AN INDEPENDENT CERTIFIED COMPUTATION EXCLUDING FOUR MUTUALLY UNBIASED BASES IN DIMENSION SIX

MANVIR JASWAL

Abstract. We show that there are no four mutually unbiased bases in $\mathbb{C}^6$, so that the maximum number of such bases is three, as Zauner conjectured. The proof is computer-assisted and assumes that the processor, compiler and C library of the computer that ran our computation carried out its binary64 (double-precision) arithmetic correctly. The computation carries out the discretization proof of a recent preprint by OpenAI, which has not appeared in a refereed journal; our programs are written from its text, and we prove every statement of the preprint that our proof uses. Four mutually unbiased bases could be taken to consist of the standard basis, the columns of a complex Hadamard matrix divided by $\sqrt{6}$, and two further bases. Finitely many balls in phase coordinates cover all complex Hadamard matrices of order six up to equivalence, and on each small ball a finite search excludes these two further bases. Every inequality that the programs decide in order to reject a case or to cover a set of matrices is decided in integer arithmetic or in interval arithmetic with outward rounding. The programs, logs and data of the computation are deposited.

Contents

1. Introduction 1
2. The method 4
3. The implementation 9
4. The computation 20
5. Checks 23
6. Concluding remarks 25
7. Data and code 26
Appendix A. The inequalities of the preprint that the programs decide 26
Appendix B. Stage C: the graph search and the exclusion of a record 40
Appendix C. Proofs of the statements of the preprint used in the proof of Theorem 1.1 43
Declarations 63
References 63

1. Introduction

Two orthonormal bases $\mathcal{B}$ and $\mathcal{C}$ of $\mathbb{C}^d$ are *mutually unbiased* if $|\langle b, c\rangle|^2 = 1/d$ for all $b \in \mathcal{B}$ and $c \in \mathcal{C}$. For $d \geq 2$, let $N(d)$ be the largest number of pairwise mutually unbiased bases of

Date: October 20, 2026.

2020 *Mathematics Subject Classification.* Primary 15B34; Secondary 81P15, 65G30, 05B20.

Key words and phrases. Mutually unbiased bases, complex Hadamard matrices, interval arithmetic, computer-assisted proof.

$\mathbb{C}^d$. Then $N(d) \leq d+1$, with equality when d is a prime power [1, 10, 38], and six is the smallest dimension that is not a prime power. Problem 13 of the Open Quantum Problems list asks for $N(d)$ and, already for $d = 6$, whether seven mutually unbiased bases exist [18]. Three mutually unbiased bases of $\mathbb{C}^6$ are obtained from the tensor product $\mathbb{C}^2 \otimes \mathbb{C}^3$ [17], and Zauner conjectured that there are no four [39, 40]; the review of McNulty and Weigert [23] gives the history of the question and the evidence. We prove the conjecture under an assumption on the floating-point arithmetic of the computer on which our computation ran (Theorem 1.1 below). Our computation independently carries out a recent computer-assisted proof of OpenAI [27].

An orthonormal basis of $\mathbb{C}^6$ is unbiased to the standard basis exactly when it consists of the columns of $H/\sqrt{6}$ for a *complex Hadamard matrix* H of order six, a matrix with entries of modulus one and $HH^* = 6I$. Grassl showed that the standard basis and the Fourier basis do not belong to four mutually unbiased bases [7]. Jaming, Matolcsi, Móra, Szöllősi and Weiner extended this to every member of the two-parameter Fourier family of complex Hadamard matrices [12, Theorem 1.4] by a discretization with rigorous error bounds. In this discretization the phases of the vectors unbiased to both bases are divided into bins refined by halving, bins that may contain orthogonal or unbiased vectors are related, and an exhaustive search finds no two further bases [12, Section 3]. Jaming, Matolcsi and Móra proposed carrying out such a discretization for all complex Hadamard matrices of order six and computed its first stage, a cover of these matrices, up to equivalence, by cells of discretized phases [11, Sections 2–4].

Numerical and computer-algebra searches support the conjecture [3, 4, 5]. Butterley and Hall found numerically, and Raynal, Lü and Englert confirmed, that the largest average squared distance between four bases of $\mathbb{C}^6$ is strictly smaller than one, in a measure of Bengtsson et al. in which mutually unbiased bases have distance one [2, 5, 28]. Matolcsi, Matszangosz, Varga and Weiner describe triplets of mutually unbiased bases by Hadamard cubes; they present an algebraic identity, conjectured to hold for every such triplet in dimension six, which together with a further conjecture would imply $N(6) = 3$ [19, Proposition 4.2]. A complete classification of the complex Hadamard matrices of order six, long an open problem, is claimed by Cárdenes Wuttig and Tindall in a recent preprint [6], which has not appeared in a refereed journal and whose arguments we have not checked.

In a preprint dated September 24, 2026 [27], OpenAI carries out a discretization of this kind for all complex Hadamard matrices of order six and concludes that $N(6) = 3$. The upper bound is computer-assisted. The main theorem of the preprint states that, under the arithmetic and compiler conditions of its Appendix A, the complete execution documented in its Section 7.5 certifies that there are no four pairwise mutually unbiased bases in $\mathbb{C}^6$ [27, Theorem 1.1], and OpenAI describes the exclusion as "a complete certified computation under the stated binary64 arithmetic and compiler conditions" [25]. Its programs work in floating point, and their rounding errors are controlled by an a priori analysis [27, Appendix A]. The preprint refers to the code, logs and data of that execution, which had not been published with it as of October 20, 2026. In another preprint, OpenAI has announced a proof that $\mathbb{C}^6$ has no seven mutually unbiased bases [24, Theorem 1.2]; this gives $N(6) \leq 5$ by Weiner's theorem that any d mutually unbiased bases of $\mathbb{C}^d$ extend to a complete set of $d+1$ [37, Corollary 3.4]. OpenAI has formalized the bound $N(6) \leq 5$ in Lean; the formalization's documentation says that it "does not establish the paper's upper bound of three" [26].

Our execution of the discretization proof of [27] uses its method and evaluates the same inequalities, but the programs are ours, written from the text of [27] without access to

its code, and they control rounding in a different way. Since both executions evaluate inequalities of the same lemmas, an error in one of these lemmas would not show up as a disagreement between them; we therefore prove every statement of [27] that our proof uses. Our main result is the following.

Theorem 1.1. *Under Assumption (A) of Section 3.1, there are no four pairwise mutually unbiased bases of* $\mathbb{C}^6$. *Since three such bases exist* [17, Lemma 3], $N(6) = 3$.

Assumption (A) says that the processor, the compiler and the C library used in the computation carried out its floating-point arithmetic as IEEE 754, the C standard and the manuals of the processor specify. The proof (Section 4.3) is computer-assisted. Besides Assumption (A), it rests on the stored outputs of the computation, from which the facts about the computation listed in Section 3.8 are read, and on the properties of the programs listed in Section 3.9; Section 5 says which of these were checked, how, and on how much of the computation.

Like the proof of [27], ours uses no classification. Whether the standard basis and the columns of $H/\sqrt{6}$ belong to four mutually unbiased bases does not change under permutations and rephasings of the rows and columns of H, transposition and complex conjugation. The proof covers the complex Hadamard matrices of order six, modulo these operations, by finitely many balls in phase coordinates, each with a certificate that confines the solutions in the ball, up to these operations, to a neighborhood of a slice of known dimension; [27] calls such a ball a record. Stage A makes records from a cover of the first two rows and columns by seed balls, Stage B refines them to small radius, and Stage C excludes two further bases for all matrices of a small record at once, by a finite search over bins of the phases of candidate vectors. In the computation, 852,120 seed balls gave 46,040 records and then 5,934 records of radius at most 0.02, and Stage C excluded each of these, directly or after one more refinement (Table 1).

Our execution differs from that of [27] in its control of rounding and in several steps of the procedure (Section 3). Every inequality that our programs decide in order to reject a case or to cover a set of matrices is decided in integer arithmetic or in interval arithmetic with outward rounding (Section 3.1), and the complex exponential is enclosed in interval arithmetic by Taylor polynomials (Section 3.2), where [27] bounds the error of its Taylor evaluation a priori [27, Lemma A.2]. Four roundings are not enclosed by the programs and are bounded by hand: those of the centers of the seed balls, of a constant in the enclosure of the exponential, of two coefficients of Stage A, and of the size of a grid of boxes in Stage B (Sections 3.4 and 3.2 and Appendices A.5 and A.6). In Stage B the programs search the whole symmetry group of the problem for earlier records that cover part of a record, where the procedure of [27] may try a limited collection of maps (Section 3.6). In Stage C they use an operator bound computed for each record, without the conditions that [27] imposes on records (Section 3.7). We prove the facts that the implementation adds: every interval endpoint of the computation is finite, the reuse rule of the seed cover is valid, seed balls that Stage A does not finish can be replaced by smaller balls, the records made by Stage B cover their parents in the form in which the programs use them, and the graph search of Stage C is exhaustive (Proposition 3.4 and Lemmas 3.7, 3.8, 3.9 and B.1). The programs are deposited with the logs and data of the computation [13].

Section 2 explains how the proof works and summarizes the method of [27] as far as the programs need it. Section 3 describes the implementation and proves the facts it adds, Section 4 describes the computation and proves Theorem 1.1, Section 5 describes the checks, Section 6 discusses what the result means for the problem, and Section 7 describes the

deposited data. Appendix A states each inequality of [27] that the programs decide and says how the computation decides it, and it proves versions for our programs of statements that [27] formulates for its own programs; Appendix B proves that the graph search is exhaustive and deduces the exclusion of a record, in place of statements of [27] about its own search routine, and Appendix C proves the statements of [27] that the proof uses and that the note does not prove elsewhere (Table 3).

2. The method

The method is that of [27], which builds on the discretization of [12, Section 3] and [11, Sections 2–4]. Its idea comes first (Section 2.1), and the rest of the section fixes the notation and states the method. Table 3 in Appendix C lists, for each statement of [27] that the proof uses, the statement of this note that proves it or, where [27] states it for its own programs, replaces it.

2.1. **How the proof works.** After a unitary change of coordinates, four mutually unbiased bases of $\mathbb{C}^6$ consist of the standard basis, the columns of $H/\sqrt{6}$ for a complex Hadamard matrix H, and two further bases. Such an H is called *extendible*, and it suffices to show that no complex Hadamard matrix of order six is extendible (Section 2.2). Extendibility is preserved by permutations and rephasings of rows and columns, transposition and complex conjugation, and we call matrices related by these operations *equivalent*.

Write $H = e(P)$, where $e(t) = \exp(2\pi i t)$ is applied entrywise to a real *phase matrix* P. The Hadamard condition becomes a system $F(P) = 0$ of real equations. Its solution set has positive dimension, even up to equivalence: it contains the phase matrices of the two-parameter Fourier family [34, Section 5.6.1] and of the four-parameter family proposed by Szöllősi [33], whose existence was proved later by Bondal and Zhdanovskiy (see [23, Section 7.1]). So the proof cannot run through a finite list of matrices. Instead it covers the solution set, up to equivalence, by finitely many balls in phase coordinates, and it shows for each ball at once that no matrix in it is extendible. Phases are taken modulo one, so the solution set is compact and finitely many balls of any fixed radius suffice. What has to be found is a description of the solutions in a ball that lets one inequality speak for all of them.

A *record* gives this description (Section 2.4). It is a ball of radius r about an approximate solution P, together with a matrix T whose k columns approximate tangent directions of the solution set at P, and with constants. Every solution in the ball is equivalent to a solution $P + \delta$ in the ball with δ horizontal (Section 2.2), and for these the constants bound, by a quadratic function of $\|\delta\|$, the part $(I - TT^*)\delta$ of the displacement that the columns of T do not account for. The solutions in the ball therefore lie, up to equivalence, close to a k-dimensional slice through P, and a statement about all of them becomes an inequality in r and in the k tangent coordinates. When $k = 0$ and $\iota + 2Cr < 1$, for the constants ι and C of Section 2.4, the solutions in the ball form at most one point up to equivalence, by (A.4).

The first records are made in two steps. Up to equivalence, the first row and column of a complex Hadamard matrix consist of ones, and its second row and column are then given by nine phases, its *seed coordinates* (Section 2.3). Dividing the range of each phase into 112 bins, the resolution chosen in [27], and discarding boxes by necessary conditions leaves finitely many boxes, which finitely many *seed balls* in $\mathbb{R}^9$ cover: the *seed cover*. On each seed ball, *Stage A* deals with the unknown lower right 4×4 block (Section 2.5). Compressed between two two-dimensional subspaces of $\mathbb{C}^4$ determined by the center of the seed ball, this block is close to $\sqrt{6}$ times a unitary 2×2 matrix V, and the Hadamard equations determine the rest of the block from the first two rows and columns and from V, up to errors bounded

uniformly on the seed ball (Lemmas C.12 and C.16; [27, Lemmas 3.2 and 3.5]). So Stage A covers the unitary group $U(2)$ by cells in four parameters of V. For each cell it shows that no completion of the first two rows and columns has its V in the cell, or makes a record that contains, up to equivalence, every such completion, or divides the cell into 16 smaller cells, or counts the cell unresolved, at the last level or once a limit on its work is reached (Section 3.5). The records of all seed balls form the *atlas*.

Stage C works on one record at a time (Section 2.7). Each vector of a third or fourth basis is unbiased to the standard basis and to the columns of $H/\sqrt{6}$, for some H in the record. Stage C covers the vectors with these two properties by finitely many small balls of vectors. Two of these vector balls are joined by an edge of a graph $\mathcal{O}$ if they may contain orthogonal vectors, and by an edge of a graph $\mathcal{U}$ if they may contain unbiased vectors (unit vectors u, v with $|\langle u, v\rangle|^2 = 1/6$). Two further bases would give two disjoint six-cliques of $\mathcal{O}$ with all 36 edges between them in $\mathcal{U}$, and a search that runs to completion without finding such a configuration *excludes* the record: no matrix in it is extendible. A search stopped by its step limit excludes nothing.

The tests of Stage C must hold for every matrix of the record at once, so their error terms grow with its radius (Appendix A.7), and [27] states Stage C for records of radius at most 0.03. Atlas records have radii up to 0.125. *Stage B* therefore first replaces each atlas record by records of smaller radius (Section 2.6). It divides the tangent coordinates of the record into boxes and covers each box by a record of radius 0.07 (a *mid* record), and then repeats this down to *fine* records of radius 0.016 or 0.02. Equivalent matrices need to be covered only once, so a box may also be covered by the image of an earlier record under the symmetries of the problem.

The tests of Stage C compare a vector with the columns of $e(P+\delta)/\sqrt{6}$ for the matrices $e(P+\delta)$ of the record, through the center $e(P)/\sqrt{6}$. This matrix is unitary only if P is an exact solution, so the error terms of the tests contain its operator norm. The number K is an upper bound for this norm, computed for each record from the constant $\varphi \geq \|F(P)\|$ of its Root certificate (Sections 2.4 and 3.7(iv)).

Two further steps close the gaps. A seed ball on which Stage A does not finish within the limits on its work is replaced by smaller balls (Section 3.5). A record of small radius that Stage C does not exclude is refined once more, and Stage C excludes its children. The proof (Section 4.3) then runs as follows. The seed balls cover the seed coordinates of every complex Hadamard matrix up to equivalence. Stage A covers every matrix whose seed coordinates lie in a seed ball by atlas records. Stage B covers the atlas records by records of small radius, and Stage C excludes each of these directly or through its children.

Tao's matrix S_6 [36] needed special care. On a seed ball that contains it, Stage A leaves cells unresolved even without the limit of Section 3.5(i), while the smaller balls that replace the ball are all resolved. Stage C does not exclude all fine records of radius 0.02 refined from the records of these smaller balls (two trials, Remark 4.2), so the second of the computation's two passes through Stages B and C used the fine radius 0.016. That pass of Stage B made its only new records, one mid and one fine record, around S_6 (Section 4.2 and Remark 4.1). The new fine record around S_6 has $k = 0$. This agrees with the geometry: S_6 has defect zero [34, Section 5.6.4], so it is isolated, and near it the solution set is a single point up to equivalence [35, Theorem 4.2].

2.2. **Normalization.** Phases are measured in cycles, $e(t) = \exp(2\pi i t)$, and e is applied entrywise to vectors and matrices. Given four pairwise mutually unbiased bases, a unitary change of coordinates makes the first one the standard basis, and the second then consists

of the columns of $H/\sqrt{6}$ for a complex Hadamard matrix H. Following [27, Definition 2.1], call H extendible (to four mutually unbiased bases) if the standard basis and the columns of $H/\sqrt{6}$ belong to a family of four pairwise mutually unbiased bases. Extendibility is invariant under permutations and rephasings of rows and columns, complex conjugation and transposition (Lemma C.4; [27, Lemma 2.2]). Matrices related by these operations are equivalent (Section 2.1); this relation is coarser than the usual equivalence of complex Hadamard matrices, which allows only permutations and rephasings. So it suffices to show that no complex Hadamard matrix of order six is extendible.

Write $H = e(P)$ with a real phase matrix $P \in \mathbb{R}^{6\times 6}$, identified with $\mathbb{R}^{36}$ in row-major order and given the Euclidean (Frobenius) norm. A real 6×6 matrix is *horizontal* if all its row and column sums vanish. The orthogonal projection Π onto horizontal matrices is double centering, and $e(P + z)$ is equivalent to $e(P + \Pi z)$ (Lemma C.3; [27, Lemma 2.3]). The Hadamard condition is $F(P) = 0$, where

$$F_{ij}(P) = \frac{1}{2\pi i} \sum_{l=0}^{5} e(P_{il} - P_{jl}) \qquad (0 \le j < i \le 5), \tag{2.1}$$

so that $F(P) \in \mathbb{C}^{15} \cong \mathbb{R}^{30}$.

2.3. **The seed cover.** The seed cover reduces the first two rows and columns of a complex Hadamard matrix to finitely many balls in $\mathbb{R}^9$. By Lemma C.5 ([27, Lemma 2.4]), every complex Hadamard matrix is equivalent to a dephased matrix (first row and column equal to one) whose first two rows have the smallest gap among all pairs of rows and of columns, the gap of a pair being the length of the longest arc of $\mathbb{R}/\mathbb{Z}$ that contains none of its six phase differences. The phases of its second row other than the first entry are, in increasing order, $x_1 \le \cdots \le x_5$, with $1 - x_5$ the gap of the first two rows, and they satisfy the orientation condition $x_1 \le x_5 - x_4$ [27, (2.3)]. Choosing the pair with the smallest gap fixes which two rows come first, and it gives the inequality between the gaps of the first two rows and of the first two columns that the second gap filter below tests. Each phase range $[0, 1]$ is divided into 112 closed bins of width $1/112$, as in [27, (2.6)], where 112 is a parameter choice. A nondecreasing list of bins for $x_1, \ldots, x_5$ determines the *shared phase*, the x_i whose bin has its midpoint nearest to $1/2$ (the first one if there are several), and its index i is the *selected position*. This rule is a parameter choice of [27], and any fixed rule is valid, since it only selects a column. The column of the shared phase is moved to second position, and the last four rows are permuted so that this column has phases 0, the shared phase and $y_2 \le \cdots \le y_5$ [27, Section 2.2]. The nine phases $q = (x_1, \ldots, x_5, y_2, \ldots, y_5) \in [0, 1]^9$ are the *seed coordinates* of the matrix. Through the selected position, they depend on the chosen list of bins. Orthogonality of the first two rows gives a vanishing sum of six exponentials in the phases of the second row, and orthogonality of the first two columns gives another in those of the second column [27, (2.5)].

A list of bins for $x_1, \ldots, x_5$ and a list for the second column, consisting of the bin of the shared phase followed by nondecreasing bins for $y_2, \ldots, y_5$, form a *bin pair*, and the product of its nine bins is its *bin box*. Necessary conditions remove bin pairs whose bin box contains no seed coordinates of a complex Hadamard matrix (Lemmas C.6 to C.9; [27, (2.7) and Lemmas 2.5–2.8]). An orientation filter and a first gap filter apply to the list for x, and a linearized test of the vanishing sum applies to each list. On the pair, a second gap filter tests that the first two columns can have a gap at least that of the first two rows, and two intervals for the shared phase, one from each list, must intersect. Appendix A.2 states these filters and tests. The surviving bin pairs are covered by closed Euclidean balls in $\mathbb{R}^9$ of

radius 0.032, as in [27, Section 2.4], about chosen bin midpoints, the *seed balls*. The radius, a parameter choice of [27], must be at least 3/224, so that the ball about the midpoint of a surviving bin pair covers its bin box, and the excess lets one center serve nearby bin pairs. After the centers are rounded to binary64, radius 0.0320001 suffices [27, Lemma 2.9 and Proposition 2.10]. Thus every complex Hadamard matrix is equivalent to one whose seed coordinates lie in some seed ball (Proposition A.3 for our seed cover).

2.4. **Certified phase balls.** Stages A and B cover sets of complex Hadamard matrices by balls about approximate solutions of $F(P) = 0$, and the following data control every solution in such a ball. A *Root certificate* [27, Definition 4.1] consists of a center $P \in \mathbb{R}^{36}$, a matrix $T \in \mathbb{R}^{36\times k}$ whose columns approximate tangent directions of the solution set of $F = 0$, and nonnegative constants $n_0, \iota, C, \omega, \chi, \kappa, \varphi$. Here $0 \le k \le 10$, as in that definition, and our programs also impose this bound (Appendix A.4); in [27] the constants are called n0, id, C, ort, hor, mnorm and froot. A Root certificate is *certified* if $\|T^*T - I\| \le \omega$ and $\|(I - \Pi)T\| \le \chi$, in operator norm, if $\|F(P)\| \le \varphi$, and if every horizontal δ with $F(P + \delta) = 0$ satisfies the normal bound

$$\|(I - TT^*)\delta\| \le n_0 + \iota \|\delta\| + C \|\delta\|^2,$$

together with two further displacement inequalities of [27, Definition 4.1], restated as (A.3) and (A.4) in Appendix A.4. The center may be an approximate solution. Sufficient conditions for certification are given in Lemma C.23 ([27, Proposition 4.5]), with two admissible choices of the constant C in Lemma C.22 ([27, Lemma 4.4]). They are computable from a matrix $M \in \mathbb{R}^{36\times 30}$ that inverts the derivative of F at P approximately on the horizontal directions normal to the columns of T, and from a bound $\kappa \ge \|M\|$. A *record*, or certified phase ball, is a certified Root certificate together with a radius $r \ge 0$. Its *solution set* is

$$\mathcal{S}(P, r) = \{\, e(P + \delta) : \ \delta \text{ horizontal}, \ \|\delta\| \le r, \ F(P + \delta) = 0 \,\},$$

and a record covers a matrix if the matrix is equivalent to a member of its solution set [27, Definition 4.14]. Permuting rows and columns, transposing and changing the sign of P and T preserve certification with the same constants, and preserve extendibility (Lemma C.24; [27, Lemma 4.7]). A record of center P and radius r is covered by a record of center Q and radius $r + \ell$, where ℓ bounds an aligned distance between the two centers (Lemma C.31; [27, Lemma 4.15]). An aligned distance is a norm $\|\Pi(D_0(gP) - D_0Q - Z)\|$, for a map g of the kind just described and an integer matrix Z, where $(D_0X)_{ij} = X_{ij} - X_{i0} - X_{0j} + X_{00}$.

2.5. **Stage A: completion over a seed ball.** Fix a seed ball. Its center determines the first two rows and columns of a dephased matrix up to a displacement of norm at most $R_s = 2\pi \cdot 0.0320001$ radians, and the lower right 4×4 block is unknown. Let B_0 be the 2×4 block of these first two rows outside the first two columns, and C_0 the 4×2 block of these first two columns outside the first two rows. If both have rank two, compressing the unknown block between the two-dimensional kernels of B_0 and C_0^* gives a 2×2 matrix Y within an explicit distance of $\sqrt{6}$ times a unitary matrix (Lemmas C.11 and C.12; [27, Lemmas 3.1 and 3.2]). This needs two *frame checks* at the seed center: that B_0 and C_0 have rank two, so that the kernels are two-dimensional, and that the bound of [27, (3.10)] for $\operatorname{tr}(6I - Y^*Y)$ is less than 6, so that Y is invertible and lies within an explicit distance of $\sqrt{6}$ times its unitary polar factor. The unitary group $U(2)$ is covered by closed cells of side $1/N_u$ in four phase parameters (Lemma C.13; [27, Lemma 3.3]), for $N_u = 16, 32, \ldots, 512$. For each cell, uniform Taylor estimates (Lemmas C.14, C.15, C.16 and C.17; [27, Lemmas 3.4–3.7]) bound the difference between the unknown block and a block computed from the seed center and

the center of the cell. The requirement that the entries of the unknown block have modulus one then gives two necessary conditions for a *completion* in the cell, that is, a dephased complex Hadamard matrix whose first two rows and columns are those determined by the center, up to a displacement of norm at most R_s, and whose matrix Y has a unitary polar factor with parameters in the cell. They are a norm test and a directional test (both stated in Appendix A.3), the second also using the two vanishing sums (Lemmas C.19 and C.20; [27, Lemmas 3.8 and 3.9 and Corollary 3.10]). A cell that fails one of them contains no completion. A surviving cell is either subdivided or covered by a record: a Root certificate is built near a proposed solution, and a radius is certified that contains every completion in the cell (Lemmas C.25 to C.30 and Lemma A.1; [27, Lemmas 4.8–4.12 and Proposition 4.13]). The record is then added to the *atlas* of Stage A, or merged into an atlas record whose radius is enlarged to cover it (Lemma C.31), and the radii of atlas records do not exceed 0.125, a cap taken from [27] (Section 3.5). A seed ball is *resolved* if it passes the frame checks and every cell is excluded, covered or subdivided within the limits on its work given in Section 3.5, and *unresolved* otherwise. If every seed ball is resolved, the atlas records cover every complex Hadamard matrix of order six up to equivalence (Propositions A.3 and A.4, under the conditions on the arithmetic stated in Section 3.1, and [27, Propositions 3.11 and 4.16] for the programs of [27]).

2.6. **Stage B: refinement.** Stage B replaces records by records of smaller radius [27, Section 5], for the reason given in Section 2.1 ([27, Section 6.1] states Stage C for records of radius at most 0.03). A record (P, R) (the *parent*) is replaced by records of a smaller radius τ (the *children*) as follows. For a solution $e(P + \delta)$ in $\mathcal{S}(P, R)$, the tangent coordinates $\eta = T^*\delta$ lie in a cube, which is divided into boxes of a fixed width, the *tangent grid* of the parent. For a box and a child (Q, r), explicit estimates, the *relation estimates* (Lemmas C.33, C.34 and A.2; [27, Proposition 5.2 and Lemmas 5.3–5.5]), bound the distance from every solution whose tangent coordinates lie in the box to the child's center, and if the bound is at most r, the box is covered by the child. In practice the estimates are turned around. The center Q determines a point η_q in the tangent coordinates of the parent, and for a child of radius r the estimates give a *threshold*: a bound on the distance from η_q, in tangent coordinates, such that every solution whose tangent coordinates lie within that bound of η_q is equivalent to a solution within r of Q. A box is covered by the child if all its points lie within the threshold of η_q (Lemma A.2). For each child, one threshold then decides every box of the parent's grid. Boxes not covered by an existing child are subdivided or receive a new child [27, (5.23) and Lemma 5.6]. The parent is *completed* when every box is covered or shown to contain no tangent coordinates of a solution, and it *fails* if its tangent grid exceeds a size limit or a box remains uncovered at the largest depth of subdivision or, when $k = 0$, at its single box [27, Section 5.6]. If every parent is completed, the union of the children's solution sets contains, up to equivalence, the union of the parents' solution sets (Lemma 3.9; [27, Proposition 5.7]). The atlas is refined twice: to *mid* records of radius 0.07, as in [27, Section 5.6], and then to *fine* records, of radius 0.02 in the first pass of the computation (our choice, for fewer fine records) and 0.016, the fine radius of [27, Section 5.6], in the second, for the reason given in Section 2.1 and Remark 4.2.

2.7. **Stage C: exclusion of two further bases.** Fix a fine record (P, r). Every vector unbiased to the standard basis is, up to a scalar factor of modulus one, of the form $e(\beta)/\sqrt{6}$ with $\beta_0 = 0$. Stage C covers, uniformly for all $H \in \mathcal{S}(P, r)$, the vectors unbiased to the standard basis and to the columns of $H/\sqrt{6}$ [27, Section 6]. Covering these vectors by bins

of phases and searching for two compatible sets of six of them goes back to [12, Section 3] and [11, Section 4], as [27] notes. The phases $\beta_1, \dots, \beta_5$ are binned at the resolutions 12, 24, 48 and 96 of [27, Section 6.3], the four *layers* of bins, and each kept bin of a layer is split into 2^5 bins of the next. Bins are removed by necessary tests (Lemmas C.37, C.39 and C.40; [27, Lemmas 6.1–6.3 and (6.12)–(6.13)]), the bin tests (1)–(3) of Appendix A.7, and the bins kept in the last layer are grouped into *vector balls* of radius less than 0.1 (Lemma C.41; [27, Lemma 6.4]). Two vectors in the same vector ball are neither orthogonal nor unbiased (Lemma C.42; [27, Lemma 6.5]). The vector balls are the vertices of two graphs: an edge of $\mathcal{O}$ joins two balls that may contain orthogonal vectors, and an edge of $\mathcal{U}$ joins two balls that may contain unbiased vectors. An edge is removed only by a necessary test, which may use that the two vectors, one from each ball, are unbiased to the columns of the same matrix $e(P+\delta)/\sqrt{6}$ (Lemmas C.43 and C.44; [27, (6.16) and Lemmas 6.6 and 6.7]). Two further bases would give disjoint sets A, B of six vertices each, both cliques in $\mathcal{O}$, with all 36 pairs in $A \times B$ edges of $\mathcal{U}$. A search for this configuration that runs to completion without finding one proves that no matrix in $\mathcal{S}(P, r)$ is extendible (Lemma B.1 and Proposition B.2). A search stopped by its step limit leaves the record unresolved.

2.8. **Assembly.** If the seed balls cover all seed coordinates, Stage A resolves every seed ball, both refinements complete every parent, and every fine record is either excluded by Stage C or completed as a parent of a further refinement all of whose children Stage C excludes, then no complex Hadamard matrix of order six is extendible, and there are no four mutually unbiased bases in $\mathbb{C}^6$, by the proof of [27, Theorem 7.1]. The inequalities of Sections 2–6 of [27] are statements about real numbers, and the proof needs them to be decided correctly for the binary64 data the programs handle. OpenAI's preprint does this by an a priori analysis of the rounding errors of its programs [27, Appendix A]. We decide every such inequality in exact integer arithmetic where its quantities are integers (Section 3.4), and otherwise in interval arithmetic with outward rounding (Section 3.1). The rounding of the seed centers to binary64 is bounded directly (Section 3.4), and so are the rounding of the constant 10^{-22} of the enclosure of $e(t)$ (Section 3.2), the rounding of the coefficients 1.45 and 0.45 of the covariance of Stage A (Appendix A.5) and the rounding in the size of the tangent grid of Stage B (Appendix A.6).

3. The implementation

The programs are written in C++ from the text of [27]. Where they depart from the procedure of [27] (Sections 3.4 to 3.7), every rejection and every covering is still justified by an inequality of [27] or by Lemmas 3.7, 3.8, 3.9, A.1, A.2 and B.1, which we prove. The properties of the programs that the proofs use are collected as (P1)–(P8) in Section 3.9, and they are cited by these labels from the start of the section.

3.1. **Interval arithmetic.** As in verified computation [30], every real number that enters a decision is represented by an interval $[a, b]$ of binary64 numbers known to contain it, and every complex number by a rectangle of two such intervals. For a binary64 number r, let $\mathrm{next}_{\mathrm{up}}(r)$ and $\mathrm{next}_{\mathrm{down}}(r)$ be the adjacent binary64 numbers above and below r, with $\mathrm{next}_{\mathrm{up}}(r) = +\infty$ for the largest finite r and $\mathrm{next}_{\mathrm{down}}(r) = -\infty$ for the smallest, as for the operations nextUp and nextDown of IEEE 754. Let $\mathrm{fl}(s)$ denote the binary64 number nearest to a real number s (ties to even), or $\pm\infty$, with the sign of s, if $|s| \geq 2^{1024} - 2^{970}$, as rounding to nearest in IEEE 754 specifies.

Lemma 3.1. *If s is real and $r = \mathrm{fl}(s)$ is finite, then* $\mathrm{next}_{\mathrm{down}}(r) \le s \le \mathrm{next}_{\mathrm{up}}(r)$.

Proof. If $s \ge r$, then $s - r$ is at most half the distance from r to $\mathrm{next}_{\mathrm{up}}(r)$, since otherwise $\mathrm{next}_{\mathrm{up}}(r)$ would be nearer to s. So $s < \mathrm{next}_{\mathrm{up}}(r)$. The case $s < r$ is symmetric. The argument does not use equal spacing on the two sides of r, so it holds at powers of two and for subnormal r. □

Each primitive operation $+, -, \times, \div, \sqrt{\ }$ is therefore applied to interval endpoints in binary64 and the result widened outward by one step: the lower endpoint is replaced by its $\mathrm{next}_{\mathrm{down}}$ and the upper endpoint by its $\mathrm{next}_{\mathrm{up}}$. Products and quotients take the minimum and maximum of the four endpoint results. A quotient requires a divisor interval that does not contain 0, and a square root is applied to the nonnegative part of an interval that is known to enclose a nonnegative number. A comparison $x < y$ is accepted only when the upper endpoint for x is below the lower endpoint for y. In particular a cell, bin or edge is rejected only when the inequality that rejects it holds for every point of the enclosures. Integer quantities, such as the bin indices of the seed cover, are handled in integer arithmetic.

Most of the computation uses a cheaper outward step, a coarser form of the computation of successors in rounding to nearest of Rump, Zimmermann, Boldo and Melquiond [31, Algorithm 1]. For finite binary64 r put

$$\mathrm{up}(r) = \mathrm{fl}\big(r + \mathrm{fl}(\mathrm{fl}(|r| \cdot 2^{-52}) + 2^{-1074})\big), \qquad \mathrm{dn}(r) = -\mathrm{up}(-r).$$

Lemma 3.2. *For finite binary64 r,* $\mathrm{up}(r) \ge \mathrm{next}_{\mathrm{up}}(r)$ *and* $\mathrm{dn}(r) \le \mathrm{next}_{\mathrm{down}}(r)$. *Hence Lemma 3.1 holds with* up, dn *in place of* $\mathrm{next}_{\mathrm{up}}, \mathrm{next}_{\mathrm{down}}$.

Proof. Let $\sigma = \mathrm{next}_{\mathrm{up}}(r) - r$, a power of two; if r is the largest finite binary64 number, let instead $\sigma = 2^{971}$, the spacing of the binary64 numbers below 2^{1024}, so that $\mathrm{fl}(r + \sigma) = +\infty = \mathrm{next}_{\mathrm{up}}(r)$. If $|r| \ge 2^{-1022}$ then $\sigma \le |r| \cdot 2^{-52}$, also when r is a negative power of two, where σ is the smaller spacing. Otherwise $\sigma = 2^{-1074}$. The product $|r| \cdot 2^{-52}$ is exact unless it is subnormal, when its rounding error is at most 2^{-1075}. So $\varepsilon = \mathrm{fl}(|r| \cdot 2^{-52})$ satisfies $\varepsilon + 2^{-1074} \ge \sigma$ in both cases. Rounding is monotone and σ is a binary64 number, so $\mathrm{fl}(\varepsilon + 2^{-1074}) \ge \sigma$, and for the same reason $\mathrm{up}(r) \ge \mathrm{fl}(r + \sigma) = \mathrm{next}_{\mathrm{up}}(r)$. The second assertion follows by symmetry. □

Applied to the computation, these two lemmas, and every enclosure built on them, rest on the following assumption about the machine of the computation (Section 4.1) and its C library.

Assumption (A). The processor and compiler of the computation of Section 4 execute the binary64 operations of its programs as IEEE 754 specifies [9], rounding each of the operations $+, -, \times, \div, \sqrt{\ }$ separately to nearest (in particular without contracting a multiplication and an addition into a fused multiply–add), and without flushing subnormal numbers to zero or treating subnormal inputs as zero. The library function `nearbyint`, in the round-to-nearest mode, which the programs never change, returns an integer nearest to its argument, as IEEE 754 and the C standard ISO/IEC 9899:2011 specify. The x87 instruction `fprem`, with which the compiler evaluates `fmod`$(n, 4)$ in Section 3.2, returns its exact result $n - 4q$, where q is the quotient $n/4$ truncated toward zero, as AMD's *AMD64 Architecture Programmer's Manual*, Volume 5, *64-Bit Media and x87 Floating-Point Instructions*, specifies. The compiler converts each decimal constant of the programs, and the library function `atof` each decimal number that the programs read from their command line or environment, to the binary64 number nearest to it. The numbers read in this way are the radius of the subseed balls of

Section 3.5(ii), the radii τ, two parameters of Stage B that only steer proposals, and the numerators and denominators of the box widths of Stage B.

Round to nearest is the default mode at program start, and the programs never change the rounding mode. They are compiled with `-ffp-contract=off` (Section 4.1), the executables contain no fused multiply–add instruction (Section 5), and every floating-point program checks at start that a test expression is not contracted. Floating-point computation that is not enclosed, including every call of sin, cos, atan2, pow and hypot from the mathematical library, is used in three ways only. It *proposes* objects, for instance centers of records, tangent matrices T, the matrices M of Lemma C.23 ([27, Proposition 4.5]), test directions, eigenvalue guesses and cluster centers. It *selects* the tests that are made: it pre-screens the vanishing sums of the seed cover, where a list that passes is kept and a rejection is confirmed in interval arithmetic, and in Stages A and B floating-point distances decide which records are tested against a cell, an atlas record or a box. And it computes two quantities whose rounding is bounded by hand: the seed centers, rounded to binary64 (Section 3.4), and the size of the tangent grid of Stage B. This grid reaches more than one box width beyond an interval upper bound for $(1+\omega)^{1/2}R$, as a bound on the rounding errors of this sizing shows (Appendix A.6). A proposed object is then checked in interval arithmetic, and a test that is not selected is not made, so a poor proposal or selection can make a test fail but cannot make a test succeed wrongly.

Lemmas 3.1 and 3.2 concern finite results. The programs stop when the argument of e is not finite and when a divisor interval contains 0, but the interval operations do not test every endpoint for finiteness. An endpoint computed from finite endpoints becomes infinite only through an overflow, and from an infinite endpoint a NaN can arise, as $\infty - \infty$ for instance. The minima and maxima of endpoints are formed with operations that return their first argument when one of their two arguments is NaN, so a NaN can be dropped: the product of $[1, +\infty]$ and $[0, 1]$ is returned as $[-2^{-1074}, 1 + 2^{-52}]$. Such a finite interval need not contain the exact value, and a comparison made with it would not be justified by Lemmas 3.1 and 3.2. The proofs therefore use the following condition.

Condition (B). Every endpoint of an interval formed in the computation is finite.

The computation tests, as it runs, the numbers from which Condition (B) follows (Lemma 3.3). Its interval arithmetic tests each number that an outward step receives and each one it returns, and each binary64 number formed into an interval, for being infinite or NaN (from the exponent field of the bit pattern). A process counts the calls in which a tested number fails and writes the counts when it ends normally. The tests are confined to the functions that carry out the outward steps and form an interval from a binary64 number, which return the same expressions as without them, and to the code that counts and reports.

Lemma 3.3. *Consider a process of the computation in which no tested number is infinite or NaN. Then every endpoint of every interval formed in the process is finite, and so is every binary64 number r to which an outward step is applied. Under Assumption (A), moreover, $r = \mathrm{fl}(s)$, so that Lemmas 3.1 and 3.2 apply to r; here s is the exact value of the quantity that r computes: the exact result of the operation that produced r, or, when r is the smallest or the largest of several numbers, as in a product or a quotient of intervals, the smallest or the largest of their exact values.*

Proof. In the programs, an endpoint of an interval is formed in one of four ways, by (P1): as the output of an outward step; as a binary64 number formed into an interval, which gives

an interval $[a, a]$, or $[-a, a]$ with $a \geq 0$; as one of the constants 0, $\pm\frac{1}{2}$ (for the shared phase, Appendix A.2) and the bounds for π and 2π of Section 3.2; or as the negative, the minimum or the maximum of endpoints formed before (no interval is read before a value is assigned to it). Numbers of the first two kinds are tested, the constants are finite, the negative of a finite number is finite, and the minimum or the maximum of two finite numbers is one of them. So, by induction over the order in which endpoints are formed, every endpoint is finite. The numbers to which outward steps are applied are tested, so they are finite.

Now assume (A). By the same induction every interval formed, except the intersections of Appendix A.2, which enter only comparisons, has its lower endpoint at most its upper endpoint. The intervals formed from binary64 numbers and from the constants have this property, the arithmetic operations preserve it, since $\mathrm{dn}(x) \leq x \leq \mathrm{up}(x)$ for finite x and rounding is monotone, and so do the formations of the fourth kind, by (P1). An operation $+, -, \times, \div, \sqrt{\ }$ on finite binary64 operands returns $\mathrm{fl}(s)$, where s is its exact result. This is $\pm\infty$ after an overflow, and never NaN, since a divisor interval lies on one side of 0 (its endpoints being ordered) and square roots are taken of nonnegative numbers (P2). A number r to which an outward step is applied is the result of such an operation, or the smallest or the largest of several such results, or the larger of two outputs of outward steps, which is exact (P2). The operands of these operations are endpoints and their absolute values, outputs of outward steps, constants, the reduced argument of Lemma 3.5, which is finite (of absolute value at most 1/8, as the program stops unless $|t| < 2^{40}$), or numbers that are not endpoints: the radius of a record, and midpoints of intervals computed in floating point. By (P2), each number of the last kind enters a tested number in such a way that it would make that number infinite or NaN if it were infinite or NaN, so all operands are finite. An infinite result of an operation would also reach a tested number (P2). In a product or a quotient of intervals, a result $+\infty$ would be the largest of the four endpoint results, which goes to the outward step of the upper endpoint, and a result $-\infty$ the smallest, which goes to that of the lower endpoint. Where the larger of the differences $b - m$ and $m - a$ between the endpoints of an interval $[a, b]$ and a midpoint m is taken, these differences sum to $b - a \geq 0$, so that if one of them were $-\infty$ the other would be $+\infty$, and so would the larger one. So every result entering r is finite, and $r = \mathrm{fl}(s)$, rounding being monotone. □

The computation ran in 154 processes, on the server and with the compiler and options of Section 4.1, each starting from inputs that are not results of interval computations, from lists of the seed balls to be replaced by subseeds (together the 1,303 that Stage A reported unresolved), or from files identical byte for byte to files, or to initial parts of files, written by other processes of the computation. All 154 processes ended normally, and each of them reports that no tested number was infinite or NaN. An earlier execution without these tests had produced the same stored outputs: the computation reproduced every one of them on which Section 4 rests, the files other than logs byte for byte and the logs in the results they report.

Proposition 3.4. *The computation satisfies Condition (B): every endpoint of an interval formed in it is finite. Under Assumption (A), Lemmas 3.1 and 3.2 apply at each of its outward steps.*

Proof. Apply Lemma 3.3 to each of the 154 processes, whose counts are 0. □

3.2. **The exponential.** IEEE 754 only recommends correctly rounded sin and cos, and the C standard leaves the accuracy of its library functions to the implementation, so the programs

enclose $e(t)$ without them, by reducing the argument and evaluating Taylor polynomials in interval arithmetic.

Lemma 3.5. *Let t be a binary64 number with $|t| < 2^{40}$, let n be an integer nearest to $4t$, and let $s = t - n/4$. Then s is computed exactly in binary64, $|s| \le 1/8$, and $e(t) = i^n e(s)$. With $x = 2\pi s$ enclosed using $7074237752028440 \cdot 2^{-51} < \pi < 7074237752028441 \cdot 2^{-51}$, one has $|x| < 0.786$, and*

$$\cos x \in \sum_{j=0}^{10} \frac{(-1)^j x^{2j}}{(2j)!} + [-10^{-22}, 10^{-22}], \qquad \sin x \in \sum_{j=0}^{10} \frac{(-1)^j x^{2j+1}}{(2j+1)!} + [-10^{-22}, 10^{-22}].$$

For an interval of center m and radius ρ, every t in it has $|e(t) - e(m)| \le 2\pi\rho$.

Proof. The reduction is that of [27, Lemma A.2]. The products $4t$ and $n/4$ are exact, since $|n| \le 2^{42}$. If $n = 0$, then $s = t$. If $n \ne 0$, then $|t - n/4| \le 1/8 \le |n|/8$, so t and $n/4$ have the same sign and lie within a factor of two of each other, and $t - n/4$ is exact by Sterbenz's lemma [32]. The cosine polynomial, of degree 20, is also the Taylor polynomial of order 21, because the coefficient of x^{21} vanishes. So the Lagrange remainders [29, Theorem 5.15] of both polynomials are of order 22 and at most $|x|^{22}/22! \le 0.8^{22}/22! < 7 \cdot 10^{-24}$. The last assertion holds because $|e'(t)| = 2\pi$. □

The program stops if $|t| \ge 2^{40}$. It encloses $x = 2\pi s$ with the two bounds for π above, evaluates the two polynomials over this enclosure in interval arithmetic, and adds the interval $[-\operatorname{fl}(10^{-22}), \operatorname{fl}(10^{-22})]$, which contains $[-10^{-22}, 10^{-22}]$, with an outward step; so the results enclose $\cos 2\pi s$ and $\sin 2\pi s$, and the enclosure of $e(t)$ accounts for the rounding of every operation. As a check, it also stops if the enclosure of x is not contained in $[-\operatorname{fl}(0.8), \operatorname{fl}(0.8)]$, which does not happen, since $|2\pi s| \le \pi/4$. It computes n with the library function `nearbyint`, and $r = \texttt{fmod}(n, 4)$ with the x87 instruction `fprem` (Section 4.1). Under Assumption (A), n is an integer nearest to $4t$, and $r = n - 4q$ with q the quotient $n/4$ truncated toward zero, so $r \in \{-3, \dots, 3\}$ and $r \equiv n \pmod 4$; r has the sign of n. The program converts r to an integer and puts $n' = (r + 4) \bmod 4$, the least nonnegative residue of n modulo 4, so that $i^{n'} = i^n$, and it multiplies the enclosure of $e(s)$ by $i^{n'}$ by exchanging the real and imaginary parts and negating endpoints, which is exact. The two bounds for π were checked with PARI/GP 2.17.3.

3.3. **Spectral bounds.** Several constants of [27] are operator norms or largest eigenvalues: the bound $\kappa \ge \|M\|$; a bound for the norm of the matrix of Lemma C.22 ([27, Lemma 4.4]) that gives the second admissible choice of C (Appendix A.4); and a number exceeding the largest eigenvalue of a positive semidefinite matrix that Lemma C.28 ([27, Lemma 4.12]) uses to bound the tangent coordinates of the completions in a cell. They are bounded as follows; for κ this is one of three upper bounds, of which Appendix A.4 takes the least.

Lemma 3.6. *Let $\mathbf{G}$ be a symmetric matrix of intervals containing a real symmetric matrix G, let G_0 be a symmetric binary64 matrix, let $\rho \ge \max_i \sum_j \max_{y \in \mathbf{G}_{ij}} |y - (G_0)_{ij}|$, and let $\hat{G}$ be G_0 with each diagonal entry $(G_0)_{ii}$ replaced by a binary64 number at least $(G_0)_{ii} + \rho$. Then $G \preceq \hat{G}$, and if the LDL^{T} factorization of $\mu I - \hat{G}$, computed in interval arithmetic, has pivots with positive lower endpoints, then $\lambda_{\max}(G) \le \lambda_{\max}(\hat{G}) < \mu$.*

Proof. By Gershgorin's theorem [8, Theorem 6.1.1] the symmetric matrix $G - G_0$ has spectral radius at most ρ, so $G \preceq G_0 + \rho I$, and $G_0 + \rho I \preceq \hat{G}$ since $\hat{G} - G_0 - \rho I$ is diagonal with nonnegative entries. The interval factorization encloses the pivots of the real matrix $\mu I - \hat{G}$. If

all of them are positive, the matrix is positive definite (by Sylvester's criterion [8, Section 7.2], as its leading principal minors are products of pivots), and $\lambda_{\max}(G) \le \lambda_{\max}(\hat{G}) < \mu$. □

The trial value μ and the matrix G_0 (normally the midpoint of $\mathbf{G}$) are proposals.

3.4. **The seed cover.** The orientation and gap filters of [27, Section 2] are inequalities between integers and are evaluated in integer arithmetic. The linearized tests of the two vanishing sums and the intervals for the shared phase (Lemmas C.8 and C.9; [27, Lemmas 2.7 and 2.8]) are evaluated in interval arithmetic, and a bin pair is rejected only if a test fails for every point of the enclosures. The bin pairs are visited in the following order: the lists of bins for $x_1, \dots, x_5$ in increasing lexicographic order of their bin indices and, after each list that passes the filters on x, the lists for the second column with its shared bin that pass the test of their vanishing sum, in increasing lexicographic order of the bins of $y_2, \dots, y_5$. Each surviving bin pair is assigned to an earlier center if the integer test of the following lemma succeeds for some earlier center with the same selected position, and otherwise its midpoint becomes a new center [27, Section 2.4], so the centers depend only on this order. The test uses only the first of the two bounds of [27, Lemma 2.9].

Lemma 3.7. *Let u be the midpoint of a bin pair and u' an earlier center with the same selected position, and suppose that $w = 112(u - u') \in \mathbb{Z}^9$ satisfies $\|w\|^2 + \sum_j |w_j| \le 10$. Then every point q of the bin box of u satisfies $\|q - u'\| < 0.032$.*

Proof. Write $q = u + h/112$ with $h \in [-\frac{1}{2}, \frac{1}{2}]^9$. Then $112^2\|q - u'\|^2 = \|w + h\|^2$, which is at most $\|w\|^2 + \sum_j |w_j| + \frac{9}{4} \le 12.25$, while $(0.032 \cdot 112)^2 = 12.845056$. □

So the seed ball about a center contains the bin boxes assigned to it, and the bin box of a new center lies within $3/224 < 0.032$ of it. The nine coordinates of a center, the midpoint of a bin pair, have the form $(b + \frac{1}{2})/112$ with integers $0 \le b < 112$. Rounding them to binary64 moves the center by less than $3 \cdot 2^{-54} < 10^{-15}$, and the binary64 number nearest to 0.0320001 exceeds $0.032 + 10^{-15}$.

3.5. **Stage A and the replacement of unresolved seed balls.** Stage A follows [27, Sections 3 and 4] with the parameters of [27, Sections 3.7, 7.2 and 7.3]: seed radius 0.0320001, cell levels $N_u = 16, \dots, 512$, cells covered only by records of radius at most 0.103, and atlas radii at most 0.125. In place of the cap of 10^6 further cells of [27, Section 7.3], our programs test at most 10^6 cells at the levels $N_u \ge 64$ for each seed ball and count the remaining ones unresolved. The constant C of each Root certificate is the smaller of the two values allowed by Lemma C.22, each bounded above as in Appendix A.4. A record may be stored with its rows and columns permuted, and possibly transposed, relative to the coordinates in which it was certified. It keeps the constants computed in those coordinates, and these remain valid for the assertions of [27, Definition 4.1] by Lemma C.24 ([27, Lemma 4.7]). The later stages use stored constants only through these assertions. There are two further departures.

(i) For most seed balls (Section 4.1), Stage A also sets a limit of 3,000 Root certificates. Root certificates are built only at the levels $N_u \ge 64$, which Stage A reaches after it has processed every cell of the levels 16 and 32. Once 3,000 Root certificates have been built for a seed ball, or it has used up its limit of 10^6 cells at the levels $N_u \ge 64$, every cell that Stage A processes afterwards is counted unresolved without being tested, and the seed ball is reported unresolved, as it is when a cell of the last level, $N_u = 512$, is neither excluded nor covered. Remark 4.2 says why the limit helps.

(ii) An unresolved seed ball is replaced by smaller balls. Let u' be its center. The *subseeds* of u' are the midpoints of all bin pairs that pass the filters, have the selected position of u' and satisfy the condition of Lemma 3.7 with respect to u'. They are enumerated by a separate program that uses the filter code of the seed cover, and Stage A is run on the ball of radius 0.0133929 about each of them, a radius just above 3/224, half the diagonal of a bin box.

Lemma 3.8. *Assume (A) and (B). Let u' be a seed center, and suppose that Stage A, run with seed radius* 0.0133929 *about every subseed of u', resolves each of these balls. Then the records it produces cover every complex Hadamard matrix that is equivalent to one arranged with the selected position of u' (Appendix A.8) whose seed coordinates lie in the bin box of u' or in the bin box of a bin pair that the seed cover assigned to u'.*

Proof. The seed cover assigns a bin pair to u' only if the pair passes the filters, has the selected position of u' and satisfies the condition of Lemma 3.7 with respect to u' (Section 3.9, (P4)). The bin pair of u' itself passes the filters, with $w = 0$. So each of these bin pairs has a subseed u of u' as its midpoint. The bin box of u lies within 3/224 of u, and rounding the nine coordinates of u to binary64 moves it by less than 10^{-15} (Section 3.4). The binary64 number nearest to 0.0133929, which the programs use as this seed radius, exceeds $3/224 + 10^{-15}$, so the ball of that radius about the rounded subseed contains the bin box of u. The lemmas of Appendix C that Proposition A.4 uses hold for every seed radius: they involve the seed radius only as a parameter r_s, with $R_s = 2\pi r_s$. The value 0.0320001 enters only statements of [27] about its programs, for instance the numerical bounds of [27, Section 4.5 and Appendix A] and the bound $q_Y < 0.32$ (with q_Y as in Appendix A.3) that [27] states after its Lemma 3.2, neither of which we use. The bound [27, (4.20)] on the center correction, proved for a routine of [27], is replaced by Lemma A.1. So, by Proposition A.4, applied with the selected position of u', which every subseed of u' has, Stage A with no unresolved ball covers every complex Hadamard matrix that is equivalent to one arranged with this selected position whose seed coordinates lie in one of these balls. □

By Proposition A.3, the seed ball of u' is needed in the cover of Section 3.4 only for the bin box of u' and for the bin boxes of the bin pairs assigned to u'. By Lemma 3.8, the balls about the subseeds of u' can take its place.

3.6. **Stage B in the quotient.** Stage B uses the symmetries of the problem to reuse records. Let $\mathcal{G}$ be the group of linear maps of $\mathbb{R}^{6\times 6}$ generated by the permutations of rows, the permutations of columns, transposition and $P \mapsto -P$. It has order $4 \cdot (6!)^2 = 2{,}073{,}600$. Each $g \in \mathcal{G}$ permutes coordinates and possibly changes all their signs, so (gP, gT) with the same constants is certified whenever (P, T) is. The solution set of the transported record consists of the correspondingly transformed matrices, which are equivalent to those of the record (Lemmas C.4 and C.24; [27, Lemmas 2.2 and 4.7]). Rephasings of rows and columns, which also belong to the equivalence of Section 2.2, are not in $\mathcal{G}$. They add to a phase matrix a matrix constant along rows or along columns, which the projection Π removes, and the integer matrices Z in the aligned distances of Section 2.4 absorb the integer parts of phases.

As in [27, Sections 5.4 and 5.5], a box of a parent's tangent grid may be marked, that is, recognized as covered, not only against a stored child, with the threshold for the radius τ of the refinement, but also against a transported copy $g^{-1}(Q, r)$ ($g \in \mathcal{G}$) of a stored child (Q, r), with the same threshold, and against a transported copy of a *blocker*, with the threshold for the blocker's own radius. A blocker is a parent whose refinement has been completed [27, Section 5.5]. The relation estimates are those of Lemmas C.33 and C.34 ([27, Proposition 5.2

and Lemma 5.3]) and Lemma A.2, evaluated in interval arithmetic for the transported record. Our use of these marks differs from that of [27, Section 5] in two respects. First, the maps tried are proposed by a search in floating point over all of $\mathcal{G}$. Comparing a parent with all 2,073,600 images of every stored record would cost too much. So each stored record is kept in a normal position, the one among its images under $\mathcal{G}$ nearest in aligned distance to a fixed matrix. Two records related by a map of $\mathcal{G}$ have the same images, and so, unless several images are equally near, the same normal position. A parent is compared only with the stored records that lie near one of its own images. OpenAI's procedure, which stores records under a canonical map, may try a limited collection of maps [27, Sections 4.7 and 5.4]. Second, the stored children and the blockers may come from an earlier refinement, as in the second pass of Section 4.2.

Children are stored with radius exactly τ when they are made, and a box is marked against a stored child, new or old, with the threshold computed for τ. This is valid when every stored child has radius at least τ, which holds in every refinement of the computation ((F5) of Section 3.8). The box widths are 13/1024, 6/1024, 5/1024 and 4/1024 for $\tau = 0.07$, 0.02, 0.016 and 0.011, the last for the fallback refinement of Section 3.7, which refines the fine records that Stage C does not exclude. These dyadic widths replace the widths 0.013, 0.005 and 0.0038 that [27, Section 5.6] uses for $\tau = 0.07$, 0.016 and 0.011, and since the depth of subdivision is at most six, every box center is a binary64 number and the 2^k subboxes of a box tile it exactly (Appendix A.6). The covering argument holds for every width (Lemmas A.2 and C.35), so the widths affect only the cost.

A refinement is carried out by processes, each of which takes a range of the parents (Section 3.8). The covering argument is the blocker induction in the proof of [27, Proposition 5.7], in the following form.

Lemma 3.9. *Assume (A) and (B). Consider a process of a refinement to radius τ that starts with some stored children, each of radius at least τ, and some blockers, and suppose that the solution set of each of these blockers is contained, up to equivalence, in the union of the solution sets of these stored children. If the process completes each of its parents, then, up to equivalence, the solution set of each of its parents and of each of its blockers is contained in the union of the solution sets of the children stored at its end.*

Proof. New children are stored with radius τ, and stored children are never removed (Section 3.9, (P6)). So it suffices to show that when the process completes a parent, the solution set of that parent is contained, up to equivalence, in the union of the solution sets of the children stored at that moment, provided that this holds for every blocker present. The proviso holds at the start by hypothesis. The completed parent then becomes a blocker, and by (P6) the process has no blockers other than those it starts with and the parents it has completed, so the proviso remains true and the lemma follows by induction over the parents in the order in which they are completed.

Let (P, R) be a parent that the process completes, and let $e(P + \delta)$ be in its solution set. The tangent coordinates $\eta = T^*\delta$ satisfy $\|\eta\| \le (1 + \omega)^{1/2} R$ (Lemma C.35). So η lies in a box of the tangent grid (Appendix A.6). The only rejection of a box, of the grid or of a subdivision, is the test that it lies outside the ball of that radius, as in the proof of [27, Proposition 5.7], and a box that contains η passes this test. A box that is neither rejected nor marked is completed only when each of its 2^k subboxes, which cover it (Lemma C.35), is completed, and one of them contains η. A box of the largest depth that is neither rejected nor marked is never completed (Section 3.9, (P6)), so the completed parent (P, R) has no such box. Since the depth of subdivision is bounded, η therefore lies in a box marked

against a stored child or a blocker, possibly transported. If the box is marked against a copy $g^{-1}(Q, r)$ of a stored child (Q, r), where $g \in \mathcal{G}$ may be the identity, with the threshold for τ, then $e(P + \delta)$ is equivalent to a member of $\mathcal{S}(g^{-1}Q, \tau)$ (Lemma A.2), and hence, by Lemma C.24, to a member of $\mathcal{S}(Q, \tau)$, which is contained in $\mathcal{S}(Q, r)$ since $\tau \le r$. If the box is marked against a copy $g^{-1}(P', R_B)$ of a blocker (P', R_B), with the threshold for R_B, then $e(P + \delta)$ is equivalent to a member of $\mathcal{S}(g^{-1}P', R_B)$ (Lemma A.2), hence (Lemma C.24) to a member of $\mathcal{S}(P', R_B)$, and so, by the proviso, to a member of the solution set of a stored child. □

3.7. **Stage C.** Our search for two cliques is exhaustive by Lemma B.1. Apart from this search, Stage C follows [27, Section 6], with the four changes below and with three proposed directions for each of bin test (3) and the joint test of Appendix A.7, where [27, Section 6.7] uses one.

(i) Clustering: a kept bin with midpoint u, whose sides have length $2a$ (the inverse of the resolution of its layer), is assigned to a vector ball with center v and a radius at least $\|h\| + \sqrt{29/6}\, a$. Here h is the difference $u - v - m$, for an integer vector m, minus the mean of its six coordinates, and $\sqrt{29/6}\, a$ bounds the norm of the displacement of a point of the bin from its midpoint, centered in the same way (Lemmas C.37 and C.41; [27, Lemmas 6.1 and 6.4]). Subtracting the mean removes the common phase of a vector, which is arbitrary. The centers are chosen greedily, and every radius is checked to be less than 0.1 (Lemma C.42; [27, Lemma 6.5]).

(ii) Resolution: Stage C is run with four layers of bins (finest resolution 96) and, if that run is inconclusive, with five and six layers (resolutions 192 and 384). A record is excluded if one of these runs ends with no bin kept in some layer or with a search that runs to completion without finding a configuration (Proposition B.2).

(iii) Limits: at most 4,096 vector balls, $4 \cdot 10^7$ bins and 10^9 steps of the graph search. A run that exceeds a limit does not exclude the record.

(iv) The operator bound $\|e(P)/\sqrt{6}\| \le (1 + 2\pi\sqrt{2}\,\varphi/6)^{1/2}$ of [27, Section 6] is evaluated for each record from its own constant φ, in place of the constant $K = 1.00001$ of [27, Section 6], and the conditions that [27, Section 6.1] imposes on the radius and the constants of a record are not checked. The tests of Stage C hold in this form: Appendix C proves them with this value and without these conditions (Lemmas C.36 to C.44), and Appendix A.7 proves [27, (6.12)–(6.13) and (6.16)] in the same way.

A record that Stage C does not exclude is refined by Stage B to radius 0.011 (and, if needed, 0.008 and 0.005; in the computation 0.011 sufficed), and Stage C tests all its children. At radius 0.011 this is the *fallback refinement* of [27, Section 7]; the radii 0.008 and 0.005 are ours.

3.8. **Facts about the computation.** The proofs use the following facts about the computation, which are read from its stored records and logs [13] and which Sections 3.1 and 4.2 and Appendix B report. Section 5 says how they were checked.

(F1) Every seed ball was processed, and none failed the frame checks of Section 2.5 (logs of Stage A).

(F2) Every seed ball that Stage A reported unresolved was replaced by its subseeds, and Stage A resolved every one of these subseeds, with no frame failure (logs of Stage A).

(F3) The parents of a refinement are the records of the preceding stage, except in two cases: those of the mid refinement of the first pass are the 11,150 records of Section 4.2, and

those of the fallback refinement are the records that Stage C reported unresolved (F7). The processes of a refinement took consecutive ranges of the list of its parents other than those of (F4), ranges that together cover the list, and each completed all the parents of its range. In the first pass, the mid refinement ran a first process on an initial range of parents, starting with no stored children and no blockers, and then the others, each starting with the children and blockers of the first process at its end. The fine refinement and the fallback refinement each ran in one process, which started with none. In the second pass, the mid refinement ran in the same way, except that its first process started with the 1,405 mid records of the first pass as stored children and the 11,150 parents completed there as blockers. The fine refinement of the second pass started with the 5,933 fine records of the first pass as stored children and the 1,405 mid records completed there as blockers. In each case the hypothesis of Lemma 3.9 holds, by Lemma 3.9 applied to the earlier processes (stored records and logs of Stage B).

(F4) In the second pass, the parents that were not refined again are exactly those with the same center, tangent matrix and constants as a parent completed in the first pass and with a radius not larger: 3,685 atlas records in the mid refinement and the 1,405 mid records of the first pass in the fine refinement (stored records).

(F5) Every stored child of a refinement to radius τ has radius at least τ (stored records: every child is stored with radius τ, and the second pass's fine refinement started with the 5,933 fine records of the first pass, of radius 0.02).

(F6) Every atlas record has radius at most 0.125, and every parent of a refinement has $\omega < 0.06$, so that $E/w < 33$ for every parent, with E and w as in Appendix A.6 (stored records; the largest ω is $2.9 \cdot 10^{-14}$).

(F7) For each fine record, Stage C reported either an exclusion or "unresolved". The records reported unresolved are the parents of the fallback refinement, and Stage C excluded every child of the fallback refinement (stored records and logs of Stage C).

(F8) Every record that Stage C tested has radius 0.02, 0.016 or 0.011, and every graph search ran with the cap $\mathsf{c} = 10^9$ of Appendix B (stored records, and the command lines of the Stage C processes).

(F9) Each of the 154 processes of the computation reports that no tested number was infinite or NaN (Proposition 3.4).

3.9. **What the proofs use about the programs.** The proofs use the following properties of the programs. Each item names the proofs that use it and the program that carries it out.

(P1) *Endpoints* (Lemma 3.3). In every program, an endpoint of an interval is formed in one of four ways: as the output of an outward step; as a binary64 number formed into an interval, which gives an interval $[a, a]$, or $[-a, a]$ with $a \geq 0$; as one of the constants 0, $\pm\frac{1}{2}$ (for the shared phase, Appendix A.2) and the bounds for π and 2π of Section 3.2; or as the negative, the minimum or the maximum of endpoints formed before. Under Assumption (A), an interval formed in this last way from intervals with finite endpoints, each with lower endpoint at most its upper endpoint, again has this property, except the intersections of Appendix A.2, which enter only comparisons. No interval is read before a value is assigned to it.

(P2) *Operands and outward steps* (Lemma 3.3). In every program, an outward step is applied to the result of an operation $+, -, \times, \div, \sqrt{\ }$, to the smallest or the largest of several such results, or to the larger of two outputs of outward steps. In a product or a quotient of intervals, the largest of the four endpoint results goes to the upper step and the

smallest to the lower one. A quotient is formed only when the divisor interval does not contain 0, and a square root only of the nonnegative part of an interval. Every operand other than an endpoint, the absolute value of an endpoint, an output of an outward step, a constant or the reduced argument of Lemma 3.5 is the radius of a record or a midpoint of an interval computed in floating point. Such an operand enters a number tested in the computation in such a way that it would make that number infinite or NaN if it were infinite or NaN. So does the larger of the differences $b - m$ and $m - a$ between the endpoints of an interval $[a, b]$ and a midpoint m, wherever it is formed.

(P3) *The finiteness tests* (Lemma 3.3 and Proposition 3.4). The tests of Condition (B) are made and counted as Section 3.1 describes, and the functions that make them return the same expressions as without them.

(P4) *The seed cover* (Proposition A.3 and Lemma 3.8; the proof of Theorem 1.1). The seed cover program visits every nondecreasing list of bins for x and, for its shared bin, every nondecreasing list for y. It rejects a bin pair only when a filter of Appendix A.2 fails as decided there, it assigns a surviving pair to an earlier center only by the test of Lemma 3.7 with the same selected position, and otherwise it writes the midpoint of the pair as a new center. Centers are never removed. The program that enumerates subseeds writes, for each center u' it is given, the midpoint of every bin pair that passes the same filters, has the selected position of u' and satisfies the condition of Lemma 3.7 with respect to u', and of no other bin pair, leaving out only pairs written before.

(P5) *Stage A* (Proposition A.4). Each Stage A program processes all cells of the first level, $N_u = 16$, and at each later level all 16 children of every cell of the level before that was neither excluded, nor covered, nor counted unresolved. A cell is excluded only by the norm test or the directional test of Appendix A.3. A cell at $N_u = 512$ that is neither excluded nor covered is counted unresolved, and so is, without being tested, a cell at a level $N_u \geq 64$ that is reached after the limits of Section 3.5. A cell is covered only by the record of a Root certificate built and certified as in Appendix A.4, and only when the radius computed as in Appendix A.5 is at most 0.103. The record then has at least this radius, radii are never lowered, and every returned record is added to the atlas as Appendix A.5 describes.

(P6) *Stage B* (Lemma 3.9). The Stage B program stores each new child with radius τ and never removes a stored child. It marks a box only against a stored child, a blocker or a transported copy of one, with the thresholds of Lemma A.2, and it rejects a box only by the test of Appendix A.6 that the box lies outside the ball of radius E_P. Its blockers are those it starts with and the parents it has completed, each with its own radius. A box that is neither rejected nor marked is completed only when its 2^k subboxes are, and the depth of subdivision is at most six.

(P7) *Stage C* (Proposition B.2 and Lemma B.1). The Stage C program tests every bin of the first layer and, unless a limit of Section 3.7(iii) stops the run (which is then reported unresolved), all children of the bins that each layer keeps, with the bin tests of Appendix A.7. It assigns each kept bin of the last layer to a vector ball as stated there, and it joins two balls in $\mathcal{O}$ or $\mathcal{U}$ unless a test of Appendix A.7 rejects the pair. It reports a record "negative" only as Appendix A.7 and Appendix B state, and its graph search consists of the three procedures of Appendix B, transcribed statement by statement.

(P8) *The decisions* (all proofs that rest on the computation). Each inequality of Appendix A is decided as the note "In the computation" beside it states, and the programs carry

out interval arithmetic, enclose $e(t)$, bound spectra and use floating-point computation that is not enclosed as Sections 3.1, 3.2 and 3.3 describe.

Section 5 says how these properties were checked, and the deposit [13] gives, for each item, the source code that carries it out.

4. The computation

The computation consists of the seed cover, Stage A with the replacement of unresolved seed balls, and two passes through Stages B and C. Its stored outputs establish the facts of Section 3.8, from which Theorem 1.1 follows (Section 4.3).

4.1. **Machine and programs.** The computation ran on one server with an AMD EPYC 4484PX processor (12 cores, 24 hardware threads) and 93 GiB of memory, under Ubuntu 24.04 with GCC 13.3.0 and glibc 2.39. The programs were compiled with `g++ -O2 -std=c++17 -ffp-contract=off` and no `-march` option, so the executables use the baseline x86-64 instruction set, in which binary64 arithmetic is carried out by SSE2 instructions. The one exception is the remainder $\texttt{fmod}(n, 4)$ in the enclosure of $e(t)$ (Section 3.2), which the compiler computes with the x87 instruction `fprem`, an exact remainder; the executables call the library function `fmod` only if this remainder is NaN, which cannot happen for the finite n of Lemma 3.5, and do not use the value it returns. Most of the programs use the outward step of Lemma 3.2. Stage A ran under four builds: three builds of the program for the seed balls, differing in the outward step and in the limit of Section 3.5(i), and one of the program for the subseed balls of Section 3.5(ii). The deposit [13] lists them. The limit applied to 752,120 of the 852,120 seed balls, and to none of the subseed balls. The lemmas above cover each of these builds, so the choice of build changes only the cost and which certified records are produced.

4.2. **Counts.** Table 1 summarizes the computation. All 1,406 mid records were refined with no failed parent, and Stage C excluded every one of the 5,934 fine records, 5,732 directly and 202 through the 2,786 records of their refinement; the details follow.

Table 1. The computation. The first pass refines the 11,150 atlas records made from the seed balls of index below 70,000, and the second pass 42,355 of the 46,040 atlas records; the text says why the other 3,685 are not refined again. The fallback refines to radius 0.011 the fine records that Stage C did not exclude at first (Section 3.7). In all there are 1,406 mid and 5,934 fine records, besides the 2,786 records of the fallback refinement.

Step	Input	Output	Not resolved at first
Seed cover	151,742,926 bin pairs	852,120 seed balls	—
Stage A	852,120 seed balls	46,040 atlas records	1,303 seed balls
replaced by subseeds	1,303 seed balls	228,274 subseeds	none
B mid, first pass	11,150 atlas records	1,405 mid records	none
B fine, first pass	1,405 mid records	5,933 fine records	none
Stage C, first pass	5,933 fine records	5,731 excluded	202 fine records
fallback B and C	202 fine records	2,786 records, all excluded	none
B mid, second pass	42,355 atlas records	1 new mid record	none
B fine, second pass	1 mid record	1 new fine record	none
Stage C, second pass	1 fine record	1 excluded	none

Seed cover. The seed cover runs through all 160,389,488 = $\binom{116}{5}$ nondecreasing lists of bins for $x_1, \dots, x_5$ and all 774,294,080 = $112\binom{115}{4}$ lists for the second column (Section 2.3). Of these, 22,829 and 829,306 pass the filters that apply to one list. Of the 298,638,554 pairs of passing lists that put the shared phase in the same bin, 190,192,620 pass the second gap filter and 151,742,926 the test on the shared phase. Lemma 3.7 assigns 150,890,806 of these to earlier centers, which leaves 852,120 centers. For comparison, [27, Section 7.5] reports 22,829 lists for x [27, Table 1], as many as ours, and 151,744,086 pairs processed by its seed cover, 1,160 more than our surviving pairs. This difference is in the direction in which the margins of [27] act: its rejection tests carry fixed safety margins (for instance 10^{-5} on the endpoints of the intervals for the shared phase [27, Appendix A]) where ours use outward rounding. The seed cover of [27] has 249,878 centers, less than a third as many as ours. Our reuse rule omits the second bound of [27, Lemma 2.9], and the number of centers also depends on the order in which bin pairs are visited and on which earlier centers are tried; we have not determined what accounts for the difference in the number of centers.

Stage A. Stage A processed the 852,120 seed balls in 19 ranges of indices, in parallel: those of index below 347,003 in seven ranges, one for each residue of the index modulo 7, and the others in twelve ranges. Within a range the seed balls are processed in increasing order of index, and their records are merged into the atlas of the range. Each range was processed by one, two or three processes in succession, 46 in all, each process after the first starting from a byte-for-byte copy of the checkpoint (the atlas of the range and its counts after a given seed ball) that the process before it wrote. So the results of each seed ball enter the atlas through exactly one process; the deposit gives the ranges and the checkpoints. The summary of the last process of each range counts all seed balls of the range, and no seed ball failed the frame checks (F1). Stage A reported 1,303 seed balls unresolved. These have 228,274 distinct subseeds, on which Stage A ran 229,112 times, since some subseeds were processed more than once, and every run ended with no frame failure and no unresolved cell (F2). The atlas has 46,040 records, with radii between 0.0711 and 0.125.

Stages B and C. These ran in two passes. The first pass took as parents the 11,150 records that the atlases of the seven ranges of index below 347,003 held after their first 10,000 seed balls each, that is, the records made from the seed balls of index below 70,000. Stage A continued from the same checkpoints, and records of later seed balls were merged into some of these 11,150 records, enlarging their radii. The second pass therefore took all 46,040 atlas records as parents, with the records of the first pass available (Section 3.6), and it used the fine radius 0.016 of [27, Section 5.6] in place of 0.02, for the reason given in Remark 4.2.

In the first pass, the 11,150 parents were refined to 1,405 mid records ($\tau = 0.07$) and these to 5,933 fine records ($\tau = 0.02$), with no failed parent. Stage C excluded 5,731 fine records, 5,307 with four layers of bins, 213 with five and 211 with six. The other 202 were refined to radius 0.011, giving 2,786 records, all excluded with four layers.

In the second pass, the 1,405 mid records of the first pass were stored children and its 11,150 completed parents were blockers. Of the 46,040 atlas records, 3,685 have the same center, tangent matrix and constants as a parent completed in the first pass and a radius not larger than that parent's, and were not refined again (F4). The other 42,355 were refined in 15 processes with no failed parent. Among them are the remaining 7,465 parents of the first pass, which reappear in the final atlas with the same center, tangent matrix and constants and a larger radius. Stage B completed these 42,355 parents with marks against transported copies of earlier parents only, except in one region, for which it made one new mid record (Remark 4.1). Its refinement at $\tau = 0.016$, with the 5,933 fine records of the first pass (of

radius $0.02 \geq 0.016$) as stored children, gave one new fine record, which Stage C excluded with four layers. This region is the neighborhood of Tao's matrix S_6 [36], whose entries are cube roots of unity. The new fine record has no tangent directions ($k = 0$), in agreement with the isolation of S_6 (Section 2.1), and its center differs from a phase matrix of a matrix equivalent to S_6 by a rephasing and a horizontal displacement (one with vanishing row and column sums, Section 2.2) of norm less than $2 \cdot 10^{-15}$, as a computation in rational arithmetic shows.

In both passes, every parent of a refinement has $\omega < 3 \cdot 10^{-14}$, and every tangent grid exceeds the ball of radius E_P by more than one box width ((F6) and Appendix A.6). Every stored child has radius τ, except the 5,933 fine records of the first pass, of radius 0.02, with which the fine refinement of the second pass started (F5).

Remark 4.1. The second pass needed one new mid record for 42,355 parents because Stage B works modulo $\mathcal{G}$: the first pass had already covered, up to equivalence, the solutions of every parent outside the neighborhood of S_6. The number of new records, and with it the cost of the fine refinement and of Stage C, therefore depends on the set of complex Hadamard matrices modulo equivalence rather than on the number of seed balls. A matrix can be covered by the records of several seed balls: if Stage A resolves a seed ball with selected position σ, its records cover every matrix equivalent to one arranged with selected position σ whose seed coordinates lie in the ball (Proposition A.4), and the seed balls overlap. Stage B marks a box of a later parent against a transported copy of an earlier record when the threshold of Lemma A.2 for this copy shows that it covers the whole box, and it makes a new child only for a box that none of the records it has related to the parent so far covers. The mid refinement still processes every atlas record (about 57,000 process-seconds for the 42,355 parents of the second pass). The counts of [27] (3,083 records from Stage A, called coarse there, 600 mid and 22,379 fine records, and 163 fine records refined into 1,127 [27, Section 7.5]) come from a different design and are not comparable record by record.

Remark 4.2. Two trials outside the computation show where the cost near S_6 lies. On a seed ball that contains the seed coordinates of a matrix equivalent to S_6, Stage A without the limit of Section 3.5(i) built 10,473 Root certificates and still left cells unresolved, while with the limit it stopped early and the 405 subseeds that replace the ball were all resolved. On fine records refined from the records of its subseeds, Stage C excluded all of 60 sampled records at radius 0.016 and 54 of 60 at radius 0.02, and it was six times faster per record at 0.016.

4.3. **Proof of Theorem 1.1.** By the reduction of Section 2.2, four mutually unbiased bases would give an extendible complex Hadamard matrix. By Proposition A.3, every complex Hadamard matrix is equivalent to one that is arranged (Appendix A.8) with the selected position of a seed center and whose seed coordinates lie in the bin box of that center or of a bin pair that the seed cover assigned to that center, and hence in the seed ball of that center. Stage A resolved every seed ball, directly or through the subseeds of Section 3.5 ((F1) and (F2) of Section 3.8), so by Proposition A.4 and Lemma 3.8 its atlas covers every complex Hadamard matrix up to equivalence. Every refinement completed all its parents other than those of (F4), and each of its processes started with stored children and blockers as Lemma 3.9 requires ((F3) and (F5)). The parents that the second pass did not refine have the same center, tangent matrix and constants as parents completed in the first pass, and radii not larger (F4), so their solution sets are contained in those of these parents. So by Lemma 3.9, which is the argument of [27, Proposition 5.7] in the form of Section 3.6, the fine records cover every complex Hadamard matrix up to equivalence, and the records of the

fallback refinement cover the solution sets of the fine records that Stage C did not exclude at first. Stage C excluded every other fine record and every record of the fallback refinement (F7). By Proposition B.2, no matrix in the solution set of an excluded record is extendible, and so, by the cover above and Lemma C.4, no complex Hadamard matrix of order six is extendible. Every inequality that the programs decided in these steps was decided in integer arithmetic or in interval arithmetic, which is valid under Assumption (A) and Condition (B) by Lemmas 3.1, 3.2, 3.5 and 3.6, and the four rounding errors that the programs do not enclose, of the seed centers, of the constant 10^{-22} of the enclosure of $e(t)$, of the coefficients 1.45 and 0.45 of the covariance of Stage A and of the size of the tangent grid of Stage B, are bounded in Sections 3.4 and 3.2 and Appendices A.5 and A.6, respectively. The computation satisfies Condition (B) by Proposition 3.4, which also rests on (F9). The properties of the programs that these steps use are those of Section 3.9, and the facts of Section 3.8 are read from the stored outputs of the computation. So the argument uses Assumption (A), which Theorem 1.1 assumes, together with these outputs and properties. Three mutually unbiased bases of $\mathbb{C}^6$ exist [17, Lemma 3], so $N(6) = 3$. □

5. Checks

Table 2 lists the checks of the computation and of the programs. Besides the readings of the code and the comparison for (P3), they are of two kinds. Reruns of the same programs show that the stored outputs are reproducible. Recomputations by separately written programs give independent evidence for the facts and decisions they cover. They are written in Python, with rational arithmetic, mpmath or Arb [14] through python-flint where they bound real numbers, or in C++: the recomputations of the seed cover and of the outward steps, and, with Arb in FLINT, the full checks of Stages B and C. The reading of the code against (P1)–(P8), the recomputations and the tests were made by AI agents of the system described in the Declarations, separately from the writing of the programs; no person has read the code. The programs and outputs of the recomputations, and a report of the code reading, are deposited [13].

The interval arithmetic was tested on the server and on an ARM64 machine with clang. Each outward step was compared with the neighboring binary64 number on every power of two in the binary64 range with its neighbors and on two million random bit patterns; the operations were compared with rational arithmetic and mpmath on random operands, subnormal numbers, the powers of two from 2^{-60} to 2^{60} with their neighbors, and random bit patterns. Every computed enclosure with finite endpoints contained the exact value. Building the sources of the computation again reproduces each of its executables bit for bit, and the disassembly of the executables contains no fused multiply–add instruction. Ten processes of the computation, of Stage A, of the enumeration of subseeds and of Stages B and C, were rerun from these executables, and separately written programs compared the outputs and logs of the computation with those of the earlier execution of Section 3.1.

The Root certificates were checked in Arb with a separately computed matrix M: every distinct certificate in the record files of parents, stored children and blockers that Stages B and C read or write, 100,949 in all, 2,404 of them in the transposed coordinates in which they were certified (Section 3.5). Stage B also reads one further record file, of which it uses only the center of the first record, as the fixed matrix of Section 3.6. This check concerns these stored certificates; it does not reach the certificates that Stage A built for cells and discarded when it merged the cell's record into an atlas record, and it repeats no decision of Stage A on a cell. Every process of Stage B was rerun by a copy of the program that logs,

TABLE 2. Checks of the computation and of the programs. "Separate" means separately written programs; "reading" means a reading of the source code.

Check	Kind	Extent	Result
Code read against (P1), (P2)	reading	every program	as stated
Code read against (P4), (P5), (P8)	reading	interval arithmetic, seed cover, Stage A	as stated
Code read against (P6)–(P8)	reading	Stages B and C, fallback, line by line	as stated
(P3)	comparison	the deposited difference between the interval arithmetic with and without the tests	as stated
Outward steps, interval operations, $e(t)$	separate	about two million values; several hundred thousand random arguments	all enclosures with finite endpoints correct
Seed cover	separate	in full	same 151,742,926 bin pairs; each covered by a center as in Lemma 3.7
Root constants	separate (Arb, 128 bits)	every distinct Root certificate in the record files of parents, stored children and blockers that Stages B and C read or write (100,949, among them those of all 46,040 atlas records)	all confirmed, 2,404 in the transposed coordinates
Stage B	separate (Arb), on logs of reruns	every relation used and every box of every parent: all 23 processes, 55,113 parents, 6,158,708 relations, 15,275,916,793 base boxes	all confirmed; outputs reproduced
Stage C	separate (Arb)	all 8,518 records excluded, every bin, ball, edge and the graph	all confirmed
Graph search	separate (brute force)	3,600 and 22,480 random graphs	same answers
(F1), (F2)	separate	from the logs, in full	confirmed
(F3), (F4), (F7)	separate	from the stored records, in full	confirmed
(F5), (F6), (F8)	separate	from the stored records and the command lines, in full, in rational arithmetic	confirmed
(F9)	separate	the counts of all 154 processes	all 0
Reruns	same programs	seed cover, parts of Stage A, ten refinement processes, Stage C on every record; ten processes of the computation from its rebuilt executables	outputs reproduced
Stage C with clang on ARM64	same source	a sample of records	outputs reproduced
Whole computation	rerun with the tests of (P3)	both executions (Section 3.1)	outputs reproduced

for each parent, the relations it uses and the decision for each box, and its outputs equal the stored ones byte for byte. A separately written program in Arb, which uses no code of the computation, recomputed from these logs and the stored records each of the 6,158,708 relations used, from Lemmas C.33 and C.34 ([27, Proposition 5.2 and Lemma 5.3]), and checked every box of the tangent grids of the 55,113 parents (15,275,916,793 base boxes, and

the 3,130,192 boxes into which 154,676 of them were subdivided), the grid of every parent and the radius of every stored child used. Stage C was recomputed from the formulas of [27, Section 6] rather than from our code, for each of the 8,518 records it excluded. Every removed bin and every removed edge (9,517,107,053 and 548,174,051 in all) violates in Arb the inequality the code used, every kept bin lies in its vector ball, and a separate clique search finds no configuration. This check ran as a C++ port of a separately written Python program of the deposit; the two print the same lines on each of 57 records on which both were run to the end, with 4, 5 and 6 layers, among them the record around S_6 and children of the fallback refinement. On a record that Stage C did not exclude with four layers, the separate search also finds a configuration. The graph search is exhaustive by Lemma B.1. In the comparison with a brute-force search on the 22,480 random graphs of Table 2, which have up to 4,092 vertices, its step limit acted, at every value tried, as Lemma B.1 states.

For the fine record around S_6 (Section 4.2), the vectors unbiased to the standard basis and to the columns of $H/\sqrt{6}$, for every H of the record, lie in 90 vector balls, and the graph $\mathcal{O}$ has no edge. In particular the standard basis and the columns of $S_6/\sqrt{6}$ have no common third unbiased basis, in agreement with Brierley and Weigert, who found 90 vectors unbiased to both and no orthonormal six among them [4, Section 4.1].

Three further computations in floating point do not enter the proof. The inequalities of Stages A, B and C were tested on complex Hadamard matrices, nearby solutions and vectors unbiased to them, in about 12,000, 2,800 and 26,000 cases respectively, with no violation. One thousand complex Hadamard matrices of order six, found by least squares from random starting phases, all lie, up to equivalence, in the ball of one of the 5,934 fine records, at a computed distance at least 0.0025 inside the smaller fine radius 0.016, and 173 of them lie, up to equivalence, in the ball of the record around S_6. For three records (two centered at the Fourier matrix, one from the computation), every vector that a numerical search finds unbiased to the standard basis and to sampled matrices of the record lies in a vector ball kept by Stage C, and for the two records at the Fourier matrix every orthogonal or unbiased pair among these vectors keeps its edge.

6. Concluding remarks

Under Assumption (A), Theorem 1.1 confirms Zauner's conjecture that $N(6) = 3$, and in particular $\mathbb{C}^6$ has no complete set of seven mutually unbiased bases. In the language of Section 2, no complex Hadamard matrix of order six is extendible. Earlier results established this for parts of the set. Jaming, Matolcsi, Móra, Szöllősi and Weiner proved it for the Fourier family [12]. Brierley and Weigert showed by computer algebra that the standard basis and the columns of $S_6/\sqrt{6}$ have no common third unbiased basis [4, Section 4.1], and that the pairs formed with the Diţă matrix $D(0)$ and with a circulant matrix belong to no four mutually unbiased bases (see [23, Theorems 7.14 and 7.15], which also records the search of Bengtsson et al. among Butson matrices of twelfth roots of unity [2]). McNulty and Weigert proved that a complete set of seven mutually unbiased bases would contain at most one product basis [21], classified the mutually unbiased product bases of $\mathbb{C}^6$ [20], and showed that no triple of mutually unbiased product bases has even one further vector unbiased to all three [22].

No classification of the complex Hadamard matrices of order six has appeared in a refereed journal. Szöllősi proposed a construction of a four-parameter family [33], whose existence was proved later by Bondal and Zhdanovskiy (see [23, Section 7.1]), and Karlsson constructed a three-parameter family that contains, up to equivalence, every matrix with

a 2×2 Hadamard submatrix [15, 16]. Bengtsson, Bruzda, Ericsson, Larsson, Tadej and Życzkowski found by computer search only triples of mutually unbiased bases, and gave evidence for a four-dimensional family [2]. Szöllősi conjectured that his family, Karlsson's family and S_6 give, up to equivalence, all complex Hadamard matrices of order six [33], and Cárdenes Wuttig and Tindall claim a proof in a recent preprint [6]. Of these matrices only S_6 is known to be isolated [23, Section 7.1]; its defect is zero [34, Section 5.6.4]. The proof above needs none of this. Modulo equivalence, the records of the first pass cover everything except a neighborhood of the isolated matrix S_6 (Remark 4.1). Which complex Hadamard matrices of order six belong to a triple of mutually unbiased bases remains open [23, Section 7.2 and Problem 10.5], and so does $N(10)$ [23, Section 1.1], in the next dimension that is not a prime power.

OpenAI reports a complete execution of its discretization proof [27, Section 7.5]. Ours is a second execution, by programs written separately and with rounding controlled in a different way, and it can be rerun from the deposit (Section 7). The two executions evaluate inequalities of the same lemmas, so a second execution cannot detect an error in these lemmas, and the note proves them (Appendix C). The mathematics of the proof can therefore be checked from the note. The properties (P1)–(P8) can be checked only from the code. Separately written programs have recomputed the seed cover, every Root certificate that Stages B and C use, every relation and box of Stage B and every record that Stage C excluded, but no decision of Stage A on a cell and none of the certificates that Stage A built for cells and did not keep (Section 5). The proof is a finite case analysis over a cover of all complex Hadamard matrices of order six, up to equivalence, by finitely many records: it shows, record by record, that no pair formed by the standard basis and the columns of $H/\sqrt{6}$, with H in the record, extends by two further bases to four mutually unbiased bases, but it gives no structural reason why. Neither execution is formalized in a proof assistant, and OpenAI's Lean formalization covers the weaker bound $N(6) \leq 5$, not the bound of three [26].

7. Data and code

The programs, the build commands, the logs of every process of the computation and those of the earlier execution of Section 3.1, the records of the atlas, of the mid and fine levels and of the fallback refinement, the list of seed centers, checksums of the executables and of the records, the difference between the interval arithmetic with and without the tests of Condition (B), the counts of these tests, the build records of the earlier execution, with checksums of source files used in its builds, and the programs, outputs and reports of the checks of Section 5 are deposited in [13]. The deposit states, for each statement of Section 4, the program, the command and the stored output that support it. Rerunning the seed cover and Stage A takes about a day on a machine like that of Section 4.1, and Stages B and C six to twelve hours.

Appendix A. The inequalities of the preprint that the programs decide

Each inequality of [27] that our programs decide is stated below, with its hypotheses and with its constants in the form in which the programs use them. A statement that Appendix C proves is followed by a reference to its proof there, and notes "In the computation" say where the computation decides the inequalities: by which program, for which objects and in which form. Where such a note rests on a fact about the computation, it cites the list (F1)–(F9) of Section 3.8. Numbers of statements and equations are those of the PDF of

[27]. The programs are the seed cover program, the program that enumerates the subseeds of Section 3.5, two Stage A programs, one for the seed balls and one for the subseed balls, and the Stage B and Stage C programs. Three results of [27] that the programs use are formulated for the programs of [27]: the bound on the center correction in [27, Lemma 4.9] (the correction ϵ of the proposed center P_0 of a cell in Lemma A.1), the threshold search of [27, Lemma 5.4] and the graph search of [27, Lemma 6.8]. For each of them we state and prove the version that holds for our programs (Lemmas A.1, A.2 and B.1). Appendix A.8 states and proves, for our programs, the seed cover and the Stage A cover of [27, Propositions 2.10, 3.11 and 4.16], and Proposition B.2 replaces [27, Proposition 6.9].

A.1. **Conventions.** Phases are measured in cycles, except for angles explicitly said to be in radians, and $e(t) = \exp(2\pi i t)$. Vectors and phase matrices carry the Euclidean (Frobenius) norm and linear maps the operator norm, unless a subscript says otherwise; X^* is the conjugate transpose of X, and the transpose if X is real.

An inequality is *decided* as follows. Both of its sides are evaluated in the interval arithmetic of Section 3.1, and an object (a bin pair, a cell, a bin, an edge) is rejected only if an inequality that every admissible object satisfies fails for every point of the enclosures, that is, if the lower endpoint of the side that must be the smaller exceeds the upper endpoint of the other side. A constant said to be *computed as an upper bound* is the upper endpoint, written $\mathrm{upper}(\cdot)$, of an enclosure of the quantity. The filters of Appendix A.2 on bin indices are exact integer comparisons. Proposals (the matrices T and M, record centers, directions y and v, cluster centers) are computed in floating point; every statement below holds for every real choice of them, so a proposal affects only whether a test succeeds.

Constants written in decimal (the seed radii 0.0320001 and 0.0133929, the radii τ, the cluster target 0.042 of Appendix A.7, the coefficients 1.45 and 0.45 of Appendix A.5) stand for the binary64 numbers nearest to them, and each statement is applied to those numbers. The fixed margins that [27] adds to computed quantities, and the ranges it imposes on the constants of a Root certificate [27, Sections 5.6 and A.5], belong to its a priori rounding analysis and to the limits of its programs. Our programs enclose every quantity instead and do not check these ranges, and none of the statements below needs them; where a statement of [27] is made under such a range, we say so.

A.2. **The seed cover.** Here $N = 112$, the bins are the closed intervals $[b/N, (b+1)/N]$ with midpoints $(b+\frac{1}{2})/N$, and $b_1 \le \cdots \le b_5$ are the bins of $x_1 \le \cdots \le x_5$. The *gap* of a list of midpoints is the length of the longest open arc of $\mathbb{R}/\mathbb{Z}$ that contains neither 0 nor any of the midpoints. The filters below are decided by the seed cover program and, in the same way, by the program that enumerates the subseeds.

[27, (2.7)]**, orientation filter.** The orientation condition $x_1 \le x_5 - x_4$ implies $b_1 \le b_5 - b_4 + 1$. (Proof: Lemma C.7.)

In the computation. The inequality is decided in integers for every list of bins for x that the traversal visits.

[27, Lemma 2.6]**, gap filters.** If the bin pair contains the seed coordinates of a complex Hadamard matrix, then the gaps of its two lists of midpoints satisfy

$$g_{x,\mathrm{mid}} \le 1 - \frac{b_5 - 1}{N}, \qquad g_{y,\mathrm{mid}} \ge 1 - \frac{b_5 + 2}{N}.$$

(Proof: Lemmas C.6 and C.7.)

In the computation. The gaps are compared exactly, in units of $1/(2N)$, in which they are integers: $2Ng_{x,\mathrm{mid}} \le 2(N - b_5 + 1)$ for every list for x that passes the orientation filter, and $2Ng_{y,\mathrm{mid}} \ge 2(N - b_5 - 2)$ for every pair of lists with the same shared bin that pass the filters that apply to one list.

[27, Lemma 2.7]**, sum test.** Let $u_0, \dots, u_4$ be the varying midpoints of a list (for y, the midpoint of the bin of the shared phase and those of the four others), and put $c = (1 + \sum_j e(u_j))/(2\pi i)$ and $J_j = e(u_j)$, as vectors of $\mathbb{R}^2$. If $1 + \sum_j e(u_j + \Delta_j) = 0$ with $|\Delta_j| \le 1/(2N)$, then for every $v \in \mathbb{R}^2$

$$|v \cdot c| \le \frac{5\pi}{4N^2}\|v\| + \frac{1}{2N}\sum_{j=0}^{4} |v \cdot J_j|.$$

(Proof: Lemma C.8.)

In the computation. With v the floating-point direction of c and the five directions perpendicular to $J_0, \dots, J_4$, a list is rejected only if the inequality fails in interval arithmetic for one of them. A floating-point pre-test only selects lists to keep. The test is applied to every list for x that passes the first gap filter, and to every list for y.

[27, Lemma 2.8]**, intervals for the shared phase.** Let t be the position of the shared phase in the list, $h = N\Delta$ the displacement in grid units and $E = 5\pi/(4N)$. Every displacement Δ as in the sum test satisfies $|h_t| \le \frac{1}{2}$ and, for every $v \in \mathbb{R}^2$ with $\alpha = v \cdot J_t \ne 0$,

$$\Big|h_t + \frac{N\, v \cdot c}{\alpha}\Big| \le \frac{1}{|\alpha|}\Big(E\|v\| + \frac{1}{2}\sum_{j \ne t} |v \cdot J_j|\Big),$$

and if the bin pair contains the seed coordinates of a complex Hadamard matrix, then the intervals for h_t obtained from its two lists intersect. (Proof: Lemma C.9.)

In the computation. The directions are $v = J_t$ and the directions perpendicular to J_j, $j \ne t$. A direction is skipped unless the enclosure of α lies outside $[-10^{-6}, 10^{-6}]$, and each interval is intersected with outward endpoints. A bin pair is rejected only if the two resulting intervals are disjoint. The test is applied to every pair of lists that passes the second gap filter.

[27, Lemma 2.9]**, first bound.** This is Lemma 3.7. It is decided in integers as $15{,}625\,(4(\|w\|^2 + \sum_j |w_j|) + 9) < 802{,}816$, the inequality of the proof of Lemma 3.7 multiplied by 250^2 (as $250 \cdot 0.032 \cdot 112 = 896$ and $896^2 = 802{,}816$), which holds if and only if $\|w\|^2 + \sum_j |w_j| \le 10$.

In the computation. The bound is tested for every surviving bin pair against the earlier centers with the same selected position, by the seed cover program in 64-bit integers, and in the enumeration of subseeds.

A.3. **Stage A: frames and cell tests.** Fix a seed ball or a subseed ball. Its center is given by binary64 phases, which are taken as exact real numbers, and its radius is $r_s = 0.0320001$ for the seed balls and $r_s = 0.0133929$ for the subseed balls (in cycles); put $R_s = 2\pi r_s$. After the shared column has been moved to the second position, let a, $b_0, \dots, b_3$ and $c_0, \dots, c_3$ be the entries of $e(\text{center})$ at the positions $(1,1)$, $(1,2), \dots, (1,5)$ and $(2,1), \dots, (5,1)$ (rows and columns numbered from 0), and let E_0 be the 2×2 matrix with rows $(1,1)$ and $(1,a)$, B_0 the 2×4 matrix with rows $(1,1,1,1)$ and $(b_0, \dots, b_3)$, and C_0 the 4×2 matrix with rows $(1, c_i)$ [27, (3.1)]. A *feasible completion* is a complex Hadamard matrix H' with first row and first column equal to $\mathbf{1}$ whose entries at these nine positions are ae^{is_a}, $b_j e^{is_{b_j}}$ and $c_i e^{is_{c_i}}$ for some $s \in \mathbb{R}^9$ (in radians) with $\|s\| \le R_s$; D' is its lower right 4×4 block. The computations

and tests below are made for every seed ball and every subseed ball by the two Stage A programs, which share the code of these computations and tests.

[27, Lemma 3.1], **frames.** Let $v \in \mathbb{C}^4$ have entries of modulus one, $S_v = \sum_j v_j$ and $M_v = (\mathbf{1}\ v)$. The squared singular values of M_v are $4 \pm |S_v|$, and if $|S_v| < 4$ then $M_v(M_v^* M_v)^{-1} = (16 - |S_v|^2)^{-1}(4\mathbf{1} - v\overline{S_v},\ 4v - \mathbf{1}S_v)$. In that case the last two of the four vectors produced by the Gram–Schmidt process from $\mathbf{1}/2$, v and two coordinate vectors whose residuals in this process are nonzero form an orthonormal basis of $\ker M_v^*$. With $v = (\overline{b_j})_j$ and $v = (c_i)_i$ this gives $G_B = B_0^*(B_0 B_0^*)^{-1}$, $G_C = C_0(C_0^* C_0)^{-1}$, $m_B = (4 - |\sum_j b_j|)^{1/2}$, $m_C = (4 - |\sum_i c_i|)^{1/2}$, $m = \min(m_B, m_C)$, and 4×2 matrices K_B, K_C with orthonormal columns spanning $\ker B_0$ and $\ker C_0^*$. (Proof: Lemma C.11.)

In the computation. When the frames are set up, the hypothesis $|S_v| < 4$ is decided for both choices of v, the two coordinate vectors are chosen in floating point, and every residual norm of the Gram–Schmidt process is required to have an enclosure above 10^{-6}; otherwise the ball fails the first frame check. These computations are made once for every seed ball and subseed ball.

[27, Lemma 3.2], **polar comparison.** Put $A_0 = \|E_0\| = (2 + |1 + a|)^{1/2}$, $A_* = \min(2, A_0 + R_s)$ and

$$q_Y = R_s^2\Big(1 + \frac{A_*^2 + 6}{m_C^2}\Big).$$

If $q_Y < 6$, then for every feasible completion the matrix $Y = K_C^* D' K_B$ has a polar factor $V \in U(2)$ with $\|Y - \sqrt{6}\,V\|_F \le p := q_Y/(\sqrt{6} + \sqrt{6 - q_Y})$. (Proof: Lemma C.12.)

In the computation. When the frames are set up, $q_Y < 6$ is decided (the second frame check), with A_* replaced by the upper bound $\min(2, \mathrm{upper}(A_0 + R_s))$. This is done once for every seed ball and subseed ball.

[27, Lemmas 3.3–3.7], **cell constants.** Every $V \in U(2)$ can be written as

$$V = e(\alpha)\begin{pmatrix} e(\beta)\cos 2\pi t & e(\gamma)\sin 2\pi t \\ -e(-\gamma)\sin 2\pi t & e(-\beta)\cos 2\pi t \end{pmatrix}$$

with $(\alpha, t, \beta, \gamma) \in [0, \frac{1}{2}] \times [0, \frac{1}{4}] \times [0, 1]^2$ [27, (3.12)], and $U(2)$ is covered by the closed cells of side $1/N_u$ in these parameters. For a cell let U be its midpoint matrix and $h = \pi/N_u$, and put $D = -C_0 E_0^* G_B^* + \sqrt{6}\,K_C U K_B^*$ [27, (3.15)]. If $|\sum_j b_j| < 4$, $|\sum_i c_i| < 4$ and $q_Y < 6$, as the frame checks ensure, then for every feasible completion whose V has a representation in the cell (a completion *associated with the cell*), and the corresponding angular displacement $\theta \in [-h, h]^4$ from the midpoint,

$$\|D' - D\|_F \le z, \qquad \|D' - D - \mathcal{J}(s, \theta)\|_F \le E_r,$$

where $\mathcal{J}$ is the linear map

$$\mathcal{J}(s, \theta) = (-C_1 E_0^* - C_0 E_1^* - D B_1^*) G_B^* + G_C(-E_0^* B_1 - C_1^* D) K_B K_B^* + \sqrt{6}\,K_C\,dU[\theta]\,K_B^*$$

of [27, (3.23)], in which E_1, B_1, C_1 are obtained from E_0, B_0, C_0 by multiplying each of the nine entries that vary with the seed by i times its component of s and replacing the other entries by 0, and $dU[\theta]$ is the differential of the parametrization above at the midpoint, with respect to the four angles in radians, applied to θ; $z = \big((R_s(\sqrt{6} + A_*)/m)^2 + (6h + p)^2\big)^{1/2}$, $L_{CD} = \max(\sqrt{6},\ (4 + |\sum_i c_i|)^{1/2}(1 + (A_0/m_B)^2)^{1/2})$, $e_{\mathrm{off}} = R_s^2(L_{CD} + A_0 + 1)/(2m) + zR_s/m$

and $E_r = \left(e_{\mathrm{off}}^2 + (\frac{1}{2}\sqrt{6\cdot 42}\,h^2 + p)^2\right)^{1/2}$ [27, (3.19), (3.20), (3.24), (3.25)]; here $(4+|\sum_i c_i|)^{1/2} = \|C_0\|$. (Proof: Lemmas C.13, C.14, C.15, C.16, C.17 and C.18.)

In the computation. The constants z, L_{CD} and E_r are computed as upper bounds, L_{CD} once for each seed ball and each subseed ball, and z and E_r once for each such ball and each level. The matrices U and D and the four angular derivatives of U are computed for each tested cell, and the coefficients of $\mathcal{J}$, for the directional test and for the cover of a cell, from the entrywise formulas of [27, Section 3.5].

[27, Lemma 3.8]**, norm test.** Every feasible completion associated with the cell satisfies

$$\sum_{i,j=0}^{3} \left(|D_{ij}| - 1\right)^2 \le z^2.$$

(Proof: Lemma C.19.)

In the computation. The norm test is applied to every cell that Stage A tests, at every level $N_u = 16, 32, \dots, 512$.

[27, Lemma 3.9 and Corollary 3.10]**, directional test.** Let $c_{\mathrm{all}} \in \mathbb{R}^{20}$ consist of the real and imaginary parts of $c_X = (1 + a + \sum_j b_j)/i$ and $c_Y = (1 + a + \sum_i c_i)/i$ followed by the sixteen numbers $c_{D,ij} = (|D_{ij}|^2 - 1)/2$, and let $J_{\mathrm{all}} \in \mathbb{R}^{20\times 13}$ consist of the real and imaginary parts of the coefficients of $J_X s = a s_a + \sum_j b_j s_{b_j}$ and $J_Y s = a s_a + \sum_i c_i s_{c_i}$ followed by those of $J_{D,ij}(s,\theta) = \mathrm{Re}(\overline{D_{ij}}\,\mathcal{J}_{ij}(s,\theta))$ [27, (3.27), (3.28)]. For every $y = (y_X, y_Y, y_D) \in \mathbb{R}^2 \times \mathbb{R}^2 \times \mathbb{R}^{16}$, with $g = J_{\mathrm{all}}^* y = (g_s, g_\theta) \in \mathbb{R}^9 \times \mathbb{R}^4$, every feasible completion associated with the cell satisfies

$$y \cdot c_{\mathrm{all}} \le R_s \|g_s\| + h\|g_\theta\|_1 + E_r \|D \circ y_D\|_F + \tfrac{1}{2} z^2 \max\left(0, \max_{i,j}(-y_{D,ij})\right) + \tfrac{1}{2} R_s^2 (\|y_X\| + \|y_Y\|),$$

where $D \circ y_D$ is the entrywise product [27, (3.29)]. (Proof: Lemma C.20.)

In the computation. The test is made for every cell that passes the norm test at a level $N_u \ge 32$, with four proposed directions and, if a projected subgradient ascent in floating point finds a promising one, a fifth. The four are $y = c_{\mathrm{all}}$ and three solutions of regularized least-squares problems, computed in floating point, that aim to make the right side small compared with the left. Each direction is divided by its largest absolute entry, and the stored quotient is the direction tested.

A.4. **Root certificates.** [27, Definition 4.1]**, certified Root.** A Root certificate (a Root, for short) consists of $P \in \mathbb{R}^{36}$, $T \in \mathbb{R}^{36\times k}$ with $0 \le k \le 10$, and nonnegative numbers $n_0, \iota, C, \omega, \chi, \kappa, \varphi$; put $n_P(t) = n_0 + \iota\, t + C\, t^2$. It is certified if

$$\|T^*T - I\| \le \omega, \qquad \|(I - \Pi)T\| \le \chi, \qquad \|F(P)\| \le \varphi, \tag{A.1}$$

and if every horizontal δ with $F(P + \delta) = 0$ satisfies, with $\eta = T^*\delta$,

$$\|(I - TT^*)\delta\| \le n_P(\|\delta\|), \tag{A.2}$$

$$\|\delta\|^2 \le (1 + \omega)\|\eta\|^2 + \|(I - TT^*)\delta\|^2, \tag{A.3}$$

and, for every horizontal v and $h' = \delta - v$,

$$\|(I - TT^*)h'\| \le \left[\iota + C(\|\delta\| + \|v\|)\right]\|h'\| + \kappa\,\|F(P + v)\| \tag{A.4}$$

[27, (4.3)–(4.7)].

[27, Lemmas 4.3 and 4.4]**, the remainder constant.** Write $F(P + x) = F(P) + L_P x + \mathcal{R}_P(x)$ with $(L_P x)_{ij} = \sum_g e(P_{ig} - P_{jg})(x_{ig} - x_{jg})$, and let $M \in \mathbb{R}^{36\times 30}$. If b satisfies

$\sum_{i>j} w_{ij}(y)\|x_i - x_j\|^2 \le b\|x\|^2$ for every horizontal x (with rows x_i) and every unit $y \in \mathbb{R}^{36}$, where $w_{ij}(y)$ is the norm of the two coordinates of M^*y that belong to the pair (i,j), then $\|M\mathcal{R}_P(x)\| \le \pi b\|x\|^2$ and $\|M(\mathcal{R}_P(x) - \mathcal{R}_P(v))\| \le \pi b\|x - v\|(\|x\| + \|v\|)$ for horizontal x, v [27, (4.10)–(4.12)]. Both $b = \sqrt{8}\,\|M\|$ and $b = \sqrt{6}\,\|\mathcal{M}\|$ are admissible, where $\mathcal{M} \in \mathbb{R}^{30\times 216}$ is defined in Lemma C.22 and $(\mathcal{M}\mathcal{M}^*)_{ll'} = ((\mathbf{e}_i - \mathbf{e}_j)\cdot(\mathbf{e}_{i'} - \mathbf{e}_{j'}))\,(M_{:,l}\cdot M_{:,l'})$ for coordinates l, l' belonging to the pairs (i,j) and (i',j') [27, (4.14)]. (Proof: Lemmas C.21 and C.22.)

[27, Proposition 4.5]**, sufficient conditions.** If (A.1) holds, M satisfies

$$\|M\| \le \kappa, \qquad \kappa\varphi \le n_0, \qquad \|\Pi - TT^* - ML_P\Pi\| \le \iota$$

[27, (4.15)], and $C \ge \pi b$ for an admissible b, then (A.2)–(A.4) hold. (Proof: Lemma C.23.)

In the computation. One routine, common to the Stage A and Stage B programs, certifies every Root built in Stages A and B, and it refuses a Root with $k > 10$. The constants are computed as upper bounds: φ of $\|F(P)\|$, ω of $\|T^*T - I\|_F$, χ of $\|(I-\Pi)T\|_F$ and ι of $\|\Pi - TT^* - ML_P\Pi\|_F$ (Frobenius norms bound operator norms), with $F(P)$, L_P and Π enclosed. The constant κ is the least of the upper bounds for $\|M\|_F$, for $(\max_l \sum_{l'} |(M^*M)_{ll'}|)^{1/2}$ (by Gershgorin's theorem) and for $\mu^{1/2}$, where $\mu > \lambda_{\max}(M^*M)$ by Lemma 3.6. The constant n_0 is an upper bound for $\kappa\cdot\varphi$, and C is the smaller of the upper bounds for $\pi\sqrt{8}\,\kappa$ and $\pi(6\mu')^{1/2}$, where $\mu' > \lambda_{\max}(\mathcal{M}\mathcal{M}^*)$ by Lemma 3.6. The proposition [27, Proposition 4.6], about the routine of [27] that builds Root certificates, and the acceptance thresholds of [27, Section A.5] ($\iota < 10^{-4}$, $\omega, \chi < 10^{-5}$, $C < 20$, $\kappa < 2$) are not used. Stages B and C use a stored Root only through (A.1)–(A.4), also for records stored in permuted, possibly transposed, coordinates (Section 3.5), which keep their constants by Lemma C.24 ([27, Lemma 4.7]).

A.5. **Stage A: from a cell to a record.** Consider a cell at a level $N_u \ge 64$ that the tests of Appendix A.3 do not exclude. At the sixteen lower right positions $j \in \mathcal{I}_D$ (rows and columns $2,\dots,5$) let $m_j = |D_j|$ and $D_j^\circ = D_j/m_j$, let $\mathcal{I}_s$ be the nine seed positions, and for a feasible completion let $d_j \in [-\pi,\pi]$ be the angle from D_j° to D_j'. Let $X : \mathbb{R}^{13} \to \mathbb{R}^{36}$ map (s,θ) to the matrix equal to s on $\mathcal{I}_s$, to $\mathrm{Im}(\overline{D_j^\circ}\,\mathcal{J}(s,\theta)_j)$ at $j \in \mathcal{I}_D$ and to 0 elsewhere [27, (4.23)]; X_s and X_θ are its restrictions to the coordinates s and θ, and $X_{\theta,l}$ is the column of X_θ for the l-th coordinate θ_l of θ. For a Root certificate $(P, T, \dots)$, T_D and $T_{j,:}$ are the rows of T at $\mathcal{I}_D$ and at j. The Stage A programs make the computations below when they attempt to cover such a cell. Those of Lemma C.25 ([27, Lemma 4.8]) and Lemma A.1 are made once for the cell, and the others for each Root against which its cover is attempted: at most six earlier Roots of the seed ball, nearest first, and then, if none of them covers the cell, at most one new Root. The atlas merge is made when a returned record is added to the atlas.

[27, Lemma 4.8]**, arc bounds.** If $\Lambda \ge 0$ is an upper bound for $z^2 - \sum_j (m_j - 1)^2$, $0 < \underline{m} \le \min_j m_j$, $q_d \ge \Lambda/\underline{m}$ and $q_d < 3.8$, then every feasible completion associated with the cell satisfies $\|d\| \le \bar{d}$ and $(\sum_j m_j d_j^2)^{1/2} \le \bar{d}_m$ whenever $\bar{d} \ge q_d^{1/2}(1 - q_d/4)^{-1/2}$ and $\bar{d}_m \ge \Lambda^{1/2}(1 - q_d/4)^{-1/2}$ [27, (4.18), (4.19)]. (In [27], Λ, $\underline{m}$, $\bar{d}$ and $\bar{d}_m$ are called slack, mi, arc and weighted.) (Proof: Lemma C.25.)

In the computation. Once for each cell: $\underline{m}$ is the lower endpoint of the enclosure of $\min_j m_j$ and is required to exceed 0.05, Λ is $\max\big(0, \mathrm{upper}(z^2 - \sum_j (m_j - 1)^2)\big)$, the enclosure of $\Lambda/\underline{m}$ is required to lie below 3.8, and $\bar{d}$ and $\bar{d}_m$ are enclosed.

The center correction of [27, Lemma 4.9] is the matrix ϵ of the following lemma, which corrects the proposed phases $(P_0)_j$, $j \in \mathcal{I}_D$, of the lower right block to phases of the entries of D°. It is bounded there by $2 \cdot 10^{-6}$ [27, (4.20)], a bound proved for the routine of [27] that proposes the phases of the lower right block. Our programs use the following version, with a bound computed for each cell.

Lemma A.1. *Assume the hypotheses of Lemma C.25. Let $P_0 \in \mathbb{R}^{36}$ vanish in the first row and column, equal the phases of the seed center on $\mathcal{I}_s$, and have arbitrary real entries $(P_0)_j$ at $j \in \mathcal{I}_D$, and let $c_j \geq |e((P_0)_j) - D^\circ_j|$ for $j \in \mathcal{I}_D$. Then the phase matrix of every feasible completion associated with the cell is congruent modulo $\mathbb{Z}^{36}$ to $P_0 + \epsilon + u/(2\pi)$, where ϵ vanishes off $\mathcal{I}_D$ and*

$$\|\epsilon\| \leq \bar{\epsilon} := \Big(\sum_{j \in \mathcal{I}_D} (c_j/4)^2 \Big)^{1/2},$$

and where u equals s on $\mathcal{I}_s$, d on $\mathcal{I}_D$ and 0 elsewhere, so that $\|u\| \leq (R_s^2 + \bar{d}^2)^{1/2}$, and $u = X(s,\theta) + e_D + e_{\sin}$ with $e_D, e_{\sin}$ vanishing off $\mathcal{I}_D$, $\|e_D\| \leq E_r$ and $\|e_{\sin}\|_1 \leq \bar{d}^3/6$.

Proof. Let ψ_j be a phase of D°_j, and let $t_j \in [0, \frac{1}{2}]$ be the distance from $\psi_j - (P_0)_j$ to $\mathbb{Z}$. Then $c_j \geq |e((P_0)_j) - e(\psi_j)| = 2\sin(\pi t_j) \geq 4t_j$, because the sine is concave on $[0, \pi/2]$. So $\psi_j \equiv (P_0)_j + \epsilon_j \pmod 1$ with $|\epsilon_j| = t_j \leq c_j/4$. The completion has the entries 1 in the first row and column, $e((P_0)_j + s_j/(2\pi))$ at $j \in \mathcal{I}_s$, and $D'_j = D^\circ_j e^{id_j} = e((P_0)_j + \epsilon_j + d_j/(2\pi))$ at $j \in \mathcal{I}_D$; this proves the representation. Since u equals s on $\mathcal{I}_s$ and d on $\mathcal{I}_D$, $\|u\|^2 = \|s\|^2 + \|d\|^2 \leq R_s^2 + \bar{d}^2$ by Lemma C.25. Let e_D and $e_{\sin}$ vanish off $\mathcal{I}_D$, with entries $(e_D)_j = \sin d_j - X(s,\theta)_j$ and $(e_{\sin})_j = d_j - \sin d_j$ for $j \in \mathcal{I}_D$; then $u = X(s,\theta) + e_D + e_{\sin}$, since $X(s,\theta)$ equals s on $\mathcal{I}_s$ and vanishes outside $\mathcal{I}_s \cup \mathcal{I}_D$. As $D'_j = D^\circ_j e^{id_j}$ and $\overline{D^\circ_j} D_j = m_j$ is real, $\operatorname{Im}(\overline{D^\circ_j}(D'_j - D_j)) = \sin d_j$, so $(e_D)_j = \operatorname{Im}(\overline{D^\circ_j}(D' - D - \mathcal{J}(s,\theta))_j)$ and $\|e_D\| \leq \|D' - D - \mathcal{J}(s,\theta)\|_F \leq E_r$ by Lemma C.17; and $\|e_{\sin}\|_1 \leq \sum_j |d_j|^3/6 \leq \|d\|^3/6 \leq \bar{d}^3/6$ by Lemma C.1(iii) and Lemma C.25. □

In the computation. Once for each cell: $(P_0)_j$ is a floating-point phase of D_j, and c_j is the upper endpoint of the enclosure of $|e((P_0)_j) - D_j/|D_j||$; $\bar{\epsilon}$ is enclosed and used wherever [27] uses $\|\epsilon\|$ below.

[27, Lemma 4.10]**, direct bound.** For a Root certificate with center P and an integer matrix Z, put $\Delta = \Pi(P_0 - D_0(P) - Z)$ [27, (4.25)], where $(D_0 Y)_{ij} = Y_{ij} - Y_{i0} - Y_{0j} + Y_{00}$. Every feasible completion associated with the cell is equivalent to $e(P+\delta)$ with $\delta = \Delta + \Pi(\epsilon + u/(2\pi))$ horizontal, and

$$\|\delta\| \leq \Big(\|\Delta\|^2 + \frac{R_s^2 + \bar{d}^2}{(2\pi)^2} + \frac{S_\Delta}{\pi} \Big)^{1/2} + \|\epsilon\|,$$

where $S_\Delta = \min(S_1, S_2)$, $S_1 = R_s \|(X^*\Delta)_s\| + h\|(X^*\Delta)_\theta\|_1 + E_r\|\Delta_D\| + \|\Delta_D\|_\infty \bar{d}^3/6$ and $S_2 = R_s\|\Delta_s\| + \bar{d}_m \, (\sum_{j \in \mathcal{I}_D} \Delta_j^2/m_j)^{1/2}$; subscripts s and D on Δ denote its restrictions to $\mathcal{I}_s$ and $\mathcal{I}_D$ [27, (4.27)–(4.29)]. (Proof: Lemma C.26.)

In the computation. The bound is evaluated for each cell and Root, with Z the entrywise nearest integers of the floating-point differences and with $\|\epsilon\|$ replaced by $\bar{\epsilon}$.

[27, (4.30) and Lemmas 4.11 and 4.12]**, tangent bound.** In the setting of the direct bound, let the Root certificate satisfy (A.1). Then $\|2\pi T^*\delta - (2\pi T^*\Delta + T^*u)\| \leq \chi \, (R_s^2 + \bar{d}^2)^{1/2} + 2\pi(1+\omega)^{1/2}\|\epsilon\|$, and $\|T^* e_{\sin}\| \leq \max_{j \in \mathcal{I}_D} \|T_{j,:}\| \, \bar{d}^3/6$. For linear maps A, B, $\|s'\| \leq \rho$, $\|v\| \leq \rho'$ and $\beta > 0$, the vector $As' + Bv$ lies in $\{G^{1/2} w : \|w\| \leq 1\}$, where $G^{1/2}$ is the positive semidefinite

square root of G [8, Theorem 7.2.6], whenever $G \succeq (1+\beta)\rho^2 AA^* + (1+1/\beta)\rho'^2 BB^*$ ([27, Lemma 4.11]); [27] applies it with $\beta = 0.45$, $A = T^*X_s$, $\rho = R_s$, $B = T_D^*$, $\rho' = E_r$ [27, (4.32)], and the matrix $1.45R_s^2(T^*X_s)(T^*X_s)^* + (1+1/0.45)E_r^2 T_D^* T_D$ is what [27] calls the *covariance*. For $G \succeq 0$, $U \in \mathbb{R}^k$, $\gamma > \lambda_{\max}(G)$ and $\|w\| \le 1$, $\|U + G^{1/2}w\|^2 \le \gamma(1 + U^*(\gamma I - G)^{-1}U)$ and $\|U + G^{1/2}w\| \le \|U\| + \lambda_{\max}(G)^{1/2}$, and for offsets in the convex hull of finitely many U_σ the maximum of the bounds at the U_σ is a bound ([27, Lemma 4.12]); moreover $U^*(\gamma I - G)^{-1}U \le U^*y + \|U\|\,\|U - (\gamma I - G)y\|/\mathrm{gap}$ for every $y \in \mathbb{R}^k$ and $0 < \mathrm{gap} \le \gamma - \lambda_{\max}(G)$ [27, (4.37)]. With the sixteen offsets $U_\sigma = 2\pi T^*\Delta + h\sum_{l=1}^4 \sigma_l T^* X_{\theta,l}$, $\sigma \in \{\pm 1\}^4$ [27, (4.31)], and a resulting bound $\mathcal{E}$ for $\max \|U + G^{1/2}w\|$,

$$\|T^*\delta\| \le \frac{\mathcal{E} + \max_{j\in\mathcal{I}_D} \|T_{j,:}\|\,\bar{d}^3/6 + \chi\,(R_s^2 + \bar{d}^2)^{1/2}}{2\pi} + (1+\omega)^{1/2}\|\epsilon\|$$

[27, (4.35)]. (Proof: Lemmas C.27, C.28 and C.29.)

In the computation. The bound is evaluated for each cell and Root with $k > 0$, with $\|\epsilon\|$ replaced by $\bar{\epsilon}$. Our code takes the coefficient $1 + 0.45$ of the covariance to be $\mathrm{fl}(1.45)$ and encloses $1 + 1/0.45$ from $\mathrm{fl}(0.45)$, with an outward step after each operation. These two values do not correspond to one parameter. But the upper endpoint of the enclosure is at least $\mathrm{next}_{\mathrm{up}}(\mathrm{fl}(1 + \mathrm{next}_{\mathrm{up}}(\mathrm{fl}(1/\,\mathrm{fl}(0.45))))) = 3.2222222222222232\ldots$, which exceeds $1 + 1/(\mathrm{fl}(1.45) - 1) = 3.2222222222222224\ldots$ (here $\mathrm{fl}(0.45) = 0.45 + 2^{-54}/5$ and $\mathrm{fl}(1.45) = 1.45 - 2^{-52}/5$) by more than $7\cdot 10^{-16}$. So the interval for $1+1/0.45$ contains $1+1/(\mathrm{fl}(1.45)-1)$, and the bound holds with $\beta = \mathrm{fl}(1.45) - 1$, for which $1 + \beta = \mathrm{fl}(1.45)$. The matrix $G = \hat{G}$ of Lemma 3.6, with the diagonal entries of $G_0 + \rho I$ (ρ the Gershgorin bound of that lemma, not $\rho = R_s$) computed as upper bounds, dominates the enclosure of the covariance, and $\mu > \lambda_{\max}(G)$ by Lemma 3.6. For each offset the smaller of the two bounds is taken, the first with four proposed $\gamma > \mu$ and with gap the lower endpoint of the enclosure of $\gamma - \mu$. The alternative covariance with $\beta = 0.8$ [27, (4.33), (4.36)] is not used.

[27, Proposition 4.13]**, bootstrap.** Let the Root certificate at P be certified. If $s_0 \ge \|\delta\|$ and $t_0 \ge \|T^*\delta\|$ for every feasible completion associated with the cell, then $\left(n_P(s_0)^2 + (1+\omega)t_0^2\right)^{1/2} \ge \|\delta\|$ for every feasible completion associated with the cell, so s_0 may be replaced by this number whenever it is smaller. (Proof: Lemma C.30.)

In the computation. For each cell and Root the bootstrap starts from the direct bound and makes at most 30 replacements while the value decreases (for $k = 0$ the direct bound is used as it is). The cell is covered by the record of the Root if the final value is at most 0.103: the radius of the record of an earlier Root is then raised to this value if it is smaller, and for a new Root a record with this radius is created.

[27, Lemma 4.15]**, atlas merge.** A record of center P and radius r is covered by the record of center Q and radius $r + \ell$ if $\ell \ge \|\Pi(D_0(gP) - D_0(Q) - Z)\|$ for a map g of Lemma C.24 and an integer matrix Z. (Proof: Lemma C.31.)

In the computation. Whenever a Stage A program adds a record to its atlas, it computes ℓ as an upper bound for this norm, with Z the entrywise nearest integers of the floating-point differences. The binary64 sum $\ell + r$ is widened by the outward step of Section 3.1, a merge is made only if the result is at most 0.125, and the radius of the atlas record merged into becomes the larger of its old radius and this result.

A.6. **Stage B: relations between records.** Let (P, R) be a parent record whose Root certificate has k columns and constants $n_{0,P}, \iota_P, C_P, \omega_P, \kappa_P, \varphi_P$ (called $\mathrm{n0}_P, \alpha_P, \gamma_P, o_P, \mu_P, \varepsilon_P$

in [27, (5.2)]), and put $n_P(s) = n_{0,P} + \iota_P s + C_P s^2$ and $A = I - TT^*$. Let $(Q, T_Q, \dots)$ be a second certified Root certificate, with k_Q columns and the same notation with subscript Q. It is a new child, or the copy, transported by some g^{-1} with $g \in \mathcal{G}$ (Section 3.6), of a stored child or of a blocker; such a copy is certified with the constants of the stored record by Lemma C.24. For an integer matrix Z put $d_q = \Pi(D_0 Q - D_0 P - Z)$, $\eta_q = T^* d_q$ and $n_q = \|A d_q\|$ [27, (5.5)], and for $e(P+\delta) \in \mathcal{S}(P,R)$ put $\eta = T^*\delta$, $h' = \delta - d_q$, $d = \|h'\|$, $\xi = \eta - \eta_q$ and $\nu = Ah'$ [27, (5.6)]. We call the pair formed by the parent and this second Root certificate a *relation*. The Stage B program makes the computations below in every refinement of the computation, for every relation that it attempts, with a new child or with a stored child or blocker, transported or not.

[27, Lemma 5.1]**, norm bounds.** $\|T\| \le (1+\omega_P)^{1/2}$, $\|A\| \le 1 + \omega_P$, and $\|x\|^2 \le (1+\omega_P)\|T^*x\|^2 + \|Ax\|^2$ for every $x \in \mathbb{R}^{36}$. (This statement is used in the proofs of Lemmas C.33, C.35 and C.36.) (Proof: Lemma C.32.)

[27, Proposition 5.2]**, relation estimates.** Suppose that $t \ge \|\xi\|$, $\hat{d} \ge R + \|d_q\|$, $v_0 \ge n_P(R) + n_q$, $\lambda \ge \iota_P + C_P\hat{d}$, $e_0 \ge \kappa_P \varphi_Q$, $\sigma \ge \|(\Pi T_Q)^* A\|$ and $\beta \ge (1+\omega_P)\big((1+\omega_P)(1+\omega_Q)\big)^{1/2}$. Then

$$d \le \hat{d}, \qquad d^2 \le (1+\omega_P)t^2 + \|\nu\|^2, \qquad \|\nu\| \le \min\{v_0, (1+\omega_P)d, \lambda d + e_0\},$$
$$\|T_Q^* h'\| \le \beta t + \sigma\|\nu\|, \qquad d^2 \le (1+\omega_Q)\|T_Q^* h'\|^2 + n_Q(d)^2$$

[27, (5.7)–(5.12)]. (Proof: Lemma C.33.)

In the computation. For each relation attempted: Z is the matrix of entrywise nearest integers of the floating-point differences of the dephased centers; d_q, η_q and n_q are enclosed; $\hat{d}$, v_0, λ, e_0 and β are computed as upper bounds; $\sigma = 0$ if $k_Q = 0$, and otherwise σ is the upper bound for $(\min(\|G\|_F, \max_b \sum_c |G_{bc}|))^{1/2}$ with $G = (A\Pi T_Q)^*(A\Pi T_Q)$ enclosed. Each of the two quantities in the minimum is an upper bound for $\|G\| = \|(\Pi T_Q)^* A\|^2$ (the second by Gershgorin's theorem); [27] uses $\max_b \sum_c |G_{bc}|$ and $\|G^2\|_F^{1/2}$ instead.

[27, Lemma 5.3]**, distance iteration.** In the setting of the relation estimates, for $t \ge 0$ put $z_t = (1+\omega_P)^{1/2} t$, $v(b) = \min\{v_0, (1+\omega_P)b, \lambda b + e_0\}$, $\psi_P(b) = (z_t^2 + v(b)^2)^{1/2}$ and $\psi_Q(b) = \big((1+\omega_Q)(\beta t + \sigma v(b))^2 + n_Q(b)^2\big)^{1/2}$, start with $b_0 = \min\{\hat{d}, (z_t^2 + v_0^2)^{1/2}\}$ and put $b_{j+1} = \min\{b_j, \psi_P(b_j), \psi_Q(b_j)\}$ [27, (5.14)–(5.16)]. Every b_j is an upper bound for d, for every $e(P+\delta) \in \mathcal{S}(P,R)$ with $\|\xi\| \le t$; this remains true if any value is replaced by a larger number and if the iteration is stopped after finitely many steps. (Proof: Lemma C.34.)

In the computation. The iteration is computed with at most 30 steps, stopping when the value does not decrease; every value is the upper endpoint of an enclosure.

The threshold search of [27, Lemma 5.4] and its use in [27, Lemma 5.5] are formulated with the margins of the search routine of [27]. Our programs use the following statement.

Lemma A.2. *In this setting let $a \ge 0$ and $\ell \ge 0$, and let b be a value of the iteration of Lemma C.34 at $t = \ell$. If $b \le a$, then:*

(i) every $e(P+\delta) \in \mathcal{S}(P,R)$ with $\|T^*\delta - \eta_q\| \le \ell$ is equivalent to a member of $\mathcal{S}(Q,a)$;

(ii) if $u \in \mathbb{R}^k$ and $h \ge 0$ satisfy $\big(\sum_{i=1}^k (|u_i - \eta_{q,i}| + h)^2\big)^{1/2} \le \ell$, then every $e(P+\delta) \in \mathcal{S}(P,R)$ with $T^*\delta \in \prod_{i=1}^k [u_i - h, u_i + h]$ is equivalent to a member of $\mathcal{S}(Q,a)$.

Proof. (i) By Lemma C.34, $\|h'\| \le b \le a$. For every real matrix Y the matrix $D_0 Y - Y$ is the sum of a matrix constant along rows and one constant along columns, so it lies in $\ker \Pi$.

Hence $Q+h'-(P+\delta)=Q-P-d_q$ is the sum of the integer matrix Z and such a matrix, and $e(Q+h')$ is obtained from $e(P+\delta)$ by multiplying rows and columns by numbers of modulus one. So $e(Q+h')$ is a complex Hadamard matrix equivalent to $e(P+\delta)$, and since h' is horizontal with $\|h'\|\le a$, it belongs to $\mathcal{S}(Q,a)$. (ii) On the box, $\|T^*\delta-\eta_q\|^2$ is at most the sum in (ii), the coordinates being bounded separately (Lemma C.35); apply (i). □

In the computation. For each relation, the threshold search returns either no threshold or a number ℓ at which the iteration of Lemma C.34 was computed with a value at most a: $\ell=0$, $\ell=\min(2,3a+0.01)$, or the last accepted of 16 bisection trials. Here $a=\tau$ for children, and a is the radius of the blocker for blockers. Wherever the program marks a box of the tangent grid, or a box of a subdivision, against a relation, it does so only if an upper bound for the left side of the inequality in (ii), computed with η_q enclosed, is at most ℓ.

[27, (5.20), (5.22), (5.23)]**, the tangent grid.** Every $e(P+\delta)\in\mathcal{S}(P,R)$ has $\|T^*\delta\|\le E_P:=(1+\omega_P)^{1/2}R$. For $u\in\mathbb{R}^k$ and $h\ge 0$ let $B(u,h)=\prod_{i=1}^k[u_i-h,u_i+h]$. Then $\operatorname{dist}(0,B(u,h))^2=\sum_i\max(0,|u_i|-h)^2$, and $B(u,h)$ is the union of the 2^k boxes $B(u+\epsilon h/2,h/2)$, $\epsilon\in\{-1,1\}^k$. (Proof: Lemma C.35.)

In the computation. For every parent, E is the upper bound for E_P, and the base boxes are $B(bw,w/2)$, $b\in\{-N_E,\dots,N_E\}^k$, with $N_E=\lceil E/w+0.500001\rceil$ computed in binary64. Each rounding in this computation has relative error at most 2^{-53}, and $E/w<33$ for every parent of the computation: every radius is at most 0.125 and every constant ω is below 0.06, by (F6), and $w\ge 4/1024$, the smallest of the widths listed below. So $N_E>E/w+\frac12$, and hence the union of the base boxes, $[-(N_E+\frac12)w,(N_E+\frac12)w]^k$, contains $[-E,E]^k$ with more than one box width to spare. A box, of the grid or of a subdivision, is dropped as lying outside only if a lower bound for its squared distance from 0 exceeds the upper bound for E^2. The widths w are 13/1024, 6/1024, 5/1024 and 4/1024 for $\tau=0.07$, 0.02, 0.016 and 0.011, and the depth of subdivision is at most six. So every box center is an integer multiple of $w/2^7$, and hence of 2^{-17}, with absolute value less than $(N_E+\frac12)w\le 34.5\,w<\frac12$; it is therefore a binary64 number, and subdivision is exact.

A.7. **Stage C: bins, vector balls and edges.** Fix a record (P,r) whose Root certificate $(P,T,\dots)$ has k columns, and put

$$r_H=(1+\omega)^{1/2}r,\qquad n=n_0+\iota\,r+C\,r^2,\qquad K=\Big(1+\frac{2\pi\sqrt{2}}{6}\,\varphi\Big)^{1/2}.$$

By (A.1) and (A.2), every horizontal δ with $\|\delta\|\le r$ and $F(P+\delta)=0$ satisfies $\|\eta\|\le r_H$ and $\|\nu\|\le n$ for $\eta=T^*\delta$ and $\nu=\delta-T\eta$ [27, (6.2)], and $\|e(P)/\sqrt{6}\|\le K$ because $\|e(P)e(P)^*-6I\|_F=2\pi\sqrt{2}\,\|F(P)\|$ [27, (6.3)] (Lemma C.36). The preprint [27] states its Section 6 for records with $r\le 0.03$, $\varphi<10^{-6}$, $\omega<10^{-5}$, $n_0<10^{-6}$, $\iota<10^{-4}$ and $C<20$ [27, (6.1), (6.2)], and uses $K=1.00001$. The statements below are proved, in Appendix C or where they are stated, with K as above and without these ranges, which our programs do not check (Section 3.7(iv)). The records tested have $r=0.02$, 0.016 or 0.011 (F8).

A vector unbiased to the standard basis is $\lambda e(\beta)/\sqrt{6}$ with $|\lambda|=1$, $\beta_0=0$ and $\beta_1,\dots,\beta_5\in[0,1)$. At the resolution M_ℓ of layer ℓ a *bin* is a product of five closed intervals $[b_j/M_\ell,(b_j+1)/M_\ell]$; let u be its midpoint, with $u_0=0$, and $a=1/(2M_\ell)$. Up to a scalar of modulus one, the vectors with β in the bin are the vectors $e(u+x)/\sqrt{6}$ with $x=d-\frac16(\sum_j d_j)\mathbf{1}$, $d_0=0$ and $|d_j|\le a$. Index the columns of the Hadamard matrix by i

and the coordinates of vectors by j, and put

$$q_{ji} = \frac{e(u_j - P_{ji})}{\sqrt{6}}, \qquad S_i = \sum_j q_{ji}, \qquad c_i = \frac{|S_i|^2 - 1}{4\pi},$$
$$J_{ij} = -\operatorname{Im}(\overline{S_i} q_{ji}), \qquad B_{il} = \sum_j J_{ij} T_{6j+i,\,l}$$

[27, (6.5), (6.8)], where row $6j+i$ of T belongs to the position (j,i). The vector $e(u+x)/\sqrt{6}$ is unbiased to the columns of $e(P+\delta)/\sqrt{6}$ if and only if $|S_i'| = 1$ for all i, where $S_i' = \sum_j q_{ji} e(x_j - \delta_{ji})$. In bin tests (1)–(3), unbiasedness means this for some $e(P+\delta) \in \mathcal{S}(P,r)$. The Stage C program makes the tests below for every record it tests, in each of its runs with four, five or six layers.

[27, Lemma 6.1], **bin displacement.** $\sum_j x_j = 0$, $\|x\| \le X_{M_\ell} := (29/6)^{1/2} a$, $\|x\|_1 \le L_{M_\ell} := 5a$ and $\|x\|_\infty \le I_{M_\ell} := \frac{3}{2} a$ [27, (6.4)]. (Proof: Lemma C.37.)
In the computation. The numbers a, X_{M_ℓ}, L_{M_ℓ} and I_{M_ℓ} are enclosed once for each layer.

[27, Lemma 6.2], **direct tests: bin test (1).** If $\|x\| \le X$, $\|x\|_1 \le L$ and $\|\delta\| \le r$, then $\|S' - S\| \le 2\pi(KX + r)$ and $|S_i' - S_i| \le 2\pi(L/\sqrt{6} + r)$. Hence, with $\vartheta = 2\pi(L/\sqrt{6} + r)$, unbiasedness requires

$$\max\{0, 1-\vartheta\}^2 \le |S_i|^2 \le (1+\vartheta)^2 \quad (0 \le i \le 5), \qquad \sum_i \big(|S_i| - 1\big)^2 \le \big(2\pi(KX + r)\big)^2$$

[27, (6.6), (6.7)]. (Proof: Lemma C.39.)
In the computation. Bin test (1) is applied to every bin of every layer, with $X = X_{M_\ell}$ and $L = L_{M_\ell}$. The lower bound on $|S_i|^2$ is tested only when the upper endpoint of the enclosure of ϑ is below 1, and the two bounds on $|S_i|^2$ are also tested first, as a quick pre-test.

[27, (6.12), (6.13)], **scalar test: bin test (2).** With $X = X_{M_\ell}$, $L = L_{M_\ell}$, $I = I_{M_\ell}$ and $S_{\max} = \max_i |S_i|$, unbiasedness requires, for each i,

$$|c_i| \le a \sum_{j>0} |J_{ij}| + r\|J_{i,:}\| + \rho,$$
$$\rho = \min\Big\{\pi\Big[(KX+r)^2 + S_{\max}\Big(KIX + \frac{2Xr + r^2}{\sqrt{6}}\Big)\Big],\ \pi\Big[\Big(\frac{L}{\sqrt{6}} + r\Big)^2 + \frac{S_{\max}(X+r)^2}{\sqrt{6}}\Big]\Big\}.$$

Proof. Fix i, let x be as above, so that $\|x\| \le X$, $\|x\|_1 \le L$ and $\|x\|_\infty \le I$ by Lemma C.37, and let δ be a real matrix with $\|\delta\| \le r$ and $|S_i'| = 1$. Put $w_j = x_j - \delta_{ji}$, $\Delta_i = S_i' - S_i$ and $R(t) = e(t) - 1 - 2\pi i t$ for real t. Integrating the first and the second derivative of e from 0 to t gives $|e(t) - 1| \le 2\pi|t|$ and $|R(t)| \le 2\pi^2 t^2$. Since $\Delta_i = \sum_j q_{ji}(2\pi i w_j + R(w_j))$ and $\operatorname{Re}(2\pi i\, \overline{S_i} q_{ji}) = 2\pi J_{ij}$, expanding $|S_i + \Delta_i|^2 = 1$ and dividing by 4π gives

$$c_i = -\sum_j J_{ij} x_j + \sum_j J_{ij}\delta_{ji} - \frac{1}{2\pi}\operatorname{Re}\Big(\overline{S_i}\sum_j q_{ji} R(w_j)\Big) - \frac{|\Delta_i|^2}{4\pi}.$$

The row $J_{i,:}$ sums to $-\operatorname{Im}(\overline{S_i} S_i) = 0$, so $\sum_j J_{ij} x_j = \sum_{j>0} J_{ij} d_j$, whose absolute value is at most $a\sum_{j>0}|J_{ij}|$, and $|\sum_j J_{ij}\delta_{ji}| \le \|J_{i,:}\|\,\|\delta_{:,i}\| \le r\|J_{i,:}\|$. The sum of the absolute values of the last two terms is at most $\rho_i = |S_i|\,|\sum_j q_{ji} R(w_j)|/(2\pi) + |\Delta_i|^2/(4\pi)$, and $|S_i| \le S_{\max}$, so it remains to show that ρ_i is at most each of the two numbers of which ρ is the minimum. For the second, $|\Delta_i| \le 2\pi(L/\sqrt{6} + r)$ by Lemma C.39, and $|q_{ji}| = 1/\sqrt{6}$ and $\sum_j w_j^2 = \|x - \delta_{:,i}\|^2 \le (X+r)^2$, so $|\sum_j q_{ji} R(w_j)| \le 2\pi^2 (X+r)^2/\sqrt{6}$ and

$\rho_i \le \pi S_{\max}(X+r)^2/\sqrt{6} + \pi(L/\sqrt{6}+r)^2$. For the first, $|\Delta_i| \le \|S'-S\| \le 2\pi(KX+r)$ by the same lemma. Moreover $R(x_j-\delta_{ji}) = R(x_j) + R(-\delta_{ji}) + \big(e(x_j)-1\big)\big(e(-\delta_{ji})-1\big)$, since $e(x_j-\delta_{ji}) = e(x_j)e(-\delta_{ji})$. The linear map Q of $\mathbb{C}^6$ that sends y to $(\sum_j q_{ji'}y_j)_{i'}$ has the matrix $e(P)^*\operatorname{diag}(e(u_0),\dots,e(u_5))/\sqrt{6}$, so $\|Q\| = \|e(P)/\sqrt{6}\| \le K$. The vector $(R(x_j))_j$ has norm at most $2\pi^2(\sum_j x_j^4)^{1/2} \le 2\pi^2\|x\|_\infty\|x\| \le 2\pi^2 IX$. As $\sum_j \delta_{ji}^2 \le r^2$ and $\sum_j |x_j\delta_{ji}| \le Xr$, it follows that

$$\Big|\sum_j q_{ji}R(w_j)\Big| \le 2\pi^2 KIX + \frac{2\pi^2}{\sqrt{6}}\sum_j \delta_{ji}^2 + \frac{4\pi^2}{\sqrt{6}}\sum_j |x_j\delta_{ji}| \le 2\pi^2\Big(KIX + \frac{2Xr+r^2}{\sqrt{6}}\Big),$$

and so $\rho_i \le \pi S_{\max}(KIX + (2Xr+r^2)/\sqrt{6}) + \pi(KX+r)^2$. □

In the computation. Bin test (2) is applied to every bin that passes test (1).

[27, Lemma 6.3]**, weighted test: bin test (3).** For $y \in \mathbb{R}^6$ put $G_y = \max_j |\sum_i y_i\overline{S_i}q_{ji}|$, $N_y = (\sum_{i,j} y_i^2 J_{ij}^2)^{1/2}$ and $S\circ y = (S_i y_i)_i$. If $\|x\| \le X$ and $\|x\|_\infty \le I$, then unbiasedness implies $|y\cdot(c+Jx-B\eta)| \le \mathcal{E}(y;X,I)$ for every $y \in \mathbb{R}^6$, where

$$\mathcal{E}(y;X,I) = nN_y + \pi\Big[\|y\|_\infty(KX+r)^2 + \min\{G_yX^2,\ K\|S\circ y\|IX\} + \frac{2}{\sqrt{6}}\|S\circ y\|Xr + \frac{1}{\sqrt{6}}\|S\circ y\|_\infty r^2\Big]$$

[27, (6.9), (6.10)]. For a bin this gives the necessary condition

$$|y\cdot c| \le a\sum_{j>0}|(J^*y)_j| + r_H\|B^*y\| + \mathcal{E}(y;X_{M_\ell},I_{M_\ell})$$

[27, (6.11)]. (Proof: Lemma C.40.)

In the computation. Bin test (3) is applied to every bin that passes test (2), with $\mathcal{E}$ evaluated with the minimum, for three proposed directions ($y = c$ and two solutions of regularized least-squares problems, computed in floating point as in Appendix A.3), each divided by its largest absolute entry.

[27, Section 6.3]**, layers.** The resolutions are $M_\ell = 12, 24, 48, 96$, and also 192 and 384 in the runs with five and six layers. The first layer tests all 12^5 bins, and each later layer tests the 32 bins with indices $2b_j$ or $2b_j+1$ in each coordinate, for every bin b kept by the layer before. A vector with phases β lies, at each layer, in the bin with indices $\lfloor M_\ell\beta_j\rfloor$, and each of these bins is a child of the one before. (Proof: Lemma C.38.)

In the computation. Every run reports "negative" if some layer keeps no bin, and "unresolved" if a layer would have more than $4\cdot 10^7$ bins.

[27, Lemma 6.4]**, vector balls.** For $v \in \mathbb{R}^6$ and $s \ge 0$ let

$$\mathcal{B}_{\mathrm{vec}}(v,s) = \{\lambda e(v+x)/\sqrt{6} :\ |\lambda| = 1,\ x\in\mathbb{R}^6,\ \sum_j x_j = 0,\ \|x\| \le s\}$$

as in [27, (6.14)]. If a bin of the last layer, with midpoint u, is assigned a center v and an integer vector m, and $s \ge \|h\| + X_{M_\ell}$ for $h = u - v - m - \frac{1}{6}\sum_j(u_j - v_j - m_j)\mathbf{1}$, then $\mathcal{B}_{\mathrm{vec}}(v,s)$ contains every vector of the bin. (Proof: Lemma C.41.)

In the computation. In the clustering step, each kept bin of the last layer is assigned to exactly one ball: to the existing ball whose center has the smallest floating-point value of $\|h\|$ among those for which this value plus the upper endpoint of the enclosure of X_{M_ℓ}

is at most 0.042 (an estimate of the radius the ball would need), and otherwise to a new ball centered at the floating-point midpoint of the enclosure of u. The target 0.042 is the clustering parameter of [27, Section 6.3], and it decides how the bins are grouped. Then m is the vector of nearest integers to the midpoint of the enclosure of $u - v$, and the stored radius of the ball is raised to the upper endpoint of the enclosure of $\|h\| + X_{M_\ell}$. Balls are never shrunk or removed.

[27, Lemma 6.5]**, distinct labels.** Two vectors in one ball $\mathcal{B}_{\mathrm{vec}}(v, s)$ with $s < 0.1$ are neither orthogonal nor unbiased. So the balls that contain the twelve vectors of two further bases are distinct, and they label these vectors (Proposition B.2). (Proof: Lemma C.42.)

In the computation. The clustering step reports failure, and the run "unresolved", unless every stored radius is below 0.1, and also if there would be more than 4,096 balls.

[27, Lemma 6.6]**, edge tests.** For two balls with centers u, v and radii $s_u, s_v < 0.1$ put $Q_j = e(u_j - v_j)$, $S_e = \sum_j Q_j$, $r_e = s_u + s_v$, let $D_{\mathcal{O}} \in \mathbb{R}^{2\times 6}$ have the columns $(-\operatorname{Im} Q_j, \operatorname{Re} Q_j)^{\mathsf{T}}$, and $(D_{\mathcal{U}})_j = (\operatorname{Re} S_e\,(D_{\mathcal{O}})_{1j} + \operatorname{Im} S_e\,(D_{\mathcal{O}})_{2j})/6$ [27, (6.15), (6.17)]. If a vector of the first ball and one of the second are orthogonal, then

$$\frac{|S_e|}{2\pi\sqrt{6}} \le r_e, \qquad \frac{|S_e|^2}{2\pi} \le 6r_e\|D_{\mathcal{U}}\| + E_{\mathcal{O}}|S_e|, \qquad E_{\mathcal{O}} = \pi r_e^2;$$

if they are unbiased, then

$$\frac{\big||S_e|/\sqrt{6} - 1\big|}{2\pi} \le r_e, \qquad |q_{\mathcal{U}}| \le r_e\|D_{\mathcal{U}}\| + E_{\mathcal{U}}, \qquad q_{\mathcal{U}} = \frac{|S_e|^2/6 - 1}{4\pi}, \quad E_{\mathcal{U}} = \pi r_e^2\Big(1 + \frac{|S_e|}{6}\Big)$$

[27, (6.16), (6.18)–(6.21)]. The first inequalities of the two displays are [27, (6.16)]. To prove them, note that, up to scalars of modulus one, the two vectors are $e(u + x)/\sqrt{6}$ and $e(v + x')/\sqrt{6}$ with $\sum_j x_j = \sum_j x'_j = 0$, $\|x\| \le s_u$ and $\|x'\| \le s_v$, and that their inner product has modulus $|S'_e|/6$, where $S'_e = \sum_j Q_j e(z_j)$ and $z = x - x'$, so that $\|z\| \le r_e$. Since $|Q_j| = 1$ and $|e(t) - 1| \le 2\pi|t|$, $|S'_e - S_e| \le \sum_j |e(z_j) - 1| \le 2\pi\|z\|_1 \le 2\pi\sqrt{6}\,\|z\| \le 2\pi\sqrt{6}\,r_e$. Orthogonality means $S'_e = 0$, and unbiasedness $|S'_e| = \sqrt{6}$, so $|S_e| \le 2\pi\sqrt{6}\,r_e$ in the first case and $\big||S_e| - \sqrt{6}\big| \le 2\pi\sqrt{6}\,r_e$ in the second; dividing by $2\pi\sqrt{6}$ gives the two inequalities. The other inequalities are proved in Lemma C.43.

In the computation. The tests are made for every pair of balls, for orthogonality and for unbiasedness.

[27, Lemma 6.7]**, joint test.** For the balls $t = 0, 1$, with centers v_t and radii s_t, form c^t, J^t, B^t, S^t and q^t as above with $u = v_t$, and the quantities of the edge tests with $u = v_0$ and $v = v_1$ (so $Q_j = e(v_{0,j} - v_{1,j})$). Let $\mathcal{E}_t^{\mathrm{ball}}(y)$ be $\mathcal{E}(y; s_t, \cdot)$ with $\min\{G_y X^2, \dots\}$ replaced by $G_y s_t^2$ [27, (6.22)]. Let $q_{\mathcal{O}} = (\operatorname{Re} S_e, \operatorname{Im} S_e)^{\mathsf{T}}/(2\pi)$, and $\ell_{\mathcal{O}} = 2$, $\ell_{\mathcal{U}} = 1$. If one vector of each ball is unbiased to the standard basis and to the columns of the same $e(P + \delta)/\sqrt{6}$, with δ horizontal, $\|\delta\| \le r$ and $F(P + \delta) = 0$, and the two vectors are orthogonal ($E = \mathcal{O}$) or unbiased ($E = \mathcal{U}$), then for all $y_0, y_1 \in \mathbb{R}^6$ and $y_e \in \mathbb{R}^{\ell_E}$

$$|y_0 \cdot c^0 + y_1 \cdot c^1 + y_e \cdot q_E| \le \sum_{t=0}^{1}\Big[s_t\big\|(J^t)^* y_t + (-1)^t D_E^* y_e\big\| + \mathcal{E}_t^{\mathrm{ball}}(y_t)\Big] + r_H\big\|(B^0)^* y_0 + (B^1)^* y_1\big\| + E_E\|y_e\|$$

[27, (6.23)]. (Proof: Lemma C.44.)

In the computation. The test is made for every pair of balls that passes the tests of [27, (6.16) and Lemma 6.6], for orthogonality and for unbiasedness separately, with three proposed directions (y_0, y_1, y_e) (solutions of regularized least-squares problems, computed in floating point), each divided by its largest absolute entry.

The graphs. The vertices are the balls. Two distinct balls are joined in $\mathcal{O}$ unless one of the tests of [27, (6.16) and Lemmas 6.6 and 6.7] for orthogonality rejects the pair, and in $\mathcal{U}$ unless one of the tests for unbiasedness rejects it. The search for two further bases in these graphs, and the exclusion of a record, are the subject of Appendix B.

A.8. **The seed cover and Stage A as programs.** The following two statements replace [27, Proposition 2.10] and [27, Propositions 3.11 and 4.16], which concern the programs of [27]. A matrix is *arranged with selected position* σ if it is dephased and arranged as in Lemma C.5 with the column of the σ-th phase of its second row moved to the second position, the other columns keeping their order, and its seed coordinates are then taken in the order of Section 2.3. At the nine positions $(1,1)$, $(1,2), \dots, (1,5)$ and $(2,1), \dots, (5,1)$ of Appendix A.3 such a matrix has the phases x_σ, then the other x_i in increasing order of i, then $y_2, \dots, y_5$; Stage A takes the coordinates of a center in the same order, and since this permutes both in the same way, it changes no distance.

Proposition A.3. *Assume (A) and (B). Every complex Hadamard matrix of order six is equivalent to a matrix arranged with some selected position σ for which there is a center u' that the seed cover program writes with the selected position σ, such that the seed coordinates of the matrix lie in the bin box of u' (that of the bin pair whose midpoint is u') or in the bin box of a bin pair that the program assigns to u'. In both cases these seed coordinates lie in the closed ball of radius* $\mathrm{fl}(0.0320001)$ *about the binary64 rounding of u'.*

Proof. By Lemma C.5, a complex Hadamard matrix H is equivalent to a dephased matrix whose second row has the phases $0, x_1 \le \cdots \le x_5$ and satisfies the orientation and gap conditions and the vanishing sum. Choose nondecreasing bins b_i with $x_i \in [b_i/N, (b_i+1)/N]$; they determine the selected position σ. Moving the column of x_σ to the second position and sorting the last four rows gives a matrix arranged with selected position σ, whose second column has the phases $0, x_\sigma, y_2 \le \cdots \le y_5$, and we choose nondecreasing bins for $y_2, \dots, y_5$. The program visits every nondecreasing list of bins for x and, for its shared bin, every nondecreasing list for y (Section 3.9, (P4)), so it visits this bin pair. The filters of Appendix A.2 are necessary conditions, decided exactly or in interval arithmetic, which under (A) and (B) encloses every quantity; so the pair is not rejected. When the program processes it, it either assigns the pair to an earlier center u' with the selected position σ by the test of Lemma 3.7, so that every point of its bin box, in particular the seed coordinates, lies within 0.032 of u', or it writes the midpoint u' of the pair as a new center, with the selected position σ of the pair; then the bin box of the pair is the bin box of u', and u' lies within $3/224 < 0.032$ of every point of it. Centers are never removed. Rounding a center to binary64 moves it by less than 10^{-15}, and $\mathrm{fl}(0.0320001) > 0.032 + 10^{-15}$ (Section 3.4). □

Proposition A.4. *Assume (A) and (B). Let $\bar{u}$ be the binary64 rounding of a seed center or of a subseed (Section 3.5(ii)) with selected position σ, let $r_s \in \{\mathrm{fl}(0.0320001), \mathrm{fl}(0.0133929)\}$, and suppose that Stage A, run on the ball of radius r_s about $\bar{u}$, reports the ball resolved, that is, the ball passes the frame checks and no cell is counted unresolved. Then every complex Hadamard matrix arranged with selected position σ whose seed coordinates lie within r_s of $\bar{u}$ is equivalent to a member of the solution set of one of the records that Stage A returns for this ball, and, once these records have been added to the atlas, to a member of the solution set of an atlas record.*

Proof. Such a matrix, with seed coordinates q, is a feasible completion of the ball in the sense of Appendix A.3, with $s = 2\pi(q - \bar{u})$ in the order of the nine positions there, so $\|s\| \le R_s$. Since $q_Y < 6$ was decided, Lemma C.12 gives it a polar factor $V \in U(2)$, and V has a representation in the closed parameter domain of Lemma C.13. Each Stage A program processes, by (P5) of Section 3.9, all cells of the first level, $N_u = 16$, which cover this domain, and at each later level all 16 children of every cell of the level before that was neither excluded, nor covered, nor counted unresolved; the children, with indices $2b$ and $2b + 1$ in each parameter, cover their parent. Follow a representation of V through these cells. The cell containing it is not excluded, since the norm and directional tests, the only tests that exclude a cell (P5), are necessary conditions decided correctly (Appendix A.3). At the levels $N_u < 64$ the cell is subdivided. At a level $N_u \ge 64$ it is covered, subdivided, or counted unresolved: at $N_u = 512$ a cell that is neither excluded nor covered is counted unresolved, and so is, without being tested, a cell at a level $N_u \ge 64$ that is reached after the ball has used up its limit of 10^6 cells at these levels or, where it applies, its limit on Root certificates (Section 3.5(i)). Since no cell is counted unresolved, the branch ends with a covered cell. A cell is covered only when the radius computed as in Appendix A.5 is at most 0.103 for a Root certificate $(P, T, \dots)$ built and certified as in Appendix A.4, and then the record of that Root has radius at least this value (the record of an earlier Root is raised to it if it is smaller, and that of a new Root is created with it); radii are never lowered. By Lemmas C.25, C.26, C.27, C.28, C.29 and C.30 and Lemma A.1, as decided in Appendix A.5, the matrix is then equivalent to $e(P + \delta)$ with δ horizontal, $F(P + \delta) = 0$ and $\|\delta\|$ at most this value, that is, to a member of the solution set of the record. Finally, adding a returned record to the atlas either merges it into an atlas record whose radius is raised as in Lemma C.31, or inserts the record transformed by a map g of Lemma C.24, whose solution set consists of matrices equivalent to those of the record; atlas radii are never lowered. □

By Proposition A.3, every complex Hadamard matrix is equivalent to one that is arranged with the selected position of a center u' and whose seed coordinates lie in the seed ball of u', and in the bin box of u' or of a bin pair assigned to u'. If Stage A resolves the ball of u', Proposition A.4 covers the matrix by an atlas record; if the ball is replaced by the balls about the subseeds of u' and Stage A resolves all of them, Lemma 3.8 and the second conclusion of Proposition A.4 do. This is the cover by the atlas that the proof of Theorem 1.1 uses.

Appendix B. Stage C: the graph search and the exclusion of a record

We describe the graph search of our Stage C program as it is written, prove that it is exhaustive, and deduce the statement that the proof of Theorem 1.1 uses in place of [27, Lemma 6.8 and Proposition 6.9], which concern the search routine of [27]. The three procedures of our search are transcribed below, statement by statement, as (P7) of Section 3.9 states.

Let $V = \{0, 1, \dots, n-1\}$, and let $\mathcal{O}$ and $\mathcal{U}$ be undirected graphs on V without loops, given by the sets $N_{\mathcal{O}}(v), N_{\mathcal{U}}(v) \subseteq V \setminus \{v\}$ of neighbors of each vertex v (so $w \in N_{\mathcal{O}}(v)$ if and only if $v \in N_{\mathcal{O}}(w)$, and likewise for $\mathcal{U}$). A *configuration* is a pair (A, B) of disjoint subsets of V with six elements each, such that A and B are cliques of $\mathcal{O}$ and every vertex of A is joined in $\mathcal{U}$ to every vertex of B [27, (6.24)]. The definition is symmetric in A and B. The search uses a counter s, initially 0, a flag g, initially false, and a cap c (the step limit of Section 3.7(iii)); in the computation $\mathsf{c} = 10^9$, the value used by the Stage C program when no other value is given, as in every invocation (F8). Subsets of V are stored as bit sets of n bits, on which cardinality $|W|$, least element $\min W$ (formed only for $W \neq \emptyset$), removal of an element and intersection are computed exactly. The counter is a 64-bit integer, which never exceeds $\mathsf{c} + 1$. The three procedures are as follows.

- CLIQUE(W, m), for $W \subseteq V$ and $0 \le m \le 6$:
  (1) $\mathsf{s} \leftarrow \mathsf{s} + 1$
  if $\mathsf{s} > \mathsf{c}$, set $\mathsf{g} \leftarrow$ true and return true
  (2) if $m = 0$, return true
  if $m = 1$, return whether $W \neq \emptyset$
  (3) repeat:
  if $|W| < m$, return false
  $v \leftarrow \min W$
  $W \leftarrow W \setminus \{v\}$
  if CLIQUE$(W \cap N_{\mathcal{O}}(v), m-1)$ returns true, return true
  if g, return true
- REC(P_1, P_2, j), for $P_1, P_2 \subseteq V$ and $1 \le j \le 6$:
  (1) $\mathsf{s} \leftarrow \mathsf{s} + 1$
  if $\mathsf{s} > \mathsf{c}$, set $\mathsf{g} \leftarrow$ true and return true
  (2) if $|P_2| < 6$, return false
  (3) if $j = 6$, return the value of CLIQUE$(P_2, 6)$
  (4) if CLIQUE$(P_2, 6)$ returns false, return false
  if g, return true
  (5) repeat:
  if $|P_1| < 6 - j$, return false
  $v \leftarrow \min P_1$
  $P_1 \leftarrow P_1 \setminus \{v\}$
  if REC$(P_1 \cap N_{\mathcal{O}}(v),\ P_2 \cap N_{\mathcal{U}}(v),\ j+1)$ returns true, return true
  if g, return true
- EXIST:
  (1) $P \leftarrow V$
  (2) repeat:
  if $|P| < 6$, return false
  $a \leftarrow \min P$
  $P \leftarrow P \setminus \{a\}$
  if REC$(P \cap N_{\mathcal{O}}(a),\ N_{\mathcal{U}}(a) \cap \{a+1, \dots, n-1\},\ 1)$ returns true, return true
  if g, return true

The Stage C program calls EXIST once and reports

- "unresolved" (cap) if g is then true,
- otherwise "unresolved" (candidate) if EXIST returned true,
- otherwise "negative".

Lemma B.1. *Let $\mathcal{O}$,$\mathcal{U}$ be undirected graphs on V without loops, and let $\mathsf{c} \geq 0$.*

(i) The search makes finitely many calls. If the search with the same graphs and no cap makes N calls of Clique *and* Rec*, then: if $N \leq \mathsf{c}$, the search with cap c performs exactly the same steps, g stays false, and* Exist *returns the same value; if $N > \mathsf{c}$, it makes exactly $\mathsf{c}+1$ calls, g becomes true,* Exist *returns true, and the report is "unresolved".*

(ii) If the graphs have a configuration, the search without cap returns true from Exist.

Consequently, if the search reports "negative", then $\mathcal{O}$,$\mathcal{U}$ have no configuration. The cap can only turn a report into "unresolved".

Proof. (i) Without the cap every call terminates: each pass of a loop removes an element of a finite set, Clique calls itself only with a smaller m, Rec calls itself only with a larger $j \leq 6$, and Rec calls Clique, which does not call Rec. So N is finite. With the cap, the counter grows by one at the start of each call. As long as the counter after this increment is at most c, step (1) only counts and g stays false, so the tests "if g" have no effect either, and the search performs the same steps as without the cap. If $N \leq \mathsf{c}$, this holds to the end. If $N > \mathsf{c}$, the call with $\mathsf{s} = \mathsf{c}+1$ sets g and returns true. Every pending call then returns true at once without a further call: in Clique, step (3) returns the true value; in Rec, step (3) returns it, step (4) finds g true, and step (5) returns it; in Exist, step (2) returns it.

(ii) Consider the search without cap. We first show: *if W contains a clique K of $\mathcal{O}$ with m vertices, then* Clique(W,m) *returns true.* This is clear for $m \leq 1$. Let $m \geq 2$ and argue by induction on m. As long as no vertex of K has been removed from W in step (3), $|W| \geq m$, so the loop does not return false. Each pass removes $\min W$; while $\min W \notin K$ the set K stays in W, and since W is finite a pass comes, unless the call has returned true before, at which $v = \min W$ lies in K. Then $K \setminus \{v\}$ is a clique of $m-1$ vertices contained in $(W \setminus \{v\}) \cap N_{\mathcal{O}}(v)$, so by induction the recursive call returns true, and so does Clique(W,m).

Now let (A,B) be a configuration. Interchanging A and B if necessary, we may assume that $a_0 = \min(A \cup B)$ lies in A; write $A = \{a_0 < a_1 < \cdots < a_5\}$. Every vertex of B is larger than a_0, since $a_0 \notin B$. We show: *if $1 \leq j \leq 6$, $P_1 \supseteq \{a_j, \ldots, a_5\}$ and $P_2 \supseteq B$, then* Rec(P_1,P_2,j) *returns true*, by induction downwards from $j = 6$. Since $|P_2| \geq 6$, step (2) does not return. If $j = 6$, step (3) returns Clique$(P_2,6)$, which is true by the claim above because $B \subseteq P_2$ is a clique of $\mathcal{O}$ with six vertices. Let $j \leq 5$. In step (4), Clique$(P_2,6)$ is true for the same reason. In step (5), as long as a_j has not been removed from P_1, also $a_{j+1}, \ldots, a_5$ have not been removed, because they are larger than a_j and each pass removes $\min P_1$; so $|P_1| \geq 6-j$ and the loop does not return false. Hence, unless the call has returned true before, a pass comes at which $v = a_j$. The new first set $(P_1 \setminus \{a_j\}) \cap N_{\mathcal{O}}(a_j)$ contains $a_{j+1}, \ldots, a_5$, because A is a clique of $\mathcal{O}$, and the new second set $P_2 \cap N_{\mathcal{U}}(a_j)$ contains B, because a_j is joined in $\mathcal{U}$ to every vertex of B. By induction the recursive call returns true, and so does Rec(P_1,P_2,j).

Finally, in Exist the vertices $0,1,2,\ldots$ are removed from P in this order. Before a_0 is removed, $P \supseteq A \cup B$ has at least 12 elements, so the loop does not return false, and unless it has returned true before, it reaches $a = a_0$ with $P \setminus \{a_0\} = \{a_0+1, \ldots, n-1\}$. Then the first set $P \cap N_{\mathcal{O}}(a_0)$ contains $a_1, \ldots, a_5$, and the second set $N_{\mathcal{U}}(a_0) \cap \{a_0+1, \ldots, n-1\}$ contains B. By the case $j = 1$, Rec returns true, and so does Exist.

For the consequence: a report "negative" requires g false, so by (i) Exist returned the value of the search without cap, which is false; by (ii) there is no configuration. □

Proposition B.2. *Assume (A) and (B) of Section 3.1. Let (P, r) be a record whose Root certificate satisfies (A.1) and (A.2). If the Stage C program, run on (P, r) with four, five or six layers, reports "negative", then no matrix in $\mathcal{S}(P, r)$ is extendible.*

Proof. Suppose that $H = e(P + \delta) \in \mathcal{S}(P, r)$ is extendible: there are orthonormal bases $\mathcal{B}_3, \mathcal{B}_4$ of $\mathbb{C}^6$ such that the standard basis, the columns of $H/\sqrt{6}$, $\mathcal{B}_3$ and $\mathcal{B}_4$ are pairwise mutually unbiased. Each $f \in \mathcal{B}_3 \cup \mathcal{B}_4$ is unbiased to the standard basis, so $f = \lambda e(\beta)/\sqrt{6}$ with $|\lambda| = 1$, $\beta_0 = 0$ and $\beta_1, \dots, \beta_5 \in [0, 1)$, and it is unbiased to the columns of $H/\sqrt{6}$. At each layer, with resolution M_ℓ, the bin with indices $\lfloor M_\ell \beta_j \rfloor$ contains β, and it is a child of the corresponding bin of the layer before (Lemma C.38). The bin tests (1)–(3) of Appendix A.7 are necessary conditions for such a vector, decided in interval arithmetic, which under (A) and (B) encloses every quantity (Lemmas 3.1, 3.2 and 3.5); so none of them rejects this bin. Here the hypotheses (A.1) and (A.2) enter: by Lemma C.36, every member $e(P + \delta')$ of $\mathcal{S}(P, r)$ has $\|T^*\delta'\| \le r_H$ and $\|\delta' - TT^*\delta'\| \le n$, and $\|e(P)/\sqrt{6}\| \le K$. The bin tests and the joint test of Appendix A.7 are derived from these bounds, so they are necessary conditions for vectors unbiased to the columns of $e(P + \delta')/\sqrt{6}$ for every such member. The Stage C program tests every bin of the first layer and, at each later layer, all children of the bins kept before (Section 3.9, (P7)), since no limit on the numbers of vector balls, bins or search steps (Section 3.7(iii)) stops a run that reports "negative". By induction over the layers, each layer keeps the bin of β. So no layer is empty, and the report "negative" comes from the graph search, after a successful clustering.

The clustering assigns the bin of β in the last layer to a vector ball, and this ball contains every vector $\lambda' e(\beta)/\sqrt{6}$ with $|\lambda'| = 1$, in particular f (Lemma C.41, as decided in Appendix A.7); call it $b(f)$. Any two of the twelve vectors are orthogonal (if they lie in the same basis) or unbiased (if not), while two vectors in one ball of radius below 0.1 are neither (Lemma C.42); the radii are below 0.1, as the clustering succeeded, so the twelve balls $b(f)$ are distinct. Put $A = \{b(f) : f \in \mathcal{B}_3\}$ and $B = \{b(f) : f \in \mathcal{B}_4\}$. If $f \ne f'$ lie in $\mathcal{B}_3$, then $f \in b(f)$ and $f' \in b(f')$ are orthogonal and unbiased to the standard basis and to the columns of the same $H/\sqrt{6}$. The tests of Appendix A.7 for orthogonality, the edge tests and the joint test, are necessary conditions for such a pair, by the proof of [27, (6.16)] in Appendix A.7 and by Lemmas C.43 and C.44, and they are decided in interval arithmetic, as the bin tests are. Hence none of them rejects the pair $b(f), b(f')$, and the two balls are joined in $\mathcal{O}$. So A, and likewise B, is a clique of $\mathcal{O}$, and in the same way every vertex of A is joined in $\mathcal{U}$ to every vertex of B. Thus (A, B) is a configuration of the graphs passed to the search, and by Lemma B.1 the search does not report "negative", a contradiction. □

In the computation, Stage C reported "negative" for 5,732 of the 5,934 fine records and for all 2,786 records of the fallback refinement (Section 4.2), so Proposition B.2 applies to each of them. A report "unresolved" proves nothing about the record; it only sends the record to the fallback refinement.

Appendix C. Proofs of the statements of the preprint used in the proof of Theorem 1.1

Every statement of [27] that the proof of Theorem 1.1 uses and that the note does not prove elsewhere is proved here. The method and the statements are those of [27]. The proofs follow those given there, with every step written out, except where a proof says at its start how it differs. Some facts that [27] states without proof, such as the formulas of Lemma C.18, are proved here as well. The heading of each statement taken from [27] gives

its number there. The statement is the one printed there, with the hypotheses that [27] leaves to the context written out, except where its proof says at its start that the statement differs. Some statements also include facts that [27] states elsewhere or uses without stating them, for instance Lemma C.3(ii) and (iv). Some assume less than [27]: for instance, those of Appendix C.10 hold without the conditions that [27, Section 6.1] imposes on the radius and the constants of a record, with the bound K of Appendix A.7 in place of $K = 1.00001$. Some leave out an assertion that the proof of Theorem 1.1 does not use or derives from statements of the note, for instance the second bound of [27, Lemma 3.6] in Lemma C.15. Table 3 lists, for each result of [27] named in Section 2 or used by the proof of Theorem 1.1, the statement of the note that proves or replaces it and where that statement is used outside this appendix.

Notation is that of Appendix A. For a complex matrix X, $\|X\|$ is its operator norm, $\|X\|_F$ its Frobenius norm, X^* its conjugate transpose (the transpose if X is real) and $\lambda_{\max}$ the largest eigenvalue of a Hermitian matrix; real vectors and phase matrices carry the Euclidean norm. We write $\mathbf{1}$ for a vector of ones, $\mathbf{e}_i$ for coordinate vectors, and $\langle u, v\rangle = \sum_j \overline{u_j} v_j$.

C.1. **Elementary facts.**

Lemma C.1. *For real numbers x, t, t':*

(i) $|e^{ix} - 1| \le |x|$ *and* $|e^{ix} - 1 - ix| \le x^2/2$*; hence* $|e(t) - 1| \le 2\pi|t|$ *and* $|e(t) - 1 - 2\pi i t| \le 2\pi^2 t^2$*;*

(ii) the function $r(t) = (e(t) - 1 - 2\pi i t)/(2\pi i)$ *satisfies* $|r(t)| \le \pi t^2$ *and* $|r(t) - r(t')| \le \pi|t - t'|\,(|t| + |t'|)$*;*

(iii) $|x - \sin x| \le |x|^3/6$.

Proof. (i) and (iii) follow by integrating $e^{ix} - 1 = \int_0^x ie^{iy}\,dy$, $e^{ix} - 1 - ix = \int_0^x i(e^{iy} - 1)\,dy$ and $x - \sin x = \int_0^x (1 - \cos y)\,dy$, where $0 \le 1 - \cos y \le y^2/2$ because $\sin v \le v$ for $v \ge 0$; putting $x = 2\pi t$ gives the bounds for $e(t)$. (ii) As $r'(t) = e(t) - 1$ and $r(0) = 0$, (i) gives $|r(t) - r(t')| \le 2\pi|t - t'| \int_0^1 |t' + u(t - t')|\,du \le \pi|t - t'|(|t| + |t'|)$, and $t' = 0$ gives the first bound. □

Lemma C.2. *Let X, Y be complex matrices.*

(i) $\|X\|^2 = \lambda_{\max}(X^*X) = \lambda_{\max}(XX^*)$, $\|X\| \le \|X\|_F$, $\|XY\|_F \le \|X\|\,\|Y\|_F$ *and* $\|XY\|_F \le \|X\|_F\,\|Y\|$*; a submatrix of X has operator norm at most $\|X\|$.*

(ii) If K has orthonormal columns, then $\|K\| = 1$ and $\|KY\|_F = \|Y\|_F = \|YK^*\|_F$.

(iii) If X_1, X_2 are Hermitian positive semidefinite and $X_1X_2 = 0$, then $\|X_1 + X_2\| = \max(\|X_1\|, \|X_2\|)$.

(iv) If $a, b, q \ge 0$, the symmetric matrix with rows (a, q) and (q, b) has operator norm at most $\max(a, b) + q$*, with equality if $a = b$. If $u, x \in \mathbb{R}^n$ and $K \in \mathbb{R}^{n\times n}$ have nonnegative entries and $u \le Kx$ entrywise, then $\|u\| \le \|K\|\,\|x\|$.*

Proof. (i) and (ii) are standard [8, Section 5.6]. For the last assertion of (i), a submatrix is RXS, where R and S select rows and columns and have norm at most one. (iii) As $X_2X_1 = (X_1X_2)^* = 0$, the sum $X_1 + X_2$ equals X_1 on $\operatorname{ran} X_1$ and X_2 on $(\operatorname{ran} X_1)^\perp = \ker X_1$, and both subspaces are invariant under it, so its norm is the larger of $\|X_1\|$ and $\|X_2\|$. (iv) The eigenvalues are $(a + b)/2 \pm ((a - b)^2/4 + q^2)^{1/2}$; their sum $a + b$ is nonnegative, so the norm is the larger one, and $((a-b)^2/4+q^2)^{1/2} \le |a-b|/2+q$, with equality if $a = b$. Finally $0 \le u \le Kx$ entrywise gives $\|u\| \le \|Kx\| \le \|K\|\,\|x\|$. □

TABLE 3. The results of [27] named in Section 2 or used by the proof of Theorem 1.1, the statements of this note that prove or replace them, and where these are used outside Appendix C. Entries of Appendices A.2, A.3 to A.5, A.6 and A.7 also stand for the uses in Propositions A.3 and A.4, Section 3.6 and Proposition B.2, respectively. A dagger marks a result that [27] states for its own programs or for its rounding analysis. For these the note proves its own version and uses it in place of the one of [27]. Lemma 5.6 of [27], the second bounds of its Lemmas 2.9 and 3.6, the second assertion of its Lemma 6.4 and the last remark of its Corollary 3.10 are not used; Lemma 5.6 is not needed because the programs store each new child with radius τ and mark boxes against stored children, which Lemma A.2 covers.

In [27]	Here	Used in
Lemma 2.2	Lemma C.4	Sections 2.2, 3.6 and 4.3
Lemma 2.3	Lemma C.3	Section 2.2
Lemma 2.4	Lemma C.5	Section 2.3, Proposition A.3
Lemmas 2.5, 2.6, (2.7)	Lemmas C.6 and C.7	Appendix A.2: filters
Lemmas 2.7, 2.8	Lemmas C.8 and C.9	Appendix A.2: sum test, shared phase
Lemma 2.9	Lemma 3.7	Appendix A.2
Proposition 2.10†	Proposition A.3	Section 4.3
(3.3), Section 3.1, Lemmas 3.1, 3.2	Lemmas C.10, C.11 and C.12	Appendix A.3: frames, polar comparison, cell constants
Lemmas 3.3–3.7, Section 3.5	Lemmas C.13, C.14, C.15, C.16, C.17 and C.18	Appendices A.3 and A.5: cell constants
Lemmas 3.8, 3.9, Corollary 3.10	Lemmas C.19 and C.20	Appendix A.3: norm and directional tests
Proposition 3.11†	Proposition A.4	Lemma 3.8, Section 4.3
Lemmas 4.3, 4.4	Lemmas C.21 and C.22	Appendix A.4: remainder constant
Proposition 4.5	Lemma C.23	Appendix A.4: sufficient conditions
Lemma 4.7	Lemma C.24	Sections 2.4 and 3.5 and Appendices A.4, A.5 and A.6
Lemma 4.8	Lemma C.25	Appendix A.5: arc bounds
Lemma 4.9†	Lemma A.1	Appendix A.5, Lemma 3.8
Lemma 4.10	Lemma C.26	Appendix A.5: direct bound
(4.30), Lemmas 4.11, 4.12, (4.35), (4.37)	Lemmas C.27, C.28 and C.29	Appendix A.5: tangent bound
Proposition 4.13	Lemma C.30	Appendix A.5: bootstrap
Lemma 4.15	Lemma C.31	Appendix A.5: atlas merge
Proposition 4.16†	Propositions A.3 and A.4 and Lemma 3.8	Section 4.3
Lemma 5.1, Proposition 5.2, Lemma 5.3	Lemmas C.32, C.33 and C.34	Appendix A.6
Lemmas 5.4, 5.5†	Lemma A.2(i), (ii)	Section 3.6
Lemma 5.6	—	not used
(5.20), (5.22)–(5.24)	Lemma C.35	Appendix A.6: tangent grid
Proposition 5.7†	Lemma 3.9	(F3), Section 4.3
(6.2), (6.3)	Lemma C.36	Appendix A.7
Lemmas 6.1–6.3, (6.11)	Lemmas C.37, C.39 and C.40	Appendix A.7: bin tests
(6.12), (6.13), (6.16)	Appendix A.7	Appendix A.7
Section 6.3	Lemma C.38	Appendix A.7: layers
Lemmas 6.4–6.7	Lemmas C.41, C.42, C.43 and C.44	Appendix A.7: vector balls and edges
Lemma 6.8†	Lemma B.1	Proposition B.2
Proposition 6.9†	Proposition B.2	Section 4.3
Theorem 7.1†	the proof of Theorem 1.1 (Section 4.3)	—

Let $C_6 = I - \mathbf{1}\mathbf{1}^\mathsf{T}/6 \in \mathbb{R}^{6\times 6}$, the orthogonal projection of $\mathbb{R}^6$ onto $\mathbf{1}^\perp$. Formula (C.1) below is the definition of Π in [27, (2.1)].

Lemma C.3 ([27, Lemma 2.3])**.** *(i) The map*

$$(\Pi Y)_{ij} = Y_{ij} - \tfrac{1}{6}\textstyle\sum_b Y_{ib} - \tfrac{1}{6}\sum_a Y_{aj} + \tfrac{1}{36}\sum_{a,b} Y_{ab}, \quad \textit{that is,} \quad \Pi Y = C_6 Y C_6, \tag{C.1}$$

is the orthogonal projection of $\mathbb{R}^{6\times 6}$ onto the horizontal matrices, and $\ker\Pi = \{r\mathbf{1}^\mathsf{T} + \mathbf{1}c^\mathsf{T} : r, c \in \mathbb{R}^6\}$.

(ii) $D_0 Y - Y \in \ker\Pi$, so $\Pi D_0 Y = \Pi Y$.

(iii) If $Y' - Y \in \mathbb{Z}^{6\times 6} + \ker\Pi$, then $e(Y') = \operatorname{diag}(e(r))\, e(Y) \operatorname{diag}(e(c))$ for some $r, c \in \mathbb{R}^6$, so $e(Y')$ and $e(Y)$ are equivalent, and $\|F(Y')\| = \|F(Y)\|$. In particular $e(P+z)$ and $e(P+\Pi z)$ are equivalent for all real P, z.

(iv) For real Y, the matrix $e(Y)e(Y)^*$ has diagonal entries 6 and the entries $2\pi i\, F_{ij}(Y)$ at the positions (i,j) with $i > j$. Hence $\|e(Y)e(Y)^* - 6I\|_F = 2\pi\sqrt{2}\,\|F(Y)\|$, and $F(Y) = 0$ if and only if $e(Y)$ is a complex Hadamard matrix.

Proof. Here the proof of (i) differs from [27], which shows that $Y - \Pi Y$ is orthogonal to the horizontal matrices. (i) Expanding $C_6 Y C_6$ gives (C.1). As C_6 is the orthogonal projection onto $\mathbf{1}^\perp$, the map $Y \mapsto C_6 Y C_6$ is the orthogonal projection onto the matrices Y with $Y\mathbf{1} = 0$ and $\mathbf{1}^\mathsf{T} Y = 0$, which are the horizontal ones. Its kernel is their orthogonal complement, which is spanned by the matrices $r\mathbf{1}^\mathsf{T}$ and $\mathbf{1}c^\mathsf{T}$. (ii) $(D_0 Y - Y)_{ij} = -Y_{i0} - Y_{0j} + Y_{00}$. (iii) Write $Y'_{ij} = Y_{ij} + Z_{ij} + r_i + c_j$ with Z integral. Then $e(Y'_{ij}) = e(r_i)e(Y_{ij})e(c_j)$, and $F_{ij}(Y') = e(r_i - r_j)F_{ij}(Y)$ by (2.1). Apply this with $Y' = P + z$, $Y = P + \Pi z$, using (i). (iv) $(e(Y)e(Y)^*)_{ij} = \sum_l e(Y_{il} - Y_{jl})$, which is 6 for $i = j$ and $2\pi i F_{ij}(Y)$ for $i > j$, and the entries with $i < j$ are their conjugates. As the entries of $e(Y)$ have modulus one, $e(Y)$ is complex Hadamard if and only if $e(Y)e(Y)^* = 6I$. □

C.2. **Equivalences and the arrangement of the seed coordinates.** An orthonormal basis of $\mathbb{C}^6$ is represented by the unitary matrix whose columns are its vectors. Two bases with matrices V, W are mutually unbiased if and only if every entry of V^*W has modulus $1/\sqrt{6}$; this does not change if the columns of V or W are permuted or multiplied by scalars of modulus one, if V, W are replaced by UV, UW for a unitary U, or if V, W are replaced by $\overline{V}, \overline{W}$.

Lemma C.4 ([27, Lemma 2.2])**.** *Let H be a complex Hadamard matrix of order six, and let H' be obtained from H by permuting or rephasing its rows or its columns, by complex conjugation or by transposition. Then H' is a complex Hadamard matrix, and H' is extendible if and only if H is.*

Proof. The entries of H' have modulus one, and $H'H'^* = 6I$: for the transpose, $H^\mathsf{T}\overline{H} = \overline{H^*H} = 6I$, since $H/\sqrt{6}$ is unitary. Each operation has an inverse of the same kind, so it suffices to show that H' is extendible if H is. Let I, $U = H/\sqrt{6}$, V_3, V_4 be pairwise mutually unbiased. (a) If $H' = HQ$, where Q is a permutation matrix times a diagonal unitary matrix, the columns of $H'/\sqrt{6}$ are those of U, permuted and rephased, so $I, H'/\sqrt{6}, V_3, V_4$ are pairwise mutually unbiased. (b) If $H' = QH$, apply the unitary Q: the bases Q, $H'/\sqrt{6}$, QV_3, QV_4 are pairwise mutually unbiased, and the columns of Q are those of I, permuted and rephased. (c) Conjugation gives $I, \overline{U}, \overline{V_3}, \overline{V_4}$. (d) Applying U^* gives U^*, I, U^*V_3, U^*V_4, and conjugating gives $U^\mathsf{T}, I, \overline{U^*V_3}, \overline{U^*V_4}$; reordering, I and $H^\mathsf{T}/\sqrt{6} = U^\mathsf{T}$ belong to four pairwise mutually unbiased bases. □

For distinct rows i, i' of a matrix $e(Y)$, the *gap* of the pair is the length of the longest open arc of $\mathbb{R}/\mathbb{Z}$ that contains none of the six numbers $Y_{i'l} - Y_{il}$ $(0 \le l \le 5)$, counted modulo one; the gap of a pair of distinct columns is defined in the same way. A largest such arc exists because the six points are finitely many, and if its length g is less than 1, both of its endpoints are among the points, since otherwise a longer arc would contain none of them.

Lemma C.5 ([27, Lemma 2.4])**.** *Every complex Hadamard matrix H of order six is equivalent to a dephased complex Hadamard matrix $e(X)$, with X vanishing in its first row and column, such that*

(i) the gap g_x of the first two rows of $e(X)$ is the smallest gap of all pairs of distinct rows and all pairs of distinct columns of $e(X)$;

(ii) the second row of X is $(0, x_1, \dots, x_5)$ with $0 \le x_1 \le \cdots \le x_5 \le 1$, $g_x = 1 - x_5$ and $x_1 \le x_5 - x_4$;

(iii) $\sum_{j=0}^{5} e(x_j) = 0$, where $x_0 = 0$.

Let $\sigma \in \{1, \dots, 5\}$. Move column σ of $e(X)$ to the second position, the other columns keeping their order, and then permute the last four rows so that the phases $y_2 \le y_3 \le y_4 \le y_5$ in $[0, 1)$ of the new second column in these rows are nondecreasing. The result is a dephased complex Hadamard matrix equivalent to H. Its first two rows have the gap g_x, which is the smallest gap of all its pairs of rows and of columns; its second row has the phases $0, x_\sigma$ followed by the other x_j in increasing order of j; its second column has the phases $(y_0, \dots, y_5) = (0, x_\sigma, y_2, \dots, y_5)$; and $\sum_{j=0}^{5} e(y_j) = 0$ and $g_y \ge g_x$, where g_y is the gap of its first two columns.

Proof. (a) *Invariance of the gaps.* Multiplying row i by $e(\rho)$ adds $\pm\rho$ to the six differences of each pair of rows containing i, a rotation of $\mathbb{R}/\mathbb{Z}$, and leaves the differences of each pair of columns unchanged; a rephasing of columns acts in the same way with rows and columns exchanged. Permutations of rows and of columns only relabel the pairs and reorder the six differences of each pair; complex conjugation negates all differences, a reflection of $\mathbb{R}/\mathbb{Z}$; transposition exchanges the pairs of rows with the pairs of columns. Rotations and reflections map open arcs to open arcs of the same length. So the collection of the gaps of all pairs of rows and of columns, with multiplicities, is the same for equivalent matrices.

(b) *Construction.* Choose a pair attaining the smallest gap g. Transposing if it is a pair of columns and then permuting the rows (Lemma C.4 keeps the matrix complex Hadamard), we may assume that it is the pair of rows $0, 1$ of $H = e(Y)$. Let $d_l = Y_{1l} - Y_{0l}$, and let A be an open arc of length g containing no d_l. If $g < 1$, let θ be the endpoint of A that comes last in the positive direction; if $g = 1$, all d_l are congruent, to θ say. In both cases $\theta \equiv d_{l_0}$ for some l_0. Move column l_0 to the first position, multiply each column l by $e(-Y_{0l})$ and then each row i by $e(-(Y_{il_0} - Y_{0l_0}))$. The result is dephased, and its second row has the phases $d_l - d_{l_0}$ modulo one; taken in $[0, 1)$, they lie in $[0, 1 - g]$, since the rotation by $-\theta$ maps A onto the arc $(1 - g, 1)$. Permute the columns other than the first so that these phases are nondecreasing. If $g < 1$, the other endpoint of A is also some d_l, mapped to $1 - g$, so $x_5 = 1 - g$; if $g = 1$, all phases are 0 and again $x_5 = 0 = 1 - g$. This gives (ii) except the last inequality, and (i) holds by (a), because the first two rows form the pair with which we started, whose gap g is the smallest.

(c) *Orientation.* Suppose that $x_1 > x_5 - x_4$. Interchange the first two rows, move a column in which the second row had the phase x_5 to the first position, and dephase as in (b). The new second row has the phases $x_5 - x_l$ $(0 \le l \le 5)$, which lie in $[0, x_5]$; after sorting they are 0 and $x'_i = x_5 - x_{5-i}$ $(1 \le i \le 5)$. The first two rows are the same pair as before, so

their gap is still $g = 1 - x_5 = 1 - x'_5$, and $x'_1 = x_5 - x_4 < x_1 = x'_5 - x'_4$. So the new matrix satisfies (ii), and (i) by (a).

(iii) The second row of $e(X)$ is orthogonal to the first, which consists of ones.

Finally, the column and row permutations of the last part keep the first column, the first row and the second row (up to the order of its entries), so the result is dephased, equivalent to H, and its first two rows have the gap g_x, which is the smallest gap of all its pairs by (a). Its first two columns are orthogonal, as $e(X)^* e(X) = 6I$, which gives $\sum_j e(y_j) = 0$. The differences of the entries of these two columns are the phases y_j, so their gap is g_y, and $g_y \geq g_x$ by the minimality of g_x. □

C.3. **The filters of the seed cover.**

Lemma C.6 ([27, Lemma 2.5])**.** *Let $a_0, \dots, a_n$ and $a'_0, \dots, a'_n$ be points of $\mathbb{R}/\mathbb{Z}$ with $|a_k - a'_k|_{\mathbb{R}/\mathbb{Z}} \leq \varepsilon$ for all k, where $|t|_{\mathbb{R}/\mathbb{Z}}$ is the distance from t to $\mathbb{Z}$. Then the gaps g, g' of the two lists (the lengths of the longest open arcs containing none of their points) satisfy $|g - g'| \leq 2\varepsilon$.*

Proof. Let $(\alpha, \alpha + g)$ be an open arc containing no a_k; here $g \leq 1$. If $g \leq 2\varepsilon$, then $g' \geq 0 \geq g - 2\varepsilon$. Otherwise no a'_k lies in $(\alpha + \varepsilon, \alpha + g - \varepsilon)$, since a point a_k within ε of such an a'_k would lie in $(\alpha, \alpha + g)$. So $g' \geq g - 2\varepsilon$, and $g \geq g' - 2\varepsilon$ by symmetry. □

Lemma C.7 ([27, (2.7) and Lemma 2.6])**.** *Let a complex Hadamard matrix be arranged as in Lemma C.5 with selected position σ, and let its seed coordinates $(x_1, \dots, x_5, y_2, \dots, y_5)$ lie in the bin box of a bin pair. Suppose that the bins of the pair for $x_1 \leq \cdots \leq x_5$ are $b_1 \leq \cdots \leq b_5$ (so $x_i \in [b_i/N, (b_i + 1)/N]$ with $N = 112$) and that its second list begins with the bin b_σ of x_σ, as it does when σ is the selected position of the pair. Then $b_1 \leq b_5 - b_4 + 1$, and the gaps of the two lists of midpoints of the pair (each list with the point 0 added) satisfy*

$$g_{x,\mathrm{mid}} \leq 1 - \frac{b_5 - 1}{N}, \qquad g_{y,\mathrm{mid}} \geq 1 - \frac{b_5 + 2}{N}.$$

Proof. By the orientation condition, $b_1/N \leq x_1 \leq x_5 - x_4 \leq (b_5 + 1)/N - b_4/N$, and b_1, b_4, b_5 are integers. Each of the phases $x_1, \dots, x_5$ lies within $1/(2N)$ of the midpoint of its bin, and so do the shared phase x_σ and $y_2, \dots, y_5$ for the second list, whose first bin is the bin b_σ of x_σ; the added point 0 is matched with the phase 0. By Lemma C.6 with $\varepsilon = 1/(2N)$, $|g_x - g_{x,\mathrm{mid}}| \leq 1/N$ and $|g_y - g_{y,\mathrm{mid}}| \leq 1/N$. Since $x_5 \in [b_5/N, (b_5 + 1)/N]$, Lemma C.5 gives $1 - (b_5 + 1)/N \leq g_x = 1 - x_5 \leq 1 - b_5/N$ and $g_y \geq g_x$. Hence $g_{x,\mathrm{mid}} \leq g_x + 1/N \leq 1 - (b_5 - 1)/N$ and $g_{y,\mathrm{mid}} \geq g_y - 1/N \geq g_x - 1/N \geq 1 - (b_5 + 2)/N$. □

Lemma C.8 ([27, Lemma 2.7])**.** *Let $u_0, \dots, u_4$ be real, $c = (1 + \sum_j e(u_j))/(2\pi i)$ and $J_j = e(u_j)$, as vectors of $\mathbb{R}^2$. If $1 + \sum_j e(u_j + \Delta_j) = 0$ with $|\Delta_j| \leq 1/(2N)$, then $\|c + \sum_j J_j \Delta_j\| \leq 5\pi/(4N^2)$, and for every $v \in \mathbb{R}^2$*

$$|v \cdot c| \leq \frac{5\pi}{4N^2} \|v\| + \frac{1}{2N} \sum_{j=0}^{4} |v \cdot J_j|.$$

Proof. Dividing $0 = 1 + \sum_j e(u_j) e(\Delta_j)$ by $2\pi i$ and writing $e(\Delta_j) = 1 + 2\pi i \Delta_j + 2\pi i\, r(\Delta_j)$, with r as in Lemma C.1(ii), gives $0 = c + \sum_j e(u_j) \Delta_j + \sum_j e(u_j) r(\Delta_j)$. So $\|c + \sum_j J_j \Delta_j\| \leq \sum_j \pi \Delta_j^2 \leq 5\pi/(4N^2)$. Taking the inner product with v, $|v \cdot c| \leq \sum_j |v \cdot J_j|\, |\Delta_j| + \|v\|\, 5\pi/(4N^2)$. □

In the seed cover, Lemma C.8 is applied with u_j the midpoints of the bins of $x_1,\dots,x_5$, or of the shared phase and $y_2,\dots,y_5$, and with Δ_j the displacements of the seed coordinates from these midpoints; the hypothesis is the vanishing sum of Lemma C.5.

Lemma C.9 ([27, Lemma 2.8])**.** *In the setting of Lemma C.8, let t be a position, $h = N\Delta$ and $E = 5\pi/(4N)$. Then $|h_t| \le \frac12$ and, for every $v \in \mathbb{R}^2$ with $\alpha = v\cdot J_t \neq 0$,*

$$\Big|h_t + \frac{N\, v\cdot c}{\alpha}\Big| \le \frac{1}{|\alpha|}\Big(E\|v\| + \frac12\sum_{j\neq t}|v\cdot J_j|\Big).$$

If a matrix is arranged as in Lemma C.5 with selected position σ, its seed coordinates lie in the bin box of a bin pair whose second list begins with the bin b_σ of x_σ, and t is the position of x_σ in each of the two lists, then the sets of values of h_t allowed by these inequalities for the two lists (intersected with $[-\frac12,\frac12]$, for any choice of directions v) have a common point.

Proof. $|h_t| = N|\Delta_t| \le \frac12$. Multiplying the first bound of Lemma C.8 by N gives $\|Nc + \sum_j J_j h_j\| \le E$, so $|N\,v\cdot c + \alpha h_t| \le E\|v\| + \sum_{j\neq t}|v\cdot J_j|\,|h_j|$ with $|h_j| \le \frac12$; divide by $|\alpha|$. The shared phase lies in the same bin in both lists, with the same midpoint, so the same number $h_t = N(x_\sigma - \text{midpoint})$ satisfies the inequalities of both lists. □

C.4. **Stage A: frames, the polar comparison and the cells.** Throughout Appendices C.4, C.5 and C.6 fix a seed ball as in Appendix A.3, with the entries $a, b_0,\dots,b_3, c_0,\dots,c_3$ of $e(\text{center})$, the matrices E_0, B_0, C_0, the radius r_s and $R_s = 2\pi r_s$. For a feasible completion H' with displacement s, write $H' = \left(\begin{smallmatrix} E' & B' \\ C' & D' \end{smallmatrix}\right)$ with blocks of sizes 2×2, 2×4, 4×2 and 4×4, and put $\Delta E = E' - E_0$, $\Delta B = B' - B_0$, $\Delta C = C' - C_0$, $e_1 = \|\Delta E\|_F$, $b_1' = \|\Delta B\|_F$, $c_1' = \|\Delta C\|_F$, $F_E = \Delta E - E_1$, $F_B = \Delta B - B_1$ and $F_C = \Delta C - C_1$, with E_1, B_1, C_1 as in Appendix A.3. Thus ΔE has the single nonzero entry $a(e^{is_a}-1)$, at position $(1,1)$, ΔB has the entries $b_j(e^{is_{b_j}}-1)$ in its second row and ΔC the entries $c_i(e^{is_{c_i}}-1)$ in its second column, and F_E, F_B, F_C have the entries $a(e^{is_a}-1-is_a)$, $b_j(e^{is_{b_j}}-1-is_{b_j})$ and $c_i(e^{is_{c_i}}-1-is_{c_i})$ at the same positions.

Lemma C.10 ([27, (3.3) and Section 3.1])**.** *For every feasible completion:*

(i) $e_1^2 + b_1'^2 + c_1'^2 \le \|s\|^2 \le R_s^2$ *and* $\|F_E\|_F^2 + \|F_B\|_F^2 + \|F_C\|_F^2 \le R_s^4/4$;

(ii) $E'^*B' + C'^*D' = 0$, $C'E'^* + D'B'^* = 0$, $B'^*B' + D'^*D' = 6I$, $\|[C'\ D']\| = \sqrt6$ *and* $\|D'\| \le \sqrt6$;

(iii) $A_0 = \|E_0\| = (2+|1+a|)^{1/2} \le 2$, *and* $A_0 \le A_*$ *and* $\|E'\| \le A_*$ *for* $A_* = \min(2, A_0 + R_s)$.

Proof. (i) By Lemma C.1(i) the entries listed above have moduli at most $|s_k|$ and $s_k^2/2$ for the corresponding component s_k of s, and $\sum_k s_k^4 \le \|s\|^4$. (ii) These are blocks of $H'^*H' = 6I$ and $H'H'^* = 6I$ ($H'/\sqrt6$ is unitary): $[C'\ D']$ consists of the last four rows of H', so $[C'\ D'][C'\ D']^* = 6I$, and D' is a submatrix of it (Lemma C.2(i)). (iii) $E_0^*E_0$ has rows $(2, 1+a)$ and $(1+\overline{a}, 2)$, with eigenvalues $2 \pm |1+a|$, and $|1+a| \le 2$. Also $\|E'\| \le \|E'\|_F = 2$ and $\|E'\| \le \|E_0\| + \|\Delta E\| \le A_0 + e_1 \le A_0 + R_s$. □

Lemma C.11 ([27, Lemma 3.1]). *Let $v \in \mathbb{C}^4$ have entries of modulus one, $S_v = \sum_j v_j$ and $M_v = (\mathbf{1}\ v)$. The squared singular values of M_v are $4 \pm |S_v|$. If $|S_v| < 4$, then $M_v(M_v^* M_v)^{-1} = (16 - |S_v|^2)^{-1}(4\mathbf{1} - v\overline{S_v},\ 4v - \mathbf{1}S_v)$, and the last two of the four vectors produced by the Gram–Schmidt process from $\mathbf{1}/2$, v and two coordinate vectors whose residuals in this process are nonzero form an orthonormal basis of $\ker M_v^*$. Suppose that $|\sum_j b_j| < 4$ and $|\sum_i c_i| < 4$, define $G_B, G_C, m_B, m_C, m, K_B, K_C$ as in Appendix A.3, and put $P_B = G_B B_0$, $P_K = K_B K_B^*$ and $P_C = G_C C_0^*$. Then:*

(a) m_B, m_C are the smallest singular values of B_0, C_0; $\|G_B\| = 1/m_B$, $\|G_C\| = 1/m_C$ and $\|C_0\| = (4 + |\sum_i c_i|)^{1/2}$;

(b) P_B and $P_K = I - P_B$ are the orthogonal projections onto $(\ker B_0)^\perp$ and $\ker B_0$, and P_C and $I - P_C = K_C K_C^*$ those onto $\operatorname{ran} C_0$ and $\ker C_0^*$;

(c) $B_0 K_B = 0$, $K_C^* C_0 = 0$, $G_B^* K_B = 0$, $G_B^* P_B = G_B^*$, $C_0^* G_C = I$, $P_C G_C = G_C$ and $P_C K_C = 0$.

Proof. $M_v^* M_v$ has rows $(4, S_v)$ and $(\overline{S_v}, 4)$, with eigenvalues $4 \pm |S_v|$; if $|S_v| < 4$, its inverse is $(16 - |S_v|^2)^{-1}$ times the matrix with rows $(4, -S_v)$ and $(-\overline{S_v}, 4)$, and multiplying by M_v gives the formula. If $|S_v| < 4$, v is not a multiple of $\mathbf{1}$, so the first two Gram–Schmidt vectors form an orthonormal basis of $\operatorname{ran} M_v$; at each later step the coordinate vectors span $\mathbb{C}^4$, so one of them has a nonzero residual, and the last two vectors are orthonormal and orthogonal to $\operatorname{ran} M_v$, hence a basis of $(\operatorname{ran} M_v)^\perp = \ker M_v^*$, which has dimension two.

For $v = (\overline{b_j})_j$ we have $M_v = B_0^*$, so $G_B = M_v(M_v^* M_v)^{-1}$, $\ker B_0 = \ker M_v^*$, and the squared singular values of B_0 are $4 \pm |\sum_j b_j|$; for $v = (c_i)_i$ we have $M_v = C_0$. (a) $G_B^* G_B = (M_v^* M_v)^{-1}$, whose largest eigenvalue is $1/(4 - |S_v|) = 1/m_B^2$, and likewise for G_C; $\|C_0\|^2 = 4 + |\sum_i c_i|$. (b) $P_B = M_v(M_v^* M_v)^{-1} M_v^*$ is Hermitian and idempotent with range $\operatorname{ran} M_v = (\ker B_0)^\perp$, and $K_B K_B^*$ is the orthogonal projection onto $\operatorname{ran} K_B = \ker B_0$; as $\ker B_0$ and $(\ker B_0)^\perp$ are orthogonal complements, $P_K = I - P_B$; similarly for $P_C = C_0(C_0^* C_0)^{-1} C_0^*$ and $K_C K_C^*$. (c) $B_0 K_B = 0$ and $C_0^* K_C = 0$ by the choice of K_B, K_C. With $G_B^* = (B_0 B_0^*)^{-1} B_0$ we get $G_B^* K_B = 0$ and $G_B^* P_B = (B_0 B_0^*)^{-1} B_0 B_0^* (B_0 B_0^*)^{-1} B_0 = G_B^*$. Finally $C_0^* G_C = C_0^* C_0 (C_0^* C_0)^{-1} = I$, so $P_C G_C = G_C$, and $P_C K_C = G_C C_0^* K_C = 0$. □

Lemma C.12 ([27, Lemma 3.2]). *Suppose that $|\sum_j b_j| < 4$ and $|\sum_i c_i| < 4$, put $A_0 = \|E_0\| = (2 + |1 + a|)^{1/2}$, $A_* = \min(2, A_0 + R_s)$ and*

$$q_Y = R_s^2\Big(1 + \frac{A_*^2 + 6}{m_C^2}\Big).$$

If $q_Y < 6$, then for every feasible completion the matrix $Y = K_C^* D' K_B$ has a polar factor $V \in U(2)$ with $\|Y - \sqrt{6}\,V\|_F \le p := q_Y/(\sqrt{6} + \sqrt{6 - q_Y})$. More precisely, $6I - Y^*Y = K_B^* B'^* B' K_B + K_B^* D'^* P_C D' K_B$ is positive semidefinite with trace at most q_Y, Y is invertible, and $V = Y(Y^*Y)^{-1/2}$. The same holds if A_* is replaced in q_Y by any larger number for which $q_Y < 6$ still holds.

Proof. Here the statement differs from [27], which proves the lemma for $A_* = \min(2, A_0 + R_s)$ only and states its (3.8)–(3.9) without the hypothesis $q_Y < 6$. The lower right 4×4 block of $H'^* H' = 6I$ is $B'^* B' + D'^* D' = 6I$. Compress it by K_B and write $D'^* D' = D'^* P_C D' + D'^* K_C K_C^* D'$ (Lemma C.11(b)); since $K_B^* K_B = I$ and $K_B^* D'^* K_C K_C^* D' K_B = Y^* Y$, this gives the identity for $6I - Y^*Y$ in the statement, whose right side is positive semidefinite. Its trace is $\|B' K_B\|_F^2 + \|P_C D' K_B\|_F^2$. Since $B_0 K_B = 0$, $\|B' K_B\|_F = \|\Delta B K_B\|_F \le b_1'$. By Lemma C.10(ii), $C_0^* D' = C'^* D' - \Delta C^* D' = -E'^* B' - \Delta C^* D'$, so

$P_C D' K_B = G_C(-E'^* \Delta B K_B - \Delta C^* D' K_B)$ and, by Lemma C.11(a), Lemma C.10 and Lemma C.2(i), (ii), $\|P_C D' K_B\|_F \le (A_* b_1' + \sqrt{6}\, c_1')/m_C$. By the Cauchy–Schwarz inequality, $(A_* b_1' + \sqrt{6}\, c_1')^2 \le (A_*^2+6)(b_1'^2 + c_1'^2)$, so the trace is at most $(b_1'^2 + c_1'^2)(1 + (A_*^2+6)/m_C^2) \le q_Y$ by Lemma C.10(i). The same bound holds with a larger A_*.

Let $\ell_1, \ell_2 \ge 0$ be the eigenvalues of $6I - Y^*Y$; then $\ell_1 + \ell_2 \le q_Y < 6$, so the eigenvalues $6 - \ell_k$ of Y^*Y are positive and Y is invertible. Then $V = Y(Y^*Y)^{-1/2}$ [8, Theorem 7.2.6] satisfies $V^*V = I$, and $Y - \sqrt{6}V = V\big((Y^*Y)^{1/2} - \sqrt{6}I\big)$, whose Frobenius norm is $\big(\sum_k (\sqrt{6} - \sqrt{6-\ell_k})^2\big)^{1/2}$. As $\sqrt{6} - \sqrt{6-\ell_k} = \ell_k/(\sqrt{6} + \sqrt{6-\ell_k}) \le \ell_k/(\sqrt{6} + \sqrt{6-q_Y})$ and $(\ell_1^2 + \ell_2^2)^{1/2} \le \ell_1 + \ell_2 \le q_Y$, the norm is at most p. Since p increases with q_Y, the bound holds for every larger $q_Y < 6$. □

Lemma C.13 ([27, Lemma 3.3])**.** *Every $V \in U(2)$ can be written as*

$$V = e(\alpha) \begin{pmatrix} e(\beta)\cos 2\pi t & e(\gamma)\sin 2\pi t \\ -e(-\gamma)\sin 2\pi t & e(-\beta)\cos 2\pi t \end{pmatrix}$$

with $(\alpha, t, \beta, \gamma) \in [0, \frac12] \times [0, \frac14] \times [0,1]^2$. If N_u is divisible by four, this domain is the union of the closed cells $\prod[k_l/N_u, (k_l+1)/N_u]$, with $N_u/2$, $N_u/4$, N_u and N_u values of k_l in the four parameters.

Proof. $\det V$ has modulus one; choose $\alpha \in [0, \frac12]$ with $e(2\alpha) = \det V$. Then $W = e(-\alpha)V$ is unitary with $\det W = 1$, so $W^* = W^{-1}$ equals the adjugate of W; comparing entries, W has rows (ξ_1, ξ_2) and $(-\overline{\xi_2}, \overline{\xi_1})$, and $|\xi_1|^2 + |\xi_2|^2 = 1$ because the first row of W is a unit vector. Choose $t \in [0, \frac14]$ with $\cos 2\pi t = |\xi_1|$, so that $\sin 2\pi t = |\xi_2|$, and $\beta, \gamma \in [0,1]$ with $\xi_1 = e(\beta)|\xi_1|$ and $\xi_2 = e(\gamma)|\xi_2|$ (any value if $\xi_1 = 0$ or $\xi_2 = 0$). The cells cover the domain because $N_u/4$ is an integer. □

For a cell with midpoint parameters $(\alpha_0, t_0, \beta_0, \gamma_0)$ let U be its midpoint matrix and $h = \pi/N_u$. Write the parametrization in the radian angles $\phi_\alpha = 2\pi\alpha$, $\phi_t = 2\pi t$, $\phi_\beta = 2\pi\beta$, $\phi_\gamma = 2\pi\gamma$ (not to be confused with the seed entries a, b_j, c_i); then the four partial derivatives at the midpoint are

$$\partial_{\phi_\alpha} U = iU, \qquad \partial_{\phi_\beta} U = \begin{pmatrix} iU_{00} & 0 \\ 0 & -iU_{11} \end{pmatrix}, \qquad \partial_{\phi_\gamma} U = \begin{pmatrix} 0 & iU_{01} \\ -iU_{10} & 0 \end{pmatrix},$$

$$\partial_{\phi_t} U = e^{i\phi_\alpha} \begin{pmatrix} -e^{i\phi_\beta}\sin\phi_t & e^{i\phi_\gamma}\cos\phi_t \\ -e^{-i\phi_\gamma}\cos\phi_t & -e^{-i\phi_\beta}\sin\phi_t \end{pmatrix},$$

and $dU[\theta] = \theta_\alpha \partial_{\phi_\alpha} U + \theta_t \partial_{\phi_t} U + \theta_\beta \partial_{\phi_\beta} U + \theta_\gamma \partial_{\phi_\gamma} U$ for $\theta = (\theta_\alpha, \theta_t, \theta_\beta, \theta_\gamma) = (\theta_1, \dots, \theta_4) \in \mathbb{R}^4$.

Lemma C.14 ([27, Lemma 3.4])**.** *If V has a representation in the cell, with angular displacement $\theta = 2\pi(\alpha - \alpha_0, t - t_0, \beta - \beta_0, \gamma - \gamma_0) \in [-h, h]^4$ from the midpoint, then*

$$\|V - U\|_F \le \sqrt{6}\, h, \qquad \|V - U - dU[\theta]\|_F \le \tfrac12 \sqrt{42}\, h^2.$$

Proof. Let $V(u)$, $0 \le u \le 1$, be the matrix with angles $\phi_\alpha = \phi_\alpha^0 + xu$, $\tau = \phi_t^0 + yu$, $\phi_\beta = \phi_\beta^0 + zu$, $\phi_\gamma = \phi_\gamma^0 + wu$, where $(x, y, z, w) = \theta$ (in this proof only; z is not the constant of Lemma C.16) and $\phi_\alpha^0, \phi_t^0, \phi_\beta^0, \phi_\gamma^0$ are the midpoint angles; so $V(0) = U$, $V(1) = V$, $V'(0) = dU[\theta]$, and $|x|, |y|, |z|, |w| \le h$. Its entries are $e^{i(\phi_\alpha + \phi_\beta)}\cos\tau$, $e^{i(\phi_\alpha + \phi_\gamma)}\sin\tau$, $-e^{i(\phi_\alpha - \phi_\gamma)}\sin\tau$ and $e^{i(\phi_\alpha - \phi_\beta)}\cos\tau$. Differentiating, the squared moduli of the derivatives of the four entries are $(x+z)^2\cos^2\tau + y^2\sin^2\tau$, $(x+w)^2\sin^2\tau + y^2\cos^2\tau$, $(x-w)^2\sin^2\tau + y^2\cos^2\tau$ and $(x-z)^2\cos^2\tau + y^2\sin^2\tau$, whose sum is $2(x^2 + y^2 + z^2\cos^2\tau + w^2\sin^2\tau) \le 6h^2$. The second

derivative of the first entry is $e^{i(\phi_\alpha+\phi_\beta)}\big(-((x+z)^2+y^2)\cos\tau - 2i(x+z)y\sin\tau\big)$, of squared modulus $((x+z)^2+y^2)^2\cos^2\tau + 4(x+z)^2y^2\sin^2\tau$; the last entry gives the same with $x-z$, and the two off-diagonal entries give the same with $x\pm w$ in place of $x\pm z$ and cos, sin interchanged. With $Q = x^2+y^2+z^2$,

$$((x+z)^2+y^2)^2 + ((x-z)^2+y^2)^2 = 2Q^2 + 8x^2z^2 \le 26h^4,$$
$$4y^2((x+z)^2+(x-z)^2) = 8y^2(x^2+z^2) \le 16h^4,$$

and likewise with w. So $\|V''(u)\|_F^2 \le 26h^4(\cos^2\tau+\sin^2\tau)+16h^4(\sin^2\tau+\cos^2\tau) = 42h^4$. Now $V(1)-V(0) = \int_0^1 V'(u)\,du$ and $V(1)-V(0)-V'(0) = \int_0^1\int_0^u V''(v)\,dv\,du = \int_0^1(1-v)V''(v)\,dv$, which give the two bounds. □

C.5. **Stage A: the cell constants.** In Appendices C.5 and C.6 assume that $|\sum_j b_j| < 4$, $|\sum_i c_i| < 4$ and $q_Y < 6$ (the frame checks), so that every feasible completion has the polar factor V of Lemma C.12. Fix a cell as in Lemma C.14, and put

$$D_{\mathrm{span}} = -C_0E_0^*G_B^*, \qquad D_{\ker} = \sqrt{6}\,K_CUK_B^*, \qquad D = D_{\mathrm{span}} + D_{\ker}.$$

A feasible completion is *associated with the cell* if its V has a representation in the cell; θ is then the angular displacement of Lemma C.14, and we put $Z = D' - D$. We write $\mathcal{J}(s,\theta) = \mathcal{J}_1+\mathcal{J}_2+\mathcal{J}_3$ for the three terms of the definition of $\mathcal{J}$ in Appendix A.3, and $P_K = K_BK_B^*$. The proofs below use A_* only through $A_0 \le A_*$, $\|E'\| \le A_*$ and Lemma C.12, so every bound of Appendices C.5 and C.6 remains valid if A_* is replaced by a larger number for which $q_Y < 6$, with q_Y and p computed from it, as the programs do (Appendix A.3).

Lemma C.15 ([27, Lemma 3.6])**.** *$DP_K = D_{\ker}$, $\|DP_K\| = \sqrt{6}$, and $\|[C_0\ D]\| \le L_{CD} = \max(\sqrt{6},\ \|C_0\|(1+(A_0/m_B)^2)^{1/2})$, where $\|C_0\| = (4+|\sum_i c_i|)^{1/2}$.*

Proof. $D_{\mathrm{span}}P_K = 0$ since $G_B^*K_B = 0$, and $D_{\ker}P_K = D_{\ker}$; and $D_{\ker}^*D_{\ker} = 6K_BK_B^*$ has the eigenvalues $6,6,0,0,0$. Also $D_{\mathrm{span}}D_{\ker}^* = 0$, and $G_B^*G_B = (B_0B_0^*)^{-1}$, so $[C_0\ D][C_0\ D]^* = C_0C_0^* + DD^* = X_1 + X_2$ with $X_1 = C_0(I + E_0^*(B_0B_0^*)^{-1}E_0)C_0^*$ and $X_2 = 6K_CK_C^*$. Both are positive semidefinite, $X_1X_2 = 0$ as $C_0^*K_C = 0$, $\|X_2\| = 6$ and $\|X_1\| \le \|C_0\|^2(1+A_0^2/m_B^2)$, since $\|(B_0B_0^*)^{-1}\| = 1/m_B^2$. Apply Lemma C.2(iii). □

Lemma C.16 ([27, Lemma 3.5])**.** *For every feasible completion associated with the cell, $Z = ZP_B + P_CZP_K + (I-P_C)ZP_K$; the three terms are pairwise orthogonal for the Frobenius inner product;*

$$ZP_B = (-\Delta C\,E_0^* - C'\Delta E^* - D'\Delta B^*)G_B^*, \qquad P_CZP_K = G_C(-E'^*\Delta B - \Delta C^*D')P_K,$$
$$(I-P_C)ZP_K = K_C(Y - \sqrt{6}\,U)K_B^*,$$

and $\|D'-D\|_F \le z = \big((R_s(\sqrt{6}+A_*)/m)^2 + (6h+p)^2\big)^{1/2}$.

Proof. $P_B + P_K = I$. If $X_1 = X_1P_B$ and $X_2 = X_2P_K$, then $\mathrm{tr}(X_1^*X_2) = \mathrm{tr}(P_BX_1^*X_2P_K) = \mathrm{tr}(X_1^*X_2P_KP_B) = 0$; if $X_2 = P_CX_2$ and $X_3 = (I-P_C)X_3$, then $\mathrm{tr}(X_2^*X_3) = 0$ likewise. This gives the decomposition and the orthogonality.

First term: $P_B = B_0^*G_B^*$ is Hermitian, $B_0 = B' - \Delta B$ and $D'B'^* = -C'E'^*$, so $D'P_B = (-C'E'^* - D'\Delta B^*)G_B^*$. Also $D_{\ker}P_B = 0$, since $K_B^*P_B = (P_BK_B)^* = 0$, and $D_{\mathrm{span}}P_B = D_{\mathrm{span}}$ by Lemma C.11(c). Hence $ZP_B = (-C'E'^* - D'\Delta B^* + C_0E_0^*)G_B^*$, and $-C'E'^* + C_0E_0^* = -\Delta C\,E_0^* - C'\Delta E^*$. Second term: $P_C = G_CC_0^*$, $C_0^*D' = -E'^*B' - \Delta C^*D'$ (Lemma C.10(ii)) and $B'P_K = \Delta BP_K$ give $P_CD'P_K = G_C(-E'^*\Delta B - \Delta C^*D')P_K$, while $P_CDP_K = P_CD_{\ker} = 0$ by Lemma C.15 and $P_CK_C = 0$. Third term: $(I-P_C)ZP_K =$

$K_C(K_C^*D'K_B - K_C^*DK_B)K_B^*$, with $K_C^*D'K_B = Y$, $K_C^*D_{\mathrm{span}} = 0$ (as $K_C^*C_0 = 0$) and $K_C^*D_{\mathrm{ker}}K_B = \sqrt{6}U$.

Bounds: with $r_{EB} = (e_1^2 + b_1'^2)^{1/2} = \|[\Delta E\ \Delta B]\|_F$, the first term is $-(\Delta C\, E_0^* + [C'\ D'][\Delta E\ \Delta B]^*)G_B^*$, so by Lemma C.2(i), Lemma C.11(a) and Lemma C.10, $\|ZP_B\|_F \le (A_0c_1' + \sqrt{6}\, r_{EB})/m_B \le (\sqrt{6}\, r_{EB} + A_*c_1')/m$. Similarly $\|P_CZP_K\|_F \le (A_*b_1' + \sqrt{6}\, c_1')/m_C \le (A_*r_{EB} + \sqrt{6}\, c_1')/m$. The matrix with rows $(\sqrt{6}, A_*)$ and $(A_*, \sqrt{6})$ has norm $\sqrt{6} + A_*$ (Lemma C.2(iv)) and $r_{EB}^2 + c_1'^2 \le R_s^2$, so $\|ZP_B\|_F^2 + \|P_CZP_K\|_F^2 \le (R_s(\sqrt{6} + A_*)/m)^2$. Finally, by Lemma C.2(ii) and Lemmas C.12 and C.14, $\|(I - P_C)ZP_K\|_F = \|Y - \sqrt{6}U\|_F \le \|Y - \sqrt{6}V\|_F + \sqrt{6}\|V - U\|_F \le p + 6h$. Add the squares. □

Lemma C.17 ([27, Lemma 3.7])**.** *For every feasible completion associated with the cell, $\|D' - D - \mathcal{J}(s,\theta)\|_F \le E_r$, where L_{CD}, e_{off} and $E_r = \left(e_{\mathrm{off}}^2 + (\frac{1}{2}\sqrt{6\cdot 42}\, h^2 + p)^2\right)^{1/2}$ are as in Appendix A.3.*

Proof. By Lemma C.11(c), $\mathcal{J}_1 = \mathcal{J}_1P_B$, $\mathcal{J}_2 = P_C\mathcal{J}_2P_K$ and $\mathcal{J}_3 = (I - P_C)\mathcal{J}_3P_K$, so by the decomposition of Lemma C.16 the matrix $Z - \mathcal{J}(s,\theta)$ is the sum of the three pairwise orthogonal matrices $ZP_B - \mathcal{J}_1$, $P_CZP_K - \mathcal{J}_2$ and $(I - P_C)ZP_K - \mathcal{J}_3$. Substituting $C' = C_0 + \Delta C$, $D' = D + Z$ and $E' = E_0 + \Delta E$ in Lemma C.16, and using $DP_K = D_{\mathrm{ker}}$,

$$\begin{aligned} ZP_B - \mathcal{J}_1 &= -(F_CE_0^* + [C_0\ D][F_E\ F_B]^*)G_B^* - (\Delta C\, \Delta E^* + Z\Delta B^*)G_B^*, \\ P_CZP_K - \mathcal{J}_2 &= -G_C(E_0^*F_BP_K + F_C^*D_{\mathrm{ker}}) - G_C(\Delta E^*\Delta B + \Delta C^*Z)P_K, \\ (I - P_C)ZP_K - \mathcal{J}_3 &= K_C(Y - \sqrt{6}\, U - \sqrt{6}\, dU[\theta])K_B^*. \end{aligned}$$

Let $x = (\|F_E\|_F^2 + \|F_B\|_F^2)^{1/2}$ and $y = \|F_C\|_F$. By Lemma C.2(i), (ii), Lemma C.11(a) and Lemma C.15, the first parts of the first two lines have Frobenius norms at most $(L_{CD}x + A_0y)/m$ and $(A_0x + \sqrt{6}\, y)/m$; the matrix with rows (L_{CD}, A_0) and $(A_0, \sqrt{6})$ has norm at most $L_{CD}+A_0$ (Lemma C.2(iv), as $L_{CD} \ge \sqrt{6}$), and $x^2+y^2 \le R_s^4/4$ (Lemma C.10(i)), so these two parts together have norm at most $(L_{CD}+A_0)R_s^2/(2m)$. The terms $\Delta C\, \Delta E^*$ and $\Delta E^*\Delta B$ have norms at most $c_1'e_1/m$ and e_1b_1'/m after the factors G_B^*, G_C, P_K, together at most $e_1(b_1'^2 + c_1'^2)^{1/2}/m \le R_s^2/(2m)$, since $2e_1(b_1'^2 + c_1'^2)^{1/2} \le e_1^2 + b_1'^2 + c_1'^2 \le R_s^2$. The terms with Z have norms at most zb_1'/m and $c_1'z/m$, together at most zR_s/m, by Lemma C.16. By the triangle inequality in $\mathbb{R}^2$ for the pairs of norms,

$$(\|ZP_B - \mathcal{J}_1\|_F^2 + \|P_CZP_K - \mathcal{J}_2\|_F^2)^{1/2} \le \frac{(L_{CD} + A_0)R_s^2}{2m} + \frac{R_s^2}{2m} + \frac{zR_s}{m} = e_{\mathrm{off}}.$$

For the third line, $Y - \sqrt{6}U - \sqrt{6}dU[\theta] = (Y - \sqrt{6}V) + \sqrt{6}(V - U - dU[\theta])$ has Frobenius norm at most $p + \frac{1}{2}\sqrt{6\cdot 42}\, h^2$ by Lemmas C.12 and C.14. Add the squares. □

The programs compute the coefficients of $\mathcal{J}$ from the following entrywise form. Index the rows and columns of D by $0, \dots, 3$ (rows and columns $2, \dots, 5$ of H'), write $(G_B)_{j0}, (G_B)_{j1}$ for the entries of the 4×2 matrix G_B, and similarly for G_C, K_B, K_C.

Lemma C.18 ([27, Section 3.5]). *For $0 \le i, j \le 3$,*

$$\begin{aligned}\mathcal{J}(s,\theta)_{ij} = &- c_i\,\overline{ia\,(G_B)_{j1}}\;s_a \\ &+ \sum_{k=0}^{3}\Big(-((G_C)_{i0} + (G_C)_{i1}\overline{a})\,ib_k\,(P_K)_{kj} - D_{ik}\,\overline{ib_k\,(G_B)_{j1}}\Big)s_{b_k} \\ &+ \sum_{k=0}^{3}\Big(-\mathbf{1}_{i=k}\,ic_k\big(\overline{(G_B)_{j0}} + \overline{a\,(G_B)_{j1}}\big) - (G_C)_{i1}\,\overline{ic_k}\,(D_{\ker})_{kj}\Big)s_{c_k} \\ &+ \sum_{l=0}^{3} W_{ij,l}\,(dU[\theta])_{\lfloor l/2\rfloor,\,l \bmod 2},\end{aligned}$$

where $W_{ij,l} = \sqrt{6}\,(K_C)_{i,\lfloor l/2\rfloor}\,\overline{(K_B)_{j,\,l \bmod 2}}$.

Proof. E_1 has the single entry ias_a at $(1,1)$, B_1 the entries $ib_k s_{b_k}$ at $(1,k)$ and C_1 the entries $ic_k s_{c_k}$ at $(k,1)$, and $\overline{\zeta s} = \overline{\zeta}s$ for real s. Hence $(C_1E_0^*G_B^*)_{ij} = ic_i s_{c_i}\big(\overline{(G_B)_{j0}} + \overline{a\,(G_B)_{j1}}\big)$, $(C_0E_1^*G_B^*)_{ij} = c_i\overline{ia\,(G_B)_{j1}}\,s_a$ and $(DB_1^*G_B^*)_{ij} = \sum_k D_{ik}\overline{ib_k\,(G_B)_{j1}}\,s_{b_k}$, which are the terms of $\mathcal{J}_1$ (rows $0,1$ of E_0 are $(1,1)$ and $(1,a)$, and C_0 has rows $(1,c_i)$). Next $(G_CE_0^*B_1P_K)_{ij} = \sum_k\big((G_C)_{i0} + (G_C)_{i1}\overline{a}\big)ib_k s_{b_k}(P_K)_{kj}$ and, since $DP_K = D_{\ker}$, $(G_CC_1^*DP_K)_{ij} = (G_C)_{i1}\sum_k \overline{ic_k}\,s_{c_k}(D_{\ker})_{kj}$, the terms of $\mathcal{J}_2$. Finally $(K_C\,dU[\theta]\,K_B^*)_{ij} = \sum_{p,q}(K_C)_{ip}(dU[\theta])_{pq}\overline{(K_B)_{jq}}$. □

C.6. **Stage A: the norm and directional tests.**

Lemma C.19 ([27, Lemma 3.8]). *Every feasible completion associated with the cell satisfies $\sum_{i,j=0}^{3}(|D_{ij}| - 1)^2 \le z^2$.*

Proof. $|D'_{ij}| = 1$, so $\big||D_{ij}| - 1\big| \le |D'_{ij} - D_{ij}|$; sum the squares and apply Lemma C.16. □

Lemma C.20 ([27, Lemma 3.9 and Corollary 3.10]). *Let c_{all}, J_{all} and $D \circ y_D$ be as in Appendix A.3. For every $y = (y_X, y_Y, y_D) \in \mathbb{R}^2\times\mathbb{R}^2\times\mathbb{R}^{16}$, with $g = J_{\mathrm{all}}^* y = (g_s, g_\theta) \in \mathbb{R}^9\times\mathbb{R}^4$, every feasible completion associated with the cell satisfies*

$$y \cdot c_{\mathrm{all}} \le R_s\|g_s\| + h\|g_\theta\|_1 + E_r\|D \circ y_D\|_F + \tfrac{1}{2}z^2\max\big(0, \max_{i,j}(-y_{D,ij})\big) + \tfrac{1}{2}R_s^2(\|y_X\| + \|y_Y\|).$$

Consequently a cell for which the inequality of Lemma C.19 or this inequality, for some y, fails has no feasible completion associated with it.

Proof. Complex numbers are identified with vectors of $\mathbb{R}^2$ (real part, imaginary part), and $\cdot$ is the real inner product. The second row and the second column of H' are orthogonal to its first row and column, which consist of ones, so $1 + ae^{is_a} + \sum_j b_j e^{is_{b_j}} = 0$ and $1 + ae^{is_a} + \sum_i c_i e^{is_{c_i}} = 0$. Dividing by i, $c_X + J_X s + \rho_X = 0$ with $\rho_X = \big(a(e^{is_a} - 1 - is_a) + \sum_j b_j(e^{is_{b_j}} - 1 - is_{b_j})\big)/i$, so $|\rho_X| \le \|s\|^2/2 \le R_s^2/2$ by Lemma C.1(i); likewise $c_Y + J_Y s + \rho_Y = 0$ with $|\rho_Y| \le R_s^2/2$. Put $R = Z - \mathcal{J}(s,\theta)$, so $\|R\|_F \le E_r$ by Lemma C.17. Since $D' = D + Z$ and $|D'_{ij}| = 1$,

$$0 = \tfrac{1}{2}(|D'_{ij}|^2 - 1) = c_{D,ij} + \mathrm{Re}(\overline{D_{ij}}Z_{ij}) + \tfrac{1}{2}|Z_{ij}|^2 = c_{D,ij} + J_{D,ij}(s,\theta) + \mathrm{Re}(\overline{D_{ij}}R_{ij}) + \tfrac{1}{2}|Z_{ij}|^2.$$

So $0 = c_{\mathrm{all}} + J_{\mathrm{all}}(s,\theta) + \varrho$, where ϱ has the components ρ_X, ρ_Y and $\mathrm{Re}(\overline{D_{ij}}R_{ij}) + \frac{1}{2}|Z_{ij}|^2$, and $y \cdot c_{\mathrm{all}} = -g_s \cdot s - g_\theta \cdot \theta - y \cdot \varrho$. Here $-g_s \cdot s \le R_s\|g_s\|$, $-g_\theta \cdot \theta \le h\|g_\theta\|_1$, $-y_X \cdot \rho_X - y_Y \cdot \rho_Y \le \frac{1}{2}R_s^2(\|y_X\| + \|y_Y\|)$, $-\sum_{i,j} y_{D,ij}\,\mathrm{Re}(\overline{D_{ij}}R_{ij}) \le \sum_{i,j}|y_{D,ij}D_{ij}|\,|R_{ij}| \le \|D \circ y_D\|_F\,E_r$, and $-\frac{1}{2}\sum_{i,j} y_{D,ij}|Z_{ij}|^2 \le \frac{1}{2}\max(0, \max_{i,j}(-y_{D,ij}))\,\|Z\|_F^2$ with $\|Z\|_F \le z$. The last assertion holds because both inequalities are satisfied by every feasible completion associated with the cell. □

C.7. **Root certificates.**

Lemma C.21 ([27, Lemma 4.3])**.** *Let $P \in \mathbb{R}^{6\times 6}$. For $x \in \mathbb{R}^{6\times 6}$ with rows x_i put $a_{ij}(x) = \|x_i - x_j\|^2$, and define $\mathcal{R}_P(x) \in \mathbb{C}^{15} \cong \mathbb{R}^{30}$ by $F(P+x) = F(P) + L_P x + \mathcal{R}_P(x)$, with $(L_P x)_{ij} = \sum_g e(P_{ig} - P_{jg})(x_{ig} - x_{jg})$ for $i > j$. Then*

$$|\mathcal{R}_P(x)_{ij}| \le \pi a_{ij}(x), \qquad |\mathcal{R}_P(x)_{ij} - \mathcal{R}_P(v)_{ij}| \le \pi a_{ij}(x-v)^{1/2}\big(a_{ij}(x)^{1/2} + a_{ij}(v)^{1/2}\big).$$

Let $M \in \mathbb{R}^{36\times 30}$. If b satisfies $\sum_{i>j} w_{ij}(y) a_{ij}(x) \le b\|x\|^2$ for every horizontal x and every unit $y \in \mathbb{R}^{36}$, where $w_{ij}(y)$ is the norm of the two coordinates of M^*y that belong to the pair (i,j), then $\|M\mathcal{R}_P(x)\| \le \pi b\|x\|^2$ and $\|M(\mathcal{R}_P(x) - \mathcal{R}_P(v))\| \le \pi b\|x-v\|(\|x\| + \|v\|)$ for horizontal x, v.

Proof. With $t_g = x_{ig} - x_{jg}$ and r as in Lemma C.1(ii), $e(t_g) = 1 + 2\pi i t_g + 2\pi i\, r(t_g)$, so $F_{ij}(P+x) = F_{ij}(P) + (L_P x)_{ij} + \sum_g e(P_{ig} - P_{jg}) r(t_g)$. Thus $\mathcal{R}_P(x)_{ij} = \sum_g e(P_{ig} - P_{jg}) r(x_{ig} - x_{jg})$, and Lemma C.1(ii) gives $|\mathcal{R}_P(x)_{ij}| \le \pi \sum_g t_g^2 = \pi a_{ij}(x)$ and, with $t'_g = v_{ig} - v_{jg}$, $|\mathcal{R}_P(x)_{ij} - \mathcal{R}_P(v)_{ij}| \le \pi \sum_g |t_g - t'_g|(|t_g| + |t'_g|)$, which is at most the stated bound by the Cauchy–Schwarz inequality. For a unit y, $y \cdot M\mathcal{R}_P(x) = (M^*y)\cdot \mathcal{R}_P(x) \le \sum_{i>j} w_{ij}(y)|\mathcal{R}_P(x)_{ij}| \le \pi b\|x\|^2$, and the supremum over y is $\|M\mathcal{R}_P(x)\|$. Likewise, by the Cauchy–Schwarz inequality with the weights $w_{ij}(y) \ge 0$ and the hypothesis applied to the horizontal matrices $x - v$, x and v,

$$\begin{aligned} y \cdot M(\mathcal{R}_P(x) - \mathcal{R}_P(v)) &\le \pi \Big(\sum_{i>j} w_{ij} a_{ij}(x-v)\Big)^{1/2} \Big[\Big(\sum_{i>j} w_{ij} a_{ij}(x)\Big)^{1/2} + \Big(\sum_{i>j} w_{ij} a_{ij}(v)\Big)^{1/2}\Big] \\ &\le \pi b\|x-v\|(\|x\| + \|v\|). \end{aligned}$$

□

Lemma C.22 ([27, Lemma 4.4])**.** *Both $b = \sqrt{8}\,\|M\|$ and $b = \sqrt{6}\,\|\mathcal{M}\|$ satisfy the hypothesis of Lemma C.21, where $\mathcal{M} \in \mathbb{R}^{30\times 216}$ has the rows $\mathcal{M}_{l,:} = (M_{:,l})^* \otimes (\mathbf{e}_i - \mathbf{e}_j)^*$ for l one of the two coordinates of the pair (i,j), so that $\|\mathcal{M}\|^2 = \lambda_{\max}(\mathcal{M}\mathcal{M}^*)$ and $(\mathcal{M}\mathcal{M}^*)_{ll'} = ((\mathbf{e}_i - \mathbf{e}_j)\cdot(\mathbf{e}_{i'} - \mathbf{e}_{j'}))(M_{:,l}\cdot M_{:,l'})$ for l, l' belonging to the pairs (i,j) and (i',j').*

Proof. Let x be horizontal, $s = \|x\|$ and $u_i = \|x_i\|^2$. The column sums of x vanish, so $\sum_i x_i = 0$, hence $\sum_{j\ne i} x_i \cdot x_j = -u_i$ and $\sum_{i\ne j} x_i \cdot x_j = -s^2$. Expanding $a_{ij} = u_i + u_j - 2x_i\cdot x_j$ gives

$$\sum_{i>j} a_{ij} = 6s^2, \qquad \sum_{i>j} a_{ij}^2 = 6\sum_i u_i^2 + s^4 + 2\sum_{i,j}(x_i\cdot x_j)^2.$$

(For the second: $\sum_{i\ne j}(u_i+u_j)^2 = 8\sum_i u_i^2 + 2s^4$, $\sum_{i\ne j}(u_i+u_j)\,x_i\cdot x_j = -2\sum_i u_i^2$ and $\sum_{i\ne j}(x_i\cdot x_j)^2 = \sum_{i,j}(x_i\cdot x_j)^2 - \sum_i u_i^2$; halve the sum over $i \ne j$.) By the Cauchy–Schwarz inequality $u_i = \|\sum_{j\ne i} x_j\|^2 \le 5(s^2 - u_i)$, so $u_i \le 5s^2/6$ and $\sum_i u_i^2 \le 5s^4/6$; and $(x_i\cdot x_j)^2 \le u_i u_j$ gives $\sum_{i,j}(x_i\cdot x_j)^2 \le s^4$. Hence $\sum_{i>j} a_{ij}^2 \le 8s^4$, and, as $\sum_{i>j} w_{ij}(y)^2 = \|M^*y\|^2 \le \|M\|^2$ for unit y, $\sum_{i>j} w_{ij} a_{ij} \le \|M\|\sqrt{8}\,s^2$.

For the second choice, coordinate l of $\mathcal{M}(y \otimes x_{:,g})$ is $(M^*y)_l\,(x_{ig} - x_{jg})$, where $x_{:,g}$ is column g of x. Summing the squared norms over g gives, for unit y, $\sum_{i>j} w_{ij}(y)^2 a_{ij}(x) \le \|\mathcal{M}\|^2 \sum_g \|x_{:,g}\|^2 = \|\mathcal{M}\|^2 s^2$. By the Cauchy–Schwarz inequality,

$$\sum_{i>j} w_{ij} a_{ij} \le \Big(\sum_{i>j} w_{ij}^2 a_{ij}\Big)^{1/2}\Big(\sum_{i>j} a_{ij}\Big)^{1/2} \le \|\mathcal{M}\| s \cdot \sqrt{6}\,s.$$

The formula for $\mathcal{M}\mathcal{M}^*$ is the inner product of the two tensor products. □

Lemma C.23 ([27, Proposition 4.5])**.** *Let P, T, n_0, ι, C, ω, χ, κ, φ be as in Appendix A.4 and satisfy (A.1), and let $M \in \mathbb{R}^{36\times 30}$ satisfy $\|M\| \le \kappa$, $\kappa\varphi \le n_0$ and $\|\Pi - TT^* - ML_P\Pi\| \le \iota$. If $C \ge \pi b$ for a number b as in Lemma C.21, then (A.2)–(A.4) hold, so the Root certificate is certified. Inequality (A.3) holds for every $\delta \in \mathbb{R}^{36}$.*

Proof. Let δ be horizontal with $F(P+\delta) = 0$, and put $E = \Pi - TT^* - ML_P\Pi$. Since $\Pi\delta = \delta$, $(I - TT^*)\delta = E\delta + ML_P\delta$, and $L_P\delta = F(P+\delta) - F(P) - \mathcal{R}_P(\delta) = -F(P) - \mathcal{R}_P(\delta)$. So $(I - TT^*)\delta = E\delta - MF(P) - M\mathcal{R}_P(\delta)$, whose norm is at most $\iota\|\delta\| + \kappa\varphi + \pi b\|\delta\|^2 \le n_P(\|\delta\|)$ by Lemma C.21. For every δ, with $\eta = T^*\delta$, $\|(I - TT^*)\delta\|^2 = \|\delta - T\eta\|^2 = \|\delta\|^2 - 2\|\eta\|^2 + \eta^*T^*T\eta \ge \|\delta\|^2 - (1+\omega)\|\eta\|^2$, since $\eta^*T^*T\eta \ge (1-\omega)\|\eta\|^2$ by (A.1). For horizontal v and $h' = \delta - v$, $(I - TT^*)h' = Eh' + ML_Ph'$ and, subtracting the expansions of F at δ and at v, $L_Ph' = -F(P+v) - (\mathcal{R}_P(\delta) - \mathcal{R}_P(v))$. So $\|(I - TT^*)h'\| \le \iota\|h'\| + \kappa\|F(P+v)\| + \pi b\|h'\|(\|\delta\| + \|v\|)$, which gives (A.4). □

Lemma C.24 ([27, Lemma 4.7])**.** *Let $g \in \mathcal{G}$ (Section 3.6), a composition of permutations of the rows and of the columns, possibly transposition and possibly $Y \mapsto -Y$, acting on $\mathbb{R}^{6\times 6}$ and on each column of a matrix in $\mathbb{R}^{36\times k}$. Then g is an orthogonal map of $\mathbb{R}^{36}$ commuting with Π and mapping $\mathbb{Z}^{6\times 6}$ onto itself. For every real Y, $\|F(gY)\| = \|F(Y)\|$ and $e(gY)$ is obtained from $e(Y)$ by permutations of rows and columns, possibly transposition and possibly complex conjugation; if $e(Y)$ is a complex Hadamard matrix, so is $e(gY)$, and the two are equivalent. If $(P, T, n_0, \iota, C, \omega, \chi, \kappa, \varphi)$ is a certified Root certificate, so is $(gP, gT, n_0, \iota, C, \omega, \chi, \kappa, \varphi)$; for $r \ge 0$, $e(gP + \delta') \in \mathcal{S}(gP, r)$ if and only if $e(P + g^{-1}\delta') \in \mathcal{S}(P, r)$, and these two matrices are equivalent. In particular one of these two matrices is extendible if and only if the other is.*

Proof. g permutes the 36 coordinates and possibly changes all their signs, so it is orthogonal and maps $\mathbb{Z}^{6\times 6}$ onto itself. Permutation matrices R satisfy $R\mathbf{1} = \mathbf{1}$ and commute with C_6, so $\Pi(RYR'^{\mathsf{T}}) = R(\Pi Y)R'^{\mathsf{T}}$; also $\Pi(Y^{\mathsf{T}}) = (\Pi Y)^{\mathsf{T}}$ and $\Pi(-Y) = -\Pi Y$. The matrix $e(gY)$ is obtained from $e(Y)$ by permutations, possibly transposition and possibly complex conjugation, as $e(-Y) = \overline{e(Y)}$; by Lemma C.4 these operations map complex Hadamard matrices to complex Hadamard matrices. Let $A = e(Y)$; by Lemma C.3(iv), $\|F(Y)\| = \|AA^* - 6I\|_F/(2\pi\sqrt{2})$. If $A' = RAR'^{\mathsf{T}}$ then $A'A'^* = RAA^*R^{\mathsf{T}}$; if $A' = \overline{A}$ then $A'A'^* = \overline{AA^*}$; if $A' = A^{\mathsf{T}}$ then $A'A'^* = \overline{A^*A}$, and $\|A^*A - 6I\|_F^2 = \|A^*A\|_F^2 - 12\operatorname{tr}(A^*A) + 216 = \|AA^* - 6I\|_F^2$, because $\|A^*A\|_F^2 = \operatorname{tr}(A^*AA^*A) = \|AA^*\|_F^2$ and $\operatorname{tr}(A^*A) = \operatorname{tr}(AA^*)$. So $\|F(gY)\| = \|F(Y)\|$ in each case.

For the certificate: $\|(gT)^*gT - I\| = \|T^*T - I\|$, $\|(I - \Pi)gT\| = \|g(I - \Pi)T\| = \|(I - \Pi)T\|$ and $\|F(gP)\| = \|F(P)\|$. If δ' is horizontal, then so is $\delta = g^{-1}\delta'$, with $\|\delta\| = \|\delta'\|$, $(gT)^*\delta' = T^*\delta$, $(I - gT(gT)^*)\delta' = g(I - TT^*)\delta$ and $\|F(gP + \delta')\| = \|F(P + \delta)\|$; so (A.2)–(A.4) for (gP, gT) at δ' and v' are those for (P, T) at δ and $v = g^{-1}v'$. The same identities give the statement on solution sets. A member of $\mathcal{S}(gP, r)$ determines its displacement only modulo $\mathbb{Z}^{6\times 6}$, and g^{-1} maps $\mathbb{Z}^{6\times 6}$ onto itself, so $e(P + g^{-1}\delta')$ does not depend on that choice. Finally, $e(gP + \delta') = e(g(P + \delta))$ is equivalent to $e(P + \delta)$; by Lemma C.4, one of them is extendible if and only if the other is. □

C.8. **Stage A: from a cell to a record.** In this subsection we consider a cell as in Appendix C.5 and use the notation of Appendix A.5; the letter Z now denotes an integer matrix, as in Appendices A.5 and A.6.

Lemma C.25 ([27, Lemma 4.8]). *Let $\Lambda \ge 0$ be an upper bound for $z^2 - \sum_j (m_j - 1)^2$, $0 < \underline{m} \le \min_j m_j$, $q_d \ge \Lambda/\underline{m}$ and $q_d < 3.8$. Then every feasible completion associated with the cell satisfies $\|d\| \le \bar{d}$ and $(\sum_j m_j d_j^2)^{1/2} \le \bar{d}_m$ whenever $\bar{d} \ge q_d^{1/2}(1 - q_d/4)^{-1/2}$ and $\bar{d}_m \ge \Lambda^{1/2}(1 - q_d/4)^{-1/2}$.*

Proof. Write $D_j' = D_j^\circ e^{id_j}$ and $c_j = |D_j' - D_j^\circ| = 2|\sin(d_j/2)|$. Since $|D_j'| = 1$ and $D_j = m_j D_j^\circ$, $|D_j' - D_j|^2 = 1 - 2m_j \cos d_j + m_j^2 = (m_j - 1)^2 + m_j c_j^2$. Summing over $j \in \mathcal{I}_D$ and using Lemma C.16, $\sum_j m_j c_j^2 \le z^2 - \sum_j (m_j - 1)^2 \le \Lambda$, so $\sum_j c_j^2 \le \Lambda/\underline{m} \le q_d < 3.8$, and each $c_j < 2$. As $|d_j| \le \pi$, $|d_j| = 2 \arcsin(c_j/2) = \int_0^{c_j} (1 - c^2/4)^{-1/2}\, dc \le c_j (1 - q_d/4)^{-1/2}$, because $c^2 \le c_j^2 \le q_d$ under the integral. Summing the squares gives $\|d\|^2 \le q_d/(1 - q_d/4)$ and $\sum_j m_j d_j^2 \le \Lambda/(1 - q_d/4)$. □

Lemma C.26 ([27, Lemma 4.10]). *Assume the hypotheses of Lemma C.25, and let $P_0, \epsilon, u, e_D, e_{\sin}$ be as in Lemma A.1. For a real matrix P (the center of a Root certificate) and an integer matrix Z, put $\Delta = \Pi(P_0 - D_0(P) - Z)$. Every feasible completion associated with the cell is equivalent to $e(P + \delta)$, where $\delta = \Delta + \Pi(\epsilon + u/(2\pi))$ is horizontal and $F(P + \delta) = 0$, and*

$$\|\delta\| \le \Big(\|\Delta\|^2 + \frac{R_s^2 + \bar{d}^2}{(2\pi)^2} + \frac{S_\Delta}{\pi} \Big)^{1/2} + \|\epsilon\|,$$

with $S_\Delta = \min(S_1, S_2)$ and S_1, S_2 as in Appendix A.5.

Proof. Here the statement differs from [27], where P_0, ϵ and Z are those of its programs [27, Lemma 4.9 and Section 4.5]; here they are those of Lemma A.1 and any integer matrix. By Lemma A.1 the completion is $e(X')$ with $X' = W + Z'$, where $W = P_0 + \epsilon + u/(2\pi)$ and Z' is integral. By Lemma C.3(ii), $\delta = \Pi(W - D_0(P) - Z) = \Pi(X' - Z' - P - Z)$, so $(P + \delta) - X' = -Z' - Z - (I - \Pi)(X' - Z' - P - Z) \in \mathbb{Z}^{6\times 6} + \ker \Pi$. By Lemma C.3(iii), (iv), $e(P + \delta)$ is obtained from $e(X')$ by rephasing rows and columns, so it is equivalent to $e(X')$ and complex Hadamard, and $F(P + \delta) = 0$; and $\delta \in \operatorname{ran} \Pi$ is horizontal. Next, $\|\delta\| \le \|\Delta + \Pi u/(2\pi)\| + \|\Pi\epsilon\|$ and $\|\Pi\epsilon\| \le \|\epsilon\|$. Since Π is an orthogonal projection and Δ is horizontal, $\Delta \cdot \Pi u = \Delta \cdot u$ and $\|\Pi u\| \le \|u\| \le (R_s^2 + \bar{d}^2)^{1/2}$ (Lemma A.1), so $\|\Delta + \Pi u/(2\pi)\|^2 \le \|\Delta\|^2 + \Delta \cdot u/\pi + (R_s^2 + \bar{d}^2)/(2\pi)^2$. It remains to show $\Delta \cdot u \le S_1$ and $\Delta \cdot u \le S_2$. First, $u = X(s, \theta) + e_D + e_{\sin}$, and $\Delta \cdot X(s, \theta) = (X^*\Delta)_s \cdot s + (X^*\Delta)_\theta \cdot \theta \le R_s \|(X^*\Delta)_s\| + h\|(X^*\Delta)_\theta\|_1$, $\Delta \cdot e_D = \Delta_D \cdot e_D \le E_r \|\Delta_D\|$ and $\Delta \cdot e_{\sin} \le \|\Delta_D\|_\infty \|e_{\sin}\|_1 \le \|\Delta_D\|_\infty \bar{d}^3/6$. Second, u equals s on $\mathcal{I}_s$, d on $\mathcal{I}_D$ and 0 elsewhere, so $\Delta \cdot u \le R_s \|\Delta_s\| + \sum_{j \in \mathcal{I}_D} (\Delta_j/\sqrt{m_j})(\sqrt{m_j}\, d_j) \le R_s \|\Delta_s\| + (\sum_j \Delta_j^2/m_j)^{1/2} \bar{d}_m$ by the Cauchy–Schwarz inequality and Lemma C.25. □

Lemma C.27 ([27, Lemma 4.11]). *Let $A \in \mathbb{R}^{k\times p}$, $B \in \mathbb{R}^{k\times q}$, $s' \in \mathbb{R}^p$ and $v \in \mathbb{R}^q$ with $\|s'\| \le \rho$ and $\|v\| \le \rho'$, and let $\beta > 0$. If $G \in \mathbb{R}^{k\times k}$ is symmetric and $G - (1 + \beta)\rho^2 AA^* - (1 + 1/\beta)\rho'^2 BB^*$ is positive semidefinite, then $As' + Bv = G^{1/2} w$ for some w with $\|w\| \le 1$.*

Proof. Let $x = As' + Bv$. For every $y \in \mathbb{R}^k$, $y \cdot x = (A^*y) \cdot s' + (B^*y) \cdot v \le \rho \|A^*y\| + \rho' \|B^*y\| \le \big((1 + \beta)\rho^2 \|A^*y\|^2 + (1 + 1/\beta)\rho'^2 \|B^*y\|^2\big)^{1/2} \le (y^*Gy)^{1/2}$, where the middle step is $(\xi + \zeta)^2 \le (1 + \beta)\xi^2 + (1 + 1/\beta)\zeta^2$, that is, $0 \le (\sqrt{\beta}\,\xi - \zeta/\sqrt{\beta})^2$. The matrix G is positive semidefinite, as the sum of two positive semidefinite matrices; write, by the spectral theorem [8, Section 2.5], $G = \sum_a \lambda_a \mathbf{f}_a \mathbf{f}_a^*$ with orthonormal eigenvectors $\mathbf{f}_a$ and $\lambda_a \ge 0$, and $x_a = \mathbf{f}_a \cdot x$. If $\lambda_a = 0$, then $y = \pm \mathbf{f}_a$ gives $\pm x_a \le 0$, so $x_a = 0$. With $y = \sum_{\lambda_a > 0} (x_a/\lambda_a)\mathbf{f}_a$ we get $\sum_{\lambda_a > 0} x_a^2/\lambda_a = y \cdot x \le (\sum_{\lambda_a > 0} x_a^2/\lambda_a)^{1/2}$, so this sum is at most

1, and $w = \sum_{\lambda_a>0}(x_a/\lambda_a^{1/2})\mathbf{f}_a$ satisfies $\|w\| \le 1$ and $G^{1/2}w = x$, since $G^{1/2} = \sum_a \lambda_a^{1/2}\mathbf{f}_a\mathbf{f}_a^*$ [8, Theorem 7.2.6]. □

Lemma C.28 ([27, Lemma 4.12 and (4.37)])**.** *Let $G \in \mathbb{R}^{k\times k}$ be symmetric positive semidefinite, $U \in \mathbb{R}^k$, $\gamma > \lambda_{\max}(G)$ and $\|w\| \le 1$. Then $\|U + G^{1/2}w\|^2 \le \gamma(1 + U^*(\gamma I - G)^{-1}U)$ and $\|U + G^{1/2}w\| \le \|U\| + \lambda_{\max}(G)^{1/2}$. If U lies in the convex hull of finitely many points U_σ, then $\|U + G^{1/2}w\| \le \max_\sigma \|U_\sigma + G^{1/2}w\|$, so $\|U + G^{1/2}w\|$ is at most the largest of the bounds at the U_σ. Moreover $U^*(\gamma I - G)^{-1}U \le U^*y + \|U\|\,\|U - (\gamma I - G)y\|/\mathrm{gap}$ for every $y \in \mathbb{R}^k$ and $0 < \mathrm{gap} \le \gamma - \lambda_{\max}(G)$.*

Proof. $A = \gamma I - G$ is positive definite and commutes with $G^{1/2}$ [8, Theorem 7.2.6]. Now $\|U + G^{1/2}w\|^2 = \|U\|^2 + 2w \cdot G^{1/2}U + w^*Gw$ and $w^*Gw = \gamma\|w\|^2 - w^*Aw \le \gamma - w^*Aw$. With $b = G^{1/2}U$, $2w \cdot b - w^*Aw = b^*A^{-1}b - (w - A^{-1}b)^*A(w - A^{-1}b) \le b^*A^{-1}b$, and $\|U\|^2 + U^*G^{1/2}A^{-1}G^{1/2}U = U^*(A + G)A^{-1}U = \gamma\, U^*A^{-1}U$. This gives the first bound; the second holds as $\|G^{1/2}\| = \lambda_{\max}(G)^{1/2}$. If $U = \sum_\sigma \mu_\sigma U_\sigma$ with $\mu_\sigma \ge 0$ and $\sum_\sigma \mu_\sigma = 1$, then $U + G^{1/2}w = \sum_\sigma \mu_\sigma(U_\sigma + G^{1/2}w)$. Finally $A^{-1}U = y + A^{-1}(U - Ay)$, so $U^*A^{-1}U = U^*y + U^*A^{-1}(U - Ay)$, and $\|A^{-1}\| = 1/(\gamma - \lambda_{\max}(G)) \le 1/\mathrm{gap}$. □

Lemma C.29 ([27, (4.30), (4.35)])**.** *In the setting of Lemma C.26, let $(P, T, \dots)$ be a Root certificate satisfying (A.1). Then*

(i) $\|2\pi T^*\delta - (2\pi T^*\Delta + T^*u)\| \le \chi\,(R_s^2 + \bar{d}^2)^{1/2} + 2\pi(1 + \omega)^{1/2}\|\epsilon\|$;

(ii) $\|T^*e_{\sin}\| \le \max_{j\in\mathcal{I}_D} \|T_{j,:}\|\,\bar{d}^3/6$;

(iii) if $\beta > 0$, G is symmetric and $G - (1 + \beta)R_s^2(T^*X_s)(T^*X_s)^* - (1 + 1/\beta)E_r^2T_D^*T_D$ is positive semidefinite, and $\mathcal{E} \ge \|U + G^{1/2}w\|$ for all U in the convex hull of the sixteen offsets $U_\sigma = 2\pi T^*\Delta + h\sum_{l=1}^4 \sigma_l T^*X_{\theta,l}$ ($\sigma \in \{\pm1\}^4$) and all $\|w\| \le 1$, then

$$\|T^*\delta\| \le \frac{\mathcal{E} + \max_{j\in\mathcal{I}_D} \|T_{j,:}\|\,\bar{d}^3/6 + \chi\,(R_s^2 + \bar{d}^2)^{1/2}}{2\pi} + (1 + \omega)^{1/2}\|\epsilon\|.$$

Proof. Here the statement differs from [27], which proves (iii) only for $\beta = 0.45$ and the matrix G of [27, (4.32)]. The programs use $\beta = \mathrm{fl}(1.45) - 1$ (Appendix A.5). (i) $2\pi\delta = 2\pi\Delta + 2\pi\Pi\epsilon + \Pi u$, so $2\pi T^*\delta - 2\pi T^*\Delta - T^*u = 2\pi T^*\Pi\epsilon - ((I - \Pi)T)^*u$, as Π is symmetric. Here $\|T\|^2 = \lambda_{\max}(T^*T) \le 1 + \omega$, $\|\Pi\epsilon\| \le \|\epsilon\|$, $\|((I - \Pi)T)^*\| \le \chi$ and $\|u\| \le (R_s^2 + \bar{d}^2)^{1/2}$. (ii) $T^*e_{\sin} = \sum_{j\in\mathcal{I}_D}(e_{\sin})_j T_{j,:}^*$, whose norm is at most $\max_{j\in\mathcal{I}_D} \|T_{j,:}\|\,\|e_{\sin}\|_1 \le \max_{j\in\mathcal{I}_D} \|T_{j,:}\|\,\bar{d}^3/6$ by Lemma A.1. (iii) By Lemma A.1, $T^*u = T^*X_s s + T^*X_\theta\theta + T_D^*e_D + T^*e_{\sin}$, where in $T_D^*e_D$ the vector e_D, which vanishes off $\mathcal{I}_D$, is restricted to $\mathcal{I}_D$, and $\|s\| \le R_s$ and $\|e_D\| \le E_r$. By Lemma C.27, $T^*X_s s + T_D^*e_D = G^{1/2}w$ with $\|w\| \le 1$. Writing $\theta_l/h = \frac{1+\theta_l/h}{2} - \frac{1-\theta_l/h}{2}$ with both weights in $[0, 1]$ and expanding the product of the four such sums shows that $2\pi T^*\Delta + T^*X_\theta\theta$ is a convex combination of the U_σ. Hence $\|2\pi T^*\Delta + T^*u\| \le \mathcal{E} + \|T^*e_{\sin}\|$, and (i) and (ii) give the bound. □

Lemma C.30 ([27, Proposition 4.13])**.** *In the setting of Lemma C.26, let the Root certificate at P be certified. If $s_0 \ge \|\delta\|$ and $t_0 \ge \|T^*\delta\|$ for every feasible completion associated with the cell, then $(n_P(s_0)^2 + (1 + \omega)t_0^2)^{1/2} \ge \|\delta\|$ for every such completion.*

Proof. By Lemma C.26, δ is horizontal with $F(P + \delta) = 0$. By (A.3) and (A.2), $\|\delta\|^2 \le (1 + \omega)\|T^*\delta\|^2 + n_P(\|\delta\|)^2 \le (1 + \omega)t_0^2 + n_P(s_0)^2$, since n_P has nonnegative coefficients and so is nondecreasing on $[0, \infty)$. □

Lemma C.31 ([27, Lemma 4.15])**.** *Let (P,r) and (Q,r') be records, let g be a map of Lemma C.24 and Z an integer matrix, and let $\ell \geq \|\Pi(D_0(gP) - D_0(Q) - Z)\|$. Then every member of $\mathcal{S}(P,r)$ is equivalent to a member of $\mathcal{S}(Q, r+\ell)$.*

Proof. Let $e(P+\delta) \in \mathcal{S}(P,r)$ and $d = \Pi(D_0(gP) - D_0(Q) - Z)$. By Lemma C.24, $e(gP+g\delta)$ is equivalent to $e(P+\delta)$, and $g\delta$ is horizontal with $\|g\delta\| \leq r$. By Lemma C.3(ii), $(Q+d+g\delta) - (gP+g\delta) = -Z - (I-\Pi)(gP-Q-Z) \in \mathbb{Z}^{6\times 6} + \ker\Pi$, so by Lemma C.3(iii), (iv) $e(Q+d+g\delta)$ is equivalent to $e(gP+g\delta)$ and $F(Q+d+g\delta) = 0$. As $d+g\delta$ is horizontal of norm at most $\ell + r$, $e(Q+d+g\delta) \in \mathcal{S}(Q, r+\ell)$. □

C.9. **Stage B: relations between records.** In this subsection we use the setting and notation of Appendix A.6: a parent record (P,R) whose Root certificate has the tangent matrix T and the constants $n_{0,P}, \iota_P, C_P, \omega_P, \kappa_P, \varphi_P$, $A = I - TT^*$, a second certified Root certificate $(Q, T_Q, \dots)$ with constants indexed by Q, an integer matrix Z, d_q, η_q, n_q, and, for horizontal δ with $\|\delta\| \leq R$ and $F(P+\delta) = 0$, η, h', d, ξ and ν; when we write $e(P+\delta) \in \mathcal{S}(P,R)$ we mean such a δ.

Lemma C.32 ([27, Lemma 5.1])**.** *$\|T\| \leq (1+\omega_P)^{1/2}$, $\|A\| \leq 1+\omega_P$, and $\|x\|^2 \leq (1+\omega_P)\|T^*x\|^2 + \|Ax\|^2$ for every $x \in \mathbb{R}^{36}$.*

Proof. $\|T\|^2 = \lambda_{\max}(T^*T) \leq 1+\omega_P$. The eigenvalues of the positive semidefinite matrix TT^* lie in $[0, \|T\|^2]$, so those of A lie in $[-\omega_P, 1]$ and, by the spectral theorem [8, Section 2.5], $\|A\| \leq \max(1, \omega_P) \leq 1+\omega_P$. With $\zeta = T^*x$, $\|Ax\|^2 = \|x\|^2 - 2\|\zeta\|^2 + \zeta^*T^*T\zeta \geq \|x\|^2 - (1+\omega_P)\|\zeta\|^2$, since $\zeta^*T^*T\zeta \geq (1-\omega_P)\|\zeta\|^2$. □

Lemma C.33 ([27, Proposition 5.2])**.** *Let $e(P+\delta) \in \mathcal{S}(P,R)$. Then h' is horizontal, $F(Q+h') = 0$, $e(Q+h')$ is equivalent to $e(P+\delta)$, and $\|F(P+d_q)\| = \|F(Q)\|$. Suppose that $t \geq \|\xi\|$, $\hat{d} \geq R + \|d_q\|$, $v_0 \geq n_P(R) + n_q$, $\lambda \geq \iota_P + C_P\hat{d}$, $e_0 \geq \kappa_P\varphi_Q$, $\sigma \geq \|(\Pi T_Q)^*A\|$ and $\beta \geq (1+\omega_P)((1+\omega_P)(1+\omega_Q))^{1/2}$. Then*

$$d \leq \hat{d}, \qquad d^2 \leq (1+\omega_P)t^2 + \|\nu\|^2, \qquad \|\nu\| \leq \min\{v_0, (1+\omega_P)d, \lambda d + e_0\},$$
$$\|T_Q^*h'\| \leq \beta t + \sigma\|\nu\|, \qquad d^2 \leq (1+\omega_Q)\|T_Q^*h'\|^2 + n_Q(d)^2.$$

Proof. Here the statement allows any β at least the value that [27] takes. By Lemma C.3(ii), $d_q = \Pi(Q-P-Z)$, so $(Q+h') - (P+\delta) = Q - P - d_q = Z + (I-\Pi)(Q-P-Z)$ and $(P+d_q) - Q = -Z - (I-\Pi)(Q-P-Z)$ lie in $\mathbb{Z}^{6\times 6} + \ker\Pi$. By Lemma C.3(iii), (iv), $e(Q+h')$ is obtained from $e(P+\delta)$ by rephasing rows and columns, so it is complex Hadamard and $F(Q+h') = 0$, and $\|F(P+d_q)\| = \|F(Q)\| \leq \varphi_Q$. Both δ and d_q are horizontal, hence so is h'.

$d \leq \|\delta\| + \|d_q\| \leq \hat{d}$. Lemma C.32 with $x = h'$ gives $d^2 \leq (1+\omega_P)\|\xi\|^2 + \|\nu\|^2$, as $T^*h' = \xi$. Next, $\|\nu\| \leq \|A\delta\| + \|Ad_q\| \leq n_P(\|\delta\|) + n_q \leq n_P(R) + n_q \leq v_0$ by (A.2) at the parent, as the constants of n_P are nonnegative, and $\|\nu\| \leq \|A\|d \leq (1+\omega_P)d$. By (A.4) at the parent with $v = d_q$, $\|\nu\| \leq (\iota_P + C_P(\|\delta\| + \|d_q\|))d + \kappa_P\|F(P+d_q)\| \leq \lambda d + e_0$. For the fourth inequality, h' is horizontal, so $T_Q^*h' = (\Pi T_Q)^*h'$. With $h' = T\xi + \nu$, $T^*\nu = T^*h' - T^*TT^*h' = (I - T^*T)\xi$ and $\nu = A\nu + TT^*\nu$ we get $h' = T(2I - T^*T)\xi + A\nu$, so $T_Q^*h' = (\Pi T_Q)^*T(2I - T^*T)\xi + (\Pi T_Q)^*A\nu$. The eigenvalues of T^*T lie in $[\max(0, 1-\omega_P), 1+\omega_P]$, so $\|2I - T^*T\| \leq 1+\omega_P$. With $\|\Pi T_Q\| \leq \|T_Q\| \leq (1+\omega_Q)^{1/2}$ (Lemma C.32 for the second Root certificate) and $\|T\| \leq (1+\omega_P)^{1/2}$, the first term has norm at most βt, and the second at most $\sigma\|\nu\|$. Finally, the Root certificate at Q is certified, h' is horizontal and $F(Q+h') = 0$, so (A.2) and (A.3) at Q give the last inequality. □

Lemma C.34 ([27, Lemma 5.3])**.** *In the setting of Lemma C.33, for $t \geq 0$ put*

$$z_t = (1+\omega_P)^{1/2}t, \qquad v(b) = \min\{v_0, (1+\omega_P)b, \lambda b + e_0\}, \qquad \psi_P(b) = (z_t^2 + v(b)^2)^{1/2},$$
$$\psi_Q(b) = \left((1+\omega_Q)(\beta t + \sigma v(b))^2 + n_Q(b)^2\right)^{1/2},$$

let $b_0 \geq \min\{\hat{d}, (z_t^2+v_0^2)^{1/2}\}$ and $b_{j+1} \geq \min\{b_j, \psi_P(b_j), \psi_Q(b_j)\}$ for $j \geq 0$. Then $d \leq b_j$ for every j and every $e(P+\delta) \in \mathcal{S}(P,R)$ with $\|\xi\| \leq t$.

Proof. By Lemma C.33, $d \leq \hat{d}$ and $d^2 \leq z_t^2 + \|\nu\|^2 \leq z_t^2 + v_0^2$, so $d \leq b_0$. If $d \leq b_j$, then $\|\nu\| \leq v(d) \leq v(b_j)$, since v is nondecreasing, so $d \leq \psi_P(b_j)$; and $\|T_Q^* h'\| \leq \beta t + \sigma v(b_j)$ and $n_Q(d) \leq n_Q(b_j)$ give $d \leq \psi_Q(b_j)$. Hence $d \leq b_{j+1}$. □

The iteration of Appendix A.6 is the case of equality, evaluated with upper bounds and stopped after finitely many steps, which this lemma allows.

Lemma C.35 ([27, (5.20), (5.22)–(5.24)])**.** *Every $e(P+\delta) \in \mathcal{S}(P,R)$ has $\|T^*\delta\| \leq (1+\omega_P)^{1/2}R$. For $u, \eta_q \in \mathbb{R}^k$ and $h \geq 0$, the box $B(u,h) = \prod_{i=1}^k [u_i - h, u_i + h]$ satisfies $\operatorname{dist}(0, B(u,h))^2 = \sum_i \max(0, |u_i| - h)^2$ and $\max_{\eta \in B(u,h)} \|\eta - \eta_q\|^2 = \sum_i (|u_i - \eta_{q,i}| + h)^2$, and it is the union of the 2^k boxes $B(u + \epsilon h/2, h/2)$, $\epsilon \in \{-1,1\}^k$.*

Proof. The first assertion follows from $\|T^*\delta\| \leq \|T\|\,\|\delta\|$ and Lemma C.32. The squared distance and the squared norm are sums over the coordinates, which vary independently over the intervals $[u_i - h, u_i + h]$; on such an interval the smallest value of $|\eta_i|$ is $\max(0, |u_i| - h)$ and the largest value of $|\eta_i - \eta_{q,i}|$ is $|u_i - \eta_{q,i}| + h$. Finally $[u_i - h, u_i + h] = [u_i - h, u_i] \cup [u_i, u_i + h]$, and a product of unions is the union of the products. □

C.10. **Stage C.** In this subsection we use the setting and notation of Appendix A.7: a record (P, r) whose Root certificate $(P, T, n_0, \iota, C, \omega, \chi, \kappa, \varphi)$ satisfies (A.1) and (A.2) (the lemmas of this subsection use nothing else), r_H, n and K, a center $u \in \mathbb{R}^6$ with the numbers $q_{ji}, S_i, c_i, J_{ij}, B_{il}$, and, for $x \in \mathbb{R}^6$ and real δ, $S_i' = \sum_j q_{ji} e(x_j - \delta_{ji})$.

Lemma C.36 ([27, (6.2), (6.3)])**.**

(i) Every horizontal δ with $\|\delta\| \leq r$ and $F(P+\delta) = 0$ satisfies $\|\eta\| \leq r_H$ and $\|\nu\| \leq n$ for $\eta = T^*\delta$ and $\nu = \delta - T\eta$.

(ii) $\|e(P)/\sqrt{6}\| \leq K = (1 + 2\pi\sqrt{2}\,\varphi/6)^{1/2}$.

(iii) The vector $e(u+x)/\sqrt{6}$ is unbiased to column i of $e(P+\delta)/\sqrt{6}$ if and only if $|S_i'| = 1$.

(iv) The linear map Q of $\mathbb{C}^6$ with $(Qw)_i = \sum_j q_{ji} w_j$ is $e(P)^* \operatorname{diag}(e(u))/\sqrt{6}$, and $\|Q\| = \|e(P)/\sqrt{6}\| \leq K$.

Proof. Here the statement differs from [27], which assumes $r \leq 0.03$, $\varphi < 10^{-6}$, $\omega < 10^{-5}$, $n_0 < 10^{-6}$, $\iota < 10^{-4}$ and $C < 20$ [27, Section 6.1], and takes $K = 1.00001$. (i) $\|\eta\| \leq \|T\|\,\|\delta\| \leq (1+\omega)^{1/2} r$ by Lemma C.32, whose proof uses only $\|T^*T - I\| \leq \omega$. Also $\nu = (I - TT^*)\delta$, so $\|\nu\| \leq n_0 + \iota\|\delta\| + C\|\delta\|^2 \leq n$ by (A.2). (ii) For a unit vector w, $\|e(P)^* w\|^2 = 6 + w^*(e(P)e(P)^* - 6I)w \leq 6 + \|e(P)e(P)^* - 6I\|_F = 6 + 2\pi\sqrt{2}\,\|F(P)\| \leq 6K^2$ by Lemma C.3(iv) and Lemma C.2(i). (iii) The inner product of column i of $e(P+\delta)/\sqrt{6}$ with $e(u+x)/\sqrt{6}$ is $\frac{1}{6}\sum_j e(u_j + x_j - P_{ji} - \delta_{ji}) = S_i'/\sqrt{6}$, and unbiasedness means that its modulus is $1/\sqrt{6}$. (iv) $q_{ji} = \overline{e(P_{ji})}\, e(u_j)/\sqrt{6}$, and $\operatorname{diag}(e(u))$ is unitary. □

Lemma C.37 ([27, Lemma 6.1]). *Let $a > 0$, $d \in \mathbb{R}^6$ with $d_0 = 0$ and $|d_j| \le a$ for $j > 0$, and $x = d - \frac{1}{6}(\sum_j d_j)\mathbf{1}$. Then $\sum_j x_j = 0$, $\|x\| \le X_{M_\ell} = (29/6)^{1/2}a$, $\|x\|_1 \le L_{M_\ell} = 5a$ and $\|x\|_\infty \le I_{M_\ell} = \frac{3}{2}a$.*

Proof. Clearly $\sum_j x_j = 0$. As a function of one of $d_1, \dots, d_5$, the others being fixed, each of $\|x\|^2 = \|d\|^2 - (\sum_j d_j)^2/6$ and $\|x\|_1 = \sum_j |d_j - \frac{1}{6}\sum_k d_k|$ is convex (a quadratic with leading coefficient $5/6$, and a sum of absolute values of affine functions), so its maximum on an interval is attained at an endpoint. Moving the coordinates one at a time, each maximum over the box is attained at a vertex, where $|d_j| = a$ for $j > 0$. There $\|d\|^2 = 5a^2$ and $\sum_j d_j$ is an odd multiple of a, so $\|x\|^2 \le 5a^2 - a^2/6$. If p coordinates equal a and $5-p$ equal $-a$, the mean is $\mu = (2p-5)a/6$ and $\|x\|_1 = |\mu| + p|a-\mu| + (5-p)|a+\mu|$, which is $10a/6$, $4a$, $5a$, $5a$, $4a$, $10a/6$ for $p = 0, \dots, 5$. Finally, for $j > 0$, $x_j = \frac{5}{6}d_j - \frac{1}{6}\sum_{k\neq 0,j} d_k$, so $|x_j| \le \frac{5}{6}a + \frac{4}{6}a$, and $|x_0| = \frac{1}{6}|\sum_k d_k| \le \frac{5}{6}a$. □

Lemma C.38 ([27, Section 6.3]). *Every vector unbiased to the standard basis is $\lambda e(\beta)/\sqrt{6}$ with $|\lambda| = 1$, $\beta_0 = 0$ and $\beta_1, \dots, \beta_5 \in [0,1)$. For an integer $M_\ell \ge 1$ the integers $b_j = \lfloor M_\ell \beta_j \rfloor$ satisfy $0 \le b_j \le M_\ell - 1$ and $\beta_j \in [b_j/M_\ell, (b_j+1)/M_\ell]$, and $\lfloor 2M_\ell\beta_j \rfloor \in \{2b_j, 2b_j+1\}$.*

Proof. Here the statement and the proof differ from [27], which lifts the phases to $[0,1]$ and uses that the closed intervals of the two children of a bin cover it. A unit vector f unbiased to the standard basis has $|f_j| = 1/\sqrt{6}$, so $f_j = e(\varphi_j)/\sqrt{6}$; take $\lambda = e(\varphi_0)$ and $\beta_j \in [0,1)$ congruent to $\varphi_j - \varphi_0$. Then $M_\ell\beta_j \in [b_j, b_j+1)$, so $2M_\ell\beta_j \in [2b_j, 2b_j+2)$. □

Lemma C.39 ([27, Lemma 6.2]). *If $\|x\| \le X$, $\|x\|_1 \le L$ and $\|\delta\| \le r$, then $\|S' - S\| \le 2\pi(KX + r)$ and $|S'_i - S_i| \le 2\pi(L/\sqrt{6} + r)$. Hence, with $\vartheta = 2\pi(L/\sqrt{6} + r)$, if $e(u+x)/\sqrt{6}$ is unbiased to the columns of $e(P+\delta)/\sqrt{6}$, then $\max\{0, 1-\vartheta\}^2 \le |S_i|^2 \le (1+\vartheta)^2$ for $0 \le i \le 5$ and $\sum_i (|S_i| - 1)^2 \le (2\pi(KX + r))^2$.*

Proof. $S'_i - S_i = \sum_j q_{ji}(e(x_j) - 1) + \sum_j q_{ji} e(x_j)(e(-\delta_{ji}) - 1)$. The first sum is $(Q(e(x) - \mathbf{1}))_i$, and $\|e(x) - \mathbf{1}\| \le 2\pi\|x\|$ by Lemma C.1(i), so by Lemma C.36(iv) these sums form a vector of norm at most $2\pi KX$; each of them has modulus at most $\frac{1}{\sqrt{6}}\sum_j 2\pi|x_j| \le 2\pi L/\sqrt{6}$. The second sum has modulus at most $\frac{2\pi}{\sqrt{6}}\sum_j |\delta_{ji}| \le 2\pi\|\delta_{:,i}\|$, and these numbers form a vector of norm at most $2\pi\|\delta\| \le 2\pi r$. If the vector is unbiased, $|S'_i| = 1$ (Lemma C.36(iii)) and $||S_i| - 1| \le |S_i - S'_i|$, which gives the two tests. □

Lemma C.40 ([27, Lemma 6.3 and (6.11)]). *Let δ be horizontal with $\|\delta\| \le r$ and $F(P+\delta) = 0$, $\eta = T^*\delta$, and let $x \in \mathbb{R}^6$ with $\|x\| \le X$ be such that $e(u+x)/\sqrt{6}$ is unbiased to every column of $e(P+\delta)/\sqrt{6}$. With G_y, N_y and $S \circ y$ as in Appendix A.7, for every $y \in \mathbb{R}^6$,*

$$|y \cdot (c + Jx - B\eta)| \le nN_y + \pi\Big[\|y\|_\infty (KX + r)^2 + G_y X^2 + \frac{2}{\sqrt{6}}\|S \circ y\| X r + \frac{1}{\sqrt{6}}\|S \circ y\|_\infty r^2\Big],$$

and if moreover $\|x\|_\infty \le I$, the same holds with $G_y X^2$ replaced by $\min\{G_y X^2, K\|S \circ y\| I X\}$, that is, $|y \cdot (c + Jx - B\eta)| \le \mathcal{E}(y; X, I)$. For a bin with midpoint u, and x as in Lemma C.37, this gives $|y \cdot c| \le a\sum_{j>0} |(J^*y)_j| + r_H\|B^*y\| + \mathcal{E}(y; X_{M_\ell}, I_{M_\ell})$.

Proof. Put $\Delta_i = S'_i - S_i$, $w_j = x_j - \delta_{ji}$ (for the fixed i) and $R(t) = e(t) - 1 - 2\pi i t$. Then $\Delta_i = 2\pi i \sum_j q_{ji} w_j + \sum_j q_{ji} R(w_j)$, and $\operatorname{Re}(i\overline{S_i} q_{ji}) = J_{ij}$. Expanding $|S'_i|^2 = |S_i|^2 + 2\operatorname{Re}(\overline{S_i}\Delta_i) + |\Delta_i|^2$ and dividing by 4π, unbiasedness gives

$$0 = c_i + \sum_j J_{ij} x_j - \sum_j J_{ij}\delta_{ji} + \frac{1}{2\pi}\operatorname{Re}\Big(\overline{S_i}\sum_j q_{ji} R(w_j)\Big) + \frac{|\Delta_i|^2}{4\pi}.$$

Write $\delta = T\eta + \nu$; then $\sum_j J_{ij}\delta_{ji} = (B\eta)_i + \sum_j J_{ij}\nu_{ji}$. Multiplying by y_i and summing over i,

$$y \cdot (c + Jx - B\eta) = \sum_{i,j} y_i J_{ij}\nu_{ji} - \frac{1}{2\pi}\sum_i y_i \operatorname{Re}\Big(\overline{S_i}\sum_j q_{ji}R(w_j)\Big) - \sum_i y_i \frac{|\Delta_i|^2}{4\pi}.$$

The first sum (the normal part) is at most $N_y\|\nu\| \le nN_y$ by the Cauchy–Schwarz inequality and Lemma C.36(i). The last is at most $\|y\|_\infty \|S' - S\|^2/(4\pi) \le \pi\|y\|_\infty (KX + r)^2$ by Lemma C.39, applied with $L = \|x\|_1$. For the remainder use $R(x_j - \delta_{ji}) = R(x_j) + R(-\delta_{ji}) + (e(x_j) - 1)(e(-\delta_{ji}) - 1)$ and $|R(t)| \le 2\pi^2 t^2$, $|e(t) - 1| \le 2\pi|t|$ (Lemma C.1(i)), and $|q_{ji}| = 1/\sqrt{6}$. The pure-x part equals $\frac{1}{2\pi}\operatorname{Re}\sum_j(\sum_i y_i\overline{S_i}q_{ji})R(x_j)$, of modulus at most $\frac{1}{2\pi}G_y\sum_j 2\pi^2 x_j^2 \le \pi G_y X^2$; it also equals $\frac{1}{2\pi}\operatorname{Re}\sum_i y_i\overline{S_i}(Q(R(x_j))_j)_i$, of modulus at most $\frac{1}{2\pi}\|S \circ y\|\, K\, 2\pi^2(\sum_j x_j^4)^{1/2} \le \pi K\|S \circ y\| IX$ when $\|x\|_\infty \le I$, as $\sum_j x_j^4 \le \|x\|_\infty^2\|x\|^2$. The pure-$\delta$ part is at most $\frac{1}{2\pi}\sum_i |y_i S_i|\frac{2\pi^2}{\sqrt{6}}\|\delta_{:,i}\|^2 \le \frac{\pi}{\sqrt{6}}\|S \circ y\|_\infty r^2$, and the product part at most $\frac{1}{2\pi}\sum_i |y_i S_i|\frac{4\pi^2}{\sqrt{6}}\sum_j |x_j\delta_{ji}| \le \frac{2\pi}{\sqrt{6}}X\sum_i |y_i S_i|\,\|\delta_{:,i}\| \le \frac{2\pi}{\sqrt{6}}\|S \circ y\| Xr$. This proves the two bounds.

For a bin, the rows of J sum to $-\operatorname{Im}(\overline{S_i}S_i) = 0$, so $y \cdot Jx = (J^*y) \cdot d = \sum_{j>0}(J^*y)_j d_j$, of modulus at most $a\sum_{j>0}|(J^*y)_j|$; and $|y \cdot B\eta| \le \|B^*y\|\,\|\eta\| \le r_H\|B^*y\|$ by Lemma C.36(i). By Lemma C.37, $\|x\| \le X_{M_\ell}$ and $\|x\|_\infty \le I_{M_\ell}$. □

Lemma C.41 ([27, Lemma 6.4])**.** *Let $\mathcal{B}_{\mathrm{vec}}(v, s)$ be as in Appendix A.7. If a bin with midpoint u and half side a is assigned a center v and an integer vector m, and $s \ge \|h\| + X_{M_\ell}$ for $h = u - v - m - \frac{1}{6}\sum_j(u_j - v_j - m_j)\mathbf{1}$, then $\mathcal{B}_{\mathrm{vec}}(v, s)$ contains every vector $\lambda e(\beta)/\sqrt{6}$ with $|\lambda| = 1$ and β in the bin.*

Proof. Write $\beta = u + d$ with $d_0 = 0$ and $|d_j| \le a$, let $x = d - \frac{1}{6}(\sum_j d_j)\mathbf{1}$ and $\mu = \frac{1}{6}\sum_j(u_j + d_j - v_j - m_j)$. Then $u + d = v + m + (h + x) + \mu\mathbf{1}$, so $\lambda e(\beta)/\sqrt{6} = \lambda e(\mu)\, e(v + h + x)/\sqrt{6}$, where $h + x$ has coordinate sum 0 and norm at most $\|h\| + X_{M_\ell} \le s$ by Lemma C.37. □

Lemma C.42 ([27, Lemma 6.5])**.** *Two vectors in one ball $\mathcal{B}_{\mathrm{vec}}(v, s)$ with $s < 0.1$ are neither orthogonal nor unbiased.*

Proof. Write them as $\lambda e(v + x)/\sqrt{6}$ and $\lambda' e(v + x')/\sqrt{6}$. Their inner product has modulus $|\sum_j e(z_j)|/6$ with $z = x' - x$, $\|z\| \le 2s < 0.2$. By Lemma C.1(i), $|\sum_j e(z_j)| \ge 6 - \sum_j |e(z_j) - 1| \ge 6 - 2\pi\|z\|_1 \ge 6 - 2\pi\sqrt{6}\,\|z\| > 6 - 0.4\pi\sqrt{6} > 6 - 0.4 \cdot \frac{22}{7} \cdot \frac{5}{2} = \frac{20}{7} > \sqrt{6}$, using $\pi < 22/7$, $\sqrt{6} < 5/2$ and $(20/7)^2 > 6$. Orthogonality requires $\sum_j e(z_j) = 0$ and unbiasedness $|\sum_j e(z_j)| = \sqrt{6}$. □

Lemma C.43 ([27, Lemma 6.6])**.** *Let two balls have centers u, v and radii s_u, s_v, and let $Q_j, S_e, r_e, D_{\mathcal{O}}, D_{\mathcal{U}}, q_{\mathcal{U}}, E_{\mathcal{O}}, E_{\mathcal{U}}$ be as in Appendix A.7 and $q_{\mathcal{O}} = (\operatorname{Re} S_e, \operatorname{Im} S_e)^{\mathsf{T}}/(2\pi)$. Let $\lambda e(u + x)/\sqrt{6}$ and $\lambda' e(v + x')/\sqrt{6}$ be vectors of the two balls (so $\sum_j x_j = \sum_j x'_j = 0$, $\|x\| \le s_u$, $\|x'\| \le s_v$), and $z = x - x'$. If they are orthogonal, then $\|q_{\mathcal{O}} + D_{\mathcal{O}}z\| \le E_{\mathcal{O}}$ and $|S_e|^2/(2\pi) \le 6r_e\|D_{\mathcal{U}}\| + E_{\mathcal{O}}|S_e|$; if they are unbiased, then $|q_{\mathcal{U}} + D_{\mathcal{U}}z| \le E_{\mathcal{U}}$ and $|q_{\mathcal{U}}| \le r_e\|D_{\mathcal{U}}\| + E_{\mathcal{U}}$. (The first inequalities of the two displays of the edge tests in Appendix A.7, [27, (6.16)], are proved in Appendix A.7 itself.)*

Proof. The inner product has modulus $|S'_e|/6$ with $S'_e = \sum_j Q_j e(z_j)$, and $\|z\| \le r_e$. Put $R = S'_e - S_e - 2\pi i\sum_j Q_j z_j = \sum_j Q_j(e(z_j) - 1 - 2\pi i z_j)$; then $|R| \le 2\pi^2\|z\|^2 \le 2\pi^2 r_e^2$ by Lemma C.1(i). In $\mathbb{R}^2$ the number $iQ_j z_j$ is $(D_{\mathcal{O}})_{:,j}z_j$. If $S'_e = 0$, dividing $0 = S_e + 2\pi i\sum_j Q_j z_j + R$ by 2π gives $q_{\mathcal{O}} + D_{\mathcal{O}}z = -R/(2\pi)$, of norm at most πr_e^2. The inner product with

$(\operatorname{Re} S_e, \operatorname{Im} S_e)$ maps $q_{\mathcal{O}}$ to $|S_e|^2/(2\pi)$ and $D_{\mathcal{O}}z$ to $6D_{\mathcal{U}}z$, so $|S_e|^2/(2\pi) \le 6|D_{\mathcal{U}}z| + |S_e|\pi r_e^2 \le 6r_e\|D_{\mathcal{U}}\| + E_{\mathcal{O}}|S_e|$. If $|S_e'|^2 = 6$, then $0 = \frac{|S_e'|^2/6-1}{4\pi} = q_{\mathcal{U}} + \frac{\operatorname{Re}(\overline{S_e}(S_e'-S_e))}{12\pi} + \frac{|S_e'-S_e|^2}{24\pi}$, and $\operatorname{Re}(\overline{S_e}\cdot 2\pi i\sum_j Q_j z_j)/(12\pi) = D_{\mathcal{U}}z$, since $-\operatorname{Im}(\overline{S_e}Q_j) = -\operatorname{Re} S_e \operatorname{Im} Q_j + \operatorname{Im} S_e \operatorname{Re} Q_j$. The remaining terms are at most $|S_e||R|/(12\pi) \le \pi|S_e|r_e^2/6$ and, as $|S_e'-S_e| \le 2\pi\|z\|_1 \le 2\pi\sqrt{6}\,r_e$, at most πr_e^2. So $|q_{\mathcal{U}} + D_{\mathcal{U}}z| \le E_{\mathcal{U}}$, and $|D_{\mathcal{U}}z| \le r_e\|D_{\mathcal{U}}\|$. □

Lemma C.44 ([27, Lemma 6.7])**.** *Let the balls $t = 0, 1$ have centers v_t and radii s_t; form c^t, J^t, B^t, S^t, q^t with $u = v_t$; and let $\mathcal{E}_t^{\mathrm{ball}}$, q_E, D_E, E_E and ℓ_E be as in Appendix A.7 and Lemma C.43, with $Q_j = e(v_{0,j} - v_{1,j})$. If one vector of each ball is unbiased to the standard basis and to the columns of the same $e(P+\delta)/\sqrt{6}$, with δ horizontal, $\|\delta\| \le r$ and $F(P+\delta) = 0$, and the two vectors are orthogonal ($E = \mathcal{O}$) or unbiased ($E = \mathcal{U}$), then for all $y_0, y_1 \in \mathbb{R}^6$ and $y_e \in \mathbb{R}^{\ell_E}$*

$$|y_0\cdot c^0 + y_1\cdot c^1 + y_e\cdot q_E| \le \sum_{t=0}^{1}\Big[s_t\|(J^t)^*y_t + (-1)^t D_E^* y_e\| + \mathcal{E}_t^{\mathrm{ball}}(y_t)\Big] + r_H\|(B^0)^*y_0 + (B^1)^*y_1\| + E_E\|y_e\|.$$

Proof. Write the two vectors as $\lambda_t e(v_t + x_t)/\sqrt{6}$ with $\sum_j x_{t,j} = 0$ and $\|x_t\| \le s_t$, and let $\eta = T^*\delta$. By the first bound of Lemma C.40 with $u = v_t$, $x = x_t$ and $X = s_t$, $|y_t\cdot(c^t + J^t x_t - B^t\eta)| \le \mathcal{E}_t^{\mathrm{ball}}(y_t)$, and by Lemma C.43 with $z = x_0 - x_1$, $|y_e\cdot(q_E + D_E(x_0 - x_1))| \le E_E\|y_e\|$. Adding the three quantities inside the absolute values gives $y_0\cdot c^0 + y_1\cdot c^1 + y_e\cdot q_E + ((J^0)^*y_0 + D_E^*y_e)\cdot x_0 + ((J^1)^*y_1 - D_E^*y_e)\cdot x_1 - ((B^0)^*y_0 + (B^1)^*y_1)\cdot\eta$, and $\|x_t\| \le s_t$, $\|\eta\| \le r_H$ (Lemma C.36(i)). □

Declarations

Use of AI. This paper was produced by a multi-agent AI research system that the author built and ran, using Anthropic Claude Opus 5.5: apart from the work of others that it cites, the ideas, proofs, computations and text are due to the system. Its results were checked by separate agents, and the computations that its proofs use by second programs (Section 5 and [13]). The author takes full responsibility for the paper, including its correctness and the integrity and accuracy of its citations.

Data availability. The programs and data used in this paper, with instructions for rerunning them, are deposited at Zenodo [13].

References

1. Somshubhro Bandyopadhyay, P. Oscar Boykin, Vwani Roychowdhury, and Farrokh Vatan, *A new proof for the existence of mutually unbiased bases*, Algorithmica **34** (2002), no. 4, 512–528, doi:10.1007/s00453-002-0980-7.
2. Ingemar Bengtsson, Wojciech Bruzda, Åsa Ericsson, Jan-Åke Larsson, Wojciech Tadej, and Karol Życzkowski, *Mutually unbiased bases and Hadamard matrices of order six*, J. Math. Phys. **48** (2007), no. 5, 052106, doi:10.1063/1.2716990.
3. Stephen Brierley and Stefan Weigert, *Maximal sets of mutually unbiased quantum states in dimension 6*, Phys. Rev. A **78** (2008), no. 4, 042312, doi:10.1103/PhysRevA.78.042312.
4. ———, *Constructing mutually unbiased bases in dimension six*, Phys. Rev. A **79** (2009), no. 5, 052316, doi:10.1103/PhysRevA.79.052316, cited by the numbering of arXiv:0901.4051v2.
5. Paul Butterley and William Hall, *Numerical evidence for the maximum number of mutually unbiased bases in dimension six*, Phys. Lett. A **369** (2007), no. 1–2, 5–8, doi:10.1016/j.physleta.2007.04.059.
6. Mateo Cárdenes Wuttig and Joseph Tindall, *A complete classification of complex Hadamard matrices of order six*, Preprint, arXiv:2608.18053v2, August 28, 2026.

7. Markus Grassl, *On SIC-POVMs and MUBs in dimension 6*, Proceedings of the ERATO Conference on Quantum Information Science (EQIS 2004) (Jozef Gruska, ed.), 2004, arXiv:quant-ph/0406175v2.
8. Roger A. Horn and Charles R. Johnson, *Matrix analysis*, second ed., Cambridge University Press, Cambridge, 2013.
9. IEEE, *IEEE standard for floating-point arithmetic*, IEEE Std 754-2019, 2019, doi:10.1109/IEEESTD.2019.8766229.
10. I. D. Ivanović, *Geometrical description of quantal state determination*, J. Phys. A **14** (1981), no. 12, 3241–3245, doi:10.1088/0305-4470/14/12/019.
11. Philippe Jaming, Máté Matolcsi, and Péter Móra, *The problem of mutually unbiased bases in dimension 6*, Cryptogr. Commun. **2** (2010), no. 2, 211–220, doi:10.1007/s12095-010-0023-1, cited by the numbering of arXiv:1201.0640v1.
12. Philippe Jaming, Máté Matolcsi, Péter Móra, Ferenc Szöllősi, and Mihály Weiner, *A generalized Pauli problem and an infinite family of MUB-triplets in dimension 6*, J. Phys. A **42** (2009), no. 24, 245305, doi:10.1088/1751-8113/42/24/245305, cited by the numbering of arXiv:0902.0882v2.
13. Manvir Jaswal, *Programs and data for "An independent certified computation excluding four mutually unbiased bases in dimension six"*, 2026, Zenodo, doi:10.5281/zenodo.23255816.
14. Fredrik Johansson, *Arb: efficient arbitrary-precision midpoint-radius interval arithmetic*, IEEE Trans. Comput. **66** (2017), no. 8, 1281–1292, doi:10.1109/TC.2017.2690633.
15. Bengt R. Karlsson, *H_2-reducible complex Hadamard matrices of order 6*, Linear Algebra Appl. **434** (2011), no. 1, 239–246, doi:10.1016/j.laa.2010.08.021.
16. ———, *Three-parameter complex Hadamard matrices of order 6*, Linear Algebra Appl. **434** (2011), no. 1, 247–258, doi:10.1016/j.laa.2010.08.020.
17. Andreas Klappenecker and Martin Rötteler, *Constructions of mutually unbiased bases*, Finite Fields and Applications, Lecture Notes in Comput. Sci., vol. 2948, Springer, Berlin, 2004, pp. 137–144, doi:10.1007/978-3-540-24633-6_10, cited by the numbering of arXiv:quant-ph/0309120v1.
18. O. Krüger and R. F. Werner (eds.), *Some open problems in quantum information theory*, 2005, arXiv:quant-ph/0504166, Problem 13, *Mutually unbiased bases*, of the Open Quantum Problems list, https://oqp.iqoqi.oeaw.ac.at/mutually-unbiased-bases, cited from the copy archived on December 2, 2024, https://web.archive.org/web/20241202140556/https://oqp.iqoqi.oeaw.ac.at/mutually-unbiased-bases.
19. Máté Matolcsi, Ákos K. Matszangosz, Dániel Varga, and Mihály Weiner, *Triplets of mutually unbiased bases*, J. Algebraic Combin. **63** (2026), no. 2, Paper No. 26, doi:10.1007/s10801-026-01506-x.
20. Daniel McNulty and Stefan Weigert, *All mutually unbiased product bases in dimension 6*, J. Phys. A **45** (2012), no. 13, 135307, doi:10.1088/1751-8113/45/13/135307.
21. ———, *The limited role of mutually unbiased product bases in dimension 6*, J. Phys. A **45** (2012), no. 10, 102001, doi:10.1088/1751-8113/45/10/102001.
22. ———, *On the impossibility to extend triples of mutually unbiased product bases in dimension six*, Int. J. Quantum Inf. **10** (2012), no. 5, 1250056, doi:10.1142/S0219749912500566.
23. ———, *Mutually unbiased bases in composite dimensions—a review*, Quantum **10** (2026), 2051, doi:10.22331/q-2026-04-01-2051.
24. OpenAI, *Exact Fourier certificates for complex Hadamard matrices of order six*, 2026, Preprint dated September 24, 2026, not refereed; in `openai/math` on GitHub, commit `adc7f124` (October 6, 2026), https://github.com/openai/math/tree/adc7f1241b42e322a6451854ab7e4b4c146bf78a.
25. ———, *Exactly three mutually unbiased bases in dimension six*, 2026, Entry 266 of the list of contents of `openai/math` on GitHub, commit `fd4aeeb2` (October 8, 2026), https://github.com/openai/math/tree/fd4aeeb2ee4fc729c18d98444fed42fd0529eeeb.
26. ———, *Exactly three mutually unbiased bases in dimension six: the Lean formalization*, 2026, Documentation of entry 266 in the Lean formalization of `openai/math` on GitHub, commit `fd4aeeb2` (October 8, 2026), https://github.com/openai/math/tree/fd4aeeb2ee4fc729c18d98444fed42fd0529eeeb.
27. ———, *The maximum number of mutually unbiased bases in dimension six*, 2026, Preprint dated September 24, 2026, not refereed; in `openai/math` on GitHub, commit `adc7f124` (October 6, 2026), the only commit to the preprint's folder as of October 20, 2026, https://github.com/openai/math/tree/adc7f1241b42e322a6451854ab7e4b4c146bf78a/preprints/The-maximum-number-of-mutually-unbiased-bases-in-dimension-six-September-24-2026.
28. Philippe Raynal, Xin Lü, and Berthold-Georg Englert, *Mutually unbiased bases in six dimensions: the four most distant bases*, Phys. Rev. A **83** (2011), no. 6, 062303, doi:10.1103/PhysRevA.83.062303.
29. Walter Rudin, *Principles of mathematical analysis*, third ed., McGraw-Hill, New York, 1976.

30. Siegfried M. Rump, *Verification methods: rigorous results using floating-point arithmetic*, Acta Numer. **19** (2010), 287–449, doi:10.1017/S096249291000005X.
31. Siegfried M. Rump, Paul Zimmermann, Sylvie Boldo, and Guillaume Melquiond, *Computing predecessor and successor in rounding to nearest*, BIT **49** (2009), no. 2, 419–431, doi:10.1007/s10543-009-0218-z.
32. Pat H. Sterbenz, *Floating-point computation*, Prentice-Hall, Englewood Cliffs, NJ, 1974.
33. Ferenc Szöllősi, *Complex Hadamard matrices of order 6: a four-parameter family*, J. London Math. Soc. (2) **85** (2012), no. 3, 616–632, doi:10.1112/jlms/jdr052.
34. Wojciech Tadej and Karol Życzkowski, *A concise guide to complex Hadamard matrices*, Open Syst. Inf. Dyn. **13** (2006), no. 2, 133–177, doi:10.1007/s11080-006-8220-2, cited by the numbering of arXiv:quant-ph/0512154v2.
35. ———, *Defect of a unitary matrix*, Linear Algebra Appl. **429** (2008), no. 2–3, 447–481, doi:10.1016/j.laa.2008.02.036, cited by the numbering of arXiv:math/0702510v2.
36. Terence Tao, *Fuglede's conjecture is false in 5 and higher dimensions*, Math. Res. Lett. **11** (2004), no. 2, 251–258, doi:10.4310/MRL.2004.v11.n2.a8.
37. Mihály Weiner, *A gap for the maximum number of mutually unbiased bases*, Proc. Amer. Math. Soc. **141** (2013), no. 6, 1963–1969, doi:10.1090/S0002-9939-2013-11487-5, cited by the numbering of arXiv:0902.0635v2.
38. William K. Wootters and Brian D. Fields, *Optimal state-determination by mutually unbiased measurements*, Ann. Physics **191** (1989), no. 2, 363–381, doi:10.1016/0003-4916(89)90322-9.
39. Gerhard Zauner, *Quantendesigns: Grundzüge einer nichtkommutativen Designtheorie*, Ph.D. thesis, Universität Wien, 1999.
40. ———, *Quantum designs: foundations of a noncommutative design theory*, Int. J. Quantum Inf. **9** (2011), no. 1, 445–507, doi:10.1142/S0219749911006776.

Toronto, Canada
Email address: manvirjaswal@icloud.com
URL: https://manvirjaswal.github.io