# Boolean CM Phase Algebra: Native Binary Realizations and Exact Detector Bounds

Prepared for Brian Droncheff

28 September 2026

**Abstract**

The four cyclic coordinates of a Boolean correspondence matrix give a concrete realization of the classical modular group algebra $\mathcal{A} = \mathbb{F}_2[C_4] \cong \mathbb{F}_2[u]/(u^4)$. We separate three questions: how to implement its operations without a primitive cyclic-convolution symbol, what information its nilpotent phase tags retain, and what a specified linear detector can read. The native binary implementation is exactly the centralizer of a four-cycle; allowing arbitrary binary gates is a strictly larger model.

For the half-turn tag $z = 1 + u^2$, we close the finite detector examples with an exact width formula. On $N = 2^n$ addresses with $n \geq 1$, $c$ constant-annihilating $\mathcal{A}$-linear output channels distinguish constant from balanced truth vectors by literal zero/nonzero pattern inspection if and only if $c \geq \lceil N/4 \rceil$. More generally, the threshold is $\lceil N/(2r) \rceil$ for a tag whose principal ideal has binary dimension $r$, when 4 divides $N$. The lower bound is an application of the classical forbidden-weight theorem of Enomoto, Frankl, Ito and Nomura; it is not claimed as a new coding theorem. We give an explicit optimal construction and a self-contained power-of-two proof of the needed coding bound.

A second boundary is exact: square-zero-tag interactions vanish across a binary linear map precisely when that map preserves the tag ideal. A reversible coordinate permutation witnesses failure outside this class. We also provide a normal form for all 512 intrinsic two-branch unitaries, including analytic proofs of the 96 involutions and 72 nonmonomial involutions, and retain reproducible finite classifications. The familiar Boolean Möbius transform explains the phase-to-ANF identity. These are algebraic and pattern-readout results, not a Born rule, an exact modal Deutsch–Jozsa algorithm, or a quantum query advantage.

## 1 Purpose and contribution boundary

A correspondence matrix (CM) records a two-input Boolean predicate in four bits. Putting those bits on a cycle and letting a quarter-turn act on them is harmless bookkeeping. Treating all four-bit patterns as phase coefficients requires an additional multiplication. That multiplication is mathematically useful, but it must not be confused with pointwise Boolean conjunction or with the ordinary product of the original $2 \times 2$ matrices.

This companion studies that additional algebra. Its purpose is not to introduce a new number system: modular group algebras, unitary subgroups of group algebras, and Boolean Möbius transforms have substantial prior theory [3, 5]. Its value is an explicit translation between CM coordinates and binary operators, a closed detector-width problem with its classical antecedent identified, and finite certificates that keep incompatible operational interpretations apart.

The principal results are Theorem 3.1 (the exact native gate algebra), Theorem 6.3 (optimal detector width), Theorem 7.1 (the exact gate boundary for square-zero interactions), and Theorem 4.2 (a complete two-branch unitary normal form). The detector theorem packages a known coding bound into this coefficient model; its construction and the ideal-boundary criterion

are elementary. No claim of historical firstness is made for these specializations or for the finite group counts.

**Readout is part of the problem.** Throughout, a *pattern detector* is a specified linear map followed by inspection of its output coordinates. It is not automatically a physically realizable measurement or a complete modal instrument. Modal quantum theory assigns possible/impossible outcomes using a declared state and measurement structure [6, 7]; it does not give free inspection of an entire coefficient description. Sections 4 and 8 make this distinction explicit.

**Scope of the revision.** The finite phase algebra and its interfaces form the paper. General compiler-performance claims, speculative applications, and attempts to recover all standard quantum algorithms are not included as contributions. A local Boolean-polynomial identity is retained in Appendix B only to connect the phase algebra back to the underlying CM notation.

# 2 Typed coordinates and the classical phase ring

## 2.1 CM coordinates and the additional product

For a CM $C = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, the row and column labels are $(1, 0)$. Thus

$$f_C(X, Y) = aXY + bX(1 + Y) + c(1 + X)Y + d(1 + X)(1 + Y). \tag{2.1}$$

Here $+$ is addition in $\mathbb{F}_2$; when a logical connective is written explicitly, $\Updownarrow$ denotes XOR. The four cyclic basis elements are

$$E_0 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad E_1 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad E_2 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \quad E_3 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

Consequently $(a_0, a_1, a_2, a_3)$ means the CM $\left(\begin{smallmatrix} a_0 & a_1 \\ a_3 & a_2 \end{smallmatrix}\right)$, not row-major order. Address-register order, used later, is separately ascending binary order.

Define a second multiplication by bilinearity and

$$E_i \star E_j = E_{i+j \bmod 4}, \qquad (a \star b)_k = \sum_{i+j \equiv k \ (4)} a_i b_j. \tag{2.2}$$

Once this algebra is declared, we use juxtaposition for its multiplication. The symbol $\star$ need not be a primitive operation in an implementation.

| Operation | Type | Identity or diagnostic |
|---|---|---|
| Pointwise conjunction | Boolean operation on corresponding CM entries | All-ones CM |
| Ordinary CM product | Contracted $2 \times 2$ product over $\mathbb{F}_2$ | Numerical $I_2$ |
| Phase product | Equation (2.2) | $E_0$ |
| Boolean polynomial product | $\mathbb{F}_2[X_1, \ldots, X_n]/(X_i^2 - X_i)$ | $X_i^2 = X_i$ |
| Native phase operator product | Ordinary product of $4 \times 4$ binary blocks | $I_4 = \rho(E_0)$ |

For example, numerical $I_2 = E_0 + E_2$ is square-zero under phase multiplication. This single example rules out identifying the second and third rows of the table.

### 2.2 Ring structure and scalar information

Put $t = E_1$, $1 = E_0$, $u = 1 + t$, $z = t^2 = 1 + u^2$, and

$$\delta = 1 + z = u^2, \qquad \Omega = u^3 = 1 + t + t^2 + t^3.$$

The group basis gives, directly,

$$\mathcal{A} = \mathbb{F}_2[t]/(t^4 - 1) = \mathbb{F}_2[u]/(u^4). \tag{2.3}$$

The quarter-turn $t$ has multiplicative order four; its half-turn $z$ is not the additive negative of 1. Indeed $-1 = 1$ in this algebra, whereas $z \neq 1$.

**Proposition 2.1.** *The units of $\mathcal{A}$ are the eight odd-weight cyclic patterns. The only ideals are*

$$0 \subset (u^3) \subset (u^2) \subset (u) \subset \mathcal{A},$$

*with cardinalities $1, 2, 4, 8, 16$. If $\nu(a)$ is the first nonzero exponent in its $u$-expansion and $\nu(0) = 4$, multiplication by $a$ has binary rank $4 - \nu(a)$ and kernel size $2^{\nu(a)}$. The only idempotents are 0 and 1.*

*Proof.* An element with constant $u$-coefficient one has the form $1 + h$, where $h^4 = 0$, and inverse $1 + h + h^2 + h^3$. An element with constant coefficient zero is nilpotent and not a unit. Evaluation at $t = 1$ shows that this constant coefficient is the parity of the cyclic pattern. Every nonzero element is $u^r v$ for a unit $v$. Choosing the least such $r$ in a nonzero ideal proves the ideal classification. Multiplication by a unit is invertible; multiplication by $u^r$ shifts and truncates the four $u$-coordinates, proving the rank and kernel assertions. If $a^2 = a$, then either $a$ is a unit and $a = 1$, or $1 + a$ is a unit and $a(1 + a) = 0$ gives $a = 0$. □

The unit group has the explicit presentation

$$\mathcal{A}^\times = \{t^j(1 + \Omega)^e : 0 \leq j < 4,\ e \in \{0, 1\}\} \cong C_4 \times C_2.$$

The two cyclic factors have trivial intersection, and the displayed eight elements exhaust the units. There are four solutions of $a^2 = z$: $t, t^3, 1 + t + t^2, 1 + t^2 + t^3$. These are elementary specializations of group-algebra unit questions, not a new theory of complex square roots.

## 3 Eliminating the star primitive without changing the model

Let $V = \mathbb{F}_2^4$ have basis $e_0, e_1, e_2, e_3$, and define the fixed wiring permutation

$$R = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

For $a = \sum_i a_i t^i$, set

$$\rho(a) = \sum_{i=0}^{3} a_i R^i. \tag{3.1}$$

Every displayed operation is now binary matrix addition or multiplication. In particular $\rho(ab) = \rho(a)\rho(b)$ and $\rho(a)e_0$ is exactly the cyclic coefficient vector of $a$.

**Theorem 3.1** (Native gate algebra)**.** *The map $\rho$ is a faithful algebra representation with*

$$\rho(\mathcal{A}) = \mathrm{Cent}_{\mathrm{Mat}_4(\mathbb{F}_2)}(R).$$

*On $m$ coefficient blocks, the binary maps commuting with $R_m = \mathrm{diag}(R, \ldots, R)$ are exactly the regular representations of $\mathrm{Mat}_m(\mathcal{A})$. Thus a circuit of $\mathcal{A}$-linear maps and its native binary block circuit have identical coefficient outputs at every stage.*

*Proof.* The four images $e_0, Re_0, R^2e_0, R^3e_0$ are a basis. Therefore the operators $I, R, R^2, R^3$ are linearly independent, which proves faithfulness. Their multiplication follows the cyclic law. If $G$ commutes with $R$, write $Ge_0 = \sum_i a_i R^i e_0$. Commutation forces $GR^j e_0 = R^j G e_0 = \rho(a)R^j e_0$ for every $j$, so $G = \rho(a)$. The converse is immediate. In block form, commutation with $R_m$ says precisely that each block commutes with $R$. The circuit assertion follows by composition. □

This resolves two different meanings of "without star." Compiling $\star$ into $\rho$ removes a primitive but leaves the model unchanged. Allowing every binary linear gate, including gates outside this centralizer, changes the model. The second move may be useful, but conclusions proved using $\mathcal{A}$-linearity must then be checked again. Section 7 identifies the exact larger gate class that still preserves the square-zero obstruction.

**An explicit star-free interferometer.** Let $U_0 = I_4 + R$ and $B = \left(\begin{smallmatrix} I_4 & 0 \\ U_0 & I_4 \end{smallmatrix}\right)$, so $B^2 = I_8$. Starting with $(e_0, 0)$ and applying $B$, then $\mathrm{diag}(R^j, I_4)$, then $B$, yields

$$(R^j e_0,\ (I_4 + R)(I_4 + R^j)e_0). \tag{3.2}$$

For $j = 0, 1, 2, 3$, the second component represents $0, \delta, \Omega, t\delta$, with Hamming weights $(0, 2, 4, 2)$. No convolution primitive, complex scalar, or trigonometric operation is needed. These four integers are pattern statistics, not probabilities.

# 4 Readout, isometries, and two-branch classification

## 4.1 Three different readouts

Literal coefficient inspection, integer Hamming weight, and the algebraic self-product $N(a) = \bar{a}a$ are different operations. Here $\bar{t} = t^{-1} = t^3$, extended linearly, is the conjugation corresponding to the transpose of the displayed CM. Also $\rho(\bar{a}) = \rho(a)^T$.

Writing $r = a_0 + a_2$ and $s = a_1 + a_3$, direct multiplication gives

$$N(a) = (r + s)1 + rs(t + t^3). \tag{4.1}$$

Every unit has self-product 1. The null-self-product set is the ideal

$$K = (\delta) = \{0, \delta, t\delta, \Omega\}, \qquad K^2 = 0.$$

Every element of $K$ is fixed by conjugation. The remaining four scalars have self-product $t + t^3$.

The Hermitian pairing on a free module is $\langle v, w\rangle = \sum_i \bar{v}_i w_i$. It is nondegenerate: pairing with coordinate vectors determines every component. It nevertheless has nonzero isotropic vectors and is not a positive real norm. In particular, zero algebraic self-product does not imply zero pattern.

**Proposition 4.1** (Global coefficient-weight isometries)**.** *The $\mathcal{A}$-linear automorphisms of $\mathcal{A}^m$ preserving the total cyclic-coordinate Hamming weight on every input are exactly block permutations with an independent cyclic rotation in each block. Their number is $m!4^m$, hence 32 when $m = 2$.*

*Proof.* A binary linear Hamming isometry sends every weight-one basis vector to a distinct weight-one vector, so is a coordinate permutation. By Theorem 3.1, it must commute with $R_m$. A permutation commuting with $m$ disjoint four-cycles permutes their orbits and, within each orbit, is fixed by the image of one coordinate, giving one of four rotations. Every such permutation is an isometry and commutes with $R_m$. □

For clarity, a full integer cyclic pair-correlation profile can be defined by $B_j(v, w) = \sum_i \operatorname{coef}(v_i)^T R^j \operatorname{coef}(w_i)$, evaluated over $\mathbb{Z}$. The same permutations preserve every $B_j$. Conversely preserving the whole profile includes $B_0(v, v) = \operatorname{wt}(v)$, so yields the same global class. No other, unspecified meaning of "correlation" is used.

## 4.2 Normal form for intrinsic unitaries

Call $U \in \mathrm{Mat}_2(\mathcal{A})$ *intrinsic unitary* when $U^\dagger U = I$, with conjugate transpose †. This condition is equivalent to binary orthogonality of its regular block matrix, but it does not imply integer Hamming-weight preservation.

**Theorem 4.2** (Complete normal form)**.** *Let* $S = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ *and* $W_k = \left(\begin{smallmatrix} 1 & k \\ k & 1 \end{smallmatrix}\right)$*. Every intrinsic unitary has a unique form*

$$U = \operatorname{diag}(a, d) W_k S^e, \qquad a, d \in \mathcal{A}^\times, \quad k \in K, \quad e \in \{0, 1\}. \tag{4.2}$$

*There are* 512 *such matrices, of which* 128 *are monomial and* 384 *nonmonomial. There are* 96 *involutions, including the identity, and* 72 *nonmonomial involutions.*

*Proof.* By (4.1), a column of self-product one has exactly one unit entry and one entry in $K$. Orthogonality of the columns prevents their unit entries from lying in the same row: a unit plus an element of the maximal ideal cannot vanish. After a unique column swap if needed, write $U = \left(\begin{smallmatrix} a & ak \\ d\ell & d \end{smallmatrix}\right)$ with $a, d$ units and $k, \ell \in K$. Column orthogonality is $\bar{a}ak + \overline{d\ell}d = k + \ell = 0$, hence $k = \ell$. Conversely, $\bar{a}a = \bar{d}d = 1$, $\bar{k} = k$, and $k^2 = 0$ show that every displayed matrix is unitary. The pattern of unit entries, followed by the two unit entries themselves and either off-diagonal quotient, proves uniqueness. The total is $8^2 \cdot 4 \cdot 2 = 512$, and $k = 0$ gives exactly 128 monomial elements.

For $e = 0$, squaring shows that involutivity requires $a^2 = d^2 = 1$. These conditions also suffice: such units have no linear $u$-term, so $a + d \in K$ and all off-diagonal terms vanish. There are four square-one units, giving $4^2 \cdot 4 = 64$ involutions.

For $e = 1$, the diagonal entries of $U^2$ equal $ad$, so the necessary condition is $d = a^{-1}$. It suffices because $a + a^{-1} = a^{-1}(a^2 + 1) \in K$ for every unit $a$, again killing the off-diagonal terms. This gives $8 \cdot 4 = 32$ more. Exactly $16 + 8 = 24$ of the 96 have $k = 0$, leaving 72 nonmonomial involutions. □

Unitary subgroups of group algebras are established objects; Balogh and Laver reproduce a general scalar-unitary order formula that already gives eight in this scalar example [3]. It is important not to equate that scalar result with the present $2 \times 2$ normal form. Nor can arbitrary local-ring unitary formulas be substituted: the hypotheses in Cruickshank et al. include an element $b$ with $b + \bar{b} = 1$, and later odd residue characteristic [4]. Here $b + \bar{b}$ is always a multiple of $t + t^3$, so the first condition already fails. The explicit proof above avoids that mismatch; it does not certify novelty of the small matrix group.

**Corollary 4.3** (A scoped self-product blind spot)**.** *For any intrinsic two-branch unitary* $U$ *and* $j \in \{0, 1, 2, 3\}$*, the two components of* $U^\dagger \operatorname{diag}(t^j, 1) U e_0$ *have self-products* $(1, 0)$*.*

*Proof.* Substitute (4.2). The diagonal unit factors cancel. If $e = 0$, the output is $(t^j, k(t^j + 1))$; if $e = 1$, it is $(1, k(t^j + 1))$. The first entry is a unit and the second lies in $K$, so (4.1) applies. □

The second component can still be a nonzero pattern. The corollary concerns this preparation, this two-branch circuit, and this self-product readout. It is not a theorem forbidding all interference in larger binary or modal models.

### 4.3 What the finite enumeration adds

Reduction modulo $(u)$ gives

$$|\operatorname{GL}_2(\mathcal{A})| = |\operatorname{GL}_2(\mathbb{F}_2)|\, 2^{3\cdot 4} = 6 \cdot 4096 = 24576.$$

Indeed each binary entry has eight lifts, and a matrix over this local ring is invertible exactly when its reduction is invertible. The reproducibility package enumerates all $16^4 = 65536$ matrices and retains their flags, not only successes.

| Class | Count | Evidence |
|---|---|---|
| Intrinsic unitaries | 512 | Theorem 4.2; exhaustive check |
| Unitary involutions / nonmonomial ones | 96 / 72 | Analytic normal-form conditions |
| Global Hamming isometries | 32 | Proposition 4.1 |
| Weight-four-shell preservers | 512 | All 70 weight-four inputs |
| Shell-preserver/unitary intersection | 256 | Complete operator inventory |
| Invertible splitters of $e_0$ | 22528 | Both output entries nonzero |
| Splitters with detector profile $(0, 2, 4, 2)$ | 8192 | Four phases, fixed architecture |

The two classes of size 512 are different. For an invertible $U = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, the second component of $U^{-1} \operatorname{diag}(t^j, 1) U e_0$ is

$$\beta(1 + t^j), \qquad \beta = ac(ad + bc)^{-1}.$$

This follows by the $2 \times 2$ inverse formula. Its four Hamming weights are $(0, 2, 2, 2)$ if $\nu(\beta) = 0$, $(0, 2, 4, 2)$ if $\nu(\beta) = 1$, $(0, 4, 0, 4)$ if $\nu(\beta) = 2$, and all zero otherwise. For valuation one, $\beta\delta = \Omega$ and the adjacent nonzero products are $\delta, t\delta$; the other cases follow directly. These profiles do not define a probability theory.

## 5 Shared half-turn tags and Boolean Möbius computation

Use the free module $\mathcal{A}^{2^n}$, indexed by subsets of $[n]$. In this section multiple logical registers are balanced over the same coefficient ring $\mathcal{A}$. Define

$$C = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \qquad M_n = C^{\otimes n}, \qquad (M_n)_{S,T} = \mathbf{1}_{T \subseteq S}.$$

The tensor notation denotes the Kronecker matrix over $\mathcal{A}$, with the entries $0, 1$ inherited from $\mathbb{F}_2$. Since $C^2 = I$, also $M_n^2 = I$.

For a Boolean truth vector $f$, the vector $a = M_n f$ is precisely its algebraic normal form coefficient vector. This is the established subset Möbius transform, not a newly introduced transform [5]. Let

$$P_f = \operatorname{diag}(z^{f(x)}) = I + \delta \operatorname{diag}(f), \qquad \delta^2 = 0.$$

Then

$$M_n P_f M_n e_\emptyset = e_\emptyset + \delta \operatorname{ANF}(f). \tag{5.1}$$

To verify this, $M_n e_\emptyset$ is the all-ones vector, and multiplication by $P_f$ makes it $\mathbf{1} + \delta f$. Applying $M_n$ gives the displayed identity. The construction is entirely star-free after replacing $\delta$ by $I_4 + R^2$ in each binary block.

**Worked two-bit example.** For $f(X_1, X_2) = X_1 \vee X_2$, ascending truth order is $00, 01, 10, 11$, the truth vector is $(0, 1, 1, 1)$, and the ANF is $X_1 + X_2 + X_1X_2$. Thus the output of (5.1), in subset order $\emptyset, \{2\}, \{1\}, \{1, 2\}$, is

$$(1, \delta, \delta, \delta).$$

The nonempty coordinates expose the three nonzero coefficients. A single modal outcome does not expose all three coordinates.

**Kernel identities.** The matrix $K_f = M_n \operatorname{diag}(f) M_n$ has entries

$$(K_f)_{S,T} = \begin{cases} \sum_{T \subseteq X \subseteq S} f(X), & T \subseteq S, \\ 0, & \text{otherwise}, \end{cases}$$

and $K_f K_g = K_{fg}$ by similarity. Meanwhile $(I + \delta K_f)(I + \delta K_g) = I + \delta K_{f+g}$ because $\delta^2 = 0$. Conjugated multiplication survives before tagging; its quadratic interaction disappears after using one shared square-zero tag. This is an algebraic explanation, not a new transform algorithm.

**Costs and scope.** An explicit output has $2^n$ ring coordinates, or $4 \cdot 2^n$ bits. A subset butterfly uses $n2^{n-1}$ coefficient additions. The existence of (5.1) does not make the preparation of an unknown truth vector, application of a diagonal oracle, or complete pattern inspection free. Structured symbolic propagation may avoid an explicit table on a particular input, but no universal compact representation or efficient arbitrary coefficient-query algorithm is established here.

## 6 Optimal constant-annihilating detector width

The finite two- and three-variable examples can be closed without an unbounded search. We first freeze the detector contract and then expose its coding-theoretic content.

**Definition 6.1** (Parallel linear pattern detectors)**.** Let $B$ be a finite-dimensional commutative unital $\mathbb{F}_2$-algebra, let $0 \neq \tau \in B$, and set $r = \dim_{\mathbb{F}_2}(\tau B)$. For $f \in \mathbb{F}_2^N$, the tagged pattern is $p_\tau(f)_x = 1 + \tau f_x$. A $c$-channel detector consists of fixed weights $w_{j,x} \in B$ and outputs

$$D_j(f) = \sum_{x=0}^{N-1} w_{j,x}(1 + \tau f_x), \qquad \sum_x w_{j,x} = 0 \quad (1 \leq j \leq c). \tag{6.1}$$

The weights do not depend on $f$. The answer is "constant" exactly when all $c$ outputs vanish, tested by literal pattern inspection. Channels are parallel and no adaptive weight choice or nonlinear preprocessing is included. Width means the number of $B$-valued channels, not oracle-query complexity, gate count, or storage size.

The zero-sum condition makes both constants vanish. For this algebraic definition $1 + \tau$ need not be a unit; if reversible phase tagging is intended it must be a unit. All tags $u, u^2, u^3$ used in $\mathcal{A}$ satisfy that requirement.

**Lemma 6.2** (Forbidden middle weight; classical bound)**.** *If $N$ is a positive multiple of four and a binary linear subspace $C \leq \mathbb{F}_2^N$ contains no vector of weight $N/2$, then* $\dim C \leq N/2$. *The bound is sharp.*

This is the theorem of Enomoto, Frankl, Ito and Nomura [1], also restated as Proposition 2 in Bassalygo, Cohen and Zémor [2]. The result is about forbidden weight, not merely minimum distance. Appendix A gives a self-contained proof of the specialization needed for power-of-two lengths and a kernel containing **1**. The general theorem, rather than a claim to rediscover it, is used below.

**Theorem 6.3** (Exact detector width)**.** *For positive even $N$, under Definition 6.1, the minimum number of channels that separates constant from balanced vectors is*

$$c_{\min}(N,\tau) = \begin{cases} 1, & N \equiv 2 \pmod 4, \\ \lceil N/(2r) \rceil, & N \equiv 0 \pmod 4. \end{cases} \tag{6.2}$$

*In particular, for $\mathcal{A} = \mathbb{F}_2[u]/(u^4)$, $\tau = \delta = u^2$, and $N = 2^n$ with $n \geq 1$,*

$$c_{\min}(n) = \left\lceil 2^{n-2} \right\rceil. \tag{6.3}$$

*Proof.* The zero-sum condition reduces (6.1) to $D_j(f) = \tau \sum_x w_{j,x} f_x$. Thus the combined output is a binary linear map

$$H : \mathbb{F}_2^N \longrightarrow (\tau B)^c, \qquad H\mathbf{1} = 0, \qquad \operatorname{rank} H \leq rc.$$

Exact separation means that $\ker H$ contains no vector of weight $N/2$. If $4 \mid N$, Lemma 6.2 gives $N - \operatorname{rank} H \leq N/2$, so $rc \geq N/2$.

For attainment, put $L = N/2$ and choose $L+1$ distinct addresses $x_0, x_1, \ldots, x_L$. Choose a binary basis $\beta_1, \ldots, \beta_r$ of $\tau B$, together with lifts $v_s \in B$ such that $\tau v_s = \beta_s$. Form the $L$ differences $h_i(f) = f(x_i) + f(x_0)$. Pack at most $r$ differences into each output as $\sum_s \beta_s h_i(f)$. A packed difference is implemented by giving its two addresses the same weight $v_s$; when several use $x_0$, their weights at $x_0$ add. Every row therefore has weight sum zero. Linear independence of the $\beta_s$ makes all outputs zero exactly when all $L$ differences vanish. Then $L+1$ chosen values are identical, impossible for a balanced vector with exactly $L$ zeros and $L$ ones. Constants do vanish. This uses $\lceil L/r \rceil$ channels.

If $N \equiv 2 \pmod 4$, give every address weight 1 in one channel. The output is $\tau \sum_x f_x$, since $N$ is even. Both constants have even weight, but a balanced vector has odd weight $N/2$, so its output is $\tau \neq 0$. Zero channels cannot separate the two nonempty promise classes. Finally $\dim_{\mathbb{F}_2}(\delta\mathcal{A}) = 2$, giving (6.3) including the $N = 2$ case. □

This is a sharp application of a classical coding theorem to a declared channel contract. The elementary packing argument also shows why dividing by the full scalar dimension four would be wrong for $\delta$: every detector output lies in the two-dimensional ideal $\delta\mathcal{A}$.

**Explicit four- and eight-address detectors.** A basis of $\delta\mathcal{A}$ is $\delta, t\delta$, with lifts $1, t$. At four addresses the single row

$$(1+t,\ 1,\ t,\ 0)$$

produces $\delta(f_1 + f_0) + t\delta(f_2 + f_0)$. Vanishing forces three equal bits, excluding balance. At eight addresses use

$$\begin{pmatrix} 1+t & 1 & t & 0 & 0 & 0 & 0 & 0 \\ 1+t & 0 & 0 & 1 & t & 0 & 0 & 0 \end{pmatrix}.$$

Both outputs vanish exactly when $f_0, f_1, f_2, f_3, f_4$ are equal, excluding four-versus-four balance. Theorem 6.3 proves that one channel cannot suffice at eight addresses. At sixteen addresses four are necessary and sufficient; this closes the earlier two- and three-variable examples within the same detector model.

**Corollary 6.4** (Unpromised constancy)**.** *For any $N \geq 2$, the minimum width in Definition 6.1 for recognizing constancy among all Boolean vectors is $\lceil (N-1)/r \rceil$.*

*Proof.* Exactness now requires $\ker H = \operatorname{span}\{\mathbf{1}\}$, so $\operatorname{rank} H = N - 1 \leq rc$. Pack all $N-1$ differences $f(x_i) + f(x_0)$ by the same construction to attain the bound. □

| Variables $n$ | Addresses $N$ | $u$ tag ($r = 3$) | $u^2$ tag ($r = 2$) | $u^3$ tag ($r = 1$) |
|---|---|---|---|---|
| 1 | 2 | 1 | 1 | 1 |
| 2 | 4 | 1 | 1 | 2 |
| 3 | 8 | 2 | 2 | 4 |
| 4 | 16 | 3 | 4 | 8 |
| 5 | 32 | 6 | 8 | 16 |
| 6 | 64 | 11 | 16 | 32 |

These are exact promised-detector widths, not numbers of oracle calls. They quantify information lost through the tag ideal and recovered through parallel coefficient channels. The abrupt $N \equiv 2 \pmod 4$ exception in (6.2) also shows why the address-length hypothesis cannot be dropped in a purported universal lower bound.

# 7 The exact gate boundary for nilpotent interactions

## 7.1 What $\mathcal{A}$-linearity guarantees

Suppose fixed $\mathcal{A}$-linear gates are interleaved with activations $I + u^p D_j$, where the entries of $D_j$ may depend on declared Boolean oracle parameters. Expanding the product, any term with $q$ activations contains $u^{pq}$, since that scalar commutes with every gate. It vanishes for $pq \geq 4$. Thus a shared $u$ tag retains at most three activation factors and a shared $u^2$ tag at most one. This bounds degree in the activation parameters, not degree in the input variables inside each predicate. It is an immediate consequence of nilpotence, not a complexity lower bound.

The $u^2$ case has a sharper characterization even after admitting some non-$\mathcal{A}$-linear binary gates. Let $V = \mathcal{A}^m$ viewed over $\mathbb{F}_2$, let $\Delta$ be multiplication by $\delta$ on every block, and let $K_m = \delta\mathcal{A}^m$.

**Theorem 7.1** (Exact ideal-preservation boundary)**.** *For every binary linear map $G : V \to V$,*

$$\Delta G \Delta = 0 \quad \Longleftrightarrow \quad G(K_m) \subseteq K_m. \tag{7.1}$$

*Consequently, a circuit of binary linear gates preserving $K_m$, interleaved with activations $I + b_j \Delta D_j$, has no term of activation degree at least two whenever the fixed binary maps $D_j$ also preserve $K_m$. Here the $b_j$ are Boolean parameters. The converse holds at the level of permitted gates: if a gate $G$ violates the right side of* (7.1)*, two uniform activations can produce a nonzero mixed coefficient.*

*Proof.* On each block, $\operatorname{im}\Delta = \ker\Delta = K$; hence on $V$ both spaces equal $K_m$. Therefore $\Delta G \Delta = 0$ exactly when $G$ maps $\operatorname{im}\Delta$ into $\ker\Delta$, proving (7.1).

A product of ideal-preserving maps preserves $K_m$. In any expanded term with two consecutive selected activations, the segment between the left factor $\Delta$ and the next factor $\Delta$ is ideal-preserving, including the relevant $D_j$. Equation (7.1) kills that term. Conversely the coefficient of $bc$ in $(I + c\Delta)G(I + b\Delta)$ is $\Delta G \Delta$, nonzero when ideal preservation fails. □

**A reversible star-free counterexample.** On one cyclic block, let $G$ swap $e_1$ and $e_2$ and fix $e_0, e_3$. This is a binary coordinate permutation, with $G^{-1} = G$ and $G^T G = I$. Nevertheless

$$\Delta G \Delta e_0 = \Delta G(e_0 + e_2) = \Delta(e_0 + e_1) = e_0 + e_1 + e_2 + e_3 \neq 0. \tag{7.2}$$

Thus even a reversible, binary-orthogonal, star-free gate can escape the shared-tag interaction obstruction. It is not $\mathcal{A}$-linear and is not an intrinsic ring-unitary map of the declared coefficient module. Calling both models "Boolean" is not enough to transfer a theorem between them.

For one block there are 16 binary maps commuting with $R$, of which eight are invertible. There are 4096 maps preserving $K$, of which 576 are invertible. To see the latter counts, use a binary decomposition $V = K \oplus L$ with two-dimensional summands. Ideal preservation gives a block upper-triangular matrix with three arbitrary $2 \times 2$ blocks, hence $2^{12}$ maps; invertibility requires both diagonal blocks invertible, giving $6^2 \cdot 16 = 576$. The symbol $\oplus$ in this paragraph is a vector-space direct sum, not an additional Boolean connective. Exhaustive enumeration of all 65536 binary maps independently checks (7.1).

### 7.2 Independent tags retain different information

In $\mathcal{A} \otimes_{\mathbb{F}_2} \mathcal{A}$, the element $\delta \otimes \delta$ is nonzero. Under multiplication into one shared copy of $\mathcal{A}$ it becomes $\delta^2 = 0$. Thus independent coefficient registers retain an interaction discarded by shared coefficients. This is a change of tensor base and state space, not an alternative notation for the same circuit. A full tensor of $m$ independent phase algebras has binary dimension $4^m$; compressed representations may behave differently on restricted families, but no universal compression result follows.

Pointwise masking offers another escape, with a different cost. For a tagged Boolean $z^b = 1+\delta b$, selecting its $t^2$ coordinate and rotating that selected coordinate back extracts $b$. Decoding two tags, applying Boolean AND, and retagging computes their conjunction, but the joint map is nonlinear in the two inputs. The linear no-go theorem does not apply to such a decode–AND–retag procedure.

## 8 Interfaces to modal computation and signed lifts

The detector theorem has a different contract from exact modal oracle computation. A zero detector output can be useful information when inspecting a stored pattern, but a zero branch is impossible in the usual modal convention; its absence is not a recorded outcome by itself. A complete linear instrument instead requires the combined map $v \mapsto (L_b v)_b$ to be injective, so every nonzero input has at least one possible branch [7]. One must explicitly build and analyze such an instrument before converting a pattern identity into an exact all-branches-correct algorithm.

This distinction keeps the present paper separate from the companion exact Bernstein–Vazirani query analysis [10]. That work concerns characteristic-two *fields*, recorded complete instruments, and charged pointwise oracle calls. The present work concerns a ring and literal linear detector patterns. A pattern that encodes all affine coefficients after one diagonal phase layer does not refute an $n$-query lower bound under the former readout contract. Nor does a constant-annihilating detector refute a one-query Deutsch–Jozsa obstruction there.

**The supplied analyzer table.** The companion ring example is worth retaining only as a boundary check. With $\chi = (1, z)^T$ and $X = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, one has $X\chi = z\chi$. However

$$H_z = \begin{pmatrix} 1 & 1 \\ 1 & z \end{pmatrix} \sim \operatorname{diag}(1, \delta)$$

by invertible row and column additions. Its $n$-fold Kronecker product over the *shared* ring $\mathcal{A}$, expanded over $\mathbb{F}_2$, has rank $4 + 2n$ for $n \geq 1$: the diagonal factors with zero occurrences of $\delta$ contribute rank four, those with one contribute $2n$, and all others vanish. Its binary dimension is $4 \cdot 2^n$. This explains the supplied ranks $6, 8, 10, 12, 14, 16$ without claiming a Fourier analyzer or importing a field theorem to a ring. The six ranks are independently reconstructed in the revision verifier.

**Changing scalars is not eliminating a primitive.** The signed construction $\mathbb{Z}[C_4]/(1+t^2) \cong \mathbb{Z}[i]$ changes the additive law: $t^2$ becomes $-1$ rather than the distinct half-turn of a characteristic-two ring. There is no unital ring homomorphism from $\mathcal{A}$ into a characteristic-zero ring, since $1 + 1 = 0$ would have to be preserved. A lift from binary patterns into integer coefficients is therefore not an XOR-preserving unital embedding. The signed/integral companion [11] and the present intrinsic algebra can share coordinate notation, but not their amplitude semantics or probability claims.

**Where each paper should own its results.** The CM/LM foundations own predicate semantics, valuation, frame transport and pointwise Boolean superposition [9]. This paper owns the explicitly added cyclic coefficient algebra and its pattern interfaces. The exact-query paper owns its field-valued adaptive lower bounds. The signed paper owns the integer quotient and complex-amplitude translation. Repeating whole modal algorithm or compiler developments across these papers would obscure, rather than strengthen, this separation.

# 9 Evidence, limitations, and use

The original finite verifier and its separate report checker were rerun for this revision. A new standard-library implementation, which imports neither original checker, tests the normal form, ideal boundary, coding subspaces, optimal constructions, and supplied analyzer ranks. The code, complete finite operator inventory, exact output summaries and execution logs accompany the manuscript. Appendix C separates exhaustive universes from bounded regression tests.

The exact detector width closes the original small-example agenda, but its lower-bound engine is classical coding theory. The normal form turns finite involution counts into a transparent proof, without claiming that this small unitary group was previously unknown. The ideal boundary gives a precise test for which broader binary implementations retain the shared-tag truncation. These are concrete reasons to retain the paper as a technical companion rather than discard it as notation alone.

No practical advantage over a matched Boolean compiler or symbolic algebra system is established. A future implementation study would need identical inputs, output contracts, preprocessing and readout costs, including a baseline allowed the same local Boolean identities. Adaptive sparse Möbius learning, for example, already has a substantial algorithmic literature; the recent real-valued additive-query formulation [8] is not an XOR-valued performance baseline without an explicit model translation.

Two focused developments are defensible beyond this note: classify useful restricted gate families between the rotation centralizer and the ideal stabilizer, or identify a concrete retained-information task on which the tag representation improves a matched implementation. A larger brute-force catalog, another spelling of convolution, or an uncharged oracle layer would not establish such an improvement.

# A A self-contained power-of-two coding argument

For the detector application at $N = 2^n$, the kernel contains $\mathbf{1}$. The following proof independently establishes the needed specialization of Lemma 6.2; its statement is already contained in the stronger classical theorem [1].

**Proposition A.1.** *Let $N = 2L$ with $L$ a power of two. If $C \leq \mathbb{F}_2^N$ contains $\mathbf{1}$ and no vector of weight $L$, then* $\dim C \leq L$.

*Proof.* Let $e_L(X)$ be the degree-$L$ elementary symmetric polynomial in $N$ variables and set

$$Q(X) = e_L(X) + e_L(X + \mathbf{1}).$$

Its homogeneous degree-$L$ terms cancel, so $\deg Q \le L - 1$. On a binary vector of weight $w$, $e_L$ has value $\binom{w}{L} \bmod 2$. For $L = 2^a$, the identity $(1+T)^w = \prod_{j:w_j=1}(1+T^{2^j})$ over $\mathbb{F}_2$ shows that this value is the $a$th binary digit of $w$. For $0 \le w \le 2L$, it is one exactly when $L \le w < 2L$. Hence

$$Q(x) = \begin{cases} 0, & \mathrm{wt}(x) \in \{0, L, 2L\}, \\ 1, & \text{otherwise.} \end{cases}$$

Choose $C = \mathrm{span}\{\mathbf{1}\} \oplus W$, and write $m = \dim W = \dim C - 1$. Every nonzero $x \in W$ has weight different from $0, L, 2L$. Therefore $Q$ restricted to $W \cong \mathbb{F}_2^m$ is zero only at the origin. If $m = 0$ the conclusion is immediate. Otherwise its unique multilinear representation is

$$1 + \prod_{j=1}^{m} (1 + Y_j),$$

which has degree $m$. Linear substitution into $Q$ and reduction by $Y_j^2 = Y_j$ cannot increase degree, so $m \le L - 1$. Thus $\dim C = m + 1 \le L$. Uniqueness of multilinear representation follows, for example, by induction on $m$, separating a polynomial into $P_0 + Y_m P_1$ and evaluating at $Y_m = 0, 1$. □

The complementary-space hypothesis is essential to this particular proof presentation. The stronger classical theorem needs no assumption that $\mathbf{1}$ belongs to $C$ and covers every length divisible by four. The sharp construction used in Theorem 6.3 has kernel dimension $N/2$, so no asymptotic estimate is being substituted for the exact finite bound.

## B Local CM nonlinearity and Boolean polynomial compilation

For (2.1), write

$$\alpha = d, \quad \beta = b + d, \quad \gamma = c + d, \quad \kappa = a + b + c + d.$$

Expansion gives

$$f_C(X, Y) = \alpha + \beta X + \gamma Y + \kappa XY. \tag{B.1}$$

The parity $\kappa$ is both the quadratic ANF coefficient of this two-input truth table and its augmentation as a cyclic coefficient. Proposition 2.1 therefore says that the corresponding phase scalar is a unit exactly when this *local two-input predicate* is nonaffine. This does not imply that every substituted expression is nonlinear: substituting the same Boolean variable into both inputs of AND gives $X^2 = X$.

Replacing $X, Y$ by Boolean polynomials $P_X, P_Y$ in (B.1) is a correct local compiler rule in the quotient $X_i^2 = X_i$. Likewise, two CMs on the same ordered operands admit pointwise Boolean folding before expansion. These are exact Boolean identities, not unique compiler optimizations. The finite verifier checks all 64 elementary CM/input cases, 1500 internal nodes across 50 seeded seven-variable DAGs, and 16384 folding valuations. The node count is not a count of 1500 independent programs. Synthetic savings against an intentionally naive expansion backend do not establish practical superiority over optimizers allowed the same identities.

## C Finite verification and reproducibility

| Check | Cases | Scope |
|---|---|---|
| Scalar multiplication | 256 | All ordered pairs |
| Associativity/distributivity | 4096 | All triples |
| Two-branch operators | 65536 | All $\mathrm{Mat}_2(\mathcal{A})$ |
| Binary orthogonality cross-check | 65536 | Separate inherited report checker |
| Phase/ANF identities | 65812 | Every Boolean function, $1 \le n \le 4$ |
| Kickback branch checks | 2120 | Original finite branch universe |
| Subset-kernel multiplication | 65808 | All function pairs, $1 \le n \le 3$ |
| Nilpotent regression circuits | 200 | Bounded seeded tests |
| New binary ideal-boundary test | 65536 | All $\mathrm{Mat}_4(\mathbb{F}_2)$ |
| New unitary normal-form comparison | 65536 | All $\mathrm{Mat}_2(\mathcal{A})$ |
| New subspace enumeration, $N = 2, 4, 8$ | 29230 | All subspaces containing $\mathbf{1}$ |
| New optimal promised detectors | 52776 | Every promised input at even $N \le 16$, three tags |
| New unpromised-constancy detectors | 262140 | Every input at even $N \le 16$, three tags |
| Companion analyzer ranks | 6 | $n = 1, \ldots, 6$ |

The three new tags are $u, u^2, u^3$; repeated input checks with different tags are counted separately. For subspace enumeration the totals are $2, 16, 29212$, respectively, and maximal balanced-avoiding dimensions are $1, 2, 4$. These finite universes do not replace the general proofs. The old two-bit marked-coordinate-peak scan remains bounded evidence for its specified local architecture, not a general search impossibility theorem.

From the package root, the new checks need only a recent Python 3 standard library:

```
python reproducibility/code/verify_revision.py
```

The inherited full inventory uses NumPy and is reproduced by

```
cd reproducibility/legacy
python code/verify_intrinsic.py
python code/check_report.py
```

The canonical revised manuscript is this single file; its bibliography is embedded below. Compile twice with `pdflatex -halt-on-error CM_Phase_Algebra_Revised.tex`. The audit directory contains review responses, overlap and priority records, and a claim crosswalk; it is not part of the submission manuscript. Original inputs and hashes are preserved separately. The verification programs make no network or account calls. Reported execution time is a reproducibility observation, not a benchmark.

**Provenance.** This is an AI-assisted technical revision prepared for author review. Specialist and adversarial assessments in the accompanying report are distinct analytical perspectives from one assistant, not independent external referee reports. Historical firstness, external peer review, and empirical performance superiority are not certified by the supplied tests.

# References


[1] H. Enomoto, P. Frankl, N. Ito and K. Nomura, "Codes with given distances," *Graphs and Combinatorics* **3** (1987), 25–38. https://doi.org/10.1007/BF01788526.

[2] L. Bassalygo, G. Cohen and G. Zémor, "Codes with forbidden distances," *Discrete Mathematics* **213** (2000), 3–11. https://doi.org/10.1016/S0012-365X(99)00161-2.

[3] Z. Balogh and V. Laver, "Unitary subgroups of commutative group algebras of characteristic two," arXiv:2007.05819 (2020). https://arxiv.org/abs/2007.05819.

[4] J. Cruickshank, A. Herman, R. Quinlan and F. Szechtman, "Unitary groups over local rings," arXiv:1303.5106 (2013). https://arxiv.org/abs/1303.5106.

[5] M. Barbier, H. Cheballah and J.-M. Le Bars, "On the computation of the Möbius transform," arXiv:2004.11146 (2020). https://arxiv.org/abs/2004.11146.

[6] B. Schumacher and M. D. Westmoreland, "Modal quantum theory," *Foundations of Physics* **42** (2012), 918–925. https://doi.org/10.1007/s10701-012-9650-z.

[7] B. Schumacher and M. D. Westmoreland, "Almost quantum theory," in *Quantum Theory: Informational Foundations and Foils*, Springer (2016), 45–81; arXiv:1204.0701. https://arxiv.org/abs/1204.0701.

[8] Y. E. Erginbas, J. S. Kang, E. Polito and K. Ramchandran, "Adaptive sparse Möbius transforms for learning polynomials," arXiv:2602.06246 (2026). https://arxiv.org/abs/2602.06246.

[9] B. Droncheff, *Correspondence and Logical Matrices: A Boolean Operator Calculus*. Supplied revised manuscript, September 2026. Cited for the project-specific CM/LM definitions and scope; not asserted to be published.

[10] *Exact Bernstein–Vazirani Query Complexity in Characteristic-Two Modal Computation*. Supplied companion manuscript, revised 27 September 2026. Cited by title as an unpublished project companion.

[11] B. Droncheff, *Signed and Integral Lifts of Correspondence Matrices*. Unpublished project companion, 27 September 2026. The comparison here concerns the scalar construction announced in its abstract.