Undistillability of Werner states from three, four and five copies

Tejasvi Singh Tomar
ORCID 0000-0003-4668-3639

hexagon:2611.00464v1

Abstract

Whether every entangled state with a non-positive partial transpose (NPT) can be distilled is a long-standing open problem of entanglement theory. It reduces to the Werner states $\rho(d,\alpha)$, which for $d \geq 3$ and $-1/2 \leq \alpha < -1/d$ are NPT but cannot be distilled from one copy; if one of them stays undistillable from every number of copies, NPT bound entanglement exists. We prove that for every $d \geq 3$ the state $\rho(d,\alpha)$ is three-copy distillable if and only if $\alpha < -1/2$, the threshold known for one and two copies, so a third copy does not help. In every dimension we also prove four-copy undistillability for $\alpha \geq -79/160$ and five-copy undistillability for $\alpha \geq -9/20$, and improved bounds of order $1/k$ for $k \geq 6$ copies. The proofs use a criterion of Costa Rico and computer-verified certificates for quartic moment relaxations that hold for all large dimensions at once; for many copies they combine the resulting inequalities with known partial-trace inequalities. Whether $-1/2$ remains the threshold from four copies on is open.

Keywords: entanglement distillation; NPT bound entanglement; Werner states; partial transpose; moment relaxation; semidefinite programming; computer-assisted proof.

MSC 2020: 81P40 (primary); 81P45, 15A45, 90C22 (secondary).

1. Introduction

Entanglement distillation converts many copies of a mixed state into fewer, nearly pure maximally entangled pairs by local operations and classical communication. A state with a positive partial transpose cannot be distilled [HHH98]. Whether the converse holds, that is, whether all states with a non-positive partial transpose (NPT) are distillable, has been open since the late 1990s [DSS+00, DCLB00]; Problem 5 in the list of Horodecki, Rudnicki and Życzkowski [HRZ22] asks whether the state $\rho(4,-1/2)$ defined below is two-copy distillable. Twirling reduces the general question to the Werner family [Wer89, HH99, DSS+00, DCLB00]

$$\rho(d,\alpha) = \frac{I + \alpha F}{d^2 + \alpha d}, \qquad -1 \leq \alpha \leq 1,$$

where F is the swap on $\mathbb{C}^d \otimes \mathbb{C}^d$. The state $\rho(d,\alpha)$ is NPT exactly when $\alpha < -1/d$, and it is one-copy distillable exactly when $\alpha < -1/2$ [DSS+00, DCLB00]. For $d \geq 3$ the window $-1/2 \leq \alpha < -1/d$ therefore consists of NPT states that are undistillable from a single copy. A state is undistillable if and only if it is k-copy undistillable for all k, so NPT bound entanglement exists in the Werner family exactly when some state in this window stays k-copy undistillable for all k. No fixed number of copies settles this in general, since for every n there are distillable states that are n-copy undistillable [Wat04]. Shor, Smolin and Terhal showed that if NPT bound entangled Werner states exist, distillable entanglement is neither additive nor convex [SST01]. An NPT bound entangled state would also show that the partial transpose, which certifies entanglement, does not certify that maximally entangled pairs can be extracted from many copies.

Costa Rico [CR25] and Qi, Gupur, Wu and Guo [QGWG24, Theorem V.1] showed that $\rho(d,\alpha)$ is k-copy undistillable exactly when $q_k(-\alpha, C) \geq 0$ for every complex matrix C of rank at most two on $(\mathbb{C}^d)^{\otimes k}$, where $q_k(t,C)$ is an alternating sum of the squared norms of the partial traces of C (Section 2). For two copies the inequality at the endpoint $\alpha = -1/2$ was proved recently and independently by Fu, Gao and Park [FGP26], Fraser, Huber, Pozsgay and Vona [FHPV26], Song and Chen [SC26] and Bharti, Gajjala and Haug [BGH26], each through a sharp partial-trace inequality for matrices of rank at most two. In particular $\rho(4,-1/2)$ is not two-copy distillable, which settles Problem 5 of [HRZ22]. For three copies, Wu and Zou [WZ26] proved the endpoint inequality for normal rank-two matrices in all dimensions and for further nonnormal sectors. An anonymous computer-assisted proof [Ano26] settled the qutrit case $d = 3$ with a quartic moment relaxation and an exact rational certificate, and Wang's dimension lifting [Wan26] turns that certificate into three-copy undistillability for $\alpha \geq -(d+5)/(5d+1)$, a bound that tends to $-1/5$ as $d \to \infty$. For three or more copies, the first bound independent of d is Theorem IV.2 of [QGWG24]: $\rho(d,\alpha)$ is k-copy undistillable for $\alpha \geq -\eta_k$, where η_k is the zero in $(0,1)$ of $1 + (1-t)^k - (1+t)^k$. For $k \geq 4$ the best such bound was $\alpha \geq -\gamma_k$ [BGH26, Corollary 9.3], with $\gamma_k > \eta_k$; both $k\eta_k$ and $k\gamma_k$ tend to $\operatorname{arsinh}(1/2) = \log\varphi \approx 0.481$.

Our main result is that a third copy does not help.

Theorem 1.1. Let $d \geq 3$ and $\alpha \in [-1, 1]$. The state $\rho(d, \alpha)$ is three-copy distillable if and only if $\alpha < -1/2$.

For $d = 2$ the statement is classical, because $\rho(2, \alpha)$ is separable for $\alpha \geq -1/2$. By Costa Rico's criterion (Section 2), Theorem 1.1 is equivalent to the following matrix inequality.

Theorem 1.2. Let H_1, H_2, H_3 be finite-dimensional Hilbert spaces and let C be an operator on $H_1 \otimes H_2 \otimes H_3$ of rank at most two. Then

$$q_3(C) := \sum_{J \subseteq \{1,2,3\}} \Big(-\frac{1}{2}\Big)^{|J|} \big\| \operatorname{Tr}_J C \big\|_F^2 \;\geq\; 0.$$

If every H_i has dimension at least two, the constant $1/2$ cannot be increased, and equality occurs: for a rank-two projector P on H_1 and unit vectors $u_i \perp v_i$ in H_i $(i = 2, 3)$, the operator $C = P \otimes |u_2\rangle\langle v_2| \otimes |u_3\rangle\langle v_3|$ has rank two and $q_3(C) = 0$, and it makes the form negative once $1/2$ is replaced by any $t > 1/2$ (Lemma 2.2). Together with the results for one and two copies, Theorem 1.1 shows that in every dimension $d \geq 3$ the copy thresholds for $k \leq 3$ all equal $-1/2$; by Lemma 2.3(b), Theorem 1.2 also implies the two-copy inequality.

For $\alpha > -1/2$ the same method proves bounds for four and five copies in every dimension and, through these, for every number of copies.

Theorem 1.3. Let $d \geq 2$. The state $\rho(d, \alpha)$ is four-copy undistillable for every $\alpha \in [-79/160, 1]$ and five-copy undistillable for every $\alpha \in [-9/20, 1]$.

Theorem 1.4. The qutrit state $\rho(3, \alpha)$ is four-copy undistillable for every $\alpha \in [-0.4979, 1]$, and five-copy undistillable for every $\alpha \in [-0.47, 1]$.

Theorem 1.5. Let $d \geq 2$. For every $k \geq 6$ the state $\rho(d, \alpha)$ is k-copy undistillable for every $\alpha \in [-11/(5k), 1]$, and for every $k \geq 9$ it is k-copy undistillable for every $\alpha \in [-56/(25k), 1]$.

Since $79/160$ and $9/20$ exceed $1/3$, Theorem 1.3 provides, in every dimension $d \geq 3$, intervals of NPT Werner states that are four-copy and five-copy undistillable, and for qutrits Theorem 1.4 comes within 0.0021 of the endpoint for four copies. Theorem 1.5 gives NPT examples whenever $d > 5k/11$. Table 1 collects the bounds. A companion paper [Tom26b] locates the equality cases of the two-copy inequality and proves the endpoint inequality for every number of copies on a structured class of operators.

Table 1. Proven bounds: $\rho(d, \alpha)$ is k-copy undistillable for α at or above the entry. For $k \leq 3$ the entry is the threshold; for $k \geq 4$ the threshold lies between $-1/2$ and the entry. Section 9 gives slightly better bounds at $k = 6, 7$ and, through Proposition 9.3, for $k \geq 47$. An entry at or above $-1/d$ adds nothing, since $\rho(d, \alpha)$ is PPT for $\alpha \geq -1/d$; for qutrits this happens from $k = 7$ on, and a dash marks these entries.

copies k	**every** $d \geq 2$	**qutrits,** $d = 3$
$1, 2, 3$	$-1/2$	$-1/2$
4	$-79/160$	-0.4979
5	$-9/20$	-0.47
6	$-11/30$	$-11/30$
$7, 8$	$-11/(5k)$	—
$k \geq 9$	$-56/(25k)$	—

The inequalities for three, four and five copies are proved with variants of the quartic moment relaxation of [Ano26]. Because C has rank at most two, it lifts to a pair of unit vectors, and q_k becomes linear in their fourth moments. The variables of the relaxation are these moments after twirling, its constraints are positive semidefinite blocks and linear equalities that all physical moments satisfy, and a certificate is a positive combination of the constraints that reproduces q_k (Section 3). The main difficulty is that the local dimension d is unbounded. For three copies, adding one class of constraints gives certificates for all large dimensions, and the reduced moment data are polynomials in d. A base certificate whose entries are polynomials in $1/d$, corrected at each d by an amount bounded uniformly in $1/d$, then covers every $d \geq 9$. For four and five copies one limiting certificate with an exactly bounded residual covers all large dimensions. By Lemma 2.3(a) these certificates cover all dimensions. Theorem 1.5 follows by applying the inequalities for up to five copies, including the known two-copy ones and a partial-trace inequality of [CR25], to disjoint groups of copies and combining them in a linear program over averaged partial-trace norms.

Section 2 sets up the reduction and Section 3 the relaxation. Section 4 describes the procedure for exact certificates at fixed dimension, Section 5 proves Theorem 1.1, Sections 6–8 prove Theorems 1.3 and 1.4, and Section 9 Theorem 1.5; Section 10 discusses the results and what remains open. Steps checked by computer are marked † and refer to rows of Table 2 in Appendix A, which also describes the Lean formalizations; they prove Theorem 1.2 again for $3 \leq d \leq 8$ and the four-copy qutrit bound.

2. Setting and reduction to the endpoint

Let ρ act on $(\mathbb{C}^d)^{\otimes 2}$, the first factor held by one party and the second by the other. The state ρ is k-copy distillable if and only if there is a vector ψ of Schmidt rank at most two, across the cut between the parties' k-fold systems, with $\langle\psi|(\rho^{\otimes k})^{\Gamma}|\psi\rangle < 0$ [DSS+00, DCLB00]. Here Γ is the partial transpose on the second party. A state is undistillable if it is k-copy undistillable for all k.

For $C \in L\big((\mathbb{C}^d)^{\otimes k}\big)$ and $J \subseteq \{1,\dots,k\}$, let $\operatorname{Tr}_J C$ denote the partial trace over the copies in J, with $\operatorname{Tr}_\emptyset C = C$. For $t \in \mathbb{R}$ put

$$q_k(t,C) = \sum_{J\subseteq\{1,\dots,k\}} (-t)^{|J|}\, \|\operatorname{Tr}_J C\|_F^2.$$

Theorem 2.1 (Costa Rico [CR25, Theorem 1]; Qi, Gupur, Wu and Guo [QGWG24, Theorem V.1]). For $\alpha \in [-1,1]$, the state $\rho(d,\alpha)$ is k-copy distillable if and only if there is $C \in L\big((\mathbb{C}^d)^{\otimes k}\big)$ of rank at most two with $q_k(-\alpha, C) < 0$.

The form $q_k(t,\cdot)$ depends only on the matrix C, and the local dimension merely restricts the space in which C lives. We write $q_3(C) = q_3(1/2, C)$, and we say that $\mathrm{EP}_3(d)$ holds if $q_3(C) \geq 0$ for all $C \in L\big((\mathbb{C}^d)^{\otimes 3}\big)$ of rank at most two.

Lemma 2.2. *(a)* For product operators, $q_k\big(t, \bigotimes_m C_m\big) = \prod_m q_1(t, C_m)$, where $q_1(t,X) = \|X\|_F^2 - t|\operatorname{Tr} X|^2$. *(b)* If $\alpha < -1/2$, then $\rho(d,\alpha)$ is three-copy distillable. *(c)* If $\mathrm{EP}_3(d)$ holds, then $\rho(d,\alpha)$ is three-copy undistillable for all $\alpha \in [-1/2, 1]$.

Proof. (a) The partial trace of a product over J is the product of the traces of the factors in J and the remaining factors. So the sum over J factorizes.

(b) Let P be a rank-two projector and let $e \perp e'$ be unit vectors in $\mathbb{C}^d$. Then $q_1(t,P) = 2-4t$ and $q_1(t, |e\rangle\langle e'|) = 1$. By (a), the rank-two operator $C = P \otimes |e\rangle\langle e'| \otimes |e\rangle\langle e'|$ has $q_3(t,C) = 2-4t$, which is negative for $t = -\alpha > 1/2$, so $\rho(d,\alpha)$ is three-copy distillable by Theorem 2.1.

(c) This is the case $k = 3$, $t = 1/2$ of Corollary 2.4 below. □

Theorem 1.1 therefore follows from $\mathrm{EP}_3(d)$ for all $d \geq 3$, which is Theorem 1.2 for equal local dimensions. Zero padding extends this to arbitrary H_1, H_2, H_3.

For more than three copies we use the following monotonicity, in the dimension and in the parameter. Write $\Phi = \sum_{i,j} |ii\rangle\langle jj|$ for the unnormalized maximally entangled projector of one copy. With $\psi_C = \operatorname{vec} C$ one has $q_k(t,C) = \langle\psi_C|(I - t\Phi)^{\otimes k}|\psi_C\rangle$.

Lemma 2.3. Let $k \geq 1$ and $0 \leq t' \leq t < 1$. *(a)* If $q_k(t,C) \geq 0$ for every C of rank at most two on $(\mathbb{C}^D)^{\otimes k}$, then the same holds on $(\mathbb{C}^d)^{\otimes k}$ for every $d \leq D$. *(b)* If $q_k(t,C) \geq 0$ for every C of rank at most two on $(\mathbb{C}^d)^{\otimes k}$, then $q_j(t',C) \geq 0$ for every $j \leq k$ and every C of rank at most two on $(\mathbb{C}^d)^{\otimes j}$.

Proof. (a) For an isometry $\iota\colon \mathbb{C}^d \to \mathbb{C}^D$ the operator $C' = \iota^{\otimes k} C\, \iota^{*\otimes k}$ has the same rank as C, and $\operatorname{Tr}_J C' = \iota^{\otimes(k-|J|)}(\operatorname{Tr}_J C)\, \iota^{*\otimes(k-|J|)}$, so $q_k(t,C') = q_k(t,C)$.

(b) First let $t' = t$. For a unit vector u, the operator $C \otimes |u\rangle\langle u|^{\otimes(k-j)}$ has rank at most two, and the argument of Lemma 2.2(a) shows that its value of $q_k(t,\cdot)$ is $q_j(t,C)(1-t)^{k-j}$. Hence $q_j(t,\cdot) \geq 0$ for $j \leq k$. Now let $t' < t$. Write $I - t'\Phi = (t'/t)(I - t\Phi) + (1 - t'/t)I$ and expand the j-fold tensor power. The term with $I - t\Phi$ on a set S of copies contributes a positive multiple of $\langle\psi_C|(I-t\Phi)^{\otimes S} \otimes I|\psi_C\rangle = \sum_{x,y} q_{|S|}(t, C_{xy})$, where C_{xy} are the matrix elements of C over the copies outside S in a product basis. Each C_{xy} has rank at most two, so every term is nonnegative. □

Corollary 2.4. If $q_k(t,C) \geq 0$ for some $t \in [0,1)$ and every C of rank at most two on $(\mathbb{C}^d)^{\otimes k}$, then $\rho(d,\alpha)$ is k-copy undistillable for every $\alpha \in [-t, 1]$.

Proof. For $-t \leq \alpha \leq 0$, Lemma 2.3(b) gives $q_k(-\alpha,\cdot) \geq 0$, and Theorem 2.1 applies. For $\alpha > 0$ every term of $q_k(-\alpha, C)$ is nonnegative. □

In Sections 6–9 each theorem is reduced in this way to an inequality $q_k(t,C) \geq 0$ at one value of t, by Corollary 2.4 and, where the inequality is proved for large dimensions only, by Lemma 2.3(a).

3. The moment relaxation

We describe the relaxation for k copies, prove that each of its constraints is valid, and state the certificate conditions. The moment families X_{31}, X_{22}, X_{13}, the lifting and the coupled Gram block are those of [Ano26],

whereas the second coupled Gram block (Section 3.3) and the classes used only for four copies are new. Our validity proof follows [Ano26, Lemmas 2–4] and replaces its basis-completeness computation [Ano26, Lemma 5] by a spanning argument.

3.1 Lifting

Let $k \geq 1$, $H = (\mathbb{C}^d)^{\otimes k}$, $Q = \mathbb{C}^2$ and $V = H \otimes Q$. Let $C \neq 0$ have rank at most two. Since $q_k(t, \cdot)$ is homogeneous of degree two, we may assume $\|C\|_F^2 = 1/2$. Choose an isometry $A\colon Q \to H$ with $\operatorname{ran} C \subseteq \operatorname{ran} A$, and put $B = 2C^*A$. Then $C = AB^*/2$, because AA^* fixes $\operatorname{ran} C$, and $\|B\|_F^2 = 4\|C\|_F^2 = 2$. Put

$$a = \tfrac{1}{\sqrt{2}} \sum_{x,r} A_{xr} \, |x\rangle \otimes |r\rangle, \qquad b = \tfrac{1}{\sqrt{2}} \sum_{x,r} B_{xr} \, |x\rangle \otimes |r\rangle \qquad \text{in } V.$$

Then $\|a\| = \|b\| = 1$, $\operatorname{Tr}_H |a\rangle\langle a| = I_Q/2$ because $A^*A = I$, and $C_{xy} = \sum_r a_{xr}\overline{b_{yr}}$. We call (a, b) a *physical pair* for C.

3.2 Moments and the source space

We work on four replicas $V^{\otimes 4}$. For a letter string $\ell = (\ell_1, \ell_2, \ell_3, \ell_4) \in \{a, b\}^4$ put $Y_\ell = |\ell_1 \otimes \ell_2 \otimes \ell_3 \otimes \ell_4\rangle\langle \ell_1 \otimes \ell_2 \otimes \ell_3 \otimes \ell_4|$. The moment families are

$$Y_{31} = Y_{aaab}, \qquad Y_{22} = Y_{aabb}, \qquad Y_{13} = Y_{bbba},$$

and for four copies also $Y_{40} = Y_{aaaa}$ and $Y_{04} = Y_{bbbb}$. Let G be the group generated by the local unitaries $g = U_1 \otimes \cdots \otimes U_k \otimes R$ on V (with $U_i \in U(d)$ and $R \in U(2)$), the permutations of the k sites, and complex conjugation in the product basis. An element of G maps a physical pair for C to a physical pair for UCU^*, for a site permutation of C, or for $\overline{C}$, and each of these has the same value of $q_k(t, \cdot)$. The *physical moments* are

$$X_f = L \, \mathbb{E}_{g \in G} \, Y_f(ga, gb), \qquad f \in \{40, 31, 22, 13, 04\}, \qquad L = (2d^k)^4,$$

with the Haar measure on the unitaries and the uniform measure on the finite part. The positive constant L is a normalization. It plays no role in validity, because each constraint is homogeneous, and the objective below carries the factor L^{-1}.

Write $V^{\otimes 4} = \bigotimes_l (\mathbb{C}^{n_l})^{\otimes 4}$ over the $k + 1$ local factors $l \in \{1, \ldots, k, Q\}$, with $n_l = d$ for the sites and $n_Q = 2$. For $p \in S_4$ let V_p permute the four replicas of one local factor. A *word* is $w = (w_1, \ldots, w_k, w_Q) \in S_4^{k+1}$, and $V_w = \bigotimes_l V_{w_l}$. Let $G_f \subseteq S_4$ be the stabilizer of the letter string f. The *source space* $\mathcal{S}_f$ is the real span of the orbit sums of words under three operations, each applied to all components at once: (i) $w \mapsto gwh$ for $g, h \in G_f$; (ii) permutations of the k site components; (iii) $w \mapsto w^{-1}$.

Lemma 3.1. For each physical pair, $X_f \in \mathcal{S}_f$.

Proof. By Schur–Weyl duality the commutant of $\{U^{\otimes 4} : U \in U(n)\}$ on $(\mathbb{C}^n)^{\otimes 4}$ is spanned by the V_p, and the commutant of a tensor product of such groups is the tensor product of the commutants. So the Haar average lies in $\operatorname{span}\{V_w\}$, and $X_f = \sum_w x_w V_w$ for some coefficients. Linear independence is not needed. The operator X_f is invariant under (i), because $V_\sigma Y_f = Y_f V_\sigma = Y_f$ for $\sigma \in G_f$ and V_σ commutes with $g^{\otimes 4}$. It is invariant under (ii) because of the site average. It is real and symmetric because of the conjugation average, and $V_w^{\mathsf{T}} = V_{w^{-1}}$ with each V_w real. Each operation permutes the coefficients of a representation. Averaging the real parts of the coefficients over the finite group generated by (i)–(iii) gives a representation with real coefficients that are constant on orbits. □

3.3 Positive blocks

Lemma 3.2 (Gram classes). Let $F \subseteq \{1, 2, 3, 4\}$ and let $x^{(1)}, \ldots, x^{(R)} \in \{a, b\}^4$ be letter strings with the same value of $s(x) = \#a(x|_{F^c}) - \#a(x|_F)$. Put $u_r = \bigotimes_i y_i^{(r)}$ with $y_i^{(r)} = x_i^{(r)}$ for $i \notin F$ and $y_i^{(r)} = \overline{x_i^{(r)}}$ for $i \in F$. *(a)* For all r, s there are a family $f \in \{40, 31, 22, 13, 04\}$ and a fixed bijection of the eight tensor indices, independent of (a, b), that turns Y_f into $|u_r\rangle\langle u_s|$. We write this rearrangement as $R_{rs}(Y_f)$. It has the form $(V_p Y_f V_q^*)^{\Gamma_F}$ for some $p, q \in S_4$, where Γ_F transposes the replicas in F. *(b)* For each physical pair, the block operator $M(X) = \big[R_{rs}(X_f)\big]_{r,s=1}^{R}$ is positive semidefinite.

Proof. (a) An entry of $|u_r\rangle\langle u_s|$ is a product of eight vector components. Four of them are unconjugated: those of $x^{(r)}$ on F^c and of $x^{(s)}$ on F. The other four are conjugated. The number of letters a among the unconjugated components minus the number among the conjugated ones is $s(x^{(r)}) - s(x^{(s)}) = 0$. So both groups carry the same letter multiset, which is the multiset of exactly one family f. Matching the unconjugated components with the ket slots of Y_f and the conjugated ones with the bra slots reproduces the entry. When a letter repeats, all matchings give the same operator, because the matched factors are equal vectors.

(b) For a unitary $g \in G$, $u_r(ga, gb) = W_g\, u_r(a, b)$ with $W_g = \bigotimes_{i\notin F} g \otimes \bigotimes_{i\in F} \overline{g}$, the same unitary for all r. Hence $M\big(Y(ga, gb)\big) = (I_R \otimes W_g)\,|w\rangle\langle w|\,(I_R \otimes W_g)^*$ with $w = \bigoplus_r u_r(a, b)$. Complex conjugation yields $|\overline{w}\rangle\langle\overline{w}|$, and site permutations replace w by a permuted copy. Since M is linear, $M(X)$ is an average of positive semidefinite matrices. □

The certificates use four kinds of Gram classes.

1. *Partial transposes* ($R = 1$): $X_f^{\Gamma_T} \succeq 0$ for whole-replica cuts T. The certificates for three and four copies use the cuts $\emptyset, \{4\}, \{1\}, \{1, 2\}$ for X_{31} and X_{13}, and $\emptyset, \{1\}, \{3\}, \{1, 2\}, \{1, 3\}$ for X_{22}. The certificate for five copies in every dimension uses the same cuts (Section 7).
2. *The coupled Gram block of [Ano26]*: $F = \{4\}$ and the rows $a \otimes a \otimes b \otimes \overline{a}$ and $b \otimes b \otimes a \otimes \overline{b}$. Its diagonal blocks come from X_{31} and X_{13} and its off-diagonal block from X_{22}.
3. *The second coupled Gram block*: $F = \{3, 4\}$ and the rows $u' = a \otimes a \otimes \overline{a} \otimes \overline{b}$ and $v'' = a \otimes b \otimes \overline{b} \otimes \overline{b}$. In index form, with replica indices $i_1 \dots i_4$ and $j_1 \dots j_4$,
$$\begin{aligned} A'(X)[i; j] &= X_{31}[i_1 i_2 j_3 j_4;\, j_1 j_2 i_3 i_4], \\ B'(X)[i; j] &= X_{22}[i_1 i_2 j_3 j_4;\, i_3 j_1 i_4 j_2], \\ D'(X)[i; j] &= X_{13}[i_2 j_3 j_4 i_1;\, j_2 i_3 i_4 j_1], \end{aligned}$$
and $\begin{bmatrix} A' & B' \\ B'^* & D' \end{bmatrix}$ is the Gram matrix of (u', v'') averaged over G. Its diagonal blocks are $X_{31}^{\Gamma_{34}}$ and a replica-permuted $X_{13}^{\Gamma_{34}}$.
4. *Four-copy classes*: the partial-transpose blocks of X_{40} and X_{04}, and three classes that use them: $F = \{4\}$ with rows $a \otimes a \otimes a \otimes \overline{a}$ and $a \otimes a \otimes b \otimes \overline{b}$; $F = \{4\}$ with rows $b \otimes b \otimes b \otimes \overline{b}$ and $a \otimes b \otimes b \otimes \overline{a}$; and $F = \{3, 4\}$ with rows $a \otimes a \otimes \overline{a} \otimes \overline{a}$, $b \otimes b \otimes \overline{b} \otimes \overline{b}$ and $a \otimes b \otimes \overline{a} \otimes \overline{b}$. They are used only in Section 8.

The relaxation of [Ano26] contains only the first two kinds. Numerically, its value is zero for $d = 3, 4$, zero to within 2×10^{-9} for $d = 5$, and -2.85×10^{-7} for $d = 6$. The second coupled Gram block is violated by the optimal pseudo-moment at $d = 6$. With all three kinds, exact certificates exist in all dimensions (Sections 4 and 5).

3.4 Equalities

Two kinds of linear equalities vanish on physical moments.

- *Stiefel contrasts.* For a replica r let $\mathrm{Tr}_{H,r}$ trace out the H-part of replica r, and $\mathrm{Tr}_{V,r}$ the whole replica r. Put $S_r(X) = \mathrm{Tr}_{H,r}\, X - (I_Q/2)_r \otimes \mathrm{Tr}_{V,r}\, X$. If f carries the letter a at replica r, then $S_r(X_f) = 0$, because $\mathrm{Tr}_H\, |a\rangle\langle a| = I_Q/2$ and $\|a\| = 1$, and because S_r commutes with the action of G. The certificates use $r = 1$ for X_{31}, X_{22} and X_{40}, and $r = 4$ for X_{13}. (At a b-replica the contrast does not vanish.)
- *Common marginals.* $\mathrm{Tr}_3\, X_{31} = \mathrm{Tr}_3\, X_{22}$, with the surviving replicas in the order $(1, 2, 4)$, and $\mathrm{Tr}_2\, X_{22}$ with the order $(1, 3, 4)$ equals $\mathrm{Tr}_2\, X_{13}$ with the order $(4, 1, 3)$. Both identities hold because $\|a\| = \|b\| = 1$. With X_{40} and X_{04} there are two more, $\mathrm{Tr}_4\, X_{31} = \mathrm{Tr}_4\, X_{40}$ and $\mathrm{Tr}_4\, X_{13} = \mathrm{Tr}_4\, X_{04}$, for the same reason.

3.5 Objective

Lemma 3.3 (swap identity). Let (a, b) be a physical pair for C. For $S \subseteq \{1, \dots, k\}$, let F_S swap the sites in S between two copies of V, and let F_Q swap the two auxiliary factors. Then $\langle a \otimes b|F_Q F_S|a \otimes b\rangle = \|\,\mathrm{Tr}_S\, C\|_F^2$.

Proof. Write $x = (x_S, x_{S^c})$ for an index of H. Put $x' = (y_S, x_{S^c})$ and $y' = (x_S, y_{S^c})$. Then
$$\langle a \otimes b|F_Q F_S|a \otimes b\rangle = \sum_{x,y,r,s} \overline{a_{xr}}\, \overline{b_{ys}}\, a_{x's}\, b_{y'r} = \sum_{x,y} \overline{C_{xy'}}\, C_{x'y}.$$
Summing over x_S and y_S turns this into $\sum_{x_{S^c}, y_{S^c}} \big|(\mathrm{Tr}_S\, C)_{x_{S^c} y_{S^c}}\big|^2$. □

For $t \in [0,1)$ let $Z_t = F_Q \prod_{i=1}^{k}(I - tF_i) = \sum_S (-t)^{|S|} F_Q F_S$, acting on replicas 1 and 4, and define the objective $c_t(X) = L^{-1} \operatorname{Tr}\left[(Z_{t,14} \otimes I_{23})X_{31}\right]$. The replicas 2 and 3 of Y_{31} carry $|a\rangle\langle a|$, of trace one. Since Z_t commutes with $g \otimes g$, Lemma 3.3 gives $c_t(X) = q_k(t, C)$ for the physical moments of each physical pair for C. For $k = 3$ and $t = 1/2$ we write $c = c_{1/2}$. On words the objective has the closed form

$$c_t(V_w) = L^{-1} \prod_{l=1}^{k} \left(d^{\,\kappa(w_l)} - t\, d^{\,\kappa((14)\circ w_l)} \right) \cdot 2^{\,\kappa((14)\circ w_Q)}, \tag{3.1}$$

where $\kappa(p)$ is the number of cycles of p, so that $\operatorname{Tr} V_p = n^{\kappa(p)}$ on $(\mathbb{C}^n)^{\otimes 4}$. Since $L = 16d^{4k}$, the objective of a word is d^{-4k} times a polynomial of degree at most $4k$ in d.

3.6 Certificates and validity

Definition 3.4. A *certificate for* (k, d, t) consists of the following data.

- Finitely many blocks $H_b(X) = K_b^* M_b(X) K_b$, where each M_b is an operator from Lemma 3.2 and each K_b is a fixed matrix.
- Real symmetric matrices $Z_b \succeq 0$.
- Finitely many equality functionals E_e, each a compression of a Stiefel contrast or a common-marginal identity of Section 3.4, with real coefficients λ_e.

The data must satisfy the identity

$$c_t(X) = \sum_b \operatorname{Tr}\left(Z_b H_b(X)\right) + \sum_e \lambda_e E_e(X) \qquad \text{for all } X \in \prod_f \mathcal{S}_f, \tag{3.2}$$

with the product over the families that the blocks use.

It suffices to check (3.2) on the orbit sums, which span the source space.

Theorem 3.5 (validity). If a certificate for (k, d, t) exists, then $q_k(t, C) \geq 0$ for every C of rank at most two on $(\mathbb{C}^d)^{\otimes k}$. For $k = 3$ and $t = 1/2$ this is $\mathrm{EP}_3(d)$.

Proof. Let C have rank at most two, with $\|C\|_F^2 = 1/2$, and let X be the physical moments of a physical pair for C. By Lemma 3.1, X lies in the source space. By (3.2) and Section 3.5,

$$q_k(t, C) = c_t(X) = \sum_b \operatorname{Tr}\left(Z_b H_b(X)\right) + \sum_e \lambda_e E_e(X).$$

Each $H_b(X) = K_b^* M_b(X) K_b$ is positive semidefinite by Lemma 3.2, so each trace is nonnegative. Each $E_e(X)$ vanishes by Section 3.4. Hence $q_k(t, C) \geq 0$. □

The compressions K_b are arbitrary: their ranks and their symmetry adaptation affect how tight the relaxation is, but not its validity. Validity does, however, depend on two parts of the data: the equality functionals must have the form of Section 3.4 at a-replicas, and each partial-transpose block must transpose whole replicas. These two parts of the data must therefore be checked for each certificate.

For four and five copies we use certificates whose identity holds up to a small residual, which a positive multiple of the trace absorbs. Let $\tau(X) = L^{-1} \operatorname{Tr} X_{31}$, so that $\tau(X) = 1$ for the physical moments. For each local factor l let $G_l = (n_l^{\kappa(p^{-1}q)})_{p,q \in S_4}$ be the Gram matrix of the replica permutations, let G_l^+ be its pseudo-inverse, and put $K = \prod_l \|G_l^+\|_\infty$, the product of row-sum norms.

Lemma 3.6 (slack certificates). Let blocks H_b and matrices $Z_b \succeq 0$, equality functionals E_e with coefficients λ_e, and a number ν be as in Definition 3.4, and define the residual functional

$$\rho(X) = c_t(X) - \nu\, \tau(X) - \sum_b \operatorname{Tr}\left(Z_b H_b(X)\right) - \sum_e \lambda_e E_e(X).$$

For each family f let $R_f(o)$ be the value of ρ on the orbit sum o of words of f, and suppose that $\nu \geq L\, K \sum_f \sum_o |R_f(o)|$. Then $q_k(t, C) \geq 0$ for every C of rank at most two.

Proof. Let X be the physical moments of a physical pair for C. They are averaged over the group G, so the minimal-norm coefficients $x = G^+ g$ of X_f in the word basis, with $g_v = \operatorname{Tr}(V_v^* X_f)$ and $G = \bigotimes_l G_l$, are constant on the orbits of Section 3.2: G and g are invariant under these operations, and so G^+ commutes with them.

Since $X_f \succeq 0$, each $|g_v| \le \operatorname{Tr} X_f = L$, and the row-sum norm of $G^+ = \bigotimes_l G_l^+$ is K. Hence $|x_w| \le KL$ and $|\rho(X)| \le LK \sum_f \sum_o |R_f(o)| \le \nu$. The blocks are positive semidefinite and the equalities vanish, as in the proof of Theorem 3.5, so $q_k(t, C) = c_t(X) \ge \nu + \rho(X) \ge 0$. □

The inequality of Lemma 3.6 is checked in exact rational arithmetic, with $|R_f(o)|$ computed modulo several primes and reconstructed by the Chinese remainder theorem.

3.7 Symmetry reduction

The certificates are written in a symmetry-adapted basis. On one local factor $(\mathbb{C}^n)^{\otimes 4}$ with a cut T, the operators commuting with the twirl are spanned by the partially transposed permutations V_p^Γ, $p \in S_4$. Their irreducible modules carry labels (f, λ, μ), where f is a number of contracted pairs and λ, μ are partitions of the numbers of uncut and cut replicas minus f, with $\operatorname{len}\lambda + \operatorname{len}\mu \le 4 - 2f$. For each label we use a basis of the multiplicity space of the form $D(d)C$, where the columns of $D(d)$ are explicit *diagram vectors* and C is a fixed matrix (Section 5.1). A *type* t is a Gram class together with one label for each site factor and for the auxiliary factor. Its reduced block is the compression $K_t^* M_t(X) K_t$ by the tensor product of the module bases of these labels, followed by fixed integer congruences (stabilizer symmetrization and site-permutation sums). As a functional of the orbit coordinates of X, each entry of a reduced block is a sum of products of local matrix elements $\langle D_i | V_p^\Gamma | D_j \rangle$, one factor for each local factor. So the dimension d enters a certificate only through the local matrix elements of the k site factors, through the equality maps, which are compressions of partial traces, and through the objective (3.1). The auxiliary factor has dimension two for all d.

4. Three copies: exact certificates at fixed dimension

This section describes how a numerical solution of the relaxation becomes an exact certificate at a fixed dimension. Section 5 builds on this procedure, and the exact certificates for $d \le 16$ are described in the supplement.

Each zero C of q_3 yields physical moments X with $c(X) = 0$. Identity (3.2) then forces $\operatorname{Tr}(Z_t H_t(X)) = 0$ for each t, hence $Z_t H_t(X) = 0$, so every certificate vanishes on the ranges of the blocks at the zeros of q_3. Such zeros are plentiful. Examples include the operators $P \otimes |u\rangle\langle v|$ with P a rank-two projector on one site, and many rank-two operators supported on two-dimensional subspaces of the three sites. On the latter, $q_3 \ge 0$ holds because $\rho(2, -1/2)$ is separable, and q_3 has many zeros. We compute the ranges exactly from finitely many zero modes with Gaussian-integer entries and restrict each multiplier to the orthogonal complement.

On this face we solve the relaxation numerically with a primal-dual interior-point method. We round the solution to rationals and then solve exactly for the equality coefficients and some of the Gram entries, so that (3.2) holds on all orbit sums. Positive semidefiniteness of each multiplier is checked exactly, through the sign pattern of the characteristic polynomial.

5. Three copies: a certificate uniform in $d \ge 9$

We now prove $\mathrm{EP}_3(d)$ for all $d \ge 9$ from one certificate whose entries are polynomials in $s = 1/d$, after corrections that are bounded uniformly in s.

5.1 Polynomial local data

Fix $m \in \{3, 4\}$ replicas of one site factor $\mathbb{C}^d$ and a cut T of transposed replicas. Fix a label (f, λ, μ) as in Section 3.7. A *diagram vector* of this label is

$$D(d) = \sum_{j \in [d]^f} e_{x(j)},$$

where the index string $x(j)$ is built as follows. The f summation indices $j_1, \dots, j_f$ sit on f contraction pairs, each consisting of one uncut and one cut replica. The remaining uncut replicas carry fixed values from $\{0, 1, \dots, \operatorname{len}\lambda - 1\}$, and the remaining cut replicas carry fixed values from $\{d-1, d-2, \dots, d - \operatorname{len}\mu\}$, in a pattern determined by the vector.

Lemma 5.1 (loop counting). Let $d \ge 4$. For all $p \in S_m$ and all diagram vectors D_i, D_j of one label,

$$\langle D_i(d) | V_p^\Gamma | D_j(d) \rangle = \varepsilon\, d^\kappa, \qquad \varepsilon \in \{0, 1\}, \quad 0 \le \kappa \le 2f,$$

with ε and κ independent of d.

Proof. In the computational basis, a matrix element of V_p^Γ is a product of Kronecker deltas over a perfect matching of the $2m$ index positions, namely the walled Brauer diagram of p. Add an edge for each contraction pair of D_i (on the row positions) and of D_j (on the column positions). In the resulting graph, positions on a pair have degree two and positions with a fixed value have degree one. Hence each component is a cycle through summed positions or a path between two fixed positions. Summing over the free indices, each cycle contributes a factor d, and each path contributes the Kronecker delta of its two endpoint values. A delta between two values from $\{0,1,2,3\}$, or between two values of the form $d-1-r$, does not depend on d. A delta between $t \in \{0,\dots,\operatorname{len}\lambda-1\}$ and $d-1-r$ with $r < \operatorname{len}\mu$ equals one only if $d = t+r+1$. But $t+r \le \operatorname{len}\lambda+\operatorname{len}\mu-2 \le 2$, so this would need $d \le 3$. Each cycle alternates between diagram edges and pair edges, and distinct cycles are disjoint, so the number κ of cycles is at most the number $2f$ of pair edges. □

At each dimension d we use module bases $J(d)$ for the labels and the local matrices $\mathrm{FT}(d) = J(d)^\mathsf{T} V_p^\Gamma J(d)$. For $d = 4,\dots,10$ these bases have the form $J(d) = D(d)\,C$ with a matrix C that does not depend on d (†, V1).

Corollary 5.2. Let $\mathrm{FT}_{\mathrm{poly}}(d)$ be the interpolant of degree at most four through $\mathrm{FT}(4),\dots,\mathrm{FT}(8)$. Then $\mathrm{FT}_{\mathrm{poly}}(d) = (D(d)C)^\mathsf{T} V_p^\Gamma (D(d)C)$ for all $d \ge 4$, and each label block of $\mathrm{FT}_{\mathrm{poly}}$ has degree at most $2f$. For each $d \ge 4$, the relaxation assembled from $\mathrm{FT}_{\mathrm{poly}}(d)$ is the relaxation of Section 3 with the local compressions $D(d)C$, so Theorem 3.5 applies to it.

Proof. By Lemma 5.1, $(D(d)C)^\mathsf{T} V_p^\Gamma (D(d)C)$ is a polynomial in d of degree at most $2f \le 4$. It agrees with $\mathrm{FT}(d)$ at the five points $d = 4,\dots,8$, so it equals $\mathrm{FT}_{\mathrm{poly}}$. The remaining data are of the same kind for all d. The three-replica data used by the equality maps have $f = 0$, so they do not depend on d, and the partial-trace maps and the objective (3.1) are explicit. Theorem 3.5 allows arbitrary compressions. □

5.2 Face, scaling and degrees

We fix a face of the relaxation: each multiplier has the form $Z_t = N_t \hat{Z}_t N_t^\mathsf{T}$ for a fixed matrix N_t. For a type t let $F_t \le 6$ be the total number of contracted pairs in its three site labels. We rescale each multiplier as $\hat{Z}_t = d^{2F_t} Z_t$, followed by one fixed congruence, and each equality coefficient by d^3. Then identity (3.2) restricted to the face becomes a linear system

$$A(s)\,x = c(s), \qquad s = 1/d,$$

with 4675 rows, one for each orbit sum. Each column of $A(s)$ and the right-hand side $c(s)$ are polynomials in s of degree at most 12. This follows from Corollary 5.2 and (3.1). Before rescaling, a block column of type t is a polynomial in d of degree at most $2F_t$, an equality column has degree at most three, and the objective is d^{-12} times a polynomial of degree at most 12. The inputs of these degree bounds are checked from the diagram data (†, V2).

5.3 The certificate

Lemma 5.3. Let A be a real $m \times n$ matrix and $c \in \mathbb{R}^m$ with c in the range of A. Let R be a set of $\rho = \operatorname{rank} A$ rows and B an $n \times \rho$ matrix with $\theta = \|I - A_R B\| < 1$. For $\tilde{x} \in \mathbb{R}^n$ put $r = c - A\tilde{x}$ and $\delta = B(A_R B)^{-1} r_R$. Then $A(\tilde{x}+\delta) = c$, and

$$\|\delta\| \le \|B r_R\| + \frac{\|B\|\,\theta\,\|r_R\|}{1-\theta}.$$

Proof. Since $\theta < 1$, the matrix $A_R B$ is invertible, so $\operatorname{rank} A_R = \rho = \operatorname{rank} A$. Hence the rows R span the row space, and $A = K A_R$ for some K. The residual r lies in the range of A, so $r = Ay$ for some y. Then $A\delta = K A_R \delta = K r_R = K A_R y = Ay = r$. For the bound, expand $(A_R B)^{-1} = \sum_{i \ge 0} (I - A_R B)^i$. □

Proposition 5.4. For every integer $d \ge 9$ the system $A(1/d)x = c(1/d)$ has a rational solution whose multipliers are positive semidefinite.

Proof. We work with $s \in [0, 1/9]$. Each block is written as $\hat{Z}_t = T_t D_t T_t^\mathsf{T}$ with a fixed integer matrix T_t, and corrections are applied to D_t.

- *Base certificate.* Each $D_t(s)$ is a polynomial of degree at most $12 - 2F_t$, written in the Bernstein basis of $[0, 1/9]$, and each equality coefficient is a polynomial of degree nine. Every Bernstein coefficient block C of $\hat{Z}_t$ satisfies $C \succeq m\,T_t T_t^\mathsf{T}$ with $m = 2.712241 \times 10^{-6}$ (†, V3). The Bernstein basis is nonnegative and sums to one, so $\hat{Z}_t(s) \succeq m\,T_t T_t^\mathsf{T}$ on $[0, 1/9]$.

- *First correction.* An explicit polynomial correction of degree 20 with dyadic coefficients changes each D_t by at most $\varepsilon_1 = 1.8771 \times 10^{-9}$ in operator norm on $[0, 1/9]$. After it, the residual $r'(s)$ of the identity has degree at most 32. Its exact values at 38 nodes, which determine it, are at most 3.934×10^{-19} in absolute value (†, V3).
- *Consistency.* Let S be a fixed set of 2634 coordinates and A_S the corresponding columns of A. A matrix $W(s)$ of 1934 constant vectors and 107 integral polynomial vectors of degree at most five satisfies $W^{\mathsf{T}} A_S \equiv 0$ and $W^{\mathsf{T}} r' \equiv 0$ as polynomial identities, and $\operatorname{rank} W(1/9) = 2041 = 4675 - 2634$ (†, V4). Hence $\operatorname{rank} A_S(s) \le 2634$ for all but finitely many s, and then for all s, since the rank of a polynomial matrix never exceeds its generic rank. The bound $\theta < 1$ below gives $\operatorname{rank} A_S(s) \ge 2634$. Thus the rank is 2634 on all of $[0, 1/9]$. At all but finitely many s the columns of $W(s)$ span the left kernel of $A_S(s)$, so $r'(s)$ lies in the range of $A_S(s)$. At constant rank the projector onto the range is continuous in s, and therefore $r'(s)$ lies in the range of $A_S(s)$ for every $s \in [0, 1/9]$.
- *Second correction.* We apply Lemma 5.3 to $A_S(s)$ and $r'(s)$, with a fixed set R of 2634 rows and with $B(s)$ interpolated from approximate inverses at 21 Chebyshev points. The matrix $I - A_R(s)B(s)$ has entries of degree at most $12 + 20 = 32$ in s, so midpoint-radius bounds at 33 Chebyshev nodes and the Lebesgue constant 3.249 of interpolation at these nodes give $\theta \le 1.2234 \times 10^{-5}$ for all $s \in [0, 1/9]$. The resulting correction changes each D_t by at most 5.1592×10^{-9} in operator norm (†, V5).

Since $\varepsilon_1 + 5.1592 \times 10^{-9} \le 7.0363 \times 10^{-9} < m$, each corrected block satisfies $\hat{Z}_t(s) \succeq (m - 7.0363 \times 10^{-9})\, T_t T_t^{\mathsf{T}} \succeq 0$ on $[0, 1/9]$. At $s = 1/d$ all data are rational, so the solution is rational. □

Theorem 5.5. $\mathrm{EP}_3(d)$ holds for every $d \ge 9$.

Proof. By Proposition 5.4 the relaxation assembled from the polynomial data at dimension d has an exact certificate. By Corollary 5.2 this is a certificate in the sense of Definition 3.4, with compressions $D(d)C$. Theorem 3.5 gives $\mathrm{EP}_3(d)$. □

Proof of Theorems 1.1 and 1.2. By Theorem 5.5, $\mathrm{EP}_3(d)$ holds for every $d \ge 9$, and by Lemma 2.3(a) for every smaller d. Theorem 1.1 then follows from Lemma 2.2, and Theorem 1.2 by the embedding in the proof of Lemma 2.3(a). □

6. Four copies in every dimension

We prove the four-copy part of Theorem 1.3. It suffices to show $q_4(t_0, C) \ge 0$, with $t_0 = 79/160$, for every C of rank at most two on $(\mathbb{C}^n)^{\otimes 4}$ and every $n \ge n_0 = 1.25 \times 10^9$. We use the relaxation of Section 3 with $k = 4$, consisting of the three families X_{31}, X_{22}, X_{13}, the partial-transpose blocks, both coupled Gram blocks, and one certificate in the slack form of Lemma 3.6 for all $n \ge n_0$.

The residual of a fixed certificate is polynomial in $1/n$. The site data of the blocks are the polynomials $\mathrm{FT}_{\mathrm{poly}}$ of Corollary 5.2, since the four replica slots of one site do not depend on k. The objective and trace factors of a site are $\sum_j s^j\big([\kappa = 4 - j] - t[\kappa((14) \circ p) = 4 - j]\big)$ and $\sum_j s^j[\kappa = 4 - j]$ in $s = 1/n$, and the scaled partial traces are linear in s. Hence, for fixed multipliers Q_b, coefficients λ_e and slack ν, the residual of a word w has the form

$$\rho^{(n)}(V_w) = R_0(w) + s\, R_1(w) + r_2(w; s), \qquad |r_2(w; s)| \le s^2 B_2(w) \quad (0 \le s \le 1),$$

where $B_2(w)$ is the absolute coefficient sum of the part of degree at least two. With $S_0 = \sum_o |R_0(o)|$, $S_1 = \sum_o |R_1(o)|$ and $S_2 = \sum_w B_2(w)$, summed over all families, the condition of Lemma 3.6 at dimension n follows from

$$\nu \;\ge\; LK(n)\big(S_0 + sS_1 + s^2 S_2\big).$$

The constant satisfies $LK(n) = 16\left(n^4 \|G_n^{-1}\|_\infty\right)^4 \|G_2^+\|_\infty$ with $\|G_2^+\|_\infty = 31/180$. A Neumann series in $G_n = n^4(I + E_n)$, where $\|E_n\|_\infty \le 6/n + 11/n^2 + 6/n^3$ by the cycle counts of S_4, gives $LK(n) \le 16 \cdot (31/180)\,(1 - 6/n - 11/n^2 - 6/n^3)^{-4}$ for $n \ge 12$.

We obtain the certificate (Q_b, λ, ν) from the limiting relaxation at $s = 0$, solved with the largest possible slack $\nu = 10^{-4}$ at t_0. Each multiplier is stored as $Q_b = M_b M_b^{\mathsf{T}}$ with an explicit rational matrix M_b, so it is positive semidefinite by construction. The relaxation at $s = 0$ is strictly feasible for $t \le 79/160$ and has negative value at $t = 0.495$. So $79/160$ is within 0.00125 of the best constant that this relaxation can give in all dimensions.

Proposition 6.1. For the four-copy certificate, with the data of Table 3 and $s_0 = 1/n_0$,

$$\nu - LK(n_0)\big(S_0 + s_0 S_1 + s_0^2 S_2\big) \;\ge\; 7.94 \times 10^{-5} > 0.$$

Proof. S_0 and S_1 are computed exactly, and S_2 is bounded by the full absolute shadow of the quadratic remainder (†, V6). The bound on $LK(n_0)$ is the Neumann bound above, evaluated exactly. □

Proof of the four-copy part of Theorem 1.3. For $n \geq n_0$ the right-hand side $LK(n)(S_0+sS_1+s^2S_2)$ is decreasing in n, so the condition of Lemma 3.6 holds at every $n \geq n_0$ by Proposition 6.1. Hence $q_4(79/160, \cdot) \geq 0$ on rank-two operators at every $n \geq n_0$, which proves the four-copy part of Theorem 1.3. □

7. Five copies in every dimension

We prove the five-copy part of Theorem 1.3 by the argument of Section 6, with $t_0 = 9/20$, $n_0 = 10^{10}$ and five site factors in place of four. Only the relaxation, the constant $LK(n)$ and the numbers change.

The relaxation of Section 3 with $k = 5$ uses the three families X_{31}, X_{22}, X_{13} and the equalities of Section 3.4, but only partial-transpose blocks: neither coupled Gram block is needed. The cuts are those of Section 3.3, except that the cut $\{1, 3\}$ of X_{22} enters only through 465 of its block types. These are the types that the optimal pseudo-moment of the relaxation without this cut violates most, by more than 5% in relative terms, so they act as cutting planes. Without them the relaxation has negative value at t_0. With them it is strictly feasible at t_0 and has negative value at $t = 0.46$. With five site factors the exponent 4 in $LK(n)$ and in its Neumann bound becomes 5. The certificate is solved at t_0 with slack $\nu = 10^{-3}$.

Proposition 7.1. For the five-copy certificate, with the data of Table 3 and $s_0 = 1/n_0$,

$$\nu - LK(n_0)\big(S_0 + s_0S_1 + s_0^2S_2\big) \;\geq\; 9.78 \times 10^{-4} > 0.$$

Proof. As for Proposition 6.1 (†, V10). □

Table 3. The two limiting certificates. S_0 and S_1 are computed exactly and shown rounded; S_2, $LK(n_0)$ and the margin $\nu - LK(n_0)(S_0 + s_0S_1 + s_0^2S_2)$ are bounded as stated.

copies	t_0	n_0	ν	S_0	S_1	$S_2 \leq$	$LK(n_0) \leq$	**margin** $\geq$
4	79/160	1.25×10^9	10^{-4}	8.800×10^{-7}	8221.29	8.09×10^9	2.7555557	7.94×10^{-5}
5	9/20	10^{10}	10^{-3}	2.2256×10^{-10}	77278.70	1.1540×10^{12}	2.7555556	9.78×10^{-4}

As in Section 6, Proposition 7.1 gives $q_5(9/20, \cdot) \geq 0$ on rank-two operators at every $n \geq n_0$, which proves the five-copy part of Theorem 1.3.

8. Four and five qutrit copies

We prove Theorem 1.4. It suffices to show

$$q_4(4979/10000, C) \geq 0 \quad \text{on } (\mathbb{C}^3)^{\otimes 4}, \qquad q_5(47/100, C) \geq 0 \quad \text{on } (\mathbb{C}^3)^{\otimes 5},$$

for every C of rank at most two. Both follow from exact certificates in the slack form of Lemma 3.6, built at $d = 3$ for the relaxation of Section 3 with $k = 4$ and $k = 5$.

For four copies we use the complete four-replica relaxation: the five families $X_{40}, X_{31}, X_{22}, X_{13}, X_{04}$, all Gram classes of Section 3.3, and the equalities of Section 3.4. Every block of the certificate at $t = 4979/10000$ is positive semidefinite, and its residual sums are computed exactly. The slack is $\nu = 1.148 \times 10^{-5}$, against $LK \sum_f \sum_o |R_f(o)| = 1.86 \times 10^{-12}$, with $L = (2 \cdot 3^4)^4$ and $K = (131/1440)^4\,(31/180)$ (†, V7). Within this relaxation the threshold is about 0.49793. The smaller relaxation without X_{40}, X_{04} and their Gram classes reaches about 0.49701.

For five copies the coupled Gram class alone suffices, together with the equalities of Section 3.4. For the certificate at $t = 47/100$ the slack is $\nu = 2.006 \times 10^{-3}$, against $LK \sum_f \sum_o |R_f(o)| = 3.51 \times 10^{-9}$, with $L = (2 \cdot 3^5)^4$ and $K = (131/1440)^5\,(31/180)$ (†, V8).

Proposition 8.1. For every C of rank at most two, $q_4(4979/10000, C) \geq 0$ on $(\mathbb{C}^3)^{\otimes 4}$ and $q_5(47/100, C) \geq 0$ on $(\mathbb{C}^3)^{\otimes 5}$.

Proof. The certificates satisfy the hypothesis of Lemma 3.6, and their blocks are of the kinds covered by Lemma 3.2 (†, V7–V9). □

Theorem 1.4 follows from Proposition 8.1.

9. Many copies

For more copies we combine the inequalities proved so far. Each of them can be applied to disjoint groups of copies, and averaging over the positions of the groups turns it into a linear inequality in averaged partial-trace norms. For $C \neq 0$ of rank at most two on $(\mathbb{C}^d)^{\otimes k}$ put

$$a_j(C) = \binom{k}{j}^{-1} \sum_{|J|=j} \frac{\|\operatorname{Tr}_J C\|_F^2}{\|C\|_F^2} \qquad (0 \le j \le k),$$

so that $a_0 = 1$ and $q_k(t, C) = \|C\|_F^2 \sum_{j=0}^k \binom{k}{j}(-t)^j a_j(C)$. We call $(a_0(C), \dots, a_k(C))$ the profile of C.

Lemma 9.1. Let $f(X) = \sum_{J \subseteq \{1,\dots,m\}} c_J \|\operatorname{Tr}_J X\|_F^2$ be nonnegative for every operator X of rank at most two on every product $H_1 \otimes \cdots \otimes H_m$ of finite-dimensional spaces. Let C be an operator of rank at most two on a product $H_1 \otimes \cdots \otimes H_k$ of finite-dimensional spaces, let $g_1, \dots, g_m \subseteq \{1, \dots, k\}$ be disjoint and nonempty, and put $g_J = \bigcup_{i \in J} g_i$. *(a)* $\sum_J c_J \|\operatorname{Tr}_{g_J} C\|_F^2 \ge 0$. *(b)* If $R \subseteq \{1, \dots, k\}$ is nonempty and disjoint from all g_i, then $\sum_J c_J \big(\|\operatorname{Tr}_{g_J} C\|_F^2 + \|\operatorname{Tr}_{g_J \cup R} C\|_F^2\big) \ge 0$.

Proof. (a) Let W be the set of factors outside $g_1 \cup \cdots \cup g_m$, and write $C = \sum_{w,w'} C_{ww'} \otimes |w\rangle\langle w'|$ in a product basis of the factors in W. Each $C_{ww'} = (I \otimes \langle w|)\, C\, (I \otimes |w'\rangle)$ has rank at most two, and it acts on the product of the groups, each group taken as one factor. No factor in W is traced, so $\|\operatorname{Tr}_{g_J} C\|_F^2 = \sum_{w,w'} \|\operatorname{Tr}_{g_J} C_{ww'}\|_F^2$ for every J, and the sum in (a) equals $\sum_{w,w'} f(C_{ww'}) \ge 0$.

(b) Let D be the dimension of the factors in R taken together, and write $C = \sum_{x,y} |x\rangle\langle y| \otimes C_{xy}$ in a basis of these factors. For a unit vector ξ put $C_\xi = (\langle \xi| \otimes I)\, C\, (|\xi\rangle \otimes I) = \sum_{x,y} \overline{\xi_x}\, \xi_y\, C_{xy}$, an operator of rank at most two on the other factors. For the uniform measure on unit vectors, $\mathbb{E}\, \overline{\xi_x}\, \xi_y\, \xi_{x'}\, \overline{\xi_{y'}} = (\delta_{xy}\delta_{x'y'} + \delta_{xx'}\delta_{yy'})/(D(D+1))$ [CS06]. Hence, for every set S of factors disjoint from R,

$$D(D+1)\, \mathbb{E}\, \|\operatorname{Tr}_S C_\xi\|_F^2 = \Big\| \sum_x \operatorname{Tr}_S C_{xx} \Big\|_F^2 + \sum_{x,y} \|\operatorname{Tr}_S C_{xy}\|_F^2 = \|\operatorname{Tr}_{S \cup R} C\|_F^2 + \|\operatorname{Tr}_S C\|_F^2.$$

Applying (a) to each C_ξ and averaging over ξ gives (b). □

The inequality in (b) is again of the form required of f, with R as one more factor. So (b) may be applied repeatedly, with disjoint sets $R_1, \dots, R_p$.

Now let C act on $(\mathbb{C}^d)^{\otimes k}$, and place the groups g_i and the sets R_l uniformly at random among the disjoint subsets of $\{1, \dots, k\}$ with prescribed sizes $r_i = |g_i|$ and $s_l = |R_l|$. Every union of some of these sets is then a uniformly random subset of its size. The expectation of each norm $\|\operatorname{Tr}_S C\|_F^2$ that occurs is therefore $a_{|S|}(C)\, \|C\|_F^2$, and the inequality becomes $\sum_j \operatorname{row}_j\, a_j(C) \ge 0$, where row_j is the coefficient of S^j in

$$\operatorname{row}(S) = \Big(\sum_J c_J\, S^{\sum_{i \in J} r_i} \Big) \prod_{l=1}^{p} \big(1 + S^{s_l}\big).$$

We call $\sum_i r_i + \sum_l s_l$, which is at most k, the size of the row.

As inputs we use the following inequalities for operators X of rank at most two on products of finite-dimensional spaces. The theorems that are stated for equal local dimensions extend to unequal ones by the embedding of Lemma 2.3(a).

- (I1) $|\operatorname{Tr} X|^2 \le 2\|X\|_F^2$, because $|\operatorname{Tr} X| \le \|X\|_1 \le \sqrt{2}\, \|X\|_F$ for rank at most two.
- (I2) $\|\operatorname{Tr}_1 X\|_F^2 + \|\operatorname{Tr}_2 X\|_F^2 \le 2\|X\|_F^2 + \frac{1}{2}|\operatorname{Tr} X|^2$, which is $q_2(1/2, X) \ge 0$ [FGP26, FHPV26, SC26, BGH26].
- (I3) $\|\operatorname{Tr}_1 X\|_F^2 - \|\operatorname{Tr}_2 X\|_F^2 \le 2\|X\|_F^2 - \frac{1}{2}|\operatorname{Tr} X|^2$ [CR25, Theorem 2].
- (I4) $q_3(1/2, X) \ge 0$, which is Theorem 1.2.
- (I5) $q_4(79/160, X) \ge 0$ and (I6) $q_5(9/20, X) \ge 0$, from Sections 6 and 7.

On groups of sizes $r_1, r_2, \dots$ the polynomials $\sum_J c_J S^{\sum_{i \in J} r_i}$ of these inputs are $2 - S^{r_1}$, $2 - S^{r_1} - S^{r_2} + \frac{1}{2} S^{r_1 + r_2}$, $2 - S^{r_1} + S^{r_2} - \frac{1}{2} S^{r_1 + r_2}$ and $\prod_i (1 - t S^{r_i})$ with $t = 1/2$, $79/160$ and $9/20$. By (I1) and Lemma 9.1(a), every profile also satisfies $0 \le a_j \le 2$.

Fix k and $X > 0$, and put $b_j = \binom{k}{j}(-X/k)^j$, so that $q_k(X/k, C) = \|C\|_F^2 \sum_j b_j a_j(C)$. A certificate consists of rows $\operatorname{row}^{(i)}$ of size at most k and rationals $y_i \ge 0$. With $r = b - \sum_i y_i \operatorname{row}^{(i)}$,

$$\sum_j b_j a_j = \sum_i y_i \sum_j \operatorname{row}_j^{(i)} a_j + \sum_j r_j a_j \;\ge\; r_0 + 2 \sum_{j \ge 1} \min(0, r_j),$$

because every row is nonnegative on profiles, $a_0 = 1$ and $0 \le a_j \le 2$. We call the right-hand side the slack of the certificate. If it is nonnegative, then $q_k(X/k, C) \ge 0$ for every C of rank at most two on $(\mathbb{C}^d)^{\otimes k}$.

Theorem 9.2. Let $d \ge 2$ and let C be an operator of rank at most two on $(\mathbb{C}^d)^{\otimes k}$. Then $q_k(11/(5k), C) \ge 0$ for every $k \ge 6$, and $q_k(56/(25k), C) \ge 0$ for every $k \ge 9$.

Proof. We describe the case $X = 11/5$; the numbers for $X = 56/25$ follow in brackets (†, V11).

- For $6 \le k \le 11$ [$9 \le k \le 13$] there is an exact certificate for each k.
- For $12 \le k \le K$ with $K = 1010$ [$14 \le k \le K$ with $K = 5450$] we use only rows of size at most $J = 12$ [14], which Lemma 9.1 makes valid for every $k \ge J$. A single limit certificate is built for the objective $(-X)^j/j! = \lim_{k\to\infty} b_j$, truncated at degree J, and its slack is computed exactly at every such k. Where it is negative, a certificate for that k replaces it. The coefficients of degree $j > J$, which no row reaches, are bounded through $\binom{k}{j}(X/k)^j \le X^j/j!$ and $0 \le a_j \le 2$.
- For $k > K$ we use $\left|\binom{k}{j}(X/k)^j - X^j/j!\right| \le \frac{X^j}{j!}\,\frac{j(j-1)}{2k}$, where the difference has the favourable sign for odd j. The slack at k is therefore at least the slack of the limit certificate for the limiting objective, minus the bound for the degrees above J, minus E_2/k with $E_2 = \sum_{2\le j\le J,\ j \text{ even}} X^j/(j-2)!$. The choice of K keeps this positive.

The smallest slack over all k is 1.80×10^{-5} [8.8×10^{-7}]. □

For $k = 6$ and $k = 7$ the linear program gives the slightly larger thresholds $0.368683\ldots$ and $0.318076\ldots$, which are roots of explicit polynomials and carry exact certificates (†, V12). Theorem 1.5 follows from Theorem 9.2.

The constant $11/5$ is about 4.6 times $\log\varphi \approx 0.481$, the common limit of $k\eta_k$ and $k\gamma_k$ for the bounds of [QGWG24] and [BGH26]. As k grows, the constants of Theorem 9.2 can be pushed up to $9/4 = 5 \cdot \frac{9}{20}$, a limit set by the five-copy input, but not beyond.

Proposition 9.3. *(a)* For every $\varepsilon \in (0, 1/200]$ there is K_ε such that $q_k(t, C) \ge 0$ for every $k \ge K_\varepsilon$, every $t \in [0,\, 9(1-\varepsilon)/(4k)]$, every d and every C of rank at most two on $(\mathbb{C}^d)^{\otimes k}$. For $10^{-4} \le \varepsilon \le 1/200$ one can take $K_\varepsilon = 47$. *(b)* No certificate built from the rows of Lemma 9.1 and the inputs (I1)–(I6) proves $q_k(t, \cdot) \ge 0$ for any $t > 9/(4k)$.

Proof. (a) Put $\tau = 9/20$, $\rho = 1 - \varepsilon$ and $x = 5\tau\rho$. As formal power series in S,

$$\Big(1 - \frac{xS}{k}\Big)^k = \varepsilon + \rho\,(1 - \tau S)^5 E_k(S), \qquad E_k(0) = 1,$$

and the coefficient of S in $\log E_k = \sum_{r\ge1} \beta_r S^r$ vanishes because $x = 5\tau\rho$. Expanding $e^{\beta S^r} = \sum_{i\ge0} e^{-\beta}\frac{\beta^i}{i!}(1 + S^r)^i$ writes E_k, modulo S^{k+1}, as a mixture of products $\prod_r (1+S^r)^{i_r}$ with weights $\prod_r e^{-\beta_r}\beta_r^{i_r}/i_r!$. These weights are nonnegative when every $\beta_r \ge 0$, and this holds for $2 \le r \le k$ whenever $k \ge 40$ and $\varepsilon \le 1/200$. We check it in exact rational arithmetic for $r \le 300$ and with an explicit bound beyond (†, V13). Each term with $\sum_r r i_r \le k-5$ is the row of (I6) on five single copies with i_r sets R_l of size r. A Chernoff bound shows that the remaining terms change $\sum_j b_j a_j$ by at most $21177\,(8/5)^{-k}$, using $0 \le a_j \le 2$. Hence $\sum_j b_j a_j \ge \varepsilon - 21177\,(8/5)^{-k}$ at $t = x/k$, which is positive for large k (†, V13). Lemma 2.3(b) covers the smaller values of t.

(b) The vector $a = (1, \frac{4}{9}, 0, \ldots, 0)$ satisfies every row. At this point only the constant and linear coefficients of a row contribute, and since every base polynomial has a positive constant coefficient, a factor $1 + S^s$ can only increase the value. With n_1 groups of size one, the base polynomials of (I6), (I5) and (I4) are at least $1 - \frac{9}{20}\cdot\frac{4}{9}n_1 = 1 - \frac{n_1}{5} \ge 0$, $1 - \frac{79}{160}\cdot\frac{4}{9}\cdot 4 > 0$ and $1 - \frac{1}{2}\cdot\frac{4}{9}\cdot 3 > 0$, and those of (I1)–(I3) are at least $2 - \frac{8}{9} > 0$. The vector also satisfies $0 \le a_j \le 2$. But there $\sum_j b_j a_j = 1 - \frac{4}{9}kt < 0$ for $t > 9/(4k)$, so no certificate exists. □

10. Discussion and open problems

Wang's theorem [Wan26] transfers k-copy undistillability at local dimension m to all $d \ge m$, at the parameter $\Lambda_{m,d}(1/2) \to (m-2)/(2m-1)$ as $d \to \infty$. For three copies this transfer is no longer needed, and for four copies the limiting certificate of Section 6 does far better: lifting the qutrit result of Theorem 1.4 yields, as $d \to \infty$, only the parameter $4937/25021 \approx 0.197$, whereas Theorem 1.3 reaches $79/160$ in every dimension.

From four copies on the copy thresholds remain open. For k copies the open range runs from $-1/2$ to the bound of Table 1, and Proposition 9.3 narrows it for $k \ge 47$. A negative answer at some k would give the first Werner state that is NPT and undistillable from one copy, yet distillable from finitely many copies.

Remark 10.1 (the endpoint for four copies). At the endpoint $t = 1/2$ and $d = 3$ the value of the four-copy relaxation, computed in floating point, is -2.61×10^{-3} with the three families of Section 3, -1.87×10^{-3}

with the second coupled Gram block added, and -1.31×10^{-3} for the complete four-replica relaxation, so by these computations it cannot certify $q_4(1/2, \cdot) \geq 0$. The two-replica profile $\left(\mathbb{E}\| \operatorname{Tr}_J C\|_F^2 / \|C\|_F^2\right)_{|J|=0,\ldots,4}$ of the optimal pseudo-moment is within 1.03×10^{-3} of the profile of a physical zero $P \otimes |u\rangle\langle v|$, and local minimization of $q_4(1/2, \cdot)$ started near this point finds no negative value, so the negative values most likely come from a gap of the relaxation, not from a negative value of q_4. A six-replica relaxation, with an estimated 10^9 orbit coordinates at $d = 3$, is out of reach, so the method of this paper does not settle four copies at the endpoint.

Data and code availability

The certificates, verifiers and Lean formalizations are in the paper's Zenodo record, doi:10.5281/zenodo.23604343, one package for each result and for each Lean formalization, each with a README. A supplement in the same record describes further checks, among them exact certificates at fixed $d \leq 16$ and an independent three-copy certificate for $d \geq 17$; their code and data are in the package `release_ep3_checks`.

References

[Ano26] Anonymous. *Three-copy undistillability of the boundary qutrit Werner state.* Version 1.1.0-candidate, Zenodo, 2026. doi:10.5281/zenodo.23134454.

[BGH26] K. Bharti, R. Gajjala and T. Haug. *Two-copy nondistillability of Werner states: sharp partial-trace inequalities and finite-copy extensions.* arXiv:2607.24479, 2026.

[CR25] P. Costa Rico. *New partial trace inequalities and distillability of Werner states.* Lett. Math. Phys. **115**, 47 (2025). doi:10.1007/s11005-025-01935-y. arXiv:2310.05726.

[CS06] B. Collins and P. Śniady. *Integration with respect to the Haar measure on unitary, orthogonal and symplectic group.* Commun. Math. Phys. **264**, 773–795 (2006). doi:10.1007/s00220-006-1554-3.

[DCLB00] W. Dür, J. I. Cirac, M. Lewenstein and D. Bruß. *Distillability and partial transposition in bipartite systems.* Phys. Rev. A **61**, 062313 (2000).

[DSS+00] D. P. DiVincenzo, P. W. Shor, J. A. Smolin, B. M. Terhal and A. V. Thapliyal. *Evidence for bound entangled states with negative partial transpose.* Phys. Rev. A **61**, 062312 (2000).

[FGP26] J. Fu, L. Gao and S.-J. Park. *A solution to 2-copy distillability of Werner states.* arXiv:2607.21367, 2026.

[FHPV26] T. C. Fraser, F. Huber, B. Pozsgay and I. Vona. *On the two-copy distillability of Werner states and a new partial trace inequality.* arXiv:2607.24309, 2026.

[HH99] M. Horodecki and P. Horodecki. *Reduction criterion of separability and limits for a class of distillation protocols.* Phys. Rev. A **59**, 4206–4216 (1999).

[HHH98] M. Horodecki, P. Horodecki and R. Horodecki. *Mixed-state entanglement and distillation: Is there a "bound" entanglement in nature?* Phys. Rev. Lett. **80**, 5239–5242 (1998).

[HRZ22] P. Horodecki, Ł. Rudnicki and K. Życzkowski. *Five open problems in quantum information theory.* PRX Quantum **3**, 010101 (2022).

[QGWG24] S.-Y. Qi, G. Gupur, Y.-C. Wu and G.-P. Guo. *Nonpositive-transpose entanglement and bound entanglement: From distillability sets to inequalities and multivariable insights.* Phys. Rev. A **110**, 012406 (2024). doi:10.1103/PhysRevA.110.012406. arXiv:2402.18037.

[SC26] Z. Song and L. Chen. *A partial-trace matrix inequality and Werner-state distillability.* arXiv:2607.23416, 2026.

[SST01] P. W. Shor, J. A. Smolin and B. M. Terhal. *Nonadditivity of bipartite distillable entanglement follows from conjecture on bound entangled Werner states.* Phys. Rev. Lett. **86**, 2681–2684 (2001).

[Tom26b] T. S. Tomar. *Equality cases and every-copy results for the Werner endpoint inequality.* Zenodo, 2026. doi:10.5281/zenodo.23718037.

[Wan26] X. Wang. *Dimension lifting of finite-copy Werner undistillability.* Zenodo, 2026. doi:10.5281/zenodo.23178611.

[Wat04] J. Watrous. *Many copies may be required for entanglement distillation.* Phys. Rev. Lett. **93**, 010502 (2004). doi:10.1103/PhysRevLett.93.010502.

[Wer89] R. F. Werner. *Quantum states with Einstein–Podolsky–Rosen correlations admitting a hidden-variable model.* Phys. Rev. A **40**, 4277–4281 (1989).

[WZ26] T. Wu and Q. Zou. *Sharp Plücker geometry for three-copy Werner distillation.* arXiv:2608.02647, 2026.

Appendix A. Computations and formal proofs

A.1 Lean formalizations

Both formalizations prove matrix inequalities, and both derive the Werner statements from them with Costa Rico's criterion (Theorem 2.1) as a hypothesis.

For $3 \le d \le 8$, $\mathrm{EP}_3(d)$ is also proved in Lean 4, from the compact certificates of the three-copy package. The validity of such certificates is proved once for all d, by a projection argument that avoids the Haar measure, and Lean's kernel checks the data of each certificate, including identity (3.2). Every theorem depends only on Lean's standard axioms, so the proof is checked by the kernel alone. The case $d \ge 9$ is not formalized.

The four-copy qutrit bound of Theorem 1.4 is formalized as well, with a larger trusted base. Lean proves that $q_4(t, C) \ge 0$ for every operator C of rank at most two on $(\mathbb{C}^3)^{\otimes 4}$, for $t = 4979/10000$ and for $t = 497/1000$, from the certificates of Section 8, and four-copy undistillability of $\rho(3, \alpha)$ for $\alpha \ge -0.4979$. The soundness of certificates whose identity holds up to residuals within the slack, the well-formedness and positive semidefiniteness of every multiplier, the class structure, the data bounds and the slack inequality are checked by Lean's kernel. The identity itself is checked by compiled code (`native_decide`), so the trusted base also includes the Lean compiler and its runtime, including big-integer arithmetic, and the compiled implementations that the evaluated code calls. Beyond Lean's standard axioms, the theorems depend only on these evaluations. A kernel-only version is future work, and the four-copy bounds in every dimension and the five-copy results are not formalized.

A.2 Table of computations

Table 2 lists the computer-verified steps of the proofs, each in exact or ball arithmetic; Section S1 of the supplement describes every row in words. Floating-point computations serve only as independent checks and as evidence. "Exact" means rational or integer arithmetic. Rows V2–V5 repeat checks of the three-copy package. The packages and their READMEs also contain independent checks, such as end-to-end tests of the certificates of Sections 6 and 7.

Table 2. Computer-verified steps of the proofs.

ID	Statement checked	Method	Used in
V1	$J(d) = D(d)C$ with C independent of d; Lemma 5.1 by brute force	exact	Sec. 5.1
V2	Diagram data of the package: labels, scaling, degree bounds, multiplier classes and equality groups	exact	Sec. 5.2
V3	Proposition 5.4: the base certificate and the first correction	exact	Prop. 5.4
V4	Proposition 5.4: the witness $W(s)$	exact, multi-modular	Prop. 5.4
V5	Proposition 5.4: the second correction	midpoint-radius arithmetic	Prop. 5.4
V6	Proposition 6.1: the residual sums, $LK(n_0)$, the margin and the admissibility of the equality rows	exact, multi-modular	Sec. 6
V7	Four qutrit copies: positive semidefiniteness, residual sums and the slack condition of Lemma 3.6 for six certificates	exact	Sec. 8
V8	Five qutrit copies: the same for two certificates	exact	Sec. 8
V9	An independent audit of V7 and V8	exact, with floating-point cross-checks	Sec. 8
V10	Proposition 7.1: the residual sums, $LK(n_0)$, the margin and the admissibility of the equality rows, with a second verifier	exact, multi-modular	Sec. 7
V11	Theorem 9.2: the slack certificates for $X = 11/5$ and $X = 56/25$, checked twice	exact rational	Sec. 9

V12	The thresholds at $k = 6, 7$: exact parametric certificates	exact	Sec. 9
V13	Proposition 9.3: $\beta_r \geq 0$ and the Chernoff constant	exact and interval arithmetic	Sec. 9