KITE MATRICES OVER $\mathbb{F}_2$: THE EXACT REACH OF A DOUBLY PERFECT CONSTRUCTION

KOREA SUPERINTELLIGENCE LABS

Abstract. The *kite matrix* A_n is the $n \times n$ zero–one matrix whose (i, j) entry is 1 exactly when $i + j \leq n + 1$. Gross and Goedicke, constructing doubly perfect functions on the discrete phase space $\mathbb{Z}_2^{2n}$ — and through them two-unitary matrices and absolutely maximally entangled states — record as a remark, supported by computer experiments, that the block-diagonal quadratic form built from two copies of A_n appears to give such a function for every $n \not\equiv 1 \pmod 3$; Goedicke's dissertation restates a sibling of that claim, for a single kite of order $2n$, as the only conjecture it puts forward, supported by a search over $n \in [500]$. We prove both, in both directions and for every n. The mechanism is that A_n is the reversed partial-sum operator, so the kernel equation of $A_n + I$ differences to a two-term recursion whose transfer matrix is the signed Fibonacci matrix $M = \left(\begin{smallmatrix} 1 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, and $M^3 = -I$ over every commutative ring. The orbit therefore has period six, and matching it against the closing condition leaves exactly the residues $n \equiv 1, 4 \pmod 6$; over $\mathbb{F}_2$ both are carried by the single factor $A_n + I$, and their union is $n \equiv 1 \pmod 3$. We also settle the same matrices over $\mathbb{Z}$, where the two residues split between the two factors of $A_n^2 - I$: $\det(A_n + I) = 0$ exactly when $n \equiv 4 \pmod 6$ and $\det(A_n - I) = 0$ exactly when $n \equiv 1 \pmod 6$, so that $\det(A_n^2 - I) = 0$ exactly when $n \equiv 1 \pmod 3$ over $\mathbb{Z}$ as well. The modulus three is thus not a feature of characteristic two; what characteristic two does is merge the two factors. Every theorem below is machine-checked in Lean 4.

1. Introduction

The construction. Fix $d \geq 2$ and $n \geq 1$ and let $V = \mathbb{Z}_d^{2n}$ be a discrete phase space. Gross and Goedicke [1] call a function $\lambda \colon V \to \mathbb{C}$ *doubly perfect* when $|\lambda| = 1$ and its standard and twisted autocorrelations both equal $d^{2n}\delta$, that is, vanish away from the origin; such functions are exactly the ones that make an associated matrix U_λ of size d^{2n} two-unitary on $\mathbb{C}^{d^n} \otimes \mathbb{C}^{d^n}$, and hence produce perfect tensors and absolutely maximally entangled states. The name is [1]'s own: it records that Rather [5] had proposed *perfectly perfect* for this class — perfect functions with no twisted autocorrelation — and opts for *doubly perfect* instead. The two-unitary route these functions belong to is the one along which the AME$(4, 6)$ state — the thirty-six officers of the title of [1] — was found [4]. Their construction proceeds through a quadratic ansatz. For a symmetric $N \in \mathbb{Z}_d^{2n \times 2n}$ put $\lambda(a) = \tau^{a^{\mathsf{T}} N a}$, with τ the root of unity fixed in [1]. Both autocorrelations then reduce to Gauss sums, and [1] obtains a criterion that is pure linear algebra. We quote it verbatim from v2 of the electronic preprint, from the passage immediately following the display that introduces the quadratic ansatz:

Date: August 30, 2026.

> "If $N \in \mathbb{Z}_d^{2n\times 2n}$, both auto-correlations reduce to a character sum, and we get the sought-for delta functions if and only if both N and $N + J$ have trivial kernel."

Here $J = \left(\begin{smallmatrix} 0 & I_n \\ -I_n & 0 \end{smallmatrix}\right)$ is the standard symplectic form. The source then specialises the criterion to block-diagonal N, again verbatim:

> "More generally, if $A, B \in \mathbb{Z}_2^{n\times n}$ then $\det \begin{pmatrix} A & I \\ I & B \end{pmatrix} = \det(AB - I)$. Therefore, if A, B are a pair of non-singular symmetric matrices such that $AB - I$ is also non-singular, one obtains a suitable quadratic form by taking N to be the block-diagonal matrix with A, B on the main diagonal."

The determinant identity is Silvester's [3], cited as such at that point in [1]; we have dropped its citation marker from the quotation. The order that matters for the example below is $d = 2$, so that everything above is linear algebra over the field $\mathbb{F}_2$, and that is the register in which the present paper works. We treat the criterion itself as given: nothing below re-proves the passage from the $\mathbb{F}_2$ singularity data to a doubly perfect function, or from there to a two-unitary matrix. Those are the theorems of [1], and they are cited, not reproved. What we settle is the question [1] leaves open, which is a question about matrices.

The kite matrices, and the two claims. Let R be a commutative ring. The *kite matrix* of order n over R is

$$A_n \in R^{n\times n}, \qquad (A_n)_{ij} = \begin{cases} 1, & i + j \le n + 1, \\ 0, & \text{otherwise}, \end{cases} \qquad 1 \le i, j \le n, \tag{1}$$

the all-ones region on and to the upper left of the main antidiagonal $i + j = n + 1$. It is symmetric, and it is a Hankel matrix. The source's example is the following remark, quoted verbatim from the same preprint:

> "As a concrete example, computer experiments indicate that the matrices with "kite-shaped support", $A_{ij} = B_{ij} = 1$ iff $i+j \le n+1$, give a solution for all n not congruent to 1 modulo 3."

Seven months after that version of the preprint appeared, the second author's dissertation [2] restated a sibling of the claim — for a *single* kite of order $2n$ rather than a block-diagonal pair of kites of order n — as the only conjecture the dissertation puts forward as its own, prefaced by the sentence "Lacking a rigorous proof …" and supported by a computer search over $n \in [500]$. We quote its Example 9 and the conjecture that follows it:

> "**Example 9.** Consider $2n \times 2n$-matrices of the form: $N_{ij} = 1$ for $i + j \le 2n - 1$, 0 otherwise. …A computer search showed that these types of matrices generate doubly perfect sequences, if n is not congruent to 1 mod 3, for all $n \in [500]$. …Lacking a rigorous proof that "kite-shaped" matrices generate doubly perfect sequences for all dimensions, one can make the following conjecture: **Conjecture:** For all n not congruent to 1 mod 3, the kite-shaped $2n\times 2n$-matrices over $\mathbb{Z}_2$ generate doubly perfect sequences of length d^{2n}."

(The dissertation indexes from 0, so its condition $i + j \le 2n - 1$ on a matrix of order $2n$ is the support (1) with n replaced by $2n$; the two sources describe the same shape. This is also the only reading that reproduces the dissertation's own

computed answer: read with indices from 1, the matrix of Example 9 has an all-zero last row and is singular for every n.) Thus the two claims are

(P) *the preprint's form*: $N = \mathrm{diag}(A_n, A_n)$ is a symmetric $2n \times 2n$ matrix over $\mathbb{F}_2$ with N and $N + J$ both nonsingular, for all $n \not\equiv 1 \pmod 3$;

(D) *the dissertation's form*: the single kite $N = A_{2n}$ over $\mathbb{F}_2$ is symmetric with N and $N + J$ both nonsingular, for all $n \not\equiv 1 \pmod 3$.

Both were open: (P) is offered as the output of computer experiments, and (D) is stated as a conjecture. Neither source claims a converse.

Results. We prove (P) and (D), in both directions, for every n, and we determine the same matrices over $\mathbb{Z}$.

- **Characteristic two** (Theorems 9, 10 and 11). Over $\mathbb{F}_2$, $A_n + I$ is singular exactly when $n \equiv 1 \pmod 3$; equivalently $A_n^2 - I$ — the matrix $AB - I$ of the source's own reduction, with $A = B = A_n$ — is nonsingular exactly when $n \not\equiv 1 \pmod 3$; and the full datum $N = \mathrm{diag}(A_n, A_n)$ asked for by the criterion of [1] satisfies its three conditions exactly when $n \not\equiv 1 \pmod 3$. This is (P), with its converse.
- **The dissertation's conjecture** (Theorem 18). The single kite A_{2n} over $\mathbb{F}_2$ satisfies the same three conditions exactly when $n \not\equiv 1 \pmod 3$. This is (D), with its converse. The reduction of (D) to (P) is not formal: the two matrices are different, and Lemma 17 is what connects them.
- **Over the integers** (Theorems 20, 22 and 23). Over $\mathbb{Z}$, $\det(A_n + I) = 0$ exactly when $n \equiv 4 \pmod 6$ and $\det(A_n - I) = 0$ exactly when $n \equiv 1 \pmod 6$. Consequently $\det(A_n^2 - I) = 0$ over $\mathbb{Z}$ exactly when $n \equiv 1 \pmod 3$: the source's own condition, with the source's own modulus, over the integers. Neither source considers the integer matrix.

The last item is what explains the modulus. The kernel recursion has a transfer matrix whose cube is $-I$, so the natural period is six and the natural answer is a pair of residues modulo 6, namely 1 and 4. Over $\mathbb{Z}$ the matrix $A_n^2 - I$ factors as $(A_n - I)(A_n + I)$ and the two residues are carried one by each factor. In characteristic two the two factors coincide, $A_n^2 - I = (A_n + I)^2$, and the single factor $A_n + I$ carries both residues; $\{1, 4\}$ mod 6 is $\{1\}$ mod 3, and that is the modulus in the source's remark. So the congruence of [1] is not an artefact of characteristic two — what characteristic two does is merge the factors.

What is new here, and what is not. The existence of doubly perfect functions on $\mathbb{Z}_2^{2n}$ is *not* new: [1] proves, by a construction that involves no kite, that they exist for every $n > 1$. Nothing below improves on that, and no absolutely maximally entangled state is constructed here that was not already available. What is new is the exact reach of the kite family: which n the concrete construction of [1] and [2] does and does not cover, proved rather than sampled, and in both directions.

The linear algebra used to get there is elementary, and we say so plainly. Its nearest relative is the folklore fact that over $\mathbb{F}_2$ the "Lights Out" matrix $I + P_n$, with P_n the adjacency matrix of the path on n vertices, is singular exactly when $n \equiv 2 \pmod 3$: writing $D_n = \det(I + P_n)$ and expanding along the last row gives $D_n = D_{n-1} + D_{n-2}$ over $\mathbb{F}_2$ with $D_0 = D_1 = 1$, so $D_n = 0$ exactly at $n \equiv 2 \pmod 3$. That runs on the same engine as the present paper: a two-term $\mathbb{F}_2$ recursion whose transfer matrix has multiplicative order three. Statements of this kind belong to the σ-automaton polynomial calculus of Sutner [6]. That the Fibonacci matrix $\left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right)$

has order 3 over $\mathbb{F}_2$ is the Pisano period $\pi(2) = 3$ and is classical. The kite *shape* also occurs elsewhere without the questions asked here: Dalfó and Fiol [7] use the anti-triangular all-ones matrix with $(T)_{ij} = 1$ iff $i + j \geq n + 1$ in a real spectral analysis of pancake graphs, and make no determinant or congruence claim about it.

The search recorded in the development's own notes — of electronic-preprint metadata and full texts, of a local 881,145-document preprint corpus, and of OEIS — did not turn up the statements of Theorems 9, 20 or 22 in print; in particular neither integer determinant sequence appears in OEIS as a matrix determinant, although OEIS does collect $\mathbb{F}_2$-nullity sequences of structured matrices, for instance [8]. That search was not exhaustive — reviewing databases such as MathSciNet and zbMATH, journal-only combinatorial matrix theory, textbooks and problem collections, and non-English literature were not covered — so the honest reading of the negative is "not found written down", not "hard". What lifts these statements above folklore is not their difficulty but their status: the people who own the object searched to $n \in [500]$ and published the claim as a conjecture.

2. Preliminaries

Throughout, R is a commutative ring, $n \geq 0$, and $A_n = A_n(R)$ is the kite matrix (1). Vectors are column vectors indexed by $1, \ldots, n$, and for $x \in R^n$ we write

$$S_k(x) = x_1 + \cdots + x_k \qquad (0 \leq k \leq n), \qquad S_0(x) = 0,$$

for its partial sums; we drop the argument and write S_k when x is clear. We write I for an identity matrix of whatever size the context forces, and $J = \left(\begin{smallmatrix} 0 & I_n \\ -I_n & 0 \end{smallmatrix}\right)$ for the standard symplectic form on a space of even dimension $2n$; over $\mathbb{F}_2$ one has $-I = I$, so there $J = \left(\begin{smallmatrix} 0 & I \\ I & 0 \end{smallmatrix}\right)$ is the permutation matrix of the half swap σ, where $\sigma(i) = i + n$ for $1 \leq i \leq n$ and $\sigma(i) = i - n$ for $n < i \leq 2n$. For matrices X, Y of order n we write $\operatorname{diag}(X, Y) = \left(\begin{smallmatrix} X & 0 \\ 0 & Y \end{smallmatrix}\right)$.

We use throughout the standard fact that a square matrix M over an integral domain satisfies $\det M = 0$ if and only if $Mx = 0$ for some $x \neq 0$; over a field "trivial kernel" and "nonzero determinant" are therefore interchangeable, and we use both. All congruences are between integers.

The first observation is the one the source itself makes.

Proposition 1 (Symmetry)**.** *For every commutative ring R and every n, the kite matrix is symmetric: $A_n^{\mathsf{T}} = A_n$.*

Proof. The defining condition $i + j \leq n + 1$ of (1) is symmetric in i and j. □

3. The kite matrix is the reversed partial-sum operator

Everything in this paper comes out of one line.

Lemma 2. *For every commutative ring R, every n, every $x \in R^n$ and every $1 \leq i \leq n$,*

$$(A_n x)_i = S_{n+1-i}(x).$$

Proof. Row i of A_n has a 1 in column j exactly when $j \leq n + 1 - i$. □

So A_n sends x to the reversal of its sequence of partial sums. Two consequences are immediate.

Proposition 3. *Over every commutative ring R and for every n, the kite matrix has trivial kernel: if $A_n x = 0$ then $x = 0$. In particular $\det A_n \neq 0$ whenever R is an integral domain.*

Proof. By Lemma 2, $A_n x = 0$ says $S_k(x) = 0$ for $1 \le k \le n$; then $x_k = S_k - S_{k-1} = 0$ for every k. □

Proposition 4 (Determinant of the kite)**.** *Over $\mathbb{F}_2$, $\det A_n = 1$ for every n.*

Proof. By Proposition 3 the determinant is nonzero, and $\mathbb{F}_2$ has only the values 0 and 1. (Over $\mathbb{Z}$ the determinant is ± 1: reversing the order of the rows turns A_n into the lower-triangular all-ones matrix.) □

Proposition 4 disposes of one of the two hypotheses in the source's reduction: the pair $A = B = A_n$ is symmetric and nonsingular for *every* n, so the entire obstruction sits in $AB - I = A_n^2 - I$. We record this as Proposition 15 below.

We turn to $A_n + I$. Let x satisfy $(A_n + I)x = 0$. By Lemma 2 this is the system

$$S_{n+1-i} = -x_i \qquad (1 \le i \le n). \tag{2}$$

Lemma 5 (Forward and backward steps)**.** *Let $(A_n + I)x = 0$. Then for $0 \le k < n$,*

$$\textit{(i)}\quad S_{k+1} = S_k - S_{n-k}, \qquad\qquad \textit{(ii)}\quad S_{n-k-1} = S_k.$$

Proof. (i) is (2) at $i = k + 1$ substituted into $S_{k+1} = S_k + x_{k+1}$. For (ii), apply (i) at the index $n - k - 1$, which is legitimate since $0 \le n - k - 1 < n$:

$$S_{n-k} = S_{n-k-1} - S_{n-(n-k-1)} = S_{n-k-1} - S_{k+1}.$$

Substituting (i) for S_{k+1} turns the right-hand side into $S_{n-k-1} - S_k + S_{n-k}$, and cancelling S_{n-k} gives $S_{n-k-1} = S_k$. □

Remark 6. Lemma 5(ii) is the step that makes the system two-term, and it is worth saying which state it is about. The natural-looking move — pairing an entry with the entry at the mirrored index, (x_k, x_{n+1-k}) — does not close: the kernel equation (2) does not force $x_{n+1-k} = x_k$, and the "consistency" one is tempted to impose on such a pair is a tautology and constrains nothing. The state that does close is a partial sum paired with a partial sum counted from the far end, and (ii) is the assertion that the second coordinate of that state is the previous value of the first.

4. The orbit

Write

$$(u_k, w_k) := (S_k,\, S_{n-k}) \qquad (0 \le k \le n), \qquad a := S_n.$$

Lemma 5 says exactly that

$$\begin{pmatrix} u_{k+1} \\ w_{k+1} \end{pmatrix} = M \begin{pmatrix} u_k \\ w_k \end{pmatrix}, \qquad M = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}, \tag{3}$$

a signed Fibonacci transfer matrix — over $\mathbb{F}_2$, where $-1 = 1$, it is the Fibonacci matrix $\left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ itself — with initial state $(u_0, w_0) = (0, a)$. Since $M^3 = -I$, the orbit has period 6 and is

$$(0,a),\ (-a,0),\ (-a,-a),\ (0,-a),\ (a,0),\ (a,a),\ (0,a),\ \ldots \tag{4}$$

The system closes at $k = n$, where by definition $(u_n, w_n) = (S_n, S_0) = (a, 0)$. Matching this against (4) gives the table

$n \bmod 6$	0	1	2	3	4	5
orbit value	$(0,a)$	$(-a,0)$	$(-a,-a)$	$(0,-a)$	$(a,0)$	(a,a)
forces	$a=0$	$2a=0$	$a=0$	$a=0$	—	$a=0$

Lemma 7. *Let R be a commutative ring and $(A_n+I)x=0$, and put $a=S_n(x)$.*

(1) *If $n \not\equiv 1$ and $n \not\equiv 4 \pmod 6$, then $a=0$.*
(2) *If $n \equiv 1 \pmod 6$, then $2a=0$.*
(3) *If $a=0$, then $x=0$.*

Proof. (1) and (2) are the last row of the table, read off (4) at the four residues $0,2,3,5$ and at the residue 1 respectively. For (3): if $a=0$ then the whole orbit (4) is $(0,0)$, so $S_k=u_k=0$ for every $0\le k\le n$, and differencing gives $x=0$. □

Lemma 7 carries the whole argument, and it is proved once, over an arbitrary commutative ring. Everything that follows is a matter of reading it in the ring one wants and supplying a kernel vector at the residues it leaves open.

5. Characteristic two: the preprint's remark

Over $\mathbb{F}_2$ the constraint $2a=0$ of Lemma 7(2) is vacuous, so both residues 1 and 4 modulo 6 survive. Their union is a single class modulo 3.

Definition 8. For $n \equiv 1 \pmod 3$ let $v^{(n)} \in \mathbb{F}_2^n$ be the vector

$$v_i^{(n)} = \begin{cases} 0, & i \equiv 2 \pmod 3, \\ 1, & \text{otherwise}, \end{cases} \qquad \text{i.e.} \quad v^{(n)} = (1,0,1,1,0,1,1,0,1,\dots).$$

Theorem 9 (The kite over $\mathbb{F}_2$)**.** *For every n, the matrix A_n+I over $\mathbb{F}_2$ is singular if and only if $n \equiv 1 \pmod 3$.*

Proof. ($\Leftarrow$) A direct computation with $v=v^{(n)}$ shows $S_k(v)=0$ if $k\equiv 0 \pmod 3$ and $S_k(v)=1$ otherwise; since $n\equiv 1 \pmod 3$ one checks that $S_{n+1-i}(v)=v_i$ for every i, which is (2) in characteristic two. As $v_1=1$, the vector is nonzero, so A_n+I is singular.

($\Rightarrow$) Suppose $n \not\equiv 1 \pmod 3$, i.e. $n \bmod 6 \notin \{1,4\}$, and let $(A_n+I)x=0$. By Lemma 7(1), $a=S_n(x)=0$, and then Lemma 7(3) gives $x=0$. So the kernel is trivial and the determinant is nonzero. □

Theorem 10 (The source's $AB-I$ form)**.** *For every n and $A=B=A_n$ over $\mathbb{F}_2$, the matrix $AB-I=A_n^2-I$ is nonsingular if and only if $n \not\equiv 1 \pmod 3$.*

Proof. In characteristic two $A_n^2-I=(A_n+I)^2$, because the cross terms A_n+A_n vanish and $-I=I$. Hence $\det(A_n^2-I)=\det(A_n+I)^2$, which is nonzero exactly when $\det(A_n+I)$ is, and Theorem 9 applies. □

Theorem 10 is literally the content of the source's remark, with the converse added. We now assemble the datum in the form the criterion of [1] asks for, so that no reduction is left implicit.

Theorem 11 (The preprint's datum, decided for every n)**.** *Let A_n be the kite matrix over $\mathbb{F}_2$ and $N=\operatorname{diag}(A_n,A_n)$, a matrix of order $2n$, and let J be the standard symplectic form. Then*

$$N^{\mathsf T}=N, \qquad \det N \neq 0, \qquad \det(N+J)\neq 0$$

all hold if and only if $n \not\equiv 1 \pmod 3$.

Proof. Symmetry of N is Proposition 1, and $\det N = (\det A_n)^2 = 1$ is Proposition 4; both hold unconditionally, so the conjunction is equivalent to its third clause. Over $\mathbb{F}_2$ we have $-I = I$, so $N + J = \left(\begin{smallmatrix} A_n & I \\ I & A_n \end{smallmatrix}\right)$, and since A_n is invertible Silvester's identity [3] gives $\det(N + J) = \det(A_n^2 - I)$. Now apply Theorem 10. □

By the criterion of [1] quoted in Section 1, Theorem 11 says that $\lambda(a) = \tau^{a^{\mathsf{T}} N a}$ is a doubly perfect function on $\mathbb{Z}_2^{2n}$ exactly for $n \not\equiv 1 \pmod 3$: the claim of the remark, together with the converse that the remark does not assert.

Remark 12. The excluded residue contains $n = 1$, and there the exclusion is forced for a reason [1] supplies independently: for $n = 1$ one has $\det(N + J) = \det N + 1$, so the criterion asks that $\det N$ and $\det N + 1$ both be coprime to d; two consecutive integers are never both odd, so for even d — in particular for the $d = 2$ of Theorem 11 — *no* symmetric N meets the criterion at $n = 1$. Theorem 11 is consistent with that, and the agreement is a control we did not arrange.

Controls. The statements above are equivalences, so they are exposed to two kinds of error: a claim that is too large (the construction works for all n) and one that is too small (only some sub-family of the excluded n actually fails). We record the small-n data, computed independently of Sections 3–4, and the two refutations.

Proposition 13 (Small-n certificates)**.** *For $n = 1, \dots, 7$, the kernel of $A_n + I$ over $\mathbb{F}_2$ is trivial exactly for $n = 2, 3, 5, 6$; at $n = 1, 4, 7$ the vectors*

$$(1), \qquad (1, 0, 1, 1), \qquad (1, 0, 1, 1, 0, 1, 1)$$

lie in the kernel and are nonzero. The determinant values that Theorem 9 predicts on this range — $\det(A_n + I) = 0$ for $n = 1, 4, 7$ and $\neq 0$ for $n = 2, 3, 5, 6$ — agree with this table.

Proof. Exhaustive evaluation. For $n = 2, 3, 5, 6$ the assertion "$(A_n + I)x = 0$ implies $x = 0$" is checked by evaluating a matrix–vector product at each of the 2^n vectors of $\mathbb{F}_2^n$ — $4 + 8 + 32 + 64 = 108$ vectors in all — and for $n = 1, 4, 7$ the three exhibited vectors are checked by one product each. This is the only exhaustive search anywhere in the paper, and it uses nothing from Sections 3–4, so it is an independent guard against an off-by-one in the index convention of (1). □

Proposition 14 (Negative controls)**.**
(1) *It is false that $A_n^2 - I$ is nonsingular over $\mathbb{F}_2$ for every n; it is singular at $n = 4$.*
(2) *The set of n at which the construction fails is not $\{1\}$: it contains 4.*
(3) *That set is not a congruence class modulo 2: the construction fails at $n = 1$ and succeeds at $n = 3$, and both are odd.*

Proof. Each item is a specialisation of Theorem 9 or Theorem 10 at the named values of n. For (3), if the failure set were $\{n : n \equiv r \pmod 2\}$ then $r = 1 \bmod 2$ by the failure at $n = 1$, whence $n = 3$ would also fail, contradicting Theorem 9. □

Proposition 15 (Non-vacuity)**.** *The datum of Theorem 11 genuinely holds at $n = 2$: there $N = \operatorname{diag}(A_2, A_2)$ is symmetric with N and $N + J$ both nonsingular over $\mathbb{F}_2$. Moreover $\det A_n \neq 0$ over $\mathbb{F}_2$ for every n, so the hypothesis "A, B nonsingular" of the source's reduction never fails and the whole obstruction is carried by $AB - I$.*

Proof. The first assertion is Theorem 11 at $n = 2$, the second Proposition 4. □

The last control is the sharpest, because it locates what about the kite support is doing the work. Let T_n be the upper-triangular all-ones matrix, $(T_n)_{ij} = 1$ iff $i \le j$. The kite matrix is obtained from T_n by reversing the order of the *columns*, equivalently from the lower-triangular all-ones matrix T_n^{T} by reversing the rows: $A_n = RT_n^{\mathsf{T}}$ with R the antidiagonal permutation matrix. Without that reversal there is no family at all.

Proposition 16 (The antidiagonal support is essential)**.** *Over* $\mathbb{F}_2$, $\det(T_n + I) = 0$ *for every* $n \ge 1$.

Proof. $T_n + I$ is upper triangular and its diagonal entries are $1 + 1 = 0$, so its determinant is the product of zeros. □

So the mod-3 answer of Theorem 9 is a property of the antidiagonal support, not of all-ones triangles in general; it cannot be an instance of a folklore statement about triangular zero–one matrices, because the corresponding triangular family is empty.

6. The single-kite form: the dissertation's conjecture

The dissertation's Example 9 is a different matrix. Where the preprint's datum is $\mathrm{diag}(A_n, A_n)$ — a block-diagonal pair of kites of order n — the dissertation's is the single kite A_{2n} of order $2n$. These are not the same matrix, and (D) does not follow formally from (P). What connects them is a splitting of the kernel equation of $A_{2n} + J$ into two copies of the kernel equation of $A_n + I$.

Recall that over $\mathbb{F}_2$ the symplectic form on $\mathbb{F}_2^{2n}$ is the permutation matrix of $i \mapsto i + n \pmod{2n}$. Write a vector $x \in \mathbb{F}_2^{2n}$ as a pair of halves, $u = (x_1, \dots, x_n)$ and $v = (x_{n+1}, \dots, x_{2n})$.

Lemma 17 (Half-splitting)**.** *Let* $x \in \mathbb{F}_2^{2n}$ *satisfy* $(A_{2n} + J)x = 0$. *Then*

$$(A_n + I)\, u = 0, \qquad \text{and then} \qquad (A_n + I)\, v = 0.$$

Conversely, if $w \in \mathbb{F}_2^n$ *satisfies* $(A_n + I)w = 0$, *then* $x = (0, w)$ *satisfies* $(A_{2n} + J)x = 0$.

Proof. By Lemma 2 applied in size $2n$, row i of $(A_{2n} + J)x = 0$ reads $S_{2n+1-i}(x) + x_{\sigma(i)} = 0$, with σ the half swap of Section 2. Take $i = n + k$ with $1 \le k \le n$: then $\sigma(i) = k$ and $2n + 1 - i = n + 1 - k$, so the equation is $S_{n+1-k}(x) + x_k = 0$. Every partial sum occurring here has index at most n, so it is a partial sum of u alone; these n equations are exactly (2) for u in characteristic two, i.e. $(A_n + I)u = 0$.

Now take $i = k$ with $1 \le k \le n$: then $\sigma(i) = n + k$ and the equation is $S_{2n+1-k}(x) + x_{n+k} = 0$. Once $u = 0$ we have $S_{n+m}(x) = S_m(v)$ for $0 \le m \le n$, and $2n + 1 - k = n + (n + 1 - k)$, so the equation becomes $S_{n+1-k}(v) + v_k = 0$: that is (2) for v. The converse is the same computation read backwards, with $u = 0$. □

Theorem 18 (The dissertation's conjecture)**.** *Let* $N = A_{2n}$ *be the single kite matrix of order* $2n$ *over* $\mathbb{F}_2$ *and let* J *be the standard symplectic form on* $\mathbb{F}_2^{2n}$. *Then*

$$N^{\mathsf{T}} = N, \qquad \det N \neq 0, \qquad \det(N + J) \neq 0$$

all hold if and only if $n \not\equiv 1 \pmod 3$.

Proof. Symmetry and $\det N = 1$ are Propositions 1 and 4 in size $2n$, and hold for every n; so again the conjunction reduces to its third clause. If $n \not\equiv 1 \pmod 3$ and $(A_{2n} + J)x = 0$, then Lemma 17 gives $(A_n + I)u = 0$ and $(A_n + I)v = 0$, and Theorem 9 forces $u = v = 0$, i.e. $x = 0$. If $n \equiv 1 \pmod 3$, the converse half of Lemma 17 turns the kernel vector $v^{(n)}$ of Definition 8 into the nonzero vector $(0, \dots, 0, v^{(n)}) \in \mathbb{F}_2^{2n}$ in the kernel of $A_{2n} + J$. □

This is the dissertation's conjecture, with the converse it does not state. Note that its kernel vector is explicit: n zeros followed by the pattern $1, 0, 1, 1, 0, 1, \dots$.

Proposition 19 (Controls for the single-kite form)**.** *At $n = 4$ the vector $(0, 0, 0, 0, 1, 0, 1, 1)$ is a nonzero element of the kernel of $A_8 + J$; at $n = 2$ the datum of Theorem 18 holds; and it is false that $\det(A_{2n} + J) \neq 0$ for every n.*

Proof. The first is one matrix–vector product; the second and third are Theorem 18 at $n = 2$ and $n = 4$. The exhibited vector is the one Lemma 17 predicts, namely four zeros followed by $v^{(4)} = (1, 0, 1, 1)$. □

7. Over the integers: where the modulus comes from

Nothing in Sections 3–4 used the base ring, and it is worth asking what the same argument says over $\mathbb{Z}$. There $2a = 0$ is not vacuous, so only one of the two residues survives.

Theorem 20 ($A_n + I$ over $\mathbb{Z}$)**.** *For every n, $\det(A_n + I) = 0$ over $\mathbb{Z}$ if and only if $n \equiv 4 \pmod 6$.*

Proof. ($\Rightarrow$) Let $(A_n + I)x = 0$ over $\mathbb{Z}$ with $x \neq 0$ and $n \not\equiv 4 \pmod 6$. If $n \equiv 1 \pmod 6$ then Lemma 7(2) gives $2a = 0$, hence $a = 0$ in $\mathbb{Z}$; otherwise Lemma 7(1) gives $a = 0$ directly. Either way Lemma 7(3) forces $x = 0$, a contradiction.

($\Leftarrow$) For $n \equiv 4 \pmod 6$ let $z^{(n)} \in \mathbb{Z}^n$ have entries depending only on $i \bmod 6$ through the period-six pattern

$$z_1^{(n)}, \dots, z_6^{(n)} = -1, 0, 1, 1, 0, -1.$$

Its partial sums then depend only on $k \bmod 6$ through $S_0, \dots, S_5 = 0, -1, -1, 0, 1, 1$, and a case check on $i \bmod 6$ shows that $z^{(n)}$ satisfies (2). It is nonzero, so the determinant vanishes. □

Over $\mathbb{F}_2$ the answer was $n \equiv 1 \pmod 3$, that is $n \equiv 1$ or $4 \pmod 6$. So the base ring is not inert here: the residue $n \equiv 1 \pmod 6$ is contributed entirely by the 2-torsion of characteristic two.

Proposition 21 (Base-ring controls)**.** $\det(A_1 + I) = 2$ *over $\mathbb{Z}$. At $n = 7$ the matrix $A_n + I$ is singular over $\mathbb{F}_2$ and nonsingular over $\mathbb{Z}$. More precisely, for every n the two rings disagree — $A_n + I$ singular over $\mathbb{F}_2$, nonsingular over $\mathbb{Z}$ — exactly when $n \equiv 1 \pmod 6$.*

Proof. The first is a 1×1 determinant. The rest is Theorem 9 against Theorem 20: $\{n \equiv 1\ (3)\} \setminus \{n \equiv 4\ (6)\} = \{n \equiv 1\ (6)\}$. □

It is tempting to conclude from Proposition 21 that the modulus 3 of the source's remark is a characteristic-two phenomenon. *That conclusion is false*, and the reason is that the source's condition is on $A_n^2 - I$, not on $A_n + I$. Over $\mathbb{F}_2$ the two are related by $A_n^2 - I = (A_n + I)^2$; over $\mathbb{Z}$ the factorisation is $A_n^2 - I = (A_n - I)(A_n + I)$ instead, and the residue that $A_n + I$ loses is picked up by the other factor.

Theorem 22 ($A_n - I$ over $\mathbb{Z}$)**.** *For every n, $\det(A_n - I) = 0$ over $\mathbb{Z}$ if and only if $n \equiv 1 \pmod 6$.*

Proof. The same calculation with the other sign. If $(A_n - I)x = 0$ then Lemma 2 gives $S_{n+1-i} = x_i$, whence $S_{k+1} = S_k + S_{n-k}$ and, by the same double application as in Lemma 5, $S_{n-k-1} = -S_k$. So $(u_k, w_k) = (S_k, S_{n-k})$ is transported by $M' = \left(\begin{smallmatrix} 1 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, which again satisfies $M'^3 = -I$; the orbit of $(0, a)$ is

$$(0,a),\ (a,0),\ (a,-a),\ (0,-a),\ (-a,0),\ (-a,a),\ (0,a),\ \ldots$$

and closing at $(u_n, w_n) = (a, 0)$ leaves a free at $n \equiv 1 \pmod 6$, forces $2a = 0$ at $n \equiv 4 \pmod 6$, and forces $a = 0$ at the other four residues — the mirror image of the table in Section 4. Over $\mathbb{Z}$, $2a = 0$ gives $a = 0$; and $a = 0$ collapses the orbit, so all partial sums vanish and $x = 0$. Hence the kernel is trivial away from $n \equiv 1 \pmod 6$. At $n \equiv 1 \pmod 6$ the vector whose entries follow the period-six pattern $1, 0, -1, -1, 0, 1$, with partial sums $0, 1, 1, 0, -1, -1$, is a nonzero kernel vector. □

Theorem 23 (The source's condition over $\mathbb{Z}$)**.** *For every n, $\det(A_n^2 - I) = 0$ over $\mathbb{Z}$ if and only if $n \equiv 1 \pmod 3$.*

Proof. Over $\mathbb{Z}$ one has $A_n^2 - I = (A_n - I)(A_n + I)$, so the determinant vanishes exactly when one of the two factor determinants does; by Theorems 20 and 22 that happens exactly when $n \equiv 4 \pmod 6$ or $n \equiv 1 \pmod 6$, i.e. exactly when $n \equiv 1 \pmod 3$. □

So the source's own condition holds over $\mathbb{Z}$ with the same modulus, and the modulus 3 is a period-six phenomenon read modulo the two factors, not an artefact of characteristic two. What characteristic two does is merge the two factors into one.

Proposition 24 (Controls for the two integer factors)**.** *No n makes both $\det(A_n - I)$ and $\det(A_n + I)$ vanish over $\mathbb{Z}$; each vanishes somewhere, at $n = 1$ for the first and $n = 4$ for the second; and $\det(A_2 - I) \neq 0$, so neither factor is identically singular.*

Proof. The residue classes 1 and 4 modulo 6 of Theorems 22 and 20 are disjoint, and $2 \not\equiv 1 \pmod 6$. □

In particular the integer determinant of $A_n^2 - I$ never has a double zero: its two residue classes come one from each factor.

Remark 25 (Numerical data outside the formal development)*.* The following computations were run as a check and are *not* part of the machine verification of Section 8; we report them as measurements only.

(1) *The full criterion, not the reduction.* Before any of the above was proved, a Gaussian elimination over $\mathbb{F}_2$ was run on the full matrices N and $N + J$ of order $2n$ — with $N = \operatorname{diag}(A_n, A_n)$ and J the symplectic form, not on the reduced $A_n^2 - I$ — for $n = 1, \ldots, 60$. The datum fails exactly at $n \equiv 1 \pmod 3$, the nullity of $N + J$ at each failure is exactly 1, and the answer agrees at every n with $\det(A_n^2 - I) \neq 0$, so Silvester's reduction is confirmed numerically as well as invoked. The same run confirms the kernel vectors of Definition 8 at $n = 1, 4, 7, 10, 13$. An independent re-implementation reproduced $\det A_n = 1$, the singularity set, the nullity and the kernel vectors for $n \leq 40$. The single-kite form of Section 6 was gated the same way for $n \leq 40$.

(2) *The integer determinants.* By exact rational elimination, for $n = 1, \dots, 20$,

$$\det(A_n + I) = 2, 1, 1, 0, -1, -1, -2, -1, -1, 0, 1, 1, 2, 1, 1, 0, -1, -1, -2, -1$$

and

$$\det(A_n - I) = 0, -1, 1, -2, 1, -1, 0, 1, -1, 2, -1, 1, 0, -1, 1, -2, 1, -1, 0, 1.$$

Both appear to have period 12, with $\det(A_{n+6} + I) = -\det(A_n + I)$, and each takes the value ± 2 exactly at the residue where the *other* factor vanishes. Only the vanishing sets are proved (Theorems 20 and 22); the closed forms are not.

(3) *Odd characteristic.* Since the entries of both determinant sequences above lie in $\{0, \pm 1, \pm 2\}$ as far as they were computed, an odd prime p divides $\det(A_n^2 - I)$ only when a factor vanishes over $\mathbb{Z}$; measurements for $p = 3, 5$ and $n \leq 16$ agree with the conclusion that Theorem 23 holds verbatim over $\mathbb{F}_p$ for every odd p. That statement is not proved here: it needs the closed forms of item (2).

8. Verification

Every numbered statement above, other than the two remarks, has been formalised and machine-checked in Lean 4 against Mathlib, and the checks are reproducible from the accompanying development; repository reference to be added at submission. The development defines the kite matrix by (1) (indexed from zero, so the support condition reads $i + j < n$), the partial-sum operator, the orbit of Section 4 and the symplectic form in both of its guises, and proves Lemmas 2, 5 and 7 over an arbitrary commutative ring, so that the characteristic-two and integer theorems are two readings of one argument rather than two arguments. No statement in the development mentions a quantum state, a two-unitary matrix or a doubly perfect function: the criterion of [1] that converts Theorems 11 and 18 into statements about $\mathbb{Z}_2^{2n}$ is cited and is the one imported fact, recorded as such in the development's own documentation. There is no search in any general theorem: Theorems 9, 10, 11, 18, 20, 22 and 23 are proofs, general in n. The only exhaustive computation inside the development is Proposition 13, whose four universally quantified clauses range over all 2^n vectors of $\mathbb{F}_2^n$ for $n \leq 7$ and are discharged by kernel reduction, together with the finitely many matrix–vector products of Propositions 13, 14, 15, 21, 19 and 24; all of these are kernel computations, and the development uses no compiled-evaluation tactic anywhere, so it introduces no evaluation axiom. An audit of the axiom set of every statement above returns exactly propositional extensionality, the axiom of choice and quotient soundness, and in particular no incomplete proof. The measurements of Remark 25 are outside this development and are reported as measurements.

9. Open questions

(1) *The exact integer determinants.* Remark 25(2) measures $\det(A_n + I)$ over $\mathbb{Z}$ as a period-12 sequence and $\det(A_n - I)$ as its mirror. Only the vanishing sets are proved. A closed form should follow from the same transfer-matrix computation carried with the determinant rather than the kernel, and it would settle item (2) below.

(2) *Odd characteristic.* Does Theorem 23 hold over $\mathbb{F}_p$ for every odd prime p? Remark 25(3) says yes as far as it was measured, and the argument needs only the divisibility statement that the closed forms of item (1) would supply.

(3) *Other Hankel supports.* Proposition 16 shows that the reversal is what makes the kite family nonempty. For which zero–one Hankel supports is $A + I$ nonsingular over $\mathbb{F}_2$ for a positive density of n? The kite achieves density $2/3$; we do not know what the maximum is, or whether density 1 is attainable by a nondegenerate family.

(4) *The source's own open problem.* The constructions of [1] give complex Hadamard two-unitaries of every order d except those of the form $d = 2d_1$ with d_1 "neither divisible by 2 nor by 3" — equivalently $\gcd(d_1, 6) = 1$ — and for those [1] writes that "it seems plausible that doubly perfect functions also exist for these orders, and we leave their construction as an open problem". The smallest such order at which a two-unitary exists at all is $d = 10$; the only smaller one, $d = 2$, is ruled out because there is no two-unitary on $\mathbb{C}^2 \otimes \mathbb{C}^2$, as [1] itself notes. Nothing here bears on the problem, and by Remark 12 the quadratic ansatz cannot supply the answer at $n = 1$, so a different construction is needed.

References

[1] D. Gross and P. Goedicke, *Thirty-six officers, artisanally entangled*, arXiv:2504.15401 (2025). All quotations are from v2 (20 June 2025), the current version as of 30 August 2026; the preprint carries no journal reference and no DOI beyond `10.48550/arXiv.2504.15401`. The second author is the author of [2], where the initials P. L. A. are the ones used.

[2] P. L. A. Goedicke, *Perfect Tensors from Multiple Angles and (Quantum) Combinatorial Structures in Category Theory*, PhD thesis, Universität zu Köln, 2026 (oral examination 16 January 2026); URN `urn:nbn:de:hbz:38-796688`, `https://kups.ub.uni-koeln.de/79668/`. Example 9 and the Conjecture immediately following it.

[3] J. R. Silvester, *Determinants of block matrices*, The Mathematical Gazette **84** (2000), no. 501, 460–467; DOI 10.2307/3620776.

[4] S. A. Rather, A. Burchardt, W. Bruzda, G. Rajchel-Mieldzioć, A. Lakshminarayan and K. Życzkowski, *Thirty-six entangled officers of Euler: Quantum solution to a classically impossible problem*, Phys. Rev. Lett. **128** (2022), 080507; arXiv:2104.05122.

[5] S. A. Rather, *Construction of perfect tensors using biunimodular vectors*, Quantum **8** (2024), 1528; DOI 10.22331/q-2024-11-20-1528; arXiv:2309.01504.

[6] K. Sutner, *σ-automata and Chebyshev polynomials*, Theoret. Comput. Sci. **230** (2000), no. 1–2, 49–73; DOI 10.1016/S0304-3975(97)00242-9. Cited for the σ-automaton polynomial calculus only; the path determinant recursion used in Section 1 is proved there in three lines rather than quoted.

[7] C. Dalfó and M. A. Fiol, *Spectra and eigenspaces from regular partitions of Cayley (di)graphs of permutation groups*, arXiv:1906.05851 (2019). The anti-triangular all-ones matrix appears in its Proposition 2.2, with $(T_n)_{ij} = 1$ iff $i + j \geq n + 1$, and again in its Proposition 2.3 with the strict condition $i + j > n + 1$.

[8] The On-Line Encyclopedia of Integer Sequences, sequence A165738, *Rank deficiency (= dimension of the null space) of the $n \times n$ "Lights Out" puzzle on a torus*, `https://oeis.org/A165738`. Cited only as an instance of the $\mathbb{F}_2$-nullity sequences that OEIS does record.