A COUNTING FORMULA FOR LINEAR SELF-ORTHOGONAL CELLULAR AUTOMATA

KOREA SUPERINTELLIGENCE LABS

Abstract. A bipermutive local rule of diameter d over $\mathbb{F}_2$ generates, through its no-boundary cellular automaton, a Latin square of order 2^{d-1}; Mariot and Mazzone call the automaton *self-orthogonal* when that square is orthogonal to its transpose. They determined the number $\mathrm{LIN}(d)$ of linear self-orthogonal cellular automata for $3 \le d \le 16$, observed that the values follow 2^{d-3} until they stop doing so at $d = 7$, reported that the sequence is not indexed in the OEIS, and asked for a counting formula. We give one. We show that $\mathrm{LIN}(d)$ is the number of invertible circulant matrices of order $d-1$ over $\mathbb{F}_2$ with zero diagonal, and that

$$\mathrm{LIN}(d) \;=\; \tfrac{1}{2}\big(\Psi(d-1) + \mu(X^{d-1}-1)\big),$$

where $\Psi(n)$ is the number of invertible circulants of order n over $\mathbb{F}_2$ (OEIS A003473) and μ is the Möbius function of $\mathbb{F}_2[X]$, so that $\mu(X^n-1)$ is 0 for even n and $(-1)^{r(n)}$ for odd n, with $r(n)$ the number of distinct irreducible factors of X^n-1. Both halves of the identity are proved, together with the classical product formula for Ψ. The closed form reproduces all fourteen published values and extends them to $d = 30$; it also settles the shape of the data exactly, in that $\mathrm{LIN}(d) = 2^{d-3}$ holds precisely when $d-1$ is a power of two or an odd prime having 2 as a primitive root, the first failure being $d = 7$. All statements below are machine-checked in Lean 4, with one explicitly labelled exception.

1. Introduction

Let $\mathbb{F}_2 = \{0,1\}$ and let $f\colon \mathbb{F}_2^d \to \mathbb{F}_2$ be a local rule of *diameter* d. The associated *no-boundary* cellular automaton applies f at every position with enough room, so on $2(d-1)$ cells it is a map $F\colon \mathbb{F}_2^{2(d-1)} \to \mathbb{F}_2^{d-1}$. Reading the two halves of the input as the row and column index of a table of order $N = 2^{d-1}$ turns F into a square array; the rule f is *bipermutive* when it is permutive in its first and in its last coordinate, and then the array is a Latin square. Mariot and Mazzone [1] single out the squares that are orthogonal to their own transpose and call the corresponding automata *self-orthogonal*. Their paper computes, by exhaustive search over all $2^{2^{d-2}}$ bipermutive rules, the number $\mathrm{SOCA}(d)$ of self-orthogonal cellular automata of diameter d for $d \le 6$, proves an algebraic characterisation of self-orthogonality in the linear case, and uses it to tabulate the number $\mathrm{LIN}(d)$ of *linear* self-orthogonal cellular automata for $3 \le d \le 16$:

$$1,\ 2,\ 4,\ 8,\ 12,\ 24,\ 64,\ 94,\ 240,\ 512,\ 768,\ 2048,\ 3136,\ 5062. \tag{1}$$

It closes with two open problems, quoted verbatim from its §5: “the most evident open problem is to determine a counting formula for the number of linear self-orthogonal CA in the general case, which from our experiments seems to follow the sequence of the powers of 2. Further, it would be interesting to assess, even experimentally, if *nonlinear* self-orthogonal CA exist.” Of the first the authors add that “the sequence does not seem to be already known in the Online Encyclopedia of Integer Sequences (OEIS)”.

This paper answers the first question. The route is a change of object. Write $n = d-1$ and $R_n = \mathbb{F}_2[X]/(X^n-1)$. The characterisation of [1] says that a linear bipermutive rule with associated polynomial p_f is self-orthogonal exactly when $\gcd(p_f, X^n+1) = 1$; bipermutivity forces the constant and leading coefficients of p_f to be 1, and reducing p_f modulo X^n-1 therefore identifies the linear

bipermutive rules of diameter d with the elements of R_n whose constant coefficient vanishes, self-orthogonality becoming invertibility. Under the standard identification of R_n with the algebra of circulant matrices of order n over $\mathbb{F}_2$, this reads:

> $\mathrm{LIN}(d)$ is the number of invertible circulant matrices of order $d-1$ over $\mathbb{F}_2$ whose diagonal is zero.

The unrestricted count $\Psi(n) = |R_n^\times|$ is a classical quantity, OEIS A003473, whose own comments already record both readings ("the number of $n \times n$ circulant invertible matrices over $GF(2)$" and "the number of units in the ring $F_2[x]/\langle x^n - 1\rangle$"). The whole content of the counting problem is therefore the cost of the single linear condition $u_0 = 0$, and that cost is exactly one Möbius sign:

$$2\,\mathrm{LIN}(n+1) \;=\; \Psi(n) + \mu(X^n - 1), \qquad \mu(X^n-1) = \begin{cases} 0, & n \text{ even}, \\ (-1)^{r(n)}, & n \text{ odd}, \end{cases} \tag{2}$$

with $r(n)$ the number of distinct irreducible factors of $X^n - 1$ over $\mathbb{F}_2$ (OEIS A000374). Theorems 4.1, 4.3 and 5.1 below prove (2) and assemble it into a closed form. This also explains why the search of [1] in the OEIS returned nothing: the sequence (1) is not indexed, but both of its ingredients are, and the paper searched for the answer rather than for its ingredients.

Two consequences are worth stating separately. First, the guess in the quotation above is correct infinitely often and wrong infinitely often, and one can say exactly where: $\mathrm{LIN}(d) = 2^{d-3}$ holds precisely when $d-1$ is a power of two — which is the case $d = 2^t + 1$ that [1] proves — or an odd prime having 2 as a primitive root (Theorem 5.3). The first failure is $d = 7$, which is the break the authors observe in their own table. Second, the closed form is a closed form, so it does not stop at $d = 16$; Table 1 carries it to $d = 30$.

The second open problem of [1] is not settled here. What the results below contribute to it is the complete picture at the two diameters adjacent to the frontier: every self-orthogonal cellular automaton of diameter at most 6 is affine (Proposition 6.2), and at $d = 7$ there are exactly 24 affine and 12 linear ones, listed in Proposition 6.3. Section 6.1 reports, as a computation and not as a theorem, an exhaustive search over all 2^{32} bipermutive rules of diameter 7 that finds no self-orthogonal rule outside that affine list.

Organisation. Section 2 fixes the objects and records the facts about them that we use. Section 3 turns the criterion of [1] into a statement about units of R_n. Section 4 proves the counting formula, in three pieces: the even case, the odd case, and the classical value of Ψ. Section 5 assembles the closed form, tabulates it, and characterises the powers of two. Section 6 gives the exhaustive picture at $d \le 7$. Section 7 collects the sharpness statements that keep the preceding sections honest, and Section 8 describes the formal verification.

2. Preliminaries

2.1. **Bipermutive rules and their Latin squares.** Throughout, $d \ge 3$ is the diameter, $n = d-1$, and $N = 2^n = 2^{d-1}$.

Definition 2.1. A local rule $f\colon \mathbb{F}_2^d \to \mathbb{F}_2$ is *permutive* in its i-th coordinate if fixing all other coordinates leaves a permutation of $\mathbb{F}_2$; over $\mathbb{F}_2$ this says $f(x_1,\dots,x_d) = x_i \oplus g(x_1,\dots,\widehat{x_i},\dots,x_d)$ for some g. It is *bipermutive* if it is permutive in the first and in the last coordinate, so that

$$f(x_1,\dots,x_d) \;=\; x_1 \oplus x_d \oplus g(x_2,\dots,x_{d-1}), \qquad g\colon \mathbb{F}_2^{d-2} \to \mathbb{F}_2 \text{ arbitrary}. \tag{3}$$

We call g the *generating function* of f. There are exactly $2^{2^{d-2}}$ bipermutive rules of diameter d, one for each g.

The *no-boundary cellular automaton* of f on $2(d-1)$ cells is $F\colon \mathbb{F}_2^{2n} \to \mathbb{F}_2^n$, whose i-th output cell is f applied to the input cells $i,\dots,i+d-1$. Writing an input as the concatenation $x\|y$ of two

words of length n and reading words of length n as integers in $[0, N)$ through the monotone bijection "the cells are the binary digits", we obtain the square array

$$L(x, y) \;=\; F(x\|y), \qquad x, y \in \mathbb{F}_2^n,$$

of order $N = 2^n$: the Cayley table of [1, Definition 4].

Proposition 2.2 ([1, Lemma 1])**.** *For every diameter d and every generating function g, every row and every column of L is a permutation of $\mathbb{F}_2^n$. In particular L is a Latin square of order $N = 2^{d-1}$.*

Proof sketch. Bipermutivity buys a triangular solve. Fix x and read y off the output from the bottom cell up: output cell k is $x_k \oplus y_k \oplus g(z_{k+1}, \ldots, z_{k+d-2})$, and the window $k+1, \ldots, k+d-2$ meets the right half of $x\|y$ only in $y_0, \ldots, y_{k-1}$. So y_k is determined by the output and by the cells of y below it, and strong induction on k gives injectivity of $y \mapsto L(x, y)$; a finite injection is a bijection. Columns are the same argument read from the top cell down, the window of cell k meeting the left half only in $x_{k+1}, \ldots, x_{n-1}$, so the induction is on $n - 1 - k$. Neither direction uses the shape of g, and neither enumerates anything. □

The lemma is not new — [1] notes that it "has been independently rediscovered in multiple works under different guises" — and is recorded here because everything below is a statement about the square it produces.

2.2. **Self-orthogonality.** Two Latin squares of order N are *orthogonal* when superposing them produces each of the N^2 ordered pairs of symbols exactly once.

Definition 2.3 ([1, Definition 6])**.** The automaton F, equivalently the rule f, equivalently the generating function g, is *self-orthogonal* when L is orthogonal to its transpose; by [1, Lemma 3] this holds if and only if the *superposition*

$$H(x, y) \;=\; \big(L(x, y),\, L(y, x)\big)$$

is a bijection of $\mathbb{F}_2^n \times \mathbb{F}_2^n$.

We write $\mathrm{SOCA}(d)$ for the number of self-orthogonal bipermutive rules of diameter d. A rule (3) is *linear* when g is linear and *affine* when g is linear plus a constant; $\mathrm{LIN}(d)$ and $\mathrm{AFF}(d)$ count the self-orthogonal ones among these. There are 2^{d-2} linear and 2^{d-1} affine bipermutive rules of diameter d, and since complementing g complements every output cell of F, hence composes H with a bijection, self-orthogonality is invariant under $g \mapsto g \oplus 1$ and $\mathrm{AFF}(d) = 2\mathrm{LIN}(d)$. This is the factor of two between the two tables of [1], whose §3 counts affine rules and whose §4 counts polynomials; the paper says as much ("the constant term in the ANF of the complemented local rule is simply neglected") without flagging that the two columns therefore count different things.

One structural consequence of Definition 2.3 is used as a filter later and is worth isolating.

Proposition 2.4. *Let g be self-orthogonal of diameter d. Then the main diagonal of L is a transversal, i.e. $x \mapsto L(x, x)$ is injective. Moreover, for every x and every cell index i, the i-th cell of $L(x, x)$ is g evaluated on the cyclic window of x starting at $i + 1$; that is, the diagonal map is the periodic-boundary cellular automaton of g on $d - 1$ cells.*

Proof. H maps the N diagonal inputs (x, x) to diagonal outputs, and there are exactly N of those, so an injective H must be injective on the diagonal; injectivity of $(x, x) \mapsto (L(x, x), L(x, x))$ is injectivity of $x \mapsto L(x, x)$. For the second statement, on the input $x\|x$ the two permutive cells of output cell i — the cells i and $i + d - 1$ of $x\|x$ — are the same cell of x, so they cancel, and what is left is g applied to the $d - 2$ cells between them, read cyclically. □

The conjunction of the two halves of Proposition 2.4 is Theorem 1 of Dennunzio, Gadouleau and Mariot [2], which states that the main diagonal of the square of a bipermutive rule is a transversal if and only if its generating function induces an invertible periodic-boundary automaton on $d - 1$ cells. We use only the direction above, and only as a computational filter.

2.3. **Two encoding checks.**

Example 2.5. At $d = 3$ the generating function has one variable and there are four bipermutive rules. For $g = \mathrm{id}$ — Wolfram's rule 150 — the square of order 4 is

$$\begin{pmatrix} 1 & 4 & 3 & 2 \\ 2 & 3 & 4 & 1 \\ 4 & 1 & 2 & 3 \\ 3 & 2 & 1 & 4 \end{pmatrix},$$

which is self-orthogonal, while $g = 0$ — rule 90 — gives a square equal to its own transpose, hence certainly not orthogonal to it. These are Figures 3 and 4 of [1], and reproducing them cell for cell is how we check that the conventions used here (φ, the window, the concatenation order) are those of the source.

Proposition 2.6. *Bipermutivity in Proposition 2.2 is not decoration. Of the* 256 *local rules of diameter* 3*, exactly* 4 *generate a Latin square, and they are precisely the* 4 *bipermutive ones; the non-bipermutive rule* $f(x_1, x_2, x_3) = x_2$ *has table* $\left(\begin{smallmatrix} 0 & 2 & 0 & 2 \\ 0 & 2 & 0 & 2 \\ 1 & 3 & 1 & 3 \\ 1 & 3 & 1 & 3 \end{smallmatrix}\right)$*, and* $f = 0$ *and* $f = x_1 x_3$ *fail as well. Conversely, being Latin is strictly weaker than being self-orthogonal:* $g = 0$ *gives a Latin square that is not self-orthogonal, both at* $d = 3$ *and at* $d = 6$*. Finally* $\mathrm{SOCA}(5) \neq 7$ *and* $\mathrm{SOCA}(5) \neq 9$*.*

3. The criterion, and the set it counts

Identify a word $z \in \mathbb{F}_2^k$ with the polynomial $\sum_j z_j T^j$. A linear bipermutive rule of diameter d has *associated polynomial*

$$p_f(X) \;=\; a_1 + a_2 X + \cdots + a_d X^{d-1}, \qquad a_1 = a_d = 1,$$

the middle coefficients $a_2, \ldots, a_{d-1}$ being the coefficients of the linear generating function; so there are $2^{d-2} = 2^{n-1}$ of them.

Theorem 3.1 ([1, Theorem 2 and Corollary 1])**.** *A linear bipermutive cellular automaton of diameter* d *is self-orthogonal if and only if* $\gcd\big(p_f(X),\, X^n + 1\big) = 1$*, where* $n = d - 1$*.*

The proof in [1] goes through the Sylvester matrix of a stacked transition matrix. The following shorter derivation is recorded because it is what makes the shape of the counted set visible; it reproves a published result and claims nothing new. Let q be the reciprocal of p_f — same shape, and the criterion is unchanged by reciprocation because $X^n + 1$ is self-reciprocal. For $z = x \| y$ one has $z(T) = x(T) + T^n y(T)$, and output cell i of the no-boundary automaton is $\sum_j a_j z_{i+j} = [T^{n+i}](z\,q)$, so $L(x, y)$ is the middle block of zq. Put $u = xq$ and $v = yq$, each of degree $< 2n$, and split each into a low and a high half of length n. Then $L(x, y) = 0$ says $u_{\mathrm{hi}} = v_{\mathrm{lo}}$ and $L(y, x) = 0$ says $v_{\mathrm{hi}} = u_{\mathrm{lo}}$, so together $v \equiv T^n u \pmod{T^{2n} + 1}$, i.e. with $w = y + T^n x$,

$$(x, y) \in \ker H \iff (T^{2n} + 1) \;\big|\; q\, w.$$

As (x, y) runs over all pairs, w runs bijectively over the polynomials of degree $< 2n$, and H is $\mathbb{F}_2$-linear, so H is injective exactly when $w = 0$ is the only solution. If $h = \gcd(q, (T^n + 1)^2)$ has positive degree then $w = (T^n + 1)^2/h$ is a nonzero witness of degree $\leq 2n - 1$; if $h = 1$ then $(T^n + 1)^2 \mid w$ forces $w = 0$. Hence F is self-orthogonal iff $\gcd(q, (T^n + 1)^2) = 1$ iff $\gcd(q, T^n + 1) = 1$, which is Theorem 3.1.

Write $R_n = \mathbb{F}_2[X]/(X^n - 1)$, let u_0 denote the constant coefficient of $u \in R_n$ (well defined, since we represent elements of R_n by polynomials of degree $< n$), and set

$$\Psi(n) = \big|R_n^\times\big|, \qquad A(n) = \big|\{u \in R_n^\times : u_0 = 0\}\big|.$$

Proposition 3.2. *Reduction modulo* $X^n - 1$ *is a bijection from the set of associated polynomials of the linear bipermutive rules of diameter* $d = n + 1$ *onto* $\{u \in R_n : u_0 = 0\}$*, with inverse* $u \mapsto u + (X^n - 1)$*. Concretely,* $p_f = u + (X^n - 1)$ *has constant term* 1*, coefficient* 1 *at* X^n *and*

arbitrary middle coefficients exactly when $u_0 = 0$; the set of such u has $2^{n-1} = 2^{d-2}$ elements; and $\gcd(p_f, X^n - 1) = 1$ if and only if u is a unit of R_n.

Proof. Over $\mathbb{F}_2$ we have $X^n - 1 = X^n + 1$, whose constant coefficient is 1 and whose middle coefficients vanish, so adding it to u turns $u_0 = 0$ into $(p_f)_0 = 1$, installs the leading coefficient at X^n, and leaves the coefficients of $X, \dots, X^{n-1}$ untouched; adding $X^n - 1$ a second time returns u, so the two maps are mutually inverse. That the u with $u_0 = 0$ number 2^{n-1} is the statement that exactly half of the 2^n coefficient vectors of length n have vanishing first entry, which follows from the fixed-point-free involution $u \mapsto u + 1$. Finally $p_f = u + (X^n - 1) \cdot 1$, so p_f and u generate the same ideal together with $X^n - 1$, and coprimality to $X^n - 1$ transfers. □

Corollary 3.3. $\mathrm{LIN}(d) = A(d-1)$*: the number of linear self-orthogonal cellular automata of diameter d is the number of units of $\mathbb{F}_2[X]/(X^{d-1} - 1)$ with vanishing constant coefficient. Under the identification of R_n with the circulant matrices of order n over $\mathbb{F}_2$, in which u is the first row of the matrix, this is the number of invertible circulant matrices of order $d - 1$ over $\mathbb{F}_2$ with zero diagonal.*

The zero diagonal is not an artefact. By Proposition 2.4 the diagonal of L is the periodic-boundary automaton of g on n cells, whose matrix is exactly the circulant of u; the vanishing of u_0 is what bipermutivity leaves after the two permutive cells of $x \| x$ cancel. This is also the closing remark of [1] — that self-orthogonality of a linear bipermutive automaton is invertibility of the corresponding periodic-boundary automaton — turned into a count.

4. The counting formula

Throughout this section $n \geq 1$ and $N = X^n - 1 \in \mathbb{F}_2[X]$. We use repeatedly that

$$g \mid N \implies g_0 = 1, \tag{4}$$

since $g_0 = 0$ would give $X \mid g \mid X^n - 1$, whereas $X^n - 1$ has constant term 1.

4.1. **The even case.**

Theorem 4.1. *For every even $n \geq 2$, exactly half of the units of R_n have vanishing constant coefficient:*

$$2A(n) = \Psi(n).$$

Equivalently, at every odd diameter d the number of linear self-orthogonal cellular automata is $\Psi(d-1)/2$, half the number of invertible circulant matrices of order $d - 1$ over $\mathbb{F}_2$.

Proof. Put $c = X^{n/2} + 1$. In characteristic 2, $c^2 = X^n + 1 = N$, so for any a,

$$\gcd(a, N) = 1 \iff \gcd(a, c) = 1 \iff \gcd(a + c, c) = 1 \iff \gcd(a + c, N) = 1,$$

the middle equivalence because a and $a + c$ differ by a multiple of c. Hence $u \mapsto u + c$ maps $R_n^\times$ to itself; it is an involution, it has no fixed point because $c \neq 0$, and it flips the constant coefficient because $c_0 = 1$. A fixed-point-free involution of a finite set that flips a predicate makes the predicate hold on exactly half of the set. □

The hypothesis is not cosmetic: the identity fails at every odd n, by Theorem **??**, and the smallest instance is $2A(7) = 48 \neq 49 = \Psi(7)$. Note also that $n = 6$, i.e. $d = 7$, is covered, and gives $A(6) = 24/2 = 12$ where the pattern 2^{d-3} of the smaller diameters would predict 16.

4.2. **The odd case.**

Lemma 4.2. *For $n \geq 1$, the polynomial $X^n - 1$ is squarefree over $\mathbb{F}_2$ if and only if n is odd. For odd n it is therefore the product of its $r(n)$ distinct monic irreducible factors, where $r(n)$ denotes the number of those factors.*

Proof. If n is odd then $n \neq 0$ in $\mathbb{F}_2$, so $X^n - 1$ is separable, hence squarefree, and a squarefree element of a unique factorisation domain is the product of its distinct irreducible factors — distinct up to associates, and over $\mathbb{F}_2$ the only unit is 1, so up to equality. If n is even then $X^n - 1 = (X^{n/2} - 1)^2$ is not squarefree; alternatively, and this is the route taken in the formal development, no factorisation into distinct irreducibles can exist for even n, because Theorem 4.3 applied to such a factorisation would contradict Theorem 4.1. □

Accordingly we set

$$\mu_n \;=\; \mu(X^n - 1) \;=\; \begin{cases} 0, & n \text{ even}, \\ (-1)^{r(n)}, & n \text{ odd}, \end{cases}$$

which is the Möbius function of $\mathbb{F}_2[X]$ evaluated at the modulus.

Theorem 4.3. *Let $n \geq 1$ and let S be a finite set of irreducible polynomials of $\mathbb{F}_2[X]$ with $\prod_{f \in S} f = X^n - 1$. Then*

$$2A(n) \;=\; \Psi(n) + (-1)^{|S|}.$$

Proof. Represent the elements of R_n by the polynomials u of degree $< n$ and put $\operatorname{sgn}(u) = (-1)^{u_0}$. The quantity to compute is the signed count

$$D(n) \;=\; \sum_{\deg u < n,\ \gcd(u,N)=1} \operatorname{sgn}(u) \;=\; \big|\{u \text{ unit} : u_0 = 0\}\big| - \big|\{u \text{ unit} : u_0 = 1\}\big| \;=\; 2A(n) - \Psi(n).$$

Step 1: a vanishing lemma. For a divisor g of N set $W(g) = \sum_{\deg u < n,\ g \mid u} \operatorname{sgn}(u)$. If $\deg g < n$ then g itself lies in the index set, and $u \mapsto u + g$ is a fixed-point-free involution of that set which flips u_0, because $g_0 = 1$ by (4). Hence the two signs occur equally often and $W(g) = 0$. If $g = N$ then the only u of degree $< n$ divisible by N is $u = 0$, so $W(N) = +1$.

Step 2: inclusion–exclusion. Because $\prod_{f \in S} f = N$ and distinct irreducibles are coprime, for every u

$$\sum_{T \subseteq S} (-1)^{|T|} \Big[\prod_{f \in T} f \;\Big|\; u \Big] \;=\; \big[\gcd(u, N) = 1\big].$$

Indeed the left-hand side is $\sum_{T \subseteq U} (-1)^{|T|}$, where U is the set of members of S dividing u, and that alternating sum is 1 if $U = \emptyset$ and 0 otherwise. This is inclusion–exclusion over the *subsets* of S; for a squarefree modulus the divisor lattice is the subset lattice, so no Möbius inversion over divisors is needed.

Step 3. Multiplying the identity of Step 2 by $\operatorname{sgn}(u)$, summing over all u of degree $< n$ and exchanging the two sums,

$$D(n) \;=\; \sum_{T \subseteq S} (-1)^{|T|}\, W\Big(\prod_{f \in T} f \Big).$$

Every proper subset $T \subsetneq S$ has $\deg \prod_{f \in T} f < n$, so its term vanishes by Step 1, and the term $T = S$ contributes $(-1)^{|S|} W(N) = (-1)^{|S|}$. Thus $2A(n) - \Psi(n) = (-1)^{|S|}$. □

Corollary 4.4. *For odd n, $2A(n) = \Psi(n) + (-1)^{r(n)}$, and consequently $\Psi(n)$ is odd. Combining with Theorem 4.1, for every $n \geq 1$*

$$2A(n) \;=\; \Psi(n) + \mu_n.$$

Proof. For odd n Lemma 4.2 supplies a set S of $r(n)$ distinct irreducibles with product $X^n - 1$, and Theorem 4.3 applies; the parity of $\Psi(n)$ follows since $\Psi(n) = 2A(n) \mp 1$. For even n, $\mu_n = 0$ and the identity is Theorem 4.1. □

4.3. **The value of the unit count.** Corollary 4.4 is a formula only once Ψ is one. The value of Ψ is classical; we record it because the same inclusion–exclusion proves it, run on the plain count instead of the signed one.

Theorem 4.5. *Let $n \geq 1$ and suppose $X^n - 1 = \prod_{f \in S} f^{\,e_f}$ with S a finite set of distinct irreducibles and every $e_f \geq 1$. Then*

$$\Psi(n) \;=\; 2^{\,n - \sum_{f \in S} \deg f} \prod_{f \in S} \bigl(2^{\deg f} - 1\bigr).$$

Writing $n = 2^k m$ with m odd, and letting $s_1, \ldots, s_r$ be the degrees of the $r = r(m)$ distinct irreducible factors of $X^m - 1$, so that $s_1 + \cdots + s_r = m$, this reads

$$\Psi(n) \;=\; 2^{\,n-m} \prod_{i=1}^{r} \bigl(2^{s_i} - 1\bigr).$$

Proof sketch. Two ingredients. First, for a fixed nonzero g of degree $\leq n$, the polynomials of degree $< n$ divisible by g number $2^{\,n - \deg g}$, the bijection being $h \mapsto gh$ from the polynomials of degree $< n - \deg g$. Second, the identity of Step 2 in the proof of Theorem 4.3 holds verbatim when the modulus is a product of *powers* of the members of S: only the radical enters the coprimality indicator. Summing that identity over all u of degree $< n$ and writing $D = \sum_{f \in S} \deg f$,

$$\Psi(n) = \sum_{T \subseteq S} (-1)^{|T|} 2^{\,n - \sum_{f \in T} \deg f} = 2^{\,n-D} \sum_{T \subseteq S} (-1)^{|T|} 2^{\,D - \sum_{f \in T} \deg f} = 2^{\,n-D} \prod_{f \in S} \bigl(2^{\deg f} - 1\bigr),$$

the last step being the expansion of a product of binomials read from right to left. For the second display, iterated Frobenius gives $X^{2^k m} - 1 = (X^m - 1)^{2^k}$, and $X^m - 1$ is squarefree by Lemma 4.2, so S may be taken to be its set of irreducible factors, with every $e_f = 2^k$ and $D = \deg(X^m - 1) = m$. □

Since $n = \sum_f e_f \deg f$, the prefactor is $\prod_f 2^{\deg f\,(e_f - 1)}$, so Theorem 4.5 is the textbook product $\Psi(n) = \prod_f (2^{\deg f} - 1)\, 2^{\deg f (e_f - 1)}$. Neither the Chinese remainder theorem nor any quotient ring appears in the argument.

Remark 4.6. Classically the s_i are also the sizes of the 2-cyclotomic cosets modulo m, the irreducible factors of $X^m - 1$ being the orbit polynomials of the Frobenius action on the m-th roots of unity; this is how the values in Table 1 are computed, and it is the identification that makes $r(n)$ the sequence A000374 and $\Psi(n)$ the sequence A003473. We use it only for evaluation, never in a proof: every statement of this paper is stated and proved with $s_i = \deg f_i$ and $r(n) = \#\{\text{distinct irreducible factors}\}$.

Proposition 4.7. *Worked instances of Theorem 4.5, obtained from explicit factorisations in $\mathbb{F}_2[X]$: from $X^2 - 1 = (X+1)^2$, $X^3 - 1 = (X+1)(X^2+X+1)$ and $X^7 - 1 = (X+1)(X^3+X+1)(X^3+X^2+1)$ one gets*

$$\Psi(2) = 2, \quad \Psi(3) = 3, \quad \Psi(7) = 49, \qquad r(3) = 2, \quad r(7) = 3,$$

and hence, by Corollary 4.4,

$$\mathrm{LIN}(3) = A(2) = 1, \qquad \mathrm{LIN}(4) = A(3) = 2, \qquad \mathrm{LIN}(8) = A(7) = 24,$$

three entries of (1) *obtained from the criterion rather than by enumeration.*

5. The closed form, its values, and the powers of two

Theorem 5.1. *For every diameter $d \geq 3$, with $n = d - 1$,*

$$\mathrm{LIN}(d) \;=\; \frac{\Psi(n) + \mu_n}{2}, \qquad \Psi(n) = 2^{\,n-m} \prod_{i=1}^{r} \bigl(2^{s_i} - 1\bigr), \qquad \mu_n = \begin{cases} 0, & n \text{ even}, \\ (-1)^r, & n \text{ odd}, \end{cases}$$

where $n = 2^k m$ with m odd and $s_1, \ldots, s_r$ are the degrees of the distinct irreducible factors of $X^m - 1$ over $\mathbb{F}_2$. The right-hand side reproduces all fourteen values (1) *published for $3 \leq d \leq 16$, agrees for every $3 \leq d \leq 15$ with an exhaustive evaluation of the criterion of Theorem 3.1 over all 2^{d-2} linear*

d	3	4	5	6	7	8	9	10	11	12	13	14	15	16
LIN(d)	1	2	4	8	12	24	64	94	240	512	768	2048	3136	5062

d	17	18	19	20	21	22	23
LIN(d)	16384	32512	48384	131072	245760	291722	1047552

d	24	25	26	27	28	29	30
LIN(d)	2095104	3145728	7864312	16773120	24772514	51380224	134217728

TABLE 1. The number of linear self-orthogonal cellular automata of diameter d, from Theorem 5.1. The first block is the table of [1]; the remaining fourteen values are new.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$\Psi(n)$	1	2	3	8	15	24	49	128	189	480	1023	1536	4095	6272
$A(n)$	0	1	2	4	8	12	24	64	94	240	512	768	2048	3136
$r(n)$	1	1	2	1	2	2	3	1	3	2	2	2	2	3
$2A-\Psi$	-1	0	1	0	1	0	-1	0	-1	0	1	0	1	0

TABLE 2. $\Psi(n) = |R_n^\times|$ (A003473), $A(n) = \mathrm{LIN}(n+1)$, and the number $r(n)$ of distinct irreducible factors of $X^n - 1$ (A000374).

bipermutive rules, and agrees for every $3 \le d \le 7$ with the count obtained from the Latin square itself — that is, by building the square of order 2^{d-1} and testing all 4^{d-1} superposition pairs against Definition 2.3. Its values for $17 \le d \le 30$ are those of Table 1.

Proof. Corollary 3.3 identifies $\mathrm{LIN}(d)$ with $A(n)$; Corollary 4.4 gives $2A(n) = \Psi(n)+\mu_n$; Theorem 4.5 evaluates Ψ; Lemma 4.2 justifies the case split defining μ_n. The three agreement statements are finite computations, each carried out in full: the first over the fourteen published entries, the second over the $\sum_{d\le 15} 2^{d-2} = 2^{14} - 2$ linear rules, the third over the 2^{d-2} linear rules of each diameter $d \le 7$ with the full 4^{d-1}-pair test on each, 4096 pairs per rule at $d = 7$. □

For orientation, Table 2 shows the two ingredients and the defect at small arguments. The defect $2A(n) - \Psi(n)$ is 0 at even n and ± 1 at odd n, with the sign $(-1)^{r(n)}$, exactly as Corollary 4.4 asserts.

The source's Lemma 6 is now one line.

Proposition 5.2 ([1, Lemma 6])**.** *For every $t \ge 1$, $\Psi(2^t) = 2^{2^t-1}$ and $\mathrm{LIN}(2^t+1) = 2^{2^t-2}$; that is, $\mathrm{LIN}(d) = 2^{d-3}$ at every diameter $d = 2^t + 1$.*

Proof. Iterated Frobenius gives $X^{2^t} - 1 = (X+1)^{2^t}$, so by Theorem 4.5 with the single factor $X+1$ we get $\Psi(2^t) = 2^{2^t-1}(2^1 - 1) = 2^{2^t-1}$; equivalently the units of R_{2^t} are exactly the polynomials of odd weight, which is the parity check [1] performs by hand. For $t \ge 1$ the argument 2^t is even, so Theorem 4.1 halves it. (At $t = 0$ the conclusion fails: $A(1) = 0$.) □

The guess of [1] that the counts follow the powers of two can now be settled exactly. Call an odd prime p an *Artin prime* if 2 is a primitive root modulo p; the smallest are $3, 5, 11, 13, 19, 29, 37, 53, 59$.

Theorem 5.3. *For $d \ge 3$, $\mathrm{LIN}(d) = 2^{d-3}$ if and only if $n = d - 1$ is a power of two or an Artin prime. In particular the guess holds at $d = 3, 4, 5, 6$ and fails first at $d = 7$, where $\mathrm{LIN}(7) = 12$ rather than 16.*

Proof sketch. By Theorem 5.1 the assertion is $\Psi(n) + \mu_n = 2^{n-1}$. If n is even then $\mu_n = 0$ and, with $n = 2^k m$ and m odd, $\Psi(n) = 2^{n-m}\prod_i (2^{s_i} - 1)$; a product of odd numbers is a power of two only when it equals 1, which happens exactly when $m = 1$, i.e. when n is a power of two. If n is

odd then $\Psi(n) = \prod_i (2^{s_i} - 1)$ with $\sum_i s_i = n$ and $s_i = 1$ for the factor $X + 1$; for odd $n \geq 3$ such a product is at most $2^{n-1} - 1$, with equality exactly for $r = 2$, i.e. for $(s_1, s_2) = (1, n-1)$, and then $\mu_n = (-1)^2 = +1$ and the total is 2^{n-1}. The other sign would require $\Psi(n) = 2^{n-1} + 1$, which exceeds the bound. Finally $r = 2$ for odd n says that $X^n - 1$ is $(X + 1)$ times a single irreducible of degree $n - 1$, which for $n > 1$ holds exactly when n is prime and 2 has order $n - 1$ modulo n. □

By Artin's conjecture the Artin primes have positive density among the primes, so — if the conjecture holds — the guess of [1] is correct for a positive proportion of prime arguments, and it is correct at every $d = 2^t + 1$ unconditionally; it is also wrong at infinitely many diameters. The formal development checks the characterisation against the closed form at every diameter $d \leq 40$.

6. Diameters up to seven

We record the exhaustive picture at the small diameters, both because it is the data the counting formula had to reproduce and because it is what is known about the second question of [1]. All statements in this section are exhaustive evaluations of Definition 2.3 on the actual Latin squares.

Proposition 6.1. *For $d = 3, 4, 5, 6$ the numbers of bipermutive rules are 4, 16, 256, 65 536, and the numbers of self-orthogonal ones are*

$$\mathrm{SOCA}(3) = 2, \quad \mathrm{SOCA}(4) = 4, \quad \mathrm{SOCA}(5) = 8, \quad \mathrm{SOCA}(6) = 16.$$

This is Table 1 of [1]; we note that the printed table gives 65 336 in the last row of its first column, whereas its own running text says $2^{16} = 65\,536$, which is the correct value and the one proved here. The search at $d = 6$ is made cheap by Proposition 2.4: a rule whose diagonal is not a transversal can be discarded before its square is built, and removing that filter again from the final statement is immediate from the same proposition.

Proposition 6.2. *Every self-orthogonal cellular automaton of diameter at most 6 is affine. Among the linear rules the counts are $\mathrm{LIN}(3) = 1$, $\mathrm{LIN}(4) = 2$, $\mathrm{LIN}(5) = 4$, so that $\mathrm{SOCA}(d) = \mathrm{AFF}(d) = 2\mathrm{LIN}(d)$ for $d \leq 6$.*

The first sentence is the observation [1] reads off its Table 1 ("among those found, there are no self-orthogonal CA defined by nonlinear local rules"), stated as a theorem: for every g below the rule count, self-orthogonality implies affineness. The second sentence pins the differing conventions of the two tables of [1], since $1, 2, 4$ is exactly half of $2, 4, 8$.

Proposition 6.3. *At $d = 7$ there are 64 affine and 32 linear bipermutive rules. Exactly 24 of the affine ones and exactly 12 of the linear ones are self-orthogonal, so $\mathrm{AFF}(7) = 24$ and $\mathrm{LIN}(7) = 12 \neq 16 = 2^{7-3}$. The twelve linear ones are those with associated polynomial*

$$\begin{array}{lll} 1 + X + X^6, & 1 + X^2 + X^6, & 1 + X^3 + X^6, \\ 1 + X^4 + X^6, & 1 + X^5 + X^6, & 1 + X + X^2 + X^4 + X^6, \\ 1 + X + X^3 + X^4 + X^6, & 1 + X + X^2 + X^5 + X^6, & 1 + X^2 + X^3 + X^5 + X^6, \\ 1 + X + X^4 + X^5 + X^6, & 1 + X^2 + X^4 + X^5 + X^6, & 1 + X + X^2 + X^3 + X^4 + X^5 + X^6. \end{array}$$

Each of these twelve is self-orthogonal in the sense of Definition 2.3, and no other linear rule of diameter 7 is.

The value 12 is the $d = 7$ entry of (1), which [1] obtains from the criterion of Theorem 3.1; here it is obtained the other way round, by building each of the thirty-two Latin squares of order 64 and testing all 4096 superposition pairs. The two routes agreeing is an independent check on the criterion, and the twelve polynomials themselves are not listed in [1]. The companion value $\mathrm{AFF}(7) = 24$ extends the first table of [1] by one row.

6.1. **A computation beyond the formal development.** The following two statements are exhaustive machine computations carried out in C. They are *not* part of the formally verified development — a search over 2^{32} rules is outside the budget of the proof assistant used here — and are reported as computations.

An exhaustive sweep of all 2^{32} bipermutive rules of diameter 7, each tested by building its Latin square of order 64 and checking that the 4096 superposition codes are pairwise distinct, returns exactly the twenty-four rules of Proposition 6.3 and no others. So $\mathrm{SOCA}(7) = 24$, and no nonlinear self-orthogonal cellular automaton of diameter 7 exists. The sweep was run twice by two independent code paths: once pruned by Proposition 2.4 together with two derived single-bit tests, and once with every prune removed, relying only on the complementation symmetry $g \mapsto g \oplus 1$; the two runs return the same twelve linear rules. This answers the second question of [1] at the smallest diameter it leaves open, and does not settle it in general: $d = 8$ has 2^{64} rules.

The same sweep counts the rules of diameter 7 whose generating function induces an invertible periodic-boundary automaton on 6 cells, equivalently — by Theorem 1 of [2] — whose Latin square has a transversal on the main diagonal. There are 105 056 of them, of which 105 032 are nonlinear. This extends by one row the exhaustive search of [2], which stops at $d = 6$ with $472 = 16 + 456$; the values of [2] for $d \le 6$ are reproduced exactly, and the $d = 6$ value 472 is also reproduced inside the formal development.

7. Consistency checks

A counting formula and a criterion are both easy to state in a way that is true and empty, or true of the wrong objects. The following are the checks that were run against that.

Proposition 7.1. (i) *The criterion of Theorem 3.1 agrees with the test of Definition 2.3* rule by rule*, not merely count by count: on all* 32 *linear rules of diameter* 7 *and on all linear rules of diameters* $3, 4, 5, 6$.

(ii) *Both verdicts occur. At* $d = 7$ *the rule with* $p_f = 1 + X^6 = (1 + X^3)^2$*, which shares* $1 + X^3$ *with* $X^6 + 1$*, fails both tests; the rule with* $p_f = 1 + X + X^6$ *passes both.*

(iii) *At every diameter* $3 \le d \le 15$ *the count is strictly between* 0 *and* 2^{d-2}*, so it is neither vacuous nor everything.*

(iv) $\mathrm{LIN}(7) = 12$*, and in particular* $\mathrm{LIN}(7) \neq 16$ *and* $\mathrm{LIN}(7) \neq 8$.

(v) *The count is about linear rules only: at* $d = 7$ *it ranges over* 32 *rules out of* 2^{32}*, and the diameter-*6 *rule with truth table* 1000_2 *is neither linear nor affine nor self-orthogonal.*

Proposition 7.2. (i) *The hypothesis of Theorem 4.3 is exactly the odd case, and it is not vacuous: for odd* n *a factorisation into distinct irreducibles exists, and for even* $n \ge 2$ *none does.*

(ii) *The identity* $2A(n) = \Psi(n) + (-1)^{r(n)}$ *is* false *at every even* $n \ge 2$*, where Theorem 4.1 gives no defect at all.*

(iii) *The defect at odd* n *is exactly* ± 1*:* $2A(n)$ *is none of* $\Psi(n)$*,* $\Psi(n) + 2$*,* $\Psi(n) - 2$.

(iv) *At* $n = 1$ *the formula reads* $2 \cdot 0 = 1 + (-1)$*, with* $\Psi(1) = 1$*,* $A(1) = 0$ *and* $r(1) = 1$*; this pins the sign and shows that neither count is vacuous.*

Proposition 7.3. *Every hypothesis of Theorem 4.5 is load-bearing.*

(i) *The prefactor* $2^{\,n - \sum \deg f}$ *is neither too small nor too large: at* $n = 2$ *the radical alone predicts* $2^1 - 1 = 1$ *and the set of all polynomials of degree* < 2 *predicts* 4*, while* $\Psi(2) = 2 = 2^{2-1} \cdot 1$.

(ii) *A non-coprime split is rejected:* $X^2 - 1 = (X - 1)(X - 1)$ *would give* $\Psi(1)\Psi(1) = 1 \neq 2 = \Psi(2)$*, whereas the coprime split at* $n = 3$ *does multiply,* $(2^1 - 1)(2^2 - 1) = 3 = \Psi(3)$.

(iii) *Dropping* $e_f \neq 0$ *breaks the formula: at* $n = 1$ *the set* $\{X + 1, X^2 + X + 1\}$ *with exponents* $(1, 0)$ *satisfies* $\prod f^{e_f} = X - 1$ *and evaluates to* 3*, not* $\Psi(1) = 1$.

(iv) *Dropping irreducibility breaks it too: at* $n = 3$ *the singleton* $\{X^3 - 1\}$ *with exponent* 1 *evaluates to* $2^3 - 1 = 7$*, not* $\Psi(3) = 3$.

(v) *The agreement of Remark 4.6 is not a tautology:* $\mathrm{LIN}(8) = 24$ *is neither* $2^{8-3} = 32$ *nor* $\Psi(7)/2$*, which is not an integer.*

8. Verification

Every theorem, proposition, lemma, corollary and example stated above — with the single, explicitly labelled exception of the two computations of Section 6.1 — has been formally verified in Lean 4 against *Mathlib* (v4.32.0), and the development contains no `sorry`. The reasoning layer is kernel-checked and depends on no axioms beyond `propext`, `Classical.choice` and `Quot.sound`: this covers Propositions 2.2, 2.4 and 3.2, Theorems 4.1, 4.3 and 4.5, Lemma 4.2, Corollaries 4.4 and 3.3, Propositions 5.2, 4.7, 7.2 and 7.3. What is delegated to compiled evaluation, through Lean's `native_decide`, is exactly the finite searches: the exhaustive counts of Propositions 6.1, 6.2, 6.3, 2.6 and 7.1, Example 2.5, and the tabulation and agreement statements of Theorems 5.1 and 5.3. The bridge between the two layers is itself a theorem: the Boolean procedure the searches filter on — an early-exiting duplicate test on the N^2 superposition codes, carrying the set of codes seen so far as a bit mask — is proved to decide Definition 2.3, so the counts are statements about the definition and not about a program.

Two caveats are recorded deliberately. First, the identification of the degrees s_i with the sizes of the 2-cyclotomic cosets (Remark 4.6) is classical but is not part of the verified development, because the factorisation of cyclotomic polynomials over a finite field is not available in the library used; the two descriptions have been checked to agree at $n = 1, 2, 3, 7$ inside the proof assistant and numerically far beyond. Second, the evaluation of the closed form in Theorem 5.1 and Table 1 is carried out in a bit-mask model of $\mathbb{F}_2[X]$, whose encoding isomorphism with the polynomial model of Sections 4–5 is not itself formalised; what ties the two together is the rule-by-rule agreement of Proposition 7.1(i) with the Latin-square test at every $d \leq 7$, and the pointwise agreement of Proposition 4.7. Every numerical value quoted in this paper was produced by at least two independent implementations before it was proved: the closed form, an exhaustive evaluation of the criterion, and — for $d \leq 10$ — an enumeration that never mentions a polynomial and works from Definition 2.3 alone. The Lean sources are available in the authors' repository: repository reference to be added at submission.

References

[1] L. Mariot and F. Mazzone, *Self-Orthogonal Cellular Automata*, in: S. Riva and A. Richard (eds.), Cellular Automata and Discrete Complex Systems (AUTOMATA 2025), Lecture Notes in Computer Science 15831, Springer, 2025, pp. 188–204, doi:10.1007/978-3-032-01570-9_13. The section, statement and table numbers cited above are those of the e-print arXiv:2504.09173 (2025).

[2] A. Dennunzio, M. Gadouleau and L. Mariot, *On the transversals of Latin squares generated by nonlinear bipermutive cellular automata*, preprint, arXiv:2605.18875 (2026).

[3] OEIS Foundation Inc., *The On-Line Encyclopedia of Integer Sequences*, `https://oeis.org`; entries A003473 (units of $\mathbb{F}_2[x]/(x^n - 1)$, equivalently invertible circulant matrices over $GF(2)$) and A000374 (number of distinct irreducible factors of $x^n - 1$ over $GF(2)$).