hexagon:2611.00505v1

ORTHOGONAL BASES OF SYMMETRIC UNITARY MATRICES IN ODD DIMENSIONS AND THE MIXED-UNITARY RANK OF THE SYMMETRIC WERNER–HOLEVO CHANNEL

Qiyuan Ma
Shanghai Jiao Tong University
mqyqwerty@sjtu.edu.cn
ORCID: 0009-0000-9532-0821

November 15, 2026
Research preprint, version 1.0

Abstract. Let $\mathcal{S}_n$ denote the space of complex symmetric $n \times n$ matrices with the Hilbert–Schmidt inner product. Girard, Leung, Levick, Li, Paulsen, Poon and Watrous showed that the symmetric Werner–Holevo channel on M_n has minimal mixed-unitary rank $\binom{n+1}{2}$ if and only if $\mathcal{S}_n$ admits an orthogonal basis consisting of unitary matrices. They established this for even n and for $n = 3$, and conjectured it for all odd n; Levick and Rahaman settled the case of primes $n \equiv 7 \pmod 8$. We introduce a family of symmetric unitaries ("chirped circulants") for odd n and prove that, for this family, the pairwise orthogonality conditions reduce exactly to a square system of $\frac{n^2-1}{4}$ real equations in as many unknown phases. Using this reduction we give (i) a fully explicit basis for $n = 5$, with all entries in an explicit degree-8 number field and an exact-arithmetic verification, and (ii) a computer-assisted proof, based on the Krawczyk operator evaluated in Arb ball arithmetic, that a symmetric unitary orthogonal basis exists for every odd n with $3 \le n \le 67$. Consequently the conjecture of Girard et al. holds for all $n \le 68$. We also record several obstructions to natural approaches for general odd n, and a further reduction for prime n.

1. Introduction

For a positive integer n let $\mathcal{S}_n = \{X \in M_n(\mathbb{C}) : X^{\mathsf{T}} = X\}$, a complex vector space of dimension $\binom{n+1}{2}$, equipped with the Hilbert–Schmidt inner product $\langle A, B\rangle = \operatorname{tr}(AB^*)$. The following question was asked on MathOverflow in 2018 [6]:

Does $\mathcal{S}_n$ admit an orthogonal basis consisting of unitary matrices?

The question has a quantum-information interpretation. The *symmetric Werner–Holevo channel* [10] is

$$\Phi_0(X) = \frac{\operatorname{tr}(X)\mathbb{1}_n + X^{\mathsf{T}}}{n+1}, \qquad X \in M_n.$$

Its Choi rank is $\binom{n+1}{2}$, and its *mixed-unitary rank* (the least number of unitaries in a decomposition $\Phi_0(X) = \sum_k p_k U_k X U_k^*$) is at least the Choi rank.

Theorem 1 ([2, Theorem 19])**.** *The channel Φ_0 on M_n has mixed-unitary rank $\binom{n+1}{2}$ if and only if $\mathcal{S}_n$ has an orthogonal basis consisting of unitary matrices.*

(Theorem numbers for [2] refer to arXiv:2003.14405.) In [2] such bases are constructed for all even n (Theorem 21 there) and for $n = 3$ (Theorem 23). For odd n only the upper bound $n(n+3)/2$ on the mixed-unitary rank is proved (Theorem 22 there). Based on numerical evidence,

the authors conjecture that Φ_0 has minimal mixed-unitary rank for every n. Numerical (non-rigorous) bases for odd n up to 11 were also reported in [6].

Levick and Rahaman [5, Theorem 3.8, Corollary 3.12] (numbering as in arXiv:2105.00975) extended a construction of Bravyi and Smolin. Using real equiangular projections obtained from a construction of Calderbank, Hardin, Rains, Shor and Sloane [1], they settled the case of primes $n = p \equiv -1 \pmod 8$. Below 70 the odd values of n covered by these results are $n = 3, 7, 23, 31, 47$. We did not find a rigorous treatment of any other odd n in the literature.[1]

Results. For odd n we introduce *chirped circulants*: matrices $D_c C D_c$ with C a symmetric circulant unitary and $D_c = \mathrm{diag}(\omega^{ca^2})$. From $\frac{n+1}{2}$ of them and the n diagonal "shifts" $V \mapsto Z^t V Z^t$ we obtain $\binom{n+1}{2}$ symmetric unitaries.

- **Reduction.** We prove (Theorem 5) that these $\binom{n+1}{2}$ matrices are pairwise orthogonal if and only if $\binom{(n+1)/2}{2}$ explicit scalar quantities E_{ij} vanish. After fixing a gauge, this is a square real system $F : \mathbb{R}^N \to \mathbb{R}^N$ with $N = \frac{n^2-1}{4}$.
- $n = 5$ (Theorem 8). An explicit orthogonal basis of $\mathcal{S}_5$ by symmetric unitaries. All entries lie in the number field $\mathbb{Q}(\zeta_5, \sqrt{4\sqrt{5} - 11})$. The proof is human-readable apart from two clearly marked polynomial identities. We also provide a complete exact-arithmetic verification.
- $3 \le n \le 67$ (Theorem 10). For every odd $n \le 67$ the square system has a solution. The proof is computer-assisted: it applies the Krawczyk operator [4, 7, 8], evaluated rigorously in Arb midpoint–radius arithmetic [3], to an approximate solution.

Corollary 2. *For every positive integer $n \le 68$, the space $\mathcal{S}_n$ has an orthogonal basis of unitary matrices. Equivalently, the symmetric Werner–Holevo channel on M_n has mixed-unitary rank $\binom{n+1}{2}$.*

Proof. For $n = 1$ the claim is trivial ($\mathcal{S}_1 = \mathbb{C}$ with basis $\{1\}$). For even n this is [2, Theorem 21]; for odd $3 \le n \le 67$ it is Theorem 10. Apply Theorem 1. □

The case of general odd n remains open; see Section 5 for a conjecture, obstructions and a reduction for prime n.

2. Chirped circulants and the reduction lemma

Throughout, n is odd, $h = \frac{n-1}{2}$ and $m = h + 1 = \frac{n+1}{2}$. Indices are taken in $\mathbb{Z}_n$, $\omega = e^{2\pi i/n}$, and $2^{-1} = \frac{n+1}{2}$ denotes the inverse of 2 in $\mathbb{Z}_n$. Let $Z = \mathrm{diag}(\omega^a)_{a\in\mathbb{Z}_n}$ and $D_c = \mathrm{diag}(\omega^{ca^2})_{a\in\mathbb{Z}_n}$ for $c \in \mathbb{Z}_n$.

Definition 3. A vector $\mu = (\mu_l)_{l\in\mathbb{Z}_n} \in \mathbb{C}^n$ is *admissible* if $|\mu_l| = 1$ and $\mu_{-l} = \mu_l$ for all l. For admissible μ put

$$k_d = \frac{1}{n} \sum_{l\in\mathbb{Z}_n} \mu_l \, \omega^{ld} \qquad (d \in \mathbb{Z}_n),$$

and let $C(\mu) = (k_{b-a})_{a,b}$ be the associated circulant. Given parameters $c_0, \dots, c_h \in \mathbb{Z}_n$ and admissible $\mu^{(0)}, \dots, \mu^{(h)}$, define

$$V^{(i)} = D_{c_i} \, C(\mu^{(i)}) \, D_{c_i}, \qquad \text{i.e.} \qquad V^{(i)}_{ab} = \omega^{c_i(a^2+b^2)} k^{(i)}_{b-a},$$

and

$$M_{i,t} = Z^t V^{(i)} Z^t, \qquad (M_{i,t})_{ab} = \omega^{t(a+b)} V^{(i)}_{ab} \qquad (0 \le i \le h, \ t \in \mathbb{Z}_n).$$

[1] We searched arXiv, the citations of [2] (via Semantic Scholar) and MathOverflow (as of November 2026). This search is necessarily incomplete.

This gives $mn = \binom{n+1}{2}$ matrices.

Lemma 4. *Each $M_{i,t}$ is symmetric and unitary.*

Proof. With $F = (\omega^{ja}/\sqrt{n})_{j,a}$ we have $C(\mu) = F^* \operatorname{diag}(\mu) F$, so $C(\mu)$ is unitary. Since $\mu_{-l} = \mu_l$ we get $k_{-d} = k_d$, so $C(\mu)$ is symmetric. If U is symmetric unitary and D is diagonal unitary, then DUD is symmetric unitary. Apply this twice. □

Theorem 5 (Reduction)**.** *For $i, j \in \{0, \dots, h\}$ put*

$$E_{ij} = \sum_{d \in \mathbb{Z}_n} \omega^{(c_i - c_j) 2^{-1} d^2} \, k_d^{(i)} \, \overline{k_d^{(j)}}.$$

Then

$$\langle M_{i,t}, M_{j,u} \rangle = E_{ij} \sum_{s \in \mathbb{Z}_n} \omega^{(t-u)s + (c_i - c_j) 2^{-1} s^2}$$

and $E_{ii} = 1$. Consequently the matrices $\{M_{i,t}\}$ are pairwise orthogonal if and only if $E_{ij} = 0$ for all $0 \le i < j \le h$. In that case $\langle M_{i,t}, M_{j,u} \rangle = n \, \delta_{ij} \delta_{tu}$, and $\{M_{i,t}\}$ is an orthogonal basis of $\mathcal{S}_n$ consisting of symmetric unitaries.

Proof. By definition

$$\langle M_{i,t}, M_{j,u} \rangle = \sum_{a,b} \omega^{(t-u)(a+b)} V_{ab}^{(i)} \overline{V_{ab}^{(j)}} = \sum_s \omega^{(t-u)s} G_{ij}(s), \qquad G_{ij}(s) = \sum_a V_{a,s-a}^{(i)} \overline{V_{a,s-a}^{(j)}}.$$

Fix s. Since n is odd, $a \mapsto d = s - 2a$ is a bijection of $\mathbb{Z}_n$. With $b = s - a$ we get $a = 2^{-1}(s - d)$, $b = 2^{-1}(s + d)$, $b - a = d$, and $a^2 + b^2 = 2^{-1}(s^2 + d^2)$. Hence

$$V_{a,s-a}^{(i)} = \omega^{c_i 2^{-1}(s^2 + d^2)} k_d^{(i)}, \qquad G_{ij}(s) = \omega^{(c_i - c_j) 2^{-1} s^2} E_{ij}.$$

This proves the displayed formula. By Parseval, $E_{ii} = \sum_d |k_d^{(i)}|^2 = \frac{1}{n} \sum_l |\mu_l^{(i)}|^2 = 1$, so $\langle M_{i,t}, M_{i,u} \rangle = \sum_s \omega^{(t-u)s} = n \delta_{tu}$.

For $i \ne j$: if $E_{ij} = 0$ the inner products vanish. Conversely, if $\langle M_{i,t}, M_{j,u} \rangle = 0$ for all t, u, then the discrete Fourier transform of $s \mapsto G_{ij}(s)$ vanishes. Hence $G_{ij} \equiv 0$, and so $E_{ij} = 0$.

Finally, $mn = \dim \mathcal{S}_n$ pairwise orthogonal nonzero matrices form a basis. □

Remark 6 (Square system). Multiplying $\mu^{(i)}$ by a unimodular constant multiplies E_{ij} by a unimodular constant, so we may fix $\mu_0^{(i)} = 1$. Write $\mu_l^{(i)} = e^{\mathrm{i}\theta_r^{(i)}}$ with $r = \min(l, n - l)$ and $\theta_0^{(i)} = 0$. The unknowns are then $\theta = (\theta_r^{(i)})_{0 \le i \le h, \, 1 \le r \le h} \in \mathbb{R}^{mh}$. The conditions $\operatorname{Re} E_{ij} = \operatorname{Im} E_{ij} = 0$ $(i < j)$ are $m(m-1) = mh$ real equations. We obtain a smooth map

$$F_n : \mathbb{R}^N \to \mathbb{R}^N, \qquad N = mh = \tfrac{n^2 - 1}{4},$$

whose zeros yield orthogonal bases of $\mathcal{S}_n$ by symmetric unitaries.

Remark 7 (Unbiased-vector form). Set $\rho_i(d) = \omega^{c_i 2^{-1} d^2} k_d^{(i)}$. Then $E_{ij} = \langle \rho_i, \rho_j \rangle_{\mathbb{C}^n}$. Hence the problem is equivalent to finding an orthonormal basis $\rho_0, \dots, \rho_h$ of the space of even functions on $\mathbb{Z}_n$ such that each ρ_i, after removing the chirp $\omega^{c_i 2^{-1} d^2}$, has a Fourier transform of constant modulus. Equivalently, ρ_i is unbiased with respect to the "chirped Fourier basis" $\{\omega^{c_i 2^{-1} d^2 + ld}/\sqrt{n}\}_l$.

3. An explicit basis for $n = 5$

Let $\omega = e^{2\pi i/5}$, $\sqrt{5} = 1 + 2(\omega + \omega^4)$, $\varphi = \frac{1+\sqrt{5}}{2}$, and

$$S = \mathrm{i}\sqrt{11 - 4\sqrt{5}}, \qquad S^2 = 4\sqrt{5} - 11 = 8\omega + 8\omega^4 - 7.$$

All quantities below lie in $K = \mathbb{Q}(\omega, S)$, a field of degree 8 over $\mathbb{Q}$. On K, complex conjugation is the automorphism $\omega \mapsto \omega^4$, $S \mapsto -S$. Put

$$A = 6 + 4\omega + 4\omega^3 - 4\omega^4, \quad B = 2 + 5\omega + 2\omega^2 - 2\omega^3 - 2\omega^4, \quad C = 4\omega + 6\omega^2 - 4\omega^3 + 4\omega^4,$$

$$\mu = \frac{-B + 5\omega S}{2A} = -\tfrac{3}{11} - \tfrac{5}{44}\omega + \tfrac{3}{11}\omega^2 + \tfrac{7}{22}\omega^3 + S\Big(\tfrac{2}{11} + \tfrac{7}{44}\omega - \tfrac{2}{11}\omega^2 - \tfrac{1}{22}\omega^3\Big) \approx -0.887915 + 0.460008\,\mathrm{i},$$

$$C_1 = (4\omega + 2\omega^2 + 4\omega^3) + \mu(2 - 3\omega - 2\omega^2 - 2\omega^4), \qquad C_0 = (6\omega - 2\omega^2 - 4\omega^3) + \mu(8 + 8\omega + 2\omega^2 + 2\omega^4),$$

and $v = -C_0/C_1$:

$$v = -\tfrac{6}{11} - \tfrac{21}{44}\omega - \tfrac{9}{44}\omega^2 - \tfrac{27}{44}\omega^3 + S\Big(\tfrac{4}{11} + \tfrac{25}{44}\omega + \tfrac{17}{44}\omega^2 + \tfrac{7}{44}\omega^3\Big) \approx -0.997329 - 0.073042\,\mathrm{i}.$$

The minimal polynomial of μ over $\mathbb{Q}$ is $176x^8 + 552x^7 + 428x^6 - 546x^5 - 1195x^4 - 546x^3 + 428x^2 + 552x + 176$. It is not monic, so μ is not a root of unity.

Let $(\mu_0, \ldots, \mu_4) = (1, \omega, \mu, \mu, \omega)$, let $k_d = \frac{1}{5}\sum_j \mu_j \omega^{jd}$, and let J be the all-ones matrix. Define

$$V^{(1)} = I + \tfrac{v-1}{5}J, \qquad V^{(2)}_{ab} = \omega^{2(a^2+b^2)} k_{b-a}, \qquad V^{(3)}_{ab} = \omega^{3(a^2+b^2)} k_{3(b-a)},$$

and $M_{i,t} = Z^t V^{(i)} Z^t$ for $i = 1, 2, 3$ and $t \in \mathbb{Z}_5$.

These are chirped circulants with $(c_1, c_2, c_3) = (0, 2, 3)$ (in this section the seeds are indexed $1, 2, 3$ instead of $0, 1, 2$). Here $V^{(1)} = C(\mu^{(1)})$ with $\mu^{(1)} = (v, 1, 1, 1, 1)$. The circulant $(k_{3(b-a)})_{a,b}$ equals $C(\mu^{(3)})$ with $\mu^{(3)}_l = \mu_{2l}$, i.e. $\mu^{(3)} = (1, \mu, \omega, \omega, \mu)$.

Theorem 8. *The* 15 *matrices $M_{i,t}$ are symmetric unitaries and satisfy $\langle M_{i,t}, M_{j,u}\rangle = 5\,\delta_{ij}\delta_{tu}$. Hence they form an orthogonal basis of $\mathcal{S}_5$, and the symmetric Werner–Holevo channel on M_5 has mixed-unitary rank* 15*.*

The theorem can be verified directly: the script `verify_exact.py` works in the ring $\mathbb{Q}[x]/(x^5 - 1)\,[S]/(S^2 - \sigma)$ using rational arithmetic only. It checks symmetry, $MM^* = I$ for all 15 matrices, and all 120 Gram entries. The script `verify_sympy.py` is an independent check via Gröbner reduction (see Section 6). The proof below explains the structure and isolates the two polynomial identities that we checked by computer.

Proof. Step 1 ($|\mu| = 1$). Note that $C = \omega^2\overline{A}$ and $B = \omega^2\overline{B}$. Conjugating $p(z) = Az^2 + Bz + C$ shows that $p(z) = 0$ implies $p(1/\bar{z}) = 0$, so the root set of p is invariant under inversion in the unit circle.

One computes

$$B^2 - 4AC = 25\,\omega^2(8\omega + 8\omega^{-1} - 7) = (5\omega S)^2 \neq 0.$$

Hence μ is a root of p, and the two roots are distinct. Moreover $|A|^2 = 80 - 20\sqrt{5}$ and $|B|^2 = 45 + 20\sqrt{5}$, so $|B|^2 < 4|A|^2$, i.e. $|B/A| < 2$.

Suppose a root z had $|z| \neq 1$. Then the other root is $1/\bar{z}$, and $|B/A| = |z + 1/\bar{z}| = |z| + |z|^{-1} > 2$, a contradiction. Thus $|\mu| = 1$, and $\mu^{(2)}, \mu^{(3)}$ are admissible.

Step 2 ($|v| = 1$). **[Computer-checked identity]** In K one has $C_0\overline{C_0} = C_1\overline{C_1}$ and $C_1 \neq 0$, hence $|v| = 1$. Thus $\mu^{(1)}$ is admissible, and by Lemma 4 all $M_{i,t}$ are symmetric unitaries.

Step 3 (reduction). By Theorem 5 it suffices to show $E_{12} = E_{13} = E_{23} = 0$. Here $k_d^{(1)} = y_d$, with $y_0 = \frac{4+v}{5}$ and $y_d = \frac{v-1}{5}$ for $d \neq 0$, and

$$E_{12} = \sum_d y_d\, \omega^{-d^2} \overline{k_d}, \qquad E_{13} = \sum_d y_d\, \omega^{d^2} \overline{k_{3d}}, \qquad E_{23} = \sum_d \omega^{2d^2} k_d \overline{k_{3d}}.$$

Substituting $d = 2e$ in E_{13} gives $3d = e$ and $d^2 \equiv -e^2$, while $y_{2e} = y_e$; hence $E_{13} = E_{12}$.

[Computer-checked identity] Expanding with $\bar{\mu} = \mu^{-1}$ and $\bar{\omega} = \omega^{-1}$ and reducing modulo Φ_5 gives

$$E_{12} = \frac{C_1 v + C_0}{25\,\omega\,\mu}, \qquad E_{23} = \frac{A\mu^2 + B\mu + C}{25\,\omega\,\mu}.$$

Both numerators vanish by the definitions of μ and v. □

Remark 9. Replacing S by $-S$ (the other root of p) gives a second basis; we checked this numerically. The two computer-checked identities are finite polynomial computations in $\mathbb{Q}(\omega)[S]$. They are verified by `verify_exact.py` (the identity $|C_0|^2 = |C_1|^2$, together with $\mu\bar{\mu} = v\bar{v} = 1$) and by `reduce_eqs.py` (the expansions of E_{12}, E_{23}).

4. Odd $n \leq 67$: a computer-assisted proof

Theorem 10. *For every odd n with $3 \leq n \leq 67$ and the choice $c_i = i$ $(0 \leq i \leq h)$, the system $F_n(\theta) = 0$ of Remark 6 has a solution. Consequently $\mathcal{S}_n$ has an orthogonal basis of $\binom{n+1}{2}$ symmetric unitary matrices.*

4.1. Method.

We use the following classical result [4, 7]; see also [8].

Krawczyk's theorem. *Let $X \subset \mathbb{R}^N$ be a box, $F : X \to \mathbb{R}^N$ continuously differentiable, $\tilde{x} \in X$, and $Y \in \mathbb{R}^{N\times N}$. Let $\mathbf{J}$ be an interval matrix containing the Jacobian $F'(x)$ for every $x \in X$, and put*

$$K(X) = \tilde{x} - YF(\tilde{x}) + (I - Y\mathbf{J})(X - \tilde{x})$$

(evaluated in interval arithmetic). If $K(X) \subseteq \operatorname{int} X$, then F has exactly one zero in X.

For each n we proceed as follows.

1. *Approximate solution.* Starting from random phases, a Levenberg–Marquardt least-squares solve followed by five Newton steps gives $\tilde{x} \in \mathbb{R}^N$ in IEEE double precision, with $\max|F_n(\tilde{x})| \lesssim 10^{-14}$. The numbers $\tilde{x}_k$ are taken as exact binary rationals.
2. *Box.* $X = \tilde{x} + [-r, r]^N$ with $r = 10^{-9}$ (rounded upward to Arb's radius format; the same radius is used for $X - \tilde{x}$).
3. *Rigorous enclosures.* Using Arb [3] through python-flint 0.9.0 [9], at a working precision of 128 bits, we compute an enclosure of $F_n(\tilde{x})$ and an interval matrix $\mathbf{J}$ enclosing $F_n'(X)$:
   - the roots of unity $\omega^k = \exp(\pi\mathrm{i} \cdot 2k/n)$ and the phases $e^{\mathrm{i}\theta}$ are evaluated as rigorous complex balls;
   - the entries of F_n' are given by the explicit formulas
   $$\partial k_d^{(i)}/\partial\theta_r^{(i)} = \tfrac{\mathrm{i}}{n} \textstyle\sum_{l:\,\min(l,n-l)=r} \mu_l^{(i)} \omega^{ld},$$
   combined by the product rule in E_{ij}.
4. *Preconditioner.* Y is the floating-point inverse of $F_n'(\tilde{x})$, converted exactly to a ball matrix. Any real Y is admissible in the theorem.
5. *Check.* We evaluate $K(X)$ in ball arithmetic and test $K(X) \subseteq \operatorname{int} X$ componentwise. In every case $\max_k |K(X)_k - \tilde{x}_k|$ (an upper bound computed in ball arithmetic) is at most 2×10^{-12}, far inside the radius 10^{-9}.

4.2. **Results.** Table 1 lists, for each odd $n \le 67$: the dimension $N = \frac{n^2-1}{4}$ of the system; the bound on $\max_k |K(X)_k - \tilde{x}_k|$; and the wall-clock time of `certify.py n --from-center` (excluding Python start-up and imports; almost all of it is the interval phase) on an 8-core Intel Xeon virtual machine (single-threaded). The last column indicates whether the case was covered by [2, 5] ("known") or not ("new"; i.e. not covered by these papers and not found in our literature search). All 33 cases are certified, which proves Theorem 10.

TABLE 1. Krawczyk certification, box radius $r = 10^{-9}$, precision 128 bits. "δ" $= \max_k |K(X)_k - \tilde{x}_k|$ (rigorous upper bound); "s" = seconds.

n	N	δ	s		n	N	δ	s	
3	2	4.646×10^{-16}	0.0	known	37	342	1.275×10^{-13}	0.4	new
5	6	5.619×10^{-15}	0.0	new	39	380	1.386×10^{-13}	0.5	new
7	12	1.360×10^{-15}	0.0	known	41	420	3.365×10^{-13}	0.6	new
9	20	5.107×10^{-15}	0.0	new	43	462	1.840×10^{-13}	0.8	new
11	30	3.553×10^{-15}	0.0	new	45	506	3.970×10^{-13}	1.0	new
13	42	9.263×10^{-15}	0.0	new	47	552	3.566×10^{-13}	1.2	known
15	56	9.963×10^{-15}	0.0	new	49	600	5.444×10^{-13}	1.4	new
17	72	6.560×10^{-15}	0.0	new	51	650	3.357×10^{-13}	1.7	new
19	90	4.204×10^{-14}	0.0	new	53	702	5.442×10^{-13}	2.1	new
21	110	5.123×10^{-14}	0.0	new	55	756	5.458×10^{-13}	2.3	new
23	132	3.152×10^{-14}	0.1	known	57	812	6.198×10^{-13}	2.8	new
25	156	6.686×10^{-14}	0.1	new	59	870	1.630×10^{-12}	3.5	new
27	182	1.696×10^{-13}	0.1	new	61	930	6.108×10^{-13}	4.6	new
29	210	1.325×10^{-13}	0.1	new	63	992	9.658×10^{-13}	4.3	new
31	240	9.280×10^{-14}	0.2	known	65	1056	6.430×10^{-13}	4.9	new
33	272	7.574×10^{-14}	0.2	new	67	1122	1.888×10^{-12}	5.7	new
35	306	3.756×10^{-13}	0.3	new					

Proof of Theorem 10. For each n in Table 1 the inclusion $K(X) \subseteq \operatorname{int} X$ holds. By Krawczyk's theorem F_n has a (unique) zero $\theta^* \in X$. By Remark 6 and Theorem 5, the corresponding matrices $M_{i,t}$ form an orthogonal basis of $\mathcal{S}_n$ by symmetric unitaries. □

4.3. **Consistency checks.** These checks are not part of the proof.

- The analytic Jacobian agrees with central finite differences to about 2.5×10^{-10}, and the ball Jacobian agrees with the floating-point one to about 2×10^{-16} (checked for $n = 7$).
- *Negative control.* Shifting the centre by 10^{-6}, so that the true zero lies outside the box, makes the script report "not certified" (checked for $n = 13$).
- For every n in Table 1, all $\binom{n+1}{2}$ matrices were also assembled in floating point directly from the archived centre (without using the formula for E_{ij}). Their Gram matrix agrees with nI to 5×10^{-13}, and symmetry and unitarity hold to 2×10^{-14}.
- The Jacobians at the solutions are well conditioned (e.g. $\operatorname{cond} F_n'(\tilde{x}) \le 8 \times 10^2$ for $n \le 41$).

5. Remarks, obstructions, and open problems

5.1. **General odd n.** In every case we tried, a handful of random starting points sufficed to find a nondegenerate zero of F_n. This suggests:

Conjecture 11. *For every odd $n \ge 3$, the system $F_n = 0$ (with $c_i = i$) has a nondegenerate real solution. In particular $\mathcal{S}_n$ has an orthogonal basis of symmetric unitaries for every n.*

A natural approach would be a direct algebraic construction or a topological existence argument. We record several obstructions.

(1) *Equal chirp parameters fail.* Suppose all c_i equal c. Let $\varphi_l(d) = \omega^{c2^{-1}d^2+ld}/\sqrt{n}$, and take the orthonormal basis $f_0 = \varphi_0$, $f_l = (\varphi_l + \varphi_{-l})/\sqrt{2}$ $(1 \le l \le h)$ of the even functions. By Remark 7, $|\langle \rho_i, f_0\rangle|^2 = 1/n$ for every i. If $\rho_0, \dots, \rho_h$ were an orthonormal basis of the even functions, the matrix $(\langle \rho_i, f_l\rangle)_{i,l}$ would be unitary. Its 0-th column would then have squared norm $m/n = \frac{n+1}{2n} \neq 1$, a contradiction.

(2) *Pure chirp spectra fail for prime $n = p$.* Suppose every $\mu_l^{(i)} = \omega^{\alpha_i l^2}$ with $\alpha_i \in \mathbb{Z}_p$. If $\alpha_i \neq 0$ then $k_d^{(i)} = \frac{1}{p} g(\alpha_i)\, \omega^{-(4\alpha_i)^{-1}d^2}$, where $g(\alpha) = \sum_l \omega^{\alpha l^2}$ is a quadratic Gauss sum with $|g(\alpha)| = \sqrt{p}$; if $\alpha_i = 0$ then $k_d^{(i)} = \delta_{d,0}$. Hence each E_{ij} is either a value $k_0^{(\cdot)}$ or its conjugate (modulus $p^{-1/2}$ or 1), or equals $p^{-2} g(\alpha_i)\overline{g(\alpha_j)} \sum_d \omega^{\beta d^2}$ for some $\beta \in \mathbb{Z}_p$, of modulus $p^{-1} \cdot \sqrt{p}$ or $p^{-1} \cdot p$. In no case does E_{ij} vanish.

(3) *Tensor products do not close the problem.* Under $M_{n_1 n_2} = M_{n_1} \otimes M_{n_2}$ one has $\mathcal{S}_{n_1 n_2} = (\mathcal{S}_{n_1} \otimes \mathcal{S}_{n_2}) \oplus (\mathcal{K}_{n_1} \otimes \mathcal{K}_{n_2})$, where $\mathcal{K}$ denotes antisymmetric matrices. Since antisymmetric matrices of odd size are singular, $\mathcal{K}_{n_i}$ contains no unitaries when n_i is odd. So bases for odd n_1, n_2 do not directly yield one for $n_1 n_2$.

(4) *No degree argument.* F_n is 2π-periodic in each variable, so it induces a map from the compact torus T^N to $\mathbb{R}^N$. Such a map is never surjective, so its degree is 0: if 0 is a regular value, the zeros on T^N counted with the sign of $\det F_n'$ sum to 0. Hence existence of zeros cannot be obtained from a global degree count alone.

5.2. **A further reduction for prime $n = p$.** For $u \in \mathbb{Z}_p^*$ let $(P_u\rho)(d) = \rho(u^{-1}d)$. Since even functions are fixed by P_{-1}, P_u depends only on the class of u in $H = \mathbb{Z}_p^*/\{\pm 1\}$, a group of order h. In the notation of Remark 7:

Proposition 12. *Let p be an odd prime. Take the chirp parameters $\{0\} \cup \{u^{-2} : u \in H\} = \{0\} \cup \mathrm{QR}_p$. Let $\rho_0 = \delta_0 + \frac{v-1}{p}\mathbf{1}$ with $|v| = 1$, and $\rho_{u^{-2}} = P_u\rho_1$, where $\rho_1(d) = \omega^{2^{-1}d^2} k(d)$ and k has admissible spectrum. Then all ρ_c are admissible for their chirp parameters. Moreover, the orthonormality conditions of Remark 7 reduce to*

$$(A) \quad \langle P_u\rho_1, \rho_1\rangle = 0 \ \ (u \in H \setminus \{1\}), \qquad (B) \quad \langle \rho_0, \rho_1\rangle = 0.$$

Proof. First, $P_u\rho_1(d) = \omega^{u^{-2}2^{-1}d^2} k(u^{-1}d)$. The Fourier spectrum of $k \circ u^{-1}$ is a permutation of that of k, so it is again admissible. Next, ρ_0 corresponds to the circulant with spectrum $(v, 1, \dots, 1)$ and is P_u-invariant. Hence

$$\langle \rho_0, P_u\rho_1\rangle = \langle P_{u^{-1}}\rho_0, \rho_1\rangle = \langle \rho_0, \rho_1\rangle \quad \text{and} \quad \langle P_u\rho_1, P_{u'}\rho_1\rangle = \langle P_{u/u'}\rho_1, \rho_1\rangle.$$

□

Up to gauge this is a square system with about $h+1$ real unknowns (namely v and the phases of the spectrum of k). For $p \le 59$ we found nondegenerate numerical solutions; this is evidence, not proof. For $p = 5$ and $p = 7$ there are solutions (verified numerically to 60 significant digits; we have not written out an exact proof) in which the spectrum of k is a single chirp off the origin, $\mu_l = \omega^{al^2}$ $(l \neq 0)$, with μ_0 free. For $p = 7$ these have $\cos(\arg \mu_0) \in \{-\frac{3}{4}, \frac{1}{8}\}$, and for $p = 5$ we get $\cos(\arg \mu_0) = \frac{13-5\sqrt{5}}{8}$. Numerically, this one-parameter family has no solutions for $11 \le p \le 43$. A heuristic Weil-bound argument suggests that it fails for all large p. Coset-wise (Gauss-period) generalizations of index 2 and 3 produced no solutions in our tests ($p \le 41$). A proof for infinitely many primes along these lines would need a genuinely new explicit family.

6. Reproducibility

The ancillary files contain the following.

- `verify_exact.py`: pure-Python exact verification of Theorem 8 (`fractions` only, about 1 s).
- `verify_sympy.py`: an independent Gröbner-basis verification (about 50 s).
- `reduce_eqs.py`: the expansions in Step 3.
- `certify.py`: the Krawczyk certification.
  - `python3 certify.py n` searches for a solution and certifies it.
  - `python3 certify.py n --from-center` re-certifies the archived centre `centers/cert_sol_n`n`.npy`, which is exactly the centre used for Table 1.
- `logs/`: the original logs and the run used for the table (`recertify_from_centers.out`).

The certification relies on the correctness of Arb's ball arithmetic and of Krawczyk's theorem. Floating-point computations are used only to produce the centre $\tilde{x}$ and the preconditioner Y, neither of which needs to be accurate for the validity of the proof.

Acknowledgements. The author used AI assistance in the literature search, in designing and running the computational experiments, in writing the accompanying verification and certification code, and in drafting the manuscript. The human author is solely responsible for verifying all results, for the correctness of the proofs and computations, and for the final text.
Tools used: Codex (OpenAI) and Claude (Anthropic), used as research and writing assistants. Specific version numbers were not recorded. AI is not listed as an author.

References

[1] A. R. Calderbank, R. H. Hardin, E. M. Rains, P. W. Shor, and N. J. A. Sloane, *A group-theoretic framework for the construction of packings in Grassmannian spaces*, J. Algebraic Combin. **9** (1999), no. 2, 129–140.
[2] Mark Girard, Debbie Leung, Jeremy Levick, Chi-Kwong Li, Vern Paulsen, Yiu Tung Poon, and John Watrous, *On the mixed-unitary rank of quantum channels*, Comm. Math. Phys. **394** (2022), no. 2, 919–951, arXiv:2003.14405.
[3] Fredrik Johansson, *Arb: efficient arbitrary-precision midpoint-radius interval arithmetic*, IEEE Trans. Comput. **66** (2017), no. 8, 1281–1292.
[4] R. Krawczyk, *Newton-Algorithmen zur Bestimmung von Nullstellen mit Fehlerschranken*, Computing **4** (1969), no. 3, 187–201.
[5] Jeremy Levick and Mizanur Rahaman, *An extension of Bravyi–Smolin's construction for UMEBs*, Quantum Inf. Process. **20** (2021), no. 11, Paper No. 369, arXiv:2105.00975.
[6] Luftbahnfahrer, *Existence of orthogonal basis of symmetric $n \times n$ matrices, where each matrix is unitary?*, MathOverflow, question 316985, 2018, https://mathoverflow.net/questions/316985.
[7] R. E. Moore, *A test for existence of solutions to nonlinear systems*, SIAM J. Numer. Anal. **14** (1977), no. 4, 611–615.
[8] Siegfried M. Rump, *Verification methods: rigorous results using floating-point arithmetic*, Acta Numer. **19** (2010), 287–449.
[9] The FLINT team, *python-flint: Python bindings for FLINT (incl. Arb), version 0.9.0*, https://github.com/flintlib/python-flint, PyPI package `python-flint`.
[10] R. F. Werner and A. S. Holevo, *Counterexample to an additivity conjecture for output purity of quantum channels*, J. Math. Phys. **43** (2002), no. 9, 4353–4357.