16 sets of 3-MOCA (listed explicitly), all of order exactly 3, and no 4-MOCA; at $d = 5$ there are 264 sets of 3-MOCA, of which exactly 192 have order 3 and 72 have order 4, then 224 sets of 4-MOCA and 96 sets of 5-MOCA, every one of order exactly 3, and no 6-MOCA. The weight is 2^{2b} and the rows are pairwise distinct in every case.
- **The answer to the open question for $d \leq 6$** (Theorem 4.3, Theorem 5.1 and Remark 5.2). No k-MOCA with $k \geq 3$ and $d \leq 6$ gives a function that is only second-order correlation immune: the order is at least 3 in all 48 984 such families, so the bound of the source's Theorem 1 is attained by nothing in the range now reachable. The largest order is 3, 4, 5 at $d = 4, 5, 6$, and for $k \geq 5$ it is exactly 3 in every family.
- **Diameter** 6 (Theorem 5.1, Remark 5.2). Named 3-MOCA of orders exactly 5, 4 and 3, a 4-MOCA of order exactly 4, and an 8-MOCA whose 40-variable function has weight 1 024 and order exactly 3, are certified individually; the full table — 266 740 orthogonal pairs, 5 808 sets of 3-MOCA, families of every size up to 8 — is computed and reported as a computation.
- **Three corrections to the source's Table 1** (Corollary 4.5, Remark 6.1). Under the counting convention of the source's own reference [3] — counts divided by 8 — which the source's $d = 4$ entry obeys exactly ($16/8 = 2$), the $d = 5$ entries should be $33 = 24 + 9$, not $36 = 27 + 9$: the order-4 count 9 of the published version is right (the arXiv version's 6 is not), the order-3 count

and the total are three too large. The arXiv caption promises a $d = 6$ row that neither version contains; it is supplied here. And the minimum-weight entry 24 at $(n, t) = (12, 4)$ duplicates the row above it, whereas the published minimum weight of a fourth-order correlation immune function of 12 variables is 128 (Kiss and Nagy [10]).

- **Maximum family sizes** (Theorems 3.2, 4.4, Remark 5.2). The largest set of MOCA has 3, 5, 8 members at $d = 4, 5, 6$. These values are not new for *linear* rules: they are the maxima N_{d-1} of Mariot, Gadouleau, Formenti and Leporati [4], Theorem 3. What the census adds is that no family of general bipermutive rules exceeds the linear maximum for $d \leq 6$; whether nonlinear rules can ever do so is asked in [7], and the census answers it in the negative for $d \leq 6$ and says nothing beyond.

d	rules	2-MOCA	3-MOCA	4-MOCA	5-MOCA	6-MOCA	7-MOCA	8-MOCA	max
3	4	4	0	—	—	—	—	—	2
4	16	36	16	0	—	—	—	—	3
5	256	852	264	224	96	0	—	—	5
6^*	65 536	266 740	5 808	6 160	11 392	13 504	8 960	2 560	8

TABLE 1. The number of sets of k-MOCA of diameter d (unordered families of k pairwise orthogonal bipermutive rules), and the largest family size. Rows $d \leq 5$ are machine-checked; the row marked * is computed (Remark 5.2), with the five families of Theorem 5.1 machine-checked. Dividing the 2-MOCA column by 4 gives $1, 9, 213, 66\,685$, the published pair counts of [3].

d	k	n	w_H	families	orders (multiplicities)	up to complementation
4	3	9	64	16	3 (16)	$2 = 2 + 0$
5	3	12	256	264	3 (192), 4 (72)	$33 = 24 + 9$
5	4	16	256	224	3 (224)	14
5	5	20	256	96	3 (96)	3
6^*	3	15	1 024	5 808	3 (4 576), 4 (960), 5 (272)	$726 = 572 + 120 + 34$
6^*	4	20	1 024	6 160	3 (5 744), 4 (416)	385
6^*	$5, 6, 7, 8$	$25, 30, 35, 40$	1 024	see Table 1	3 (all)	$356, 211, 70, 10$

TABLE 2. The exact correlation immunity order of f_A over all k-MOCA with $k \geq 3$. The last column counts complementation orbits (Lemma 2.1), which is the source's "divided by 8" at $k = 3$. Rows marked * are computed (Remark 5.2); the reduced counts 14, 3 and those at $d = 6$ are outside the formal development, all other entries are machine-checked.

What is new and what is not. We are careful about attribution. The construction, Lemma 3 and Theorem 1 (order at least 2), the observation "at least 3" on the families the source classified, the values $(n, w_H) = (9, 64), (12, 256)$, the order 3 at $d = 4$ with reduced count 2, and the presence of order-4 functions at $d = 5$ are all the source's [1, 2], and are reproduced here exactly, not discovered. The orthogonal pair counts $1, 9, 213, 66\,685$ (divided by 8) are Table 2 of Mariot, Formenti and Leporati [3], and the same numbers multiplied by 8, i.e. $8, 72, 1\,704, 533\,480$ ordered pairs, are tabulated by Mariot [6]; our 2-MOCA column reproduces both at every diameter including $d = 6$. The maximum sizes $3, 5, 8$ of families of *linear* bipermutive rules are Theorem 3 of [4]. The minimum weight 128 at $(12, 4)$ is Proposition 3 of Kiss and Nagy [10]. The characterisation of correlation immunity by orthogonal arrays is [11], the spectral characterisation is Xiao and Massey [12], and correlation immunity itself is Siegenthaler's [13]. What we claim is: the unreduced census with the explicit $d = 4$ list and the fact that 3 and 5 are the largest family sizes at $d = 4, 5$ over all bipermutive rules; the exact order of every function for $d \le 5$ and every k; the answer "never 2" for $d \le 6$; the five certified $d = 6$ families and the computed $d = 6$ table; and the three corrections. A full-text sweep of 890 835 arXiv e-prints on 2026-09-07 for the phrase "mutually orthogonal cellular automata" returns twelve papers, all from the same group of authors; adding the acronym "MOCA" restricted to papers that also mention orthogonal or bipermutive cellular automata adds two more ([7] and arXiv:2504.09173). None tabulates correlation immunity orders of MOCA-derived functions, and the numbers 264, 192, 72, 33, 5 808, 726 occur in none of them; the nearest neighbour outside this circle, Prévost and Martin [9], builds 9-variable functions from a single iterated rule with no orthogonality and reports first-order correlation immunity only. OpenAlex lists no citing work for either version of the source; Semantic Scholar lists two (the survey [5] and [8], which mentions correlation immunity only in its reference list). We read every negative as "not found", not as "new".

Verification. Every theorem and proposition below carries a formal counterpart, listed by name in Section 8 and reproduced verbatim in Appendix A. The statements are decided by compiled evaluation (`native_decide`) of executable definitions transcribed from the source. Where the text says more than its formal counterpart — the closed forms of the rules named in Theorem 5.1, the general form of Lemma 2.1, the $d = 6$ table of Remark 5.2, and Remark 6.1 — it says so at that place.

2. Preliminaries

2.1. **Boolean functions, the Walsh transform, orthogonal arrays.** For $f \colon \mathbb{F}_2^n \to \mathbb{F}_2$ the *support* is $\operatorname{supp}(f) = \{x : f(x) \neq 0\}$, the *Hamming weight* is $w_H(f) = |\operatorname{supp}(f)|$, and the *Walsh transform* is

$$W_f(a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus a \cdot x}, \qquad a \in \mathbb{F}_2^n$$

(Eq. (3) of [1], Eq. (2) of [2]). Following the source (Section 2.1, after Xiao and Massey [12]), f is *correlation immune of order t* if $W_f(a) = 0$ for every a with $1 \le w_H(a) \le t$. The *correlation immunity order* $\operatorname{ci}(f)$ is the largest such $t \le n$, and $\operatorname{ci}(f) = 0$ when some a of weight 1 has $W_f(a) \neq 0$. An *orthogonal array* $\mathrm{OA}(N, n, 2, t)$ is an $N \times n$ binary array in which every $N \times t$ subarray contains each of the 2^t binary t-tuples exactly $\lambda = N/2^t$ times; λ is its *index*, necessarily an integer. For an array with pairwise distinct rows, strength t is the same as: for every nonempty set of at most t columns, the parity of those columns is 0 on exactly half of the rows. The link is the source's Lemma 1, due to Camion, Carlet, Charpin and Sendrier [11]: *f is correlation immune of order t if and only if* $\operatorname{supp}(f)$*, written as an array with pairwise distinct rows, is an* $\mathrm{OA}(w_H(f), n, 2, t)$. Two consequences are used below: the weight of a t-th order correlation immune function is divisible by 2^t, and $\operatorname{ci}(f)$ can be evaluated either from the full Walsh spectrum (a transform over 2^n inputs) or from the balance of column parities over the $w_H(f)$ support rows. Both routes are implemented, and they are checked against each other.

2.2. **Bipermutive rules, Latin squares, MOCA.** We index the bipermutive rules of diameter d by their central function: the rule with central function $\varphi \colon \mathbb{F}_2^{d-2} \to \mathbb{F}_2$ is named by the integer

$$\langle \varphi \rangle = \sum_{z \in \mathbb{F}_2^{d-2}} \varphi(z)\, 2^Z, \qquad Z = \sum_{i=1}^{d-2} z_i\, 2^{\,d-2-i}$$

(z_1 most significant), so the rules are $0, 1, \ldots, 2^{2^{d-2}} - 1$ and rule 0 is $x_1 \oplus x_d$. At $d = 3$, rules 0 and 2 are $x_1 \oplus x_3$ and $x_1 \oplus x_2 \oplus x_3$ (Wolfram's rules 90 and 150), the pair of the source's Figure 1. Write $\mathcal{B}_d$ for the set of rules, L_φ for the Latin square of order 2^b of the rule φ (rows: left half of the input; columns: right half; entry: the b output cells read as a b-bit number, first cell most significant), and call φ, ψ *orthogonal* when $x \mapsto (L_\varphi(x), L_\psi(x))$ is injective on $\mathbb{F}_2^{2b}$ (equivalently, since there are 2^{2b} cells and 2^{2b} pairs, surjective: Eq. (6) of [1], Eq. (4) of [2]). A *set of k-MOCA* is a k-element subset of $\mathcal{B}_d$ of pairwise orthogonal rules; $\mathcal{M}_k(d)$ denotes the set of all of them, so $\mathcal{M}_2(d)$ is the set of unordered orthogonal pairs. For $S \in \mathcal{M}_k(d)$ listed in increasing order as $\varphi_1 < \cdots < \varphi_k$, the array A_S has the 2^{2b} rows $(L_{\varphi_1}(x), \ldots, L_{\varphi_k}(x))$, each read as an $n = kb$-bit number with L_{φ_1} most significant, and $f_S \colon \mathbb{F}_2^n \to \mathbb{F}_2$ is the indicator of the set of rows; $w_H(f_S)$ is the number of *distinct* rows, which equals

2^{2b} exactly when the rows are pairwise distinct — and for $k \geq 2$ they always are, since already the first two blocks $(L_{\varphi_1}(x), L_{\varphi_2}(x))$ determine x. The order of the columns does not affect $\mathrm{ci}(f_S)$, so nothing below depends on this reading convention; the convention is fixed so that families can be named. The source's Theorem 1 says $\mathrm{ci}(f_S) \geq 2$ for every $S \in \mathcal{M}_k(d)$, and the remark following it disposes of $k = 2$: the 2^{2b} rows of a 2-MOCA are all of $\mathbb{F}_2^{2b}$, so $f_S \equiv 1$.

2.3. **Complementation, and what the source's table counts.** Complementing a rule, $\varphi \mapsto \varphi \oplus 1$, gives again a bipermutive rule ($\langle \varphi \oplus 1\rangle = \langle \varphi\rangle \oplus (2^{2^{d-2}} - 1)$).

Lemma 2.1. *Let $S = \{\varphi_1, \ldots, \varphi_k\} \in \mathcal{M}_k(d)$ and let S' be obtained by complementing any subset of its rules. Then $S' \in \mathcal{M}_k(d)$, $w_H(f_{S'}) = w_H(f_S)$ and $\mathrm{ci}(f_{S'}) = \mathrm{ci}(f_S)$. The group $(\mathbb{Z}/2)^k$ of such complementations acts freely on $\mathcal{M}_k(d)$, every orbit has 2^k elements, and the families all of whose rules satisfy $\varphi(0, \ldots, 0) = 0$ (even indices $\langle\varphi\rangle$) form a system of representatives. In particular $|\mathcal{M}_3(d)|/8$ is the number of orbits at $k = 3$.*

Proof. Complementing φ complements every entry of L_φ bitwise, i.e. replaces $L_\varphi(x)$ by $L_\varphi(x) \oplus (1, \ldots, 1)$; the map $x \mapsto (L_\varphi(x), L_\psi(x))$ stays injective, so orthogonality is preserved (this is also Lemma 2 of [3]). On the array, the rows of $A_{S'}$ are the rows of A_S translated by a fixed vector $e \in \mathbb{F}_2^n$, so $f_{S'}(x) = f_S(x \oplus e)$, the weight is unchanged and $W_{f_{S'}}(a) = (-1)^{a \cdot e} W_{f_S}(a)$ has the same zeros. A rule and its complement are never orthogonal (the superposition of L_φ and $L_{\varphi\oplus 1}$ takes only 2^b values on 2^{2b} cells), so no family contains both, and complementing a nonempty set of rules changes the family: the action is free. Each orbit contains exactly one family in which every $\varphi(0, \ldots, 0)$ vanishes, because each rule can be complemented independently. □

The lemma is proved in the text; its $d = 4$, $k = 3$ instance is among the machine-checked controls of Proposition 7.1. Its role is to make the source's table comparable with an unreduced census. The source generated its pairs "by using the combinatorial algorithm described in [15]" (reference numbers of the published version; the arXiv version cites the same work), and [15] is [3]. Its Table 2 of orthogonal pairs is captioned "Distribution of CA-based orthogonal Latin squares up to $n = 6$", and the text that discusses it fixes the counting convention: "Notice that all reported numbers are divided by 8, since we have to take into account the pairs with swapped order, which halve the resulting sets, and the reversal and complementation transformations, which by Lemma 2 additionally reduce them to a quarter." That table reads $1, 9, 213, 66\,685$ for $d = 3, 4, 5, 6$, i.e. $2|\mathcal{M}_2(d)|/8$ with $|\mathcal{M}_2(d)| = 4, 36, 852, 266\,740$ (Proposition 3.1 for $d \leq 5$, Remark 5.2 for $d = 6$). Applied to families of three, "divided by 8" is the orbit count of Lemma 2.1, and it reproduces the source's $d = 4$ entry exactly: $|\mathcal{M}_3(4)| = 16$ and $16/8 = 2$. Every count below is therefore given both unreduced and as the number of orbits.

3. Diameters three and four

The definitions above are transcriptions; the first proposition pins them to data the source and its reference print in full.

Proposition 3.1 (definition fidelity)**.** (a) *Every one of the* 4*,* 16*,* 256 *bipermutive rules of diameter* $3, 4, 5$ *induces a Latin square of order* 2^{d-1}*.*

(b) *At $d = 3$ the rules 0 and 2 (rules 90 and 150) are orthogonal, and on the eight 3-bit windows* $000, 100, 010, 110, 001, 101, 011, 111$ *— the fusions of the eight edges of the source's Figure 1, in its order — the pair of labels (l_f, l_g) is* $(0, 0), (1, 1), (0, 1), (1, 0), (1, 1), (0, 0), (1, 0), (0, 1)$*, exactly the eight rows of that figure's table.*

(c) $2|\mathcal{M}_2(d)|/8 = 1, 9, 213$ *for $d = 3, 4, 5$, the three entries of Table 2 of* [3] *at those diameters.*

Theorem 3.2 (diameters 3 and 4: the census)**.** (a) $|\mathcal{M}_2(3)| = 4$ *and* $\mathcal{M}_3(3) = \varnothing$*: there is no set of 3-MOCA of diameter* 3*.*

(b) $|\mathcal{B}_4| = 16$*,* $|\mathcal{M}_2(4)| = 36$*, and* $\mathcal{M}_3(4)$ *consists of exactly the* 16 *families*

$$\{0,3,5\}, \{0,3,10\}, \{0,5,12\}, \{0,10,12\}, \{3,5,6\}, \{3,5,9\}, \{3,5,15\}, \{3,6,10\},$$
$$\{3,9,10\}, \{3,10,15\}, \{5,6,12\}, \{5,9,12\}, \{5,12,15\}, \{6,10,12\}, \{9,10,12\}, \{10,12,15\}.$$

Exactly two of them, $\{0,10,12\}$ *and* $\{6,10,12\}$*, consist of rules with* $\varphi(0,0)=0$*, so there are* 2 *families up to complementation.*

(c) $\mathcal{M}_4(4)=\varnothing$*: no four bipermutive rules of diameter* 4 *are pairwise orthogonal, so* 3 *is the largest family size at diameter* 4*.*

The eight rules that occur in (b) are, by the encoding of Section 2, $0=x_1\oplus x_4$, $10=x_1\oplus x_3\oplus x_4$, $12=x_1\oplus x_2\oplus x_4$, $6=x_1\oplus x_2\oplus x_3\oplus x_4$ and their complements $15,5,3,9$; every family of 3-MOCA of diameter 4 is affine. The two representatives are, in the polynomial language of [4], the two triples of pairwise coprime polynomials among $1+X^3=(1+X)(1+X+X^2)$, $1+X+X^3$, $1+X^2+X^3$ and $(1+X)^3$, the first and last of which share the factor $1+X$ (rules 0 and 6 are not orthogonal). The reduced count 2 is the source's; the list, and the fact that $k=3$ is not a budget choice at $d=4$ but the maximum, are not stated in the source. The value 3 is the linear maximum N_3 of [4].

Theorem 3.3 (diameter 4: the order is exactly 3)**.** *Every* $S\in\mathcal{M}_3(4)$ *has* 64 *pairwise distinct rows, so* f_S *is a function of* $n=9$ *variables and weight* 64*; and* $\mathrm{ci}(f_S)=3$ *for every one of the* 16 *families — never* 2 *and never* 4*.*

The source's Table 1 prints $n=9$, $w_H=64$, CI $=3$, #CI $=2$ at $d=4$, which Theorem 3.3 reproduces under the reduction of Lemma 2.1; that no family reaches order 4 is implicit in the source's #CI column exhausting its total.

Proof of Proposition 3.1 and Theorems 3.2 and 3.3. All statements are finite and are decided by exhaustive evaluation: the 2^{2b} entries of each of the $2^{2^{d-2}}$ Latin squares are computed from the rule, orthogonality is tested on all $\binom{|\mathcal{B}_d|}{2}$ pairs, $\mathcal{M}_k(d)$ is enumerated as the set of k-cliques of the orthogonality graph, and for each family the 2^{2b} rows are formed and $\mathrm{ci}(f_S)$ is read off the Walsh spectrum of the full 2^n-entry truth table. At $d=4$ this is 16 squares of order 8, 120 pair tests, 16 transforms of length 512. □

4. Diameter five

Theorem 4.1 (diameter 5, $k=3$: the census)**.** $|\mathcal{B}_5|=256$*,* $|\mathcal{M}_2(5)|=852$ *and* $|\mathcal{M}_3(5)|=264$*; exactly* 33 *of the* 264 *consist of rules with* $\varphi(0,0,0)=0$*, so there are* 33 *families of* 3*-MOCA of diameter* 5 *up to complementation. Every* $S\in\mathcal{M}_3(5)$ *has* 256 *pairwise distinct rows, so* f_S *is a function of* $n=12$ *variables and weight* 256*.*

Theorem 4.2 (diameter 5, $k=3$: the order distribution)**.** *Of the* 264 *families in* $\mathcal{M}_3(5)$*, exactly* 192 *have* $\mathrm{ci}(f_S)=3$ *and exactly* 72 *have* $\mathrm{ci}(f_S)=4$*; no other order occurs. Among the* 33 *representatives with* $\varphi(0,0,0)=0$ *the split is* 24 *of order* 3 *and* 9 *of order* 4*. Moreover the two evaluation routes — the Walsh spectrum of the* 2^n*-entry truth table, and the strength of the support as an orthogonal array — return the same order on all* $16+264=280$ *families of* 3*-MOCA of diameters* 4 *and* 5*.*

Theorem 4.3 (the open question at diameter 5)**.** *No set of* 3*-MOCA of diameter* 5 *gives a function that is only second-order correlation immune:* $\mathrm{ci}(f_S)\geq 3$ *for every* $S\in\mathcal{M}_3(5)$*. Also* $\mathrm{ci}(f_S)\leq 4$ *for every* S*, and both* 3 *and* 4 *are attained.*

Theorem 4.4 (diameter 5, $k\geq 4$)**.** $|\mathcal{M}_4(5)|=224$*,* $|\mathcal{M}_5(5)|=96$ *and* $\mathcal{M}_6(5)=\varnothing$*, so* 5 *is the largest family size at diameter* 5*. Every* $S\in\mathcal{M}_4(5)$ *and every* $S\in\mathcal{M}_5(5)$ *has* 256 *pairwise distinct rows, so* f_S *has weight* 256 *on* $n=16$*, respectively* $n=20$*, variables, and* $\mathrm{ci}(f_S)=3$ *exactly for all* $224+96$ *of them. Every one of the* 852 *pairs in* $\mathcal{M}_2(5)$ *has* 256 *pairwise distinct rows in* $\mathbb{F}_2^8$*, so its* f_S *is the constant function* 1*, of order* 8*; the value* 8 *is machine-checked on the first pair in the enumeration and follows for the others from the distinctness of their rows.*

Proof of Theorems 4.1–4.4. Exhaustive evaluation as in Section 3: 256 Latin squares of order 16, $\binom{256}{2}=32\,640$ orthogonality tests on 256 cells each, clique enumeration for $k=2,\dots,6$, and one order evaluation per family. For $k=3$ ($n=12$) the order is computed twice, from the 4 096-entry Walsh spectrum and from the column parities over the 256 support rows (the source's Lemma 1); the second route costs $|\operatorname{supp} f|/64$ word operations per coefficient instead of a transform over 2^n inputs and is the one used for $n = 16$ and $n = 20$, where it is justified by the agreement statement of Theorem 4.2. For $k = 2$ the support has 256 distinct rows in $\mathbb{F}_2^8$, hence is all of $\mathbb{F}_2^8$. $\square$

Corollary 4.5 (comparison with Table 1 of the source)**.** *Under the reduction of Lemma 2.1, which is the "divided by 8" of the source's reference* [3] *and reproduces the source's $d = 4$ row exactly, the $d = 5$ rows of Table 1 should read*

$$d = 5: \quad \#3\text{-}MOCA = 33, \qquad n = 12,\ w_H = 256, \qquad \#\mathrm{CI} = 24 \textit{ at order } 3, \quad \#\mathrm{CI} = 9 \textit{ at order } 4.$$

The published version prints 36, 27, 9: the order-4 count is correct and the arXiv version's 6 is not; the order-3 count is three too large, and so, by the same three, is the total. The arXiv version's two $d = 5$ rows already fail to add up ($27 + 6 = 33 \neq 36$); the published version made the row add up by changing 6 to 9 rather than 27 to 24 and 36 to 33.

Remark 4.6 (on the reduction). The comparison rests on identifying the source's count with the orbit count of Lemma 2.1, and that identification is forced by its $d = 4$ row: outside the formal development we also computed, for $d = 5$, the number of orbits of $\mathcal{M}_3(5)$ under complementation together with simultaneous reversal of all three rules (19), and the number of triples obtained by extending one representative ordered pair per orbit of the symmetry group of [3] by every third rule orthogonal to both (244, the same for every choice of representatives we tried); neither is 36, and no reduction of 264 families under a group of order 8 can have more than 33 orbits. The source publishes no per-family data, so no mechanism for the surplus is claimed; the statement is only that the true reduced values are $33 = 24 + 9$.

The value 5 for the largest family at diameter 5 is again the linear maximum N_4 of [4]; the census says no family of general bipermutive rules is larger. Outside the formal development we note that each of the 3 complementation orbits of $\mathcal{M}_5(5)$, and each of the 14 orbits of $\mathcal{M}_4(5)$, contains a family of linear rules.

5. Diameter six

The arXiv caption's $d = 6$ column is out of reach of the interpreter-based verification used for $d \leq 5$: the pair scan is $\binom{65\,536}{2} \approx 2.1 \cdot 10^9$ orthogonality tests. We therefore certify one named family per cell of interest and report the full table as a computation. Rule indices are as in Section 2 with φ a function of (x_2, x_3, x_4, x_5); the closed forms below are read off the indices and are not part of the formal statements:

$$\begin{aligned} 0 &= x_1 \oplus x_6, & 255 &= x_1 \oplus x_2 \oplus x_6 \oplus 1, \\ 3855 &= x_1 \oplus x_3 \oplus x_6 \oplus 1, & 13107 &= x_1 \oplus x_4 \oplus x_6 \oplus 1, \\ 15555 &= x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_6 \oplus 1, & 23205 &= x_1 \oplus x_2 \oplus x_3 \oplus x_5 \oplus x_6 \oplus 1, \\ 26265 &= x_1 \oplus x_2 \oplus x_4 \oplus x_5 \oplus x_6 \oplus 1, & 26985 &= x_1 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_6 \oplus 1. \end{aligned}$$

Theorem 5.1 (diameter 6: certified families)**.** *At $d = 6$ ($b = 5$, weight $1\,024$):*

(a) $\{0, 255, 15555\}$ *is a set of 3-MOCA with $1\,024$ pairwise distinct rows and $\mathrm{ci}(f_S) = 5$; so the largest order at diameter 6 is at least 5, strictly above the largest order 4 at diameter 5.*
(b) $\{0, 255, 23205\}$ *is a set of 3-MOCA with $\mathrm{ci}(f_S) = 4$, and* $\{0, 255, 3855\}$ *is a set of 3-MOCA with $\mathrm{ci}(f_S) = 3$.*
(c) $\{0, 3855, 15555, 23205\}$ *is a set of 4-MOCA with $\mathrm{ci}(f_S) = 4$, an order no 4-MOCA of diameter 5 reaches.*
(d) $\{0, 255, 3855, 13107, 15555, 23205, 26265, 26985\}$ *is a set of 8-MOCA with $1\,024$ pairwise distinct rows; f_S is a function of $n = 40$ variables, weight $1\,024$ and $\mathrm{ci}(f_S) = 3$.*

Proof. For each named family only its own Latin squares (of order 32) are built; pairwise orthogonality is decided on the $1\,024$ cells, the $1\,024$ rows are formed and sorted, and the order is decided through the column-parity route: every set of at most t of the n columns is tested for balance over the $1\,024$ rows, with $t = 6$ ruled out at (a) by an unbalanced 6-set, and similarly at the other orders. At (d) this is at most $\sum_{j=1}^{4} \binom{40}{j} = 102\,090$ parity masks over $1\,024$ rows. $\square$

Remark 5.2 (the full diameter-6 table; computed, not certified)*.* A C program following the same exhaustive procedure as at $d \leq 5$, with orders decided by column parities, gives, in 442 seconds for the pair scan and 14 seconds for the clique enumeration on one core (re-run for this paper; a second, independent C program deciding orders by a fast Walsh–Hadamard transform agrees with it on the $k = 3$ row, as recorded when the programs were written): 266 740 orthogonal pairs ($2 \cdot 266\,740/8 = 66\,685$, the $d = 6$ entry of Table 2 of [3], whose $d = 6$ search space took "approximately 22 hours" to enumerate "on a 64-bit Linux machine with 40 Intel Xeon cores" in 2017; $2 \cdot 266\,740 = 533\,480$ is the ordered count of [6]); 5 808 sets of 3-MOCA on $n = 15$ variables, of orders 3, 4, 5 in 4 576, 960, 272 cases ($726 = 572 + 120 + 34$ orbits); 6 160 sets of 4-MOCA of which 416 have order 4 and 5 744 order 3; 11 392, 13 504, 8 960, 2 560 sets of 5-, 6-, 7-, 8-MOCA, every one of order exactly 3; and no 9-MOCA. The minimum order over every family of every $k \geq 3$ at diameter 6 is 3. The five families of Theorem 5.1 are drawn from this table, and their orders were recomputed independently for this paper. The output listing every family with its order (SHA-256 `77b446a1dc26d42ca80df0fde39252852edf3c2e085ec04b5295c29333ba4b63`, 1 868 356 bytes) was regenerated for this paper and the orbit counts were recomputed from it. The largest family size 8 is the linear maximum N_5 of [4]; every one of the 10 orbits of 8-MOCA contains a family of linear rules, and every rule occurring in an 8-MOCA is affine. Their formula gives $N_6 = 13$ at $d = 7$, a value this method cannot test: 2^{32} rules and $\approx 9.2 \cdot 10^{18}$ candidate pairs.

Combining Theorems 3.3, 4.3, 4.4 with Remark 5.2: in every one of the $16 + 264 + 224 + 96 + 5\,808 + 6\,160 + 11\,392 + 13\,504 + 8\,960 + 2\,560 = 48\,984$ families with $k \geq 3$ and $d \leq 6$, the order is at least 3 (machine-checked for the 600 families with $d \leq 5$ and for the five named ones, computed for the rest). This is the strongest finite evidence now available for the strength-3 refinement the source asks for, and nothing more: the refinement is a statement for every d and is not reachable by enumeration.

6. The minimum-weight column

Remark 6.1 (a literature check; no formal counterpart)*.* The source describes the last column of its Table 1 as "the best known lower bound on the Hamming weight for the corresponding order of correlation immunity ($\mathrm{Min}(w_H)$), taken from [2]", where [2] is Carlet's book [14], and prints 24 both for $(n, t) = (12, 3)$ and for $(12, 4)$. For $(12, 4)$ this contradicts a published value: Kiss and Nagy [10] write "Let $\omega_{n,t}$ denote the minimum weight of t-CI Boolean functions in n variables" and prove $\omega_{11,4} = \omega_{12,4} = \omega_{13,4} = \omega_{14,4} = \omega_{15,4} = 128$ (Proposition 1, Eq. (3), in Section 2 of the journal version; the same statement is Proposition 3, Eq. (4), in Section 3 of arXiv:2011.09935v2). Consequently the source's sentence "For $n = 12$ variables the gap is even greater, since the weight of our functions is 256, while the lower bound is 24" is right for its order-3 row and wrong for its order-4 row, where the ratio is $256/128 = 2$, the smallest of the three. Separately, the entry 20 at $(9, 3)$ cannot be a minimum weight: the weight of a third-order correlation immune function is divisible by 8 (the index of the array is an integer), and the Rao bound for an $\mathrm{OA}(N, 9, 2, 3)$, $N \geq 1 + 9 + 8 = 18$ (Hedayat, Sloane and Stufken [16]), already excludes 16, so the least admissible weight is 24; a lower bound of 20 is a true statement, so this is not by itself an error, but the gap $64/20$ is really at most $64/24$.

We were not able to consult the relevant table of [14] — no full text was legally reachable — and make no claim about what that book prints. What can be checked is the literature it draws on. The Delsarte linear-programming lower bounds on the minimum weight $w_{n,t}$ of a t-th order correlation immune function of n variables are tabulated by Bhasin, Carlet and Guilley [15], Table 1: 20 at $(9, 3)$ and 24 at $(12, 3)$, the two values the source prints, and 112 at $(12, 4)$, where the source prints 24 again. Their Table 3, of exact minima, gives $w_{9,3} = 24$ and leaves $(12, 4)$ open — the cell Kiss and Nagy later filled with 128. So the printed 24 at $(12, 4)$ matches neither of those, and duplicates the row above it.

7. Controls

A census whose definitions are subtly wrong can pass every statement above and still show nothing; the following statements refute a too-large and a too-small claim, recover published values, and check that no hypothesis is vacuous.

Proposition 7.1 (controls)**.** (a) *The linear function $x_1 \oplus \cdots \oplus x_6$ (support: the* 32 *odd-weight vectors) has correlation immunity order exactly* 5 *by both evaluation routes; this is the extremal case $t = n - \deg f$ of Siegenthaler's inequality* [13]*.*

(b) *The indicator of a single point of $\mathbb{F}_2^4$ has order* 0 *by both routes.*

(c) *On the family $\{0, 3, 5\}$ of diameter* 4 *($n = 9$), the fast Walsh–Hadamard transform agrees in all* 512 *coefficients with the defining sum of the Walsh transform (Eq. (3) of* [1]*) written out over $\mathbb{F}_2^9$.*

(d) *Rule* 0 *of diameter* 4 *is orthogonal to exactly the rules* $3, 5, 10, 12$*; and rules* 0 *and* 3 *of diameter* 3 *are not orthogonal. So orthogonality is neither always true nor always false.*

(e) *The* 16 *rule indices of diameter* 4 *give* 16 *pairwise distinct Latin squares.*

(f) *The triple $\{0, 1, 2\}$ of diameter* 4 *is not pairwise orthogonal; its array still has* 64 *distinct rows, and the strength of that array is* 1 *— below the* 2 *of the source's Theorem 1, so the orthogonality hypothesis does work.*

(g) *Complementing the three rules of any family in $\mathcal{M}_3(4)$ gives a family in $\mathcal{M}_3(4)$ with the same order (the $d = 4$ instance of Lemma 2.1).*

(h) *"Every family in $\mathcal{M}_3(4)$ has order at least* 4*" is false, and "some family in $\mathcal{M}_3(4)$ has order at most* 2*" is false.*

8. Verification

Proposition 3.1, Theorems 3.2–4.4, Theorem 5.1 and Proposition 7.1 rest on 37 declarations checked in Lean 4 (version 4.32.0; apart from this project's own ledger-tagging attribute, which itself imports only `Lean`, the development imports nothing beyond Lean's core library — in particular no *Mathlib*), whose statements are reproduced verbatim in Appendix A. The development is six modules, 895 lines in all. The first (314 lines) defines, as executable functions on natural numbers and arrays, the rule $\varphi \mapsto f$ (`ruleBit`), the automaton and its Latin square (`caOut`, `square`), the Latin-square and orthogonality tests (`isLatin`, `orthSq`), the clique enumeration (`families`), the array and its function (`rowsOf`, `ttPM`), the fast Walsh–Hadamard transform and the order read off it (`walshSpectrum`, `ciOrderOf`, `ciListOf`), the column-parity route (`strengthOf`, `ciStrengthList`), the single-family variants used at $d = 6$ (`isMocaAt`, `ciStrengthAt`, `rowsDistinctAt`), and the textbook coefficient `walshSpec` used only in control (c). The other five modules state and decide the results: diameters 3 and 4 with the fidelity anchors (12 theorems, `moca_latin_squares`, `moca_fig1_labels`, `moca_d3_none`, `moca_d4_families`, `moca_d4_no_four`, `moca_d4_ci_three`, …); diameter 5 at $k = 3$ (6 theorems, `moca_d5_census`, `moca_d5_ci_split`, `moca_d5_ci_ge_three`, `moca_d5_ci_le_four`, `moca_agree_d45`, …); diameter 5 at $k \geq 4$ (4 theorems, `moca_d5_clique_ladder`, `moca_d5_high_ci_three`, …); the diameter-6 families (5 theorems, `moca_d6_ci_five`, …, `moca_d6_eight`); and the controls (10 theorems, `moca_control_*`, plus `moca_control_mfl2017_table2` for Proposition 3.1(c)). Every one of the 37 is proved by compiled evaluation of a decidable closed statement (`native_decide`), so each rests on the trust in Lean's compiler in addition to its kernel. The axiom print (`#print axioms`) of all 37, re-run read-only for this paper against the compiled modules, contains `propext` (36 declarations), `Quot.sound` (34) and one `native_decide` axiom per compiled evaluation (74 in all); there is no `sorry`, no `Classical.choice`, and no axiom declared by hand. As recorded when the development was written, the diameter-5, $k = 3$ module checks in about 200 seconds and the others in under a minute each, with a peak resident set of 1.56 GB; the whole development re-checks in under five minutes. Outside Lean, and labelled as such where they occur, are Lemma 2.1 (proved in the text), Remark 4.6, Remark 5.2 and Remark 6.1. For this paper the census for $d \leq 5$ and every k — Latin squares, orthogonal pairs, cliques, the explicit list of Theorem 3.2(b), row distinctness, orders by both routes, complementation orbits — was re-implemented from the definitions in Python and agrees with every number stated; the five families of Theorem 5.1 were re-checked the same way; and the diameter-6 program was re-run and its output re-analysed as described in Remark 5.2. The development is currently in a private repository: repository reference to be added at submission.

Appendix A. The formal statements

The Lean statements pinned to the results above, verbatim (statements only; proofs, docstrings and attributes omitted; the namespace `MocaCiOrder` omitted). `families d k` enumerates $\mathcal{M}_k(d)$ as increasing lists of rule indices; `squares d` is the array of all Latin squares of diameter `d`; `sq5`, `sqH5` are two copies of `squares 5`; `fam53`, `fam54`, `fam55` are $\mathcal{M}_3(5)$, $\mathcal{M}_4(5)$, $\mathcal{M}_5(5)$; `fam53norm` the 33 representatives; `ci53` the orders of `fam53` by the Walsh route; `numRules d` is $2^{2^{d-2}}$; `#[...]` is an array literal and `[...]` a list.

Definition fidelity (Proposition 3.1).

```
theorem moca_latin_squares :
    (squares 3).all (isLatin 2) = true ∧
    (squares 4).all (isLatin 3) = true ∧
    (squares 5).all (isLatin 4) = true

theorem moca_fig1_rules_90_150_orthogonal :
    orthSq 2 (square 3 0) (square 3 2) = true

theorem moca_fig1_labels :
    ([0, 4, 2, 6, 1, 5, 3, 7].map (fun w => (ruleBit 3 0 w, ruleBit 3 2 w)))
      = [(0,0), (1,1), (0,1), (1,0), (1,1), (0,0), (1,0), (0,1)]

theorem moca_control_mfl2017_table2 :
    2 * (families 3 2).size / 8 = 1 ∧
    2 * (families 4 2).size / 8 = 9 ∧
    2 * (families 5 2).size / 8 = 213
```

Diameters 3 and 4 (Theorems 3.2 and 3.3).

```
theorem moca_d3_none :
    (families 3 2).size = 4 ∧ families 3 3 = #[]

theorem moca_d4_pairs_36 :
    numRules 4 = 16 ∧ (families 4 2).size = 36

theorem moca_d4_families :
    families 4 3 =
      #[[0, 3, 5], [0, 3, 10], [0, 5, 12], [0, 10, 12],
        [3, 5, 6], [3, 5, 9], [3, 5, 15], [3, 6, 10], [3, 9, 10], [3, 10, 15],
        [5, 6, 12], [5, 9, 12], [5, 12, 15],
        [6, 10, 12], [9, 10, 12], [10, 12, 15]]

theorem moca_d4_count : (families 4 3).size = 16

theorem moca_d4_norm_two :
    ((families 4 3).filter (fun fam => fam.all (fun p => p % 2 == 0)))
      = #[[0, 10, 12], [6, 10, 12]]

theorem moca_d4_no_four : families 4 4 = #[]

theorem moca_d4_weight_64 :
    (families 4 3).all (fun fam => rowsDistinct 4 (squares 4) fam) = true ∧
    (families 4 3).all (fun fam => weightOf 4 (squares 4) fam == 64) = true

theorem moca_d4_ci_three :
```

```
    ciListOf 4 (squares 4) (families 4 3) = Array.replicate 16 3

theorem moca_d4_ci_bounds :
    (ciListOf 4 (squares 4) (families 4 3)).all (fun t => 3 ≤ t) = true ∧
    (ciListOf 4 (squares 4) (families 4 3)).all (fun t => t ≤ 3) = true
```

Diameter 5 (Theorems 4.1–4.4).

```
def sq5 : Array (Array Nat) := squares 5
def fam53 : Array (List Nat) := familiesOf 5 3 sq5
def ci53 : Array Nat := ciListOf 5 sq5 fam53
def fam53norm : Array (List Nat) := fam53.filter (fun fam => fam.all (fun p => p % 2 == 0))

theorem moca_d5_census :
    numRules 5 = 256 ∧
    (familiesOf 5 2 sq5).size = 852 ∧
    fam53.size = 264 ∧
    fam53norm.size = 33

theorem moca_d5_weight_256 :
    fam53.all (fun fam => rowsDistinct 5 sq5 fam) = true ∧
    fam53.all (fun fam => weightOf 5 sq5 fam == 256) = true

theorem moca_d5_ci_split :
    (ci53.filter (fun t => t == 3)).size = 192 ∧
    (ci53.filter (fun t => t == 4)).size = 72 ∧
    ci53.all (fun t => t == 3 || t == 4) = true ∧
    ((ciListOf 5 sq5 fam53norm).filter (fun t => t == 3)).size = 24 ∧
    ((ciListOf 5 sq5 fam53norm).filter (fun t => t == 4)).size = 9

theorem moca_d5_ci_ge_three : ci53.all (fun t => 3 ≤ t) = true

theorem moca_d5_ci_le_four :
    ci53.all (fun t => t ≤ 4) = true ∧ ci53.contains 4 = true ∧ ci53.contains 3 = true

theorem moca_agree_d45 :
    ciStrengthList 4 (squares 4) (families 4 3) = ciListOf 4 (squares 4) (families 4 3) ∧
    ciStrengthList 5 sq5 fam53 = ci53

def sqH5 : Array (Array Nat) := squares 5
def fam54 : Array (List Nat) := familiesOf 5 4 sqH5
def fam55 : Array (List Nat) := familiesOf 5 5 sqH5

theorem moca_d5_clique_ladder :
    fam54.size = 224 ∧ fam55.size = 96 ∧ familiesOf 5 6 sqH5 = #[]

theorem moca_d5_high_weight :
    fam54.all (fun fam => rowsDistinct 5 sqH5 fam) = true ∧
    fam55.all (fun fam => rowsDistinct 5 sqH5 fam) = true

theorem moca_d5_high_ci_three :
    ciStrengthList 5 sqH5 fam54 = Array.replicate 224 3 ∧
    ciStrengthList 5 sqH5 fam55 = Array.replicate 96 3
```

```
theorem moca_d5_k2_constant :
    (familiesOf 5 2 sqH5).all (fun fam => rowsDistinct 5 sqH5 fam) = true ∧
    ciStrengthOf 5 sqH5 (familiesOf 5 2 sqH5)[0]! = 8
```

Diameter 6 (Theorem 5.1).

```
theorem moca_d6_ci_five :
    isMocaAt 6 [0, 255, 15555] = true ∧
    rowsDistinctAt 6 [0, 255, 15555] = true ∧
    ciStrengthAt 6 [0, 255, 15555] = 5

theorem moca_d6_ci_four :
    isMocaAt 6 [0, 255, 23205] = true ∧ ciStrengthAt 6 [0, 255, 23205] = 4

theorem moca_d6_ci_three :
    isMocaAt 6 [0, 255, 3855] = true ∧ ciStrengthAt 6 [0, 255, 3855] = 3

theorem moca_d6_k4_ci_four :
    isMocaAt 6 [0, 3855, 15555, 23205] = true ∧
    ciStrengthAt 6 [0, 3855, 15555, 23205] = 4

theorem moca_d6_eight :
    isMocaAt 6 [0, 255, 3855, 13107, 15555, 23205, 26265, 26985] = true ∧
    rowsDistinctAt 6 [0, 255, 3855, 13107, 15555, 23205, 26265, 26985] = true ∧
    ciStrengthAt 6 [0, 255, 3855, 13107, 15555, 23205, 26265, 26985] = 3
```

Controls (Proposition 7.1).

```
def oddRows (n : Nat) : Array Nat :=
  (Array.range (2 ^ n)).filter (fun x => wtBits n x % 2 == 1)

theorem moca_control_linear_order :
    (oddRows 6).size = 32 ∧
    strengthOf 6 (oddRows 6) = 5 ∧
    ciOrderOf 6 (walshSpectrum 6 (ttPM 6 (oddRows 6))) = 5

theorem moca_control_point_not_immune :
    strengthOf 4 #[0] = 0 ∧ ciOrderOf 4 (walshSpectrum 4 (ttPM 4 #[0])) = 0

theorem moca_control_walsh_spec :
    (let rows := rowsAt 4 [0, 3, 5]
     let W := walshSpectrum 9 (ttPM 9 rows)
     (List.range 512).all (fun a => W[a]! == walshSpec 9 rows a)) = true

theorem moca_control_orth_nontrivial :
    ((Array.range 16).filter (fun j => orthSq 3 (square 4 0) (square 4 j)))
      = #[3, 5, 10, 12] ∧
    orthSq 2 (square 3 0) (square 3 3) = false

theorem moca_control_squares_distinct :
    ((List.range 16).all (fun i =>
      (List.range 16).all (fun j => i == j || square 4 i != square 4 j))) = true

theorem moca_control_non_moca :
```

```
    isMocaAt 4 [0, 1, 2] = false ∧
    rowsDistinctAt 4 [0, 1, 2] = true ∧
    ciStrengthAt 4 [0, 1, 2] = 1

def complementFam (d : Nat) (fam : List Nat) : List Nat :=
  ((fam.map (fun p => p ^^^ (numRules d - 1))).toArray.qsort (· < ·)).toList

theorem moca_control_complement :
    ((families 4 3).all (fun fam =>
      (families 4 3).contains (complementFam 4 fam) &&
      ciStrengthAt 4 (complementFam 4 fam) == ciStrengthAt 4 fam)) = true

theorem moca_control_not_four :
    (ciListOf 4 (squares 4) (families 4 3)).all (fun t => 4 ≤ t) = false

theorem moca_control_not_two :
    (ciListOf 4 (squares 4) (families 4 3)).any (fun t => t ≤ 2) = false
```

References

[1] L. Mariot and L. Manzoni, *Building correlation immune functions from sets of mutually orthogonal cellular automata*, arXiv:2207.08280v1 [cs.CR], 17 July 2022. Version 1 is the only version as of 2026-09-07, and the arXiv record carries no journal reference. Read in full from the PDF compiled here with `tectonic` from the arXiv e-print; statement, figure, table and equation numbers are those resolved in its `.aux`: Lemma 1 (the orthogonal-array characterisation), Definition 1 (the automaton), Eqs. (3), (5), (6), (7) (Walsh transform, automaton, orthogonality, the array A), Lemma 2, Lemma 3, Theorem 1, Figure 1, Table 1, Sections 2.1, 2.2, 4 and 5; all quotations are verbatim from that PDF.

[2] L. Mariot and L. Manzoni, *Building correlation immune functions from sets of mutually orthogonal cellular automata*, in: Cellular Automata and Discrete Complex Systems (AUTOMATA 2023), Lecture Notes in Computer Science **14152**, Springer, Cham, 2023, pp. 153–164. Bibliographic data checked against Crossref (doi:10.1007/978-3-031-42250-8_11); the publisher's PDF was read in full. Its Lemmas 1–3 and Theorem 1 carry the same numbers as in [1]; the array A is its Eq. (5), and it adds a Remark 1 (a shorter proof of Lemma 3). Its Table 1 differs from the arXiv table in the two places recorded in Section 1; its reference [15] is [3] and its reference [2] is [14].

[3] L. Mariot, E. Formenti and A. Leporati, *Enumerating orthogonal Latin squares generated by bipermutive cellular automata*, in: Cellular Automata and Discrete Complex Systems (AUTOMATA 2017), Lecture Notes in Computer Science **10248**, Springer, Cham, 2017, pp. 151–164. Bibliographic data checked against Crossref (doi:10.1007/978-3-319-58631-1_12). Read from the authors' postprint (`lucamariot.org/files/papers/mfl_automata_2017_postprint.pdf`, 13 pages, carrying Springer's notice "The final publication is available at Springer via http://dx.doi.org/10.1007/978-3-319-58631-1_12"): Lemma 2 (reversal and complementation preserve orthogonality), Table 2 (the pair counts $1, 9, 213, 66\,685$, captioned "Distribution of CA-based orthogonal Latin squares up to $n = 6$"), the "divided by 8" sentence in the text discussing that table, and the "approximately 22 hours" remark are quoted from that postprint. The published LNCS text was not reachable, so the lemma and table numbers used here are the postprint's and the published numbering is not verified.

[4] L. Mariot, M. Gadouleau, E. Formenti and A. Leporati, *Mutually orthogonal Latin squares based on cellular automata*, Designs, Codes and Cryptography **88** (2020), no. 2, 391–411. Bibliographic data checked against Crossref (doi:10.1007/s10623-019-00689-8); also arXiv:1906.08249. Read from the arXiv PDF (the accepted preprint): Problem 1 and Theorem 3 with its Eq. (48), $N_n = I_n + \sum_{k=1}^{\lfloor n/2 \rfloor} I_k$, giving $N_3, N_4, N_5, N_6 = 3, 5, 8, 13$ for $q = 2$, are cited with the numbering resolved from that e-print's own `.aux` file (`problem.1`, `theorem.3`, `equation.5.48`); its v2 is dated 31 October 2019, two days after the online publication date Crossref records for the journal version. The journal version itself was not reachable, so its internal numbering is not verified. The pair count $(4^{n-1} - 1)/3$ ("a shifted version of OEIS sequence A002450") is also there.

[5] L. Manzoni, L. Mariot and G. Menara, *Combinatorial designs and cellular automata: A survey*, Discrete Applied Mathematics **379** (2026), 656–674. Bibliographic data checked against Crossref (doi:10.1016/j.dam.2025.10.014); also arXiv:2503.10320. The quotation in Section 1 is from the e-print.

[6] L. Mariot, *Hip to be (Latin) square: Maximal period sequences from orthogonal cellular automata*, in: 2021 Ninth International Symposium on Computing and Networking (CANDAR), IEEE, 2021, pp. 29–37. Bibliographic data checked against Crossref (doi:10.1109/candar53791.2021.00012); also arXiv:2106.07750. Its table of search-space sizes lists $0, 8, 72, 1\,704, 533\,480$ ordered orthogonal pairs for $d = 2, \ldots, 6$, stated there to be 8 times the counts of [3]; read from the e-print.

[7] L. Mariot, F. Mazzone, L. Manzoni and A. Leporati, *How to reconstruct (anonymously) a secret cellular automaton*, arXiv:2604.11362v1 [cs.CR], 13 April 2026. Its closing paragraph states, verbatim: "while the construction for maximal MOCA families exhibited in […] based on linear CA is the best known so far, it is not known whether one can construct even larger families of MOCA with nonlinear CA." Read from the e-print.

[8] A. Dennunzio, M. Gadouleau and L. Mariot, *On the transversals of Latin squares generated by nonlinear bipermutive cellular automata*, arXiv:2605.18875, 2026. One of the two citers of [1] listed by Semantic Scholar; read from the e-print, which computes no correlation immunity orders.

[9] T. Prévost and B. Martin, *Testing a cellular automata construction method to obtain 9-variable cryptographic Boolean functions*, Journal of Cellular Automata **18** (2024), no. 2–3, 187–205; also arXiv:2501.09380. The arXiv journal-reference field gives only "Journal of Cellular Automata, 2024, 18 (2/3), pp.19" together with doi:10.32908/jca.v18.100924, a DOI Crossref does not resolve; the page range above is from the publisher's table of contents for that issue and from the second author's own publication list, which agree, and is consistent with the 19 pages of the arXiv field. Read from the e-print; cited as the nearest neighbour found by the full-text search.

[10] R. Kiss and G. P. Nagy, *On the nonexistence of certain orthogonal arrays of strength four*, Prikladnaya Diskretnaya Matematika (2021), no. 52, 65–68. Bibliographic data checked against Crossref (doi:10.17223/20710410/52/3) and against the journal's own record; also arXiv:2011.09935v2 [math.CO], 14 December 2020. Both versions were read, the journal PDF from `mathnet.ru` and the arXiv e-print. They number the result differently, so Remark 6.1 cites it both ways: in the journal version it is Proposition 1, Eq. (3), in Section 2, "Minimum weight of correlation-immune Boolean functions"; in arXiv v2 it is Proposition 3, Eq. (4), in Section 3 of the same title. The sentence defining $\omega_{n,t}$ and the displayed equality are word for word the same in both.

[11] P. Camion, C. Carlet, P. Charpin and N. Sendrier, *On correlation-immune functions*, in: Advances in Cryptology — CRYPTO '91, Lecture Notes in Computer Science **576**, Springer, Berlin, 1992, pp. 86–100. Bibliographic data checked against Crossref (doi:10.1007/3-540-46766-1_6). Cited, as the source does, for the orthogonal-array characterisation of correlation immunity; not read for this work.

[12] G.-Z. Xiao and J. L. Massey, *A spectral characterization of correlation-immune combining functions*, IEEE Transactions on Information Theory **34** (1988), no. 3, 569–571. Bibliographic data checked against Crossref (doi:10.1109/18.6037); not read for this work.

[13] T. Siegenthaler, *Correlation-immunity of nonlinear combining functions for cryptographic applications*, IEEE Transactions on Information Theory **30** (1984), no. 5, 776–780. Bibliographic data checked against Crossref (doi:10.1109/TIT.1984.1056949); not read for this work.

[14] C. Carlet, *Boolean Functions for Cryptography and Coding Theory*, Cambridge University Press, Cambridge, 2021. Bibliographic data checked against Crossref (doi:10.1017/9781108606806, which records the online publication date as 31 October 2020). The source's reference for its minimum-weight column; not consulted for this work, no full text being legally reachable (Remark 6.1).

[15] S. Bhasin, C. Carlet and S. Guilley, *Theory of masking with codewords in hardware: low-weight dth-order correlation-immune Boolean functions*, IACR Cryptology ePrint Archive, Report 2013/303; published, under the title *Correlation-immune Boolean functions for easing counter measures to side-channel attacks*, as Chapter 3 of Algebraic Curves and Finite Fields, Radon Series on Computational and Applied Mathematics **16**, De Gruyter, Berlin, 2014, pp. 41–70 (that attribution is the one given in the reference list of [10]). The e-print was read (`eprint.iacr.org/2013/303.pdf`, 37 pages, title page dated 23 January 2014); its Table 1 ("Lower bounds on $w_{n,d}$ obtained by the Delsarte LP algorithm") and Table 3 ("Minimal value $w_{n,d}$ of the cardinal of $supp(f)$, where $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ is d-CI") are the two tables read in Remark 6.1; the table numbers are the e-print's and the published chapter was not consulted.

[16] A. S. Hedayat, N. J. A. Sloane and J. Stufken, *Orthogonal Arrays: Theory and Applications*, Springer Series in Statistics, Springer, New York, 1999. Bibliographic data checked against Crossref (doi:10.1007/978-1-4612-1478-6). Cited, as the source does, for orthogonal arrays, the integrality of the index and the Rao bound; not read for this work.

[17] L. de Moura and S. Ullrich, *The Lean 4 theorem prover and programming language*, in: Automated Deduction — CADE 28, Lecture Notes in Computer Science **12699**, Springer, 2021, pp. 625–635. Bibliographic data checked against Crossref (doi:10.1007/978-3-030-79876-5_37).