Supplementary Information.

A Preliminaries of Algebraic geometry

Here, let us briefly introduce notation and concepts of algebraic geometry. Readers can find a more comprehensive introduction in [50, 77]. We denote the set of non-negative integers by $\mathbb{N} = \{0, 1, 2, \cdots\}$.

A.1 Projective space

Definition 8 For $d \in \mathbb{N}$, a projective d-space $\mathbb{P}^d$ is the set of equivalent classes $[x_0 : \cdots : x_d]$ of vectors $(x_0, \cdots, x_d) \in \mathbb{C}^{d+1} \setminus \{0\}$ under the equivalence relation given by $(x_0, \cdots, x_d) \sim (y_0, \cdots, y_d)$ if $(x_0, \cdots, x_d) \propto (y_0, \cdots, y_d)$.

Definition 9 A (linear) subspace $\mathcal{V}$ in the projective space $\mathbb{P}^{d-1}$ is defined as the zero set of a family of homogeneous polynomials in $\mathbb{C}[x_0, \cdots, x_{d-1}]$ of degree at most 1.

For example, $\emptyset$ and $\mathbb{P}^{d-1}$ are subspaces. We can verify that for a non-empty subspace $(\emptyset \neq)\mathcal{V} \subseteq \mathbb{P}^{d-1}$, there exists a rank-$d'(\geq 1)$ matrix $V : \mathbb{C}^{d'} \to \mathbb{C}^d$ such that $\mathcal{V} = V\mathbb{P}^{d'-1}$. Note that the intersection of a family of subspaces is a subspace.

Definition 10 The (linear) span $\mathrm{span}\,(\mathbb{E})$ of a subset $\mathbb{E} \subseteq \mathbb{P}^{d-1}$ is the minimum subspace $\mathcal{V}$ containing $\mathbb{E}$.

An alternative definition of the span is given as follows: For a subset $\mathbb{E} \subseteq \mathbb{P}^{d-1}$, $\mathrm{span}\,(\mathbb{E})$ is the zero set of a family of homogeneous polynomials in $\mathbb{C}[x_0, \cdots, x_{d-1}]$ of degree at most 1 that vanishes on $\mathbb{E}$.

Let $p : \mathbb{C}^d \setminus \{0\} \to \mathbb{P}^{d-1}$ be the canonical projection from the ambient complex vector space into a projective space. We can verify that $p^{-1}(\mathrm{span}\,(\mathbb{E})) \cup \{0\} = \mathrm{span}\,(\{|\phi\rangle : |\phi\rangle \in p^{-1}(\mathbb{E})\})$.

While there is no standard notion of a tensor product of projective spaces, we use the tensor product notation

$$[x_0 : x_1 : \cdots : x_{d-1}] \otimes [y_0 : y_1 : \cdots : y_{d'-1}] = [x_0 y_0 : x_0 y_1 : \cdots : x_1 y_0 : x_1 y_1 : \cdots : x_{d-1} y_{d'-1}]$$

to denote the image of the Segre embedding from $\mathbb{P}^{d-1} \times \mathbb{P}^{d'-1}$ into $\mathbb{P}^{dd'-1}$.

A.2 Algebraic set in projective space

Definition 11 A (commutative) ring S is called a graded ring if $S = \oplus_{n\in\mathbb{N}} S_n \left(= \left\{\sum_{n\in N} f_n : f_n \in S_n, |N| < \infty\right\}\right)$, where each S_n is an abelian group and $S_n \cdot S_m \subseteq S_{m+n}$ for any $m, n \in \mathbb{N}$. An element of S_n is called a homogeneous element of degree n.

For example, the polynomial ring $\mathbb{C}[x_0, x_1, \cdots, x_{d-1}]$ in (finite) d variables over the field $\mathbb{C}$ is a graded ring, where S_n is the set consisting of 0 and homogeneous polynomials with degree n. Note that S_n is isomorphic to the set of linear functionals $\langle f| : \vee_n \mathbb{C}^d \to \mathbb{C}$ via the isomorphism $f(|x\rangle) = \langle f|(|x\rangle^{\otimes n})$, where $f \in S_n$ and $|x\rangle = (x_0, x_1, \cdots, x_{d-1})^T$ [33].

Definition 12 An ideal $\mathfrak{a} \subseteq S$ of a graded ring $S = \oplus_{n\in\mathbb{N}} S_n$ is a homogeneous ideal if $\mathfrak{a} = \oplus_{n\in\mathbb{N}}(\mathfrak{a} \cap S_n)$.

Since $\mathfrak{a} \supseteq \oplus_{n\in\mathbb{N}}(\mathfrak{a} \cap S_n)$ holds for any ideal $\mathfrak{a}$, the condition that $\mathfrak{a}$ be homogeneous can equivalently be stated as follows: for any $f \in \mathfrak{a}$ and any $n \in \mathbb{N}$, the homogeneous element of f with degree n also belongs to $\mathfrak{a}$. The following facts are known:

- An ideal $\mathfrak{a}$ is homogeneous if and only if it is generated by a set of homogeneous elements, i.e., $\mathfrak{a} = \langle \{f_\alpha\}_{\alpha\in A} \rangle$, where $f_\alpha \in S_{n_\alpha}$.
- If $\mathfrak{a}$ and $\mathfrak{b}$ are homogeneous ideals, $\mathfrak{a} + \mathfrak{b}$, $\mathfrak{a}\mathfrak{b}$, $\mathfrak{a} \cap \mathfrak{b}$, and $\sqrt{\mathfrak{a}}$ are homogeneous ideals.

Definition 13 The zero set of a family $T \subseteq \mathbb{C}[x_0, \cdots, x_{d-1}]$ of homogeneous polynomials is defined by $Z(T) := \{x \in \mathbb{P}^{d-1} : \forall f \in T, f(x) = 0\}$. For a homogeneous ideal $\mathfrak{a}$, we define $Z(\mathfrak{a}) := Z(T)$, where T is the set of homogeneous elements in $\mathfrak{a}$.

Definition 14 $\mathbb{E} \subseteq \mathbb{P}^{d-1}$ is an algebraic set if there exists a family T of homogeneous polynomials such that $\mathbb{E} = Z(T)$.

Definition 15 The Zariski topology on $\mathbb{P}^{d-1}$ is defined by taking the closed sets to be the algebraic sets.

Definition 16 A nonempty subset $\mathbb{E}$ of a topological space X is irreducible if it cannot be decomposed as a union $\mathbb{E} = \mathbb{E}_1 \cup \mathbb{E}_2$ of two proper subsets, each one of which is closed in $\mathbb{E}$.

Definition 17 An irreducible algebraic set in $\mathbb{P}^{d-1}$ with respect to the Zariski topology is called a projective variety.

Definition 18 For a subset $\mathbb{E}$ of $\mathbb{P}^{d-1}$, the homogeneous ideal $I(\mathbb{E})$ of $\mathbb{E}$ is defined by $\langle \{f \in \cup_{n\in\mathbb{N}} S_n : \forall |x\rangle \in \mathbb{E}, f(|x\rangle) = 0\}\rangle$, i.e., the ideal generated by homogeneous polynomials that vanishes on $\mathbb{E}$.

The following facts are known:

- An algebraic set $\mathbb{E} \subseteq \mathbb{P}^{d-1}$ is irreducible if and only if $I(\mathbb{E})$ is a prime ideal [50, Exercise 2.4].
- An algebraic set $\mathbb{E} \subseteq \mathbb{P}^{d-1}$ can be uniquely decomposed into irreducible components; i.e., there exists a unique finite family $\{\mathbb{I}_k\}_{k\in K}$ of projective varieties such that $\mathbb{E} = \cup_{k\in K}\mathbb{I}_k$ and $\mathbb{I}_k \not\subseteq \mathbb{I}_{k'}$ for any $k \neq k'$ [50, Exercise 2.5].
- Any nonempty subspace in $\mathbb{P}^{d-1}$ is a projective variety.
- For a subset $\mathbb{E}$ of $\mathbb{P}^{d-1}$, $Z(I(\mathbb{E})) = \overline{\mathbb{E}}$ [50, Exercise 2.3].
- A subset $\mathbb{E}$ of a topological space X is irreducible if and only if its closure $\overline{\mathbb{E}}$ is irreducible [50, Example 1.1.4].
- The set $\{\otimes_{n=1}^N |\phi_n\rangle : |\phi_n\rangle \in \mathbb{P}^{d_n-1}\} = p(\mathbb{S}\left(\mathbb{C}^{d_1} : \cdots : \mathbb{C}^{d_N}\right) \setminus \{0\})$ is a projective variety in $\mathbb{P}^{d_1\cdots d_N-1}$ [50, Exercise 2.14].
- Any nonempty open set $\mathbb{V}$ in an irreducible set $\mathbb{E}$ is irreducible [50, Example 1.1.3].

The following fact is also known (in a different notation) [33]. For completeness, we provide a proof.

Proposition 5 *For a subset $\mathbb{E} \subseteq \mathbb{P}^{d-1}$ and positive integer m, $|x\rangle \in Z(I_m(\mathbb{E}))$ if and only if $|x\rangle^{\otimes m} \in \vee_m\mathbb{E} := \mathrm{span}\left(\{|x\rangle^{\otimes m} : |x\rangle \in \mathbb{E}\}\right)$.*

In the proof, we use the following lemma.

Lemma 1 *For a subset $\mathbb{E}$ of $\mathbb{P}^{d-1}$ and $m \in \mathbb{N}$, $Z(I_m(\mathbb{E})) = Z(\langle I(\mathbb{E}) \cap S_m\rangle)$.*

Proof Since $I_m(\mathbb{E}) \supseteq I(\mathbb{E}) \cap S_m$, we find $Z(I_m(\mathbb{E})) \subseteq Z(\langle I(\mathbb{E}) \cap S_m\rangle)$. To complete the proof, we show that $\forall |x\rangle \in Z(\langle I(\mathbb{E}) \cap S_m\rangle), \forall f \in I_m(\mathbb{E}), f(|x\rangle) = 0$. This is equivalent to $\forall |x\rangle \in Z(\langle I(\mathbb{E}) \cap S_m\rangle), \forall f \in \cup_{n=0}^m S_m, (\forall |y\rangle \in \mathbb{E}, f(|y\rangle) = 0) \Rightarrow f(|x\rangle) = 0$. For all $|x\rangle \in Z(\langle I(\mathbb{E}) \cap S_m\rangle)$ and for all $f \in S_n$ such that $0 \leq n \leq m$ and $\forall |y\rangle \in \mathbb{E}, f(|y\rangle) = 0$, there exists $g \in S_{m-n}$ such that $g(|x\rangle) \neq 0$. Since $fg \in I(\mathbb{E}) \cap S_m$, $f(|x\rangle)g(|x\rangle) = 0$. Thus, $f(|x\rangle) = 0$. □

Proof of Proposition 5

$$\begin{aligned}
& |x\rangle \in Z(I_m(\mathbb{E})) = Z(\langle I(\mathbb{E}) \cap S_m\rangle) && (53)\\
\Leftrightarrow\ & \forall f \in I(\mathbb{E}) \cap S_m, f(|x\rangle) = 0 && (54)\\
\Leftrightarrow\ & \forall f \in S_m, (\forall |x\rangle \in \mathbb{E}, f(|x\rangle) = 0) \Rightarrow f(|x\rangle) = 0 && (55)\\
\Leftrightarrow\ & \forall |f\rangle \in \vee_m\mathbb{C}^d, (\forall |x\rangle \in \mathbb{E}, \langle f|(|x\rangle^{\otimes m}) = 0) \Rightarrow \langle f|(|x\rangle^{\otimes m}) = 0 && (56)\\
\Leftrightarrow\ & \forall |f\rangle \in \mathbb{C}^{md}, (\forall |x\rangle \in \mathbb{E}, \langle f|(|x\rangle^{\otimes m}) = 0) \Rightarrow \langle f|(|x\rangle^{\otimes m}) = 0 && (57)\\
\Leftrightarrow\ & |x\rangle^{\otimes m} \in Z(I_1(\{|x\rangle^{\otimes m} : |x\rangle \in \mathbb{E}\})) = \mathrm{span}\left(\{|x\rangle^{\otimes m} : |x\rangle \in \mathbb{E}\}\right). && (58)
\end{aligned}$$

□

B Application of MFLCs in two qubits to unambiguous local state discrimination

Unambiguous state discrimination tries to distinguish without error quantum states that are not necessarily orthogonal. At a glance, this contradicts the nature of quantum mechanics. However, it is possible by allowing an "I don't know" outcome [78–84]. Since the non-orthogonal quantum states are at the heart of quantum cryptography, the possibility of unambiguous state discrimination is used in quantum cryptographic protocols [85].

In [6], Koashi et al. consider an unambiguous local-state discrimination of

$$\hat{\rho}_0 = |00\rangle\langle 00|,\ \hat{\rho}_1 = \frac{1}{2}\left(|{+}{+}\rangle\langle{+}{+}| + |{-}{-}\rangle\langle{-}{-}|\right), \tag{59}$$

where $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ under LOCC and SEP channels. To generalize the scenario of SEP channels, we examine unambiguous local discrimination of general two-qubit mixed states ρ_0 and ρ_1 by using a separable instrument. Formally, we construct a positive operator-valued measure (POVM) $\{M_0, M_1, M_2\} \subseteq \mathbf{SEP}\left(\mathbb{C}^2 : \mathbb{C}^2\right)$ such that

$$\mathrm{tr}\left[\rho_0 M_1\right] = \mathrm{tr}\left[\rho_1 M_0\right] = 0,\ \sum_{m=0}^{2} M_m = I. \tag{60}$$

By following [6], we focus on the success probability $\gamma_m := \mathrm{tr}\,[\rho_m M_m]$ of guessing ρ_m and analyze the maximum $P_{opt}^{(sep)}(\gamma_0)$ of γ_1 when γ_0 is given. Formally, $P_{opt}^{(sep)}(\gamma_0)$ is the maximum value of γ_1 when $\mathrm{tr}\,[\rho_0 M_0] = \gamma_0$ and Eqs. (60) are satisfied.

Eqs. (60) imply that

$$\mathrm{range}\,(M_1) \subseteq \mathcal{V}_0, \mathrm{range}\,(M_0) \subseteq \mathcal{V}_1, \tag{61}$$

where $\mathcal{V}_m$ is the orthogonal complement of $\mathrm{range}\,(\rho_m)$. This implies that M_0 (or M_1) is a convex combination of $|\Pi\rangle\langle\Pi|$, where $|\Pi\rangle$ is contained in the MFLC of $\mathbb{S}\left(\mathbb{C}^2 : \mathbb{C}^2\right) \cap \mathcal{V}_1$ (or $\mathbb{S}\left(\mathbb{C}^2 : \mathbb{C}^2\right) \cap \mathcal{V}_0$). Combined with Propositions 3, this fact makes it simpler to calculate $P_{opt}^{(sep)}(\gamma_0)$. For example, it is known that $P_{opt}^{(sep)}(\gamma_0)$ can be computed by using an SDP since $\mathbf{SEP}\left(\mathbb{C}^2 : \mathbb{C}^2\right) = \mathbf{PPT}\left(\mathbb{C}^2 : \mathbb{C}^2\right)$ [20]. We can obtain a simpler SDP by incorporating the constraints resulting from the MFLCs. Below, we demonstrate this simplification by using a specific class of ρ_0 and ρ_1.

Here, we consider

$$\begin{aligned} \rho_0 &= |00\rangle\langle 00|, &(62)\\ \rho_1 &= a|{+}{+}\rangle\langle{+}{+}| + c|{-}{-}\rangle\langle{-}{-}| + b|{+}{+}\rangle\langle{-}{-}| + b|{-}{-}\rangle\langle{+}{+}|, &(63)\end{aligned}$$

where $a \in (0,1)$, $c = 1-a$ and $b^2 < ac$. Note that $\mathrm{range}\,(\rho_1) = \mathrm{span}\left(\{|{+}{+}\rangle, |{-}{-}\rangle\}\right)$ under these conditions. We can show that $\mathcal{V}_0 = \mathrm{span}\left(\{|01\rangle, |10\rangle, |11\rangle\}\right)$ and $\mathcal{V}_1 = \mathrm{span}\left(\{|{+}{-}\rangle, |{-}{+}\rangle\}\right)$ through a straightforward calculation. By following the calculation in the proof of Proposition 3, we obtain their irreducible components, which coincide with their MFLCs:

$$\begin{aligned} \mathbb{S} \cap \mathcal{V}_0 &= (|1\rangle \otimes \mathbb{C}^2) \cup (\mathbb{C}^2 \otimes |1\rangle) &(64)\\ \mathbb{S} \cap \mathcal{V}_1 &= \mathrm{span}\left(\{|{+}{-}\rangle\}\right) \cup \mathrm{span}\left(\{|{-}{+}\rangle\}\right). &(65)\end{aligned}$$

Observe that the values $\mathrm{tr}\,[\rho_n M_m]$ and $\sum_{m=0}^{2} M_m$ do not change if we replace M_m by $\hat{M}_m = \frac{1}{4}(M_m + \overline{M}_m + P(M_m + \overline{M}_m)P)$ with the swap operator $P = \sum_{i,j} |ij\rangle\langle ji|$ since ρ_1, ρ_2 and I are invariant under swap and complex-conjugation. By considering the MFLCs and the invariance of $\hat{M}_m$ under swap and complex conjugation, we can let

$$\begin{aligned} \hat{M}_0 &= p(|{+}{-}\rangle\langle{+}{-}| + |{-}{+}\rangle\langle{-}{+}|) &(66)\\ \hat{M}_1 &= |1\rangle\langle 1| \otimes S + S \otimes |1\rangle\langle 1| + q|1\rangle\langle 1| \otimes |1\rangle\langle 1|, &(67)\end{aligned}$$

where $p \geq 0$, $q \in \mathbb{R}$, $S^T = S$, $S \in \mathbf{Pos}\left(\mathbb{C}^2\right)$, and $S + q|1\rangle\langle 1| \in \mathbf{Pos}\left(\mathbb{C}^2\right)$. Since $\mathbf{Pos}\,(\mathcal{H})$ is convex, $S, S + q|1\rangle\langle 1| \in \mathbf{Pos}\left(\mathbb{C}^2\right)$ implies $S + \frac{q}{2}|1\rangle\langle 1| \in \mathbf{Pos}\left(\mathbb{C}^2\right)$. Thus, we can let

$$\hat{M}_1 = |1\rangle\langle 1| \otimes S + S \otimes |1\rangle\langle 1|, \tag{68}$$

where $S^T = S$ and $S \in \mathbf{Pos}\left(\mathbb{C}^2\right)$ without loss of generality.

By using these parameterizations, we can represent the success probability γ_n of guessing ρ_n as

$$\gamma_0 = \mathrm{tr}\left[\rho_0 \hat{M}_0\right] = \frac{p}{2}, \quad \gamma_1 = \mathrm{tr}\left[\rho_1 \hat{M}_1\right] = \mathrm{tr}\,[S\sigma], \tag{69}$$

where $\sigma = a|+\rangle\langle +| + c|-\rangle\langle -| + b|+\rangle\langle -| + b|-\rangle\langle +|$. Thus, $P_{opt}^{(sep)}(\gamma_0)$ can be formulated as the following optimization problem:

$$\begin{aligned} P_{opt}^{(sep)}(\gamma_0) &= \max \mathrm{tr}\,[S\sigma] &(70)\\ &s.t.\ S \geq 0, S^T = S &(71)\\ &\quad 2\gamma_0(|{+}{-}\rangle\langle{+}{-}| + |{-}{+}\rangle\langle{-}{+}|) \\ &\quad + |1\rangle\langle 1| \otimes S + S \otimes |1\rangle\langle 1| \leq I. &(72)\end{aligned}$$

Note that Eq. (72) is imposed under the condition $\hat{M}_0 + \hat{M}_1 \leq I$, which guarantees the existence of $\hat{M}_2$ such that $\hat{M}_2 = I - \hat{M}_0 - \hat{M}_1 \in \mathbf{Pos}\left(\mathbb{C}^4\right)$ and $\sum_{m=0}^{2} \hat{M}_m = I$. We do not explicitly impose $\hat{M}_2 \in \mathbf{SEP}\left(\mathbb{C}^2 : \mathbb{C}^2\right)$ in the optimization problem. However, this condition is satisfied since $\hat{M}_2^{T_1} = I - \hat{M}_0 - \hat{M}_1 = \hat{M}_2 \in \mathbf{Pos}\left(\mathbb{C}^4\right)$ and $\mathbf{SEP}\left(\mathbb{C}^2 : \mathbb{C}^2\right) = \mathbf{PPT}\left(\mathbb{C}^2 : \mathbb{C}^2\right)$, where T_1 represents partial transposition on the first qubit.

It is important to note that this optimization problem, defined in Eqs. (70)–(72), is an SDP without any condition resulting from the DPS hierarchy. This illustrates that the MFLC is advantageous for optimization over **SEP**, independently of the DPS hierarchy. We can ensure the validity of the optimization problem by plotting its numerical solutions (Fig. 6).

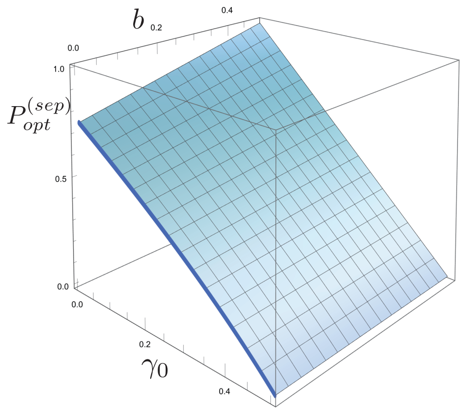

Fig. 6 Plot of $P_{opt}^{(sep)}(\gamma_0)$ solved by an SDP represented by Eqs. (70)–(72) for $a = c = \frac{1}{2}$. For the case of $b = 0$, the solution of the SDP coincides with the analytical curve $1 - \gamma_0 - (4(1-\gamma_0))^{-1}$ derived in [6], depicted by the thick blue curve.

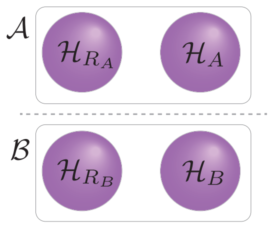

Fig. 7 Partitioning of the composite Hilbert spaces where the canonical subspace is defined. We consider the product vectors between $\mathcal{A}$ and $\mathcal{B}$.

C Proofs for MFLCs of canonical subspace

Let $\mathcal{A} = \mathcal{H}_A \otimes \mathcal{H}_{R_A}$, $\mathcal{B} = \mathcal{H}_{R_B} \otimes \mathcal{H}_B$, and $\dim \mathcal{H}_A = \dim \mathcal{H}_{R_A} = \dim \mathcal{H}_B = \dim \mathcal{H}_{R_B} = d$ (see Fig. 7). A canonical subspace $\mathcal{V}_d$ and a related subspace $\mathcal{V}_d^\circ$ is defined as

$$\mathcal{V}_d := \{|\Xi\rangle \in \mathcal{A} \otimes \mathcal{B} : \langle I_d|_{R_A R_B} |\Xi\rangle \in \operatorname{span}(\{|I_d\rangle_{AB}\})\}, \tag{73}$$
$$\mathcal{V}_d^\circ := \{|\Xi\rangle \in \mathcal{A} \otimes \mathcal{B} : \langle I_d|_{R_A R_B} |\Xi\rangle = 0\}. \tag{74}$$

Proposition 6 *$\hat{\mathcal{P}}(d) \cup \mathcal{V}_d^\circ$ forms an irredundant FLC of $\mathbb{S}(\mathcal{A} : \mathcal{B}) \cap \mathcal{V}_d$, where*

$$\hat{\mathcal{P}}(d) := \mathcal{V}_d \cap \mathcal{V}_d^\dagger, \tag{75}$$
$$\mathcal{V}_d^\dagger := \{|\Xi\rangle \in \mathcal{A} \otimes \mathcal{B} : \langle I_d|_{AB} |\Xi\rangle \in \operatorname{span}(\{|I_d\rangle_{R_A R_B}\})\}. \tag{76}$$

Proof First, through a straightforward calculation, we can show

$$\mathbb{S}(\mathcal{A} : \mathcal{B}) \cap \mathcal{V}_d = \{|A\rangle|B\rangle : [A][B]^T \in \{0, I\}\} \tag{77}$$
$$= \{|A\rangle|B\rangle : [A][B]^T = 0\} \cup \{|A\rangle|B\rangle : [A][B]^T = I\}, \tag{78}$$

where $|A\rangle_{AR_A} = (A \otimes I^{(R_A)})|I_d\rangle_{R_A R_A}$ and $|B\rangle_{R_B B} = (I^{(R_B)} \otimes B)|I_d\rangle_{R_B R_B}$ for $A \in \mathbf{L}(\mathcal{H}_{R_A} : \mathcal{H}_A)$ and $B \in \mathbf{L}(\mathcal{H}_{R_B} : \mathcal{H}_B)$, and $[A]$ and $[B]$ are matrix representations of A and B with respect to the computational basis defining the maximally entangled states. This can be done by observing $\langle I_d|_{R_A R_B}(|A\rangle|B\rangle) \in \{0, |I_d\rangle_{AB}\} \Leftrightarrow [A][B]^T = \{0, I\}$. Note that we regard each vector as an element of a projective space.

Since $\langle I_d|_{AB}(|A\rangle|B\rangle) \in \{0, |I_d\rangle_{R_A R_B}\} \Leftrightarrow [B]^T[A] = \{0, I\}$ and $[A][B]^T = I \Leftrightarrow [B]^T[A] = I$, we find that

$$\{|A\rangle|B\rangle : [A][B]^T = I\} \subseteq \mathcal{V}_d \cap \mathcal{V}_d^\dagger = \hat{\mathcal{P}}(d), \tag{79}$$
$$\{|A\rangle|B\rangle : [A][B]^T = I\} \cap \mathcal{V}_d^\circ = \emptyset, \tag{80}$$
$$\{|A\rangle|B\rangle : [A][B]^T = 0\} \subseteq \mathcal{V}_d^\circ, \tag{81}$$
$$\{|A\rangle|B\rangle : [A][B]^T = 0\} \not\subseteq \mathcal{V}_d^\dagger. \tag{82}$$

This completes the proof. □

Proposition 7 *$\mathbb{V} := (\mathbb{S}(\mathcal{A} : \mathcal{B}) \cap \mathcal{V}_d) \setminus \mathcal{V}_d^\circ$ is irreducible.*

Proof In the proof of Proposition 6, we obtained $\mathbb{S}(\mathcal{A}:\mathcal{B})\cap\mathcal{V}_d = \{|A\rangle|B\rangle : [A][B]^T = I\}\cup\{|A\rangle|B\rangle : [A][B]^T = 0\}$, $\{|A\rangle|B\rangle : [A][B]^T = I\}\cap\mathcal{V}_d^\circ = \emptyset$, and $\{|A\rangle|B\rangle : [A][B]^T = 0\}\subseteq\mathcal{V}_d^\circ$. These imply that

$$\mathbb{V} = \{|A\rangle|B\rangle : [A][B]^T = I\} = \{|A\rangle|B\rangle : [B] = \mathrm{adj}([A])^T, \det([A]) \neq 0\}, \tag{83}$$

where $\mathrm{adj}([A])$ is the adjugate matrix of $[A]$, and we used $[A]\mathrm{adj}([A]) = \det([A])I$. Since $\mathbb{D} := \{|A\rangle : \det([A]) \neq 0\} \subset \mathbb{P}^{\dim\mathcal{A}-1}$ is an open set in an irreducible set $\mathbb{P}^{\dim\mathcal{A}-1}$, $\mathbb{D}$ is also irreducible. Since $f : \mathbb{D}\to\mathbb{V}$ defined by $f(|A\rangle) := |A\rangle|B(A)\rangle$ with $[B(A)] = \mathrm{adj}([A])^T$ satisfies the condition of Proposition 2, we find that $\mathbb{V} = f(\mathbb{D})$ is irreducible. □

Proposition 8 *Let $\mathbb{V} := (\mathbb{S}(\mathcal{A}:\mathcal{B})\cap\mathcal{V}_d)\setminus\mathcal{V}_d^\circ$ and $\hat{\mathcal{P}}(d)$ be defined as Proposition 6. Then, $\hat{\mathcal{P}}(d)\subseteq\mathrm{span}(\mathbb{V})$.*

Proof Since we obtained $\mathbb{V} = \{|A\rangle|B\rangle : [A][B]^T = I\}$ in the proof of Proposition 7, we find that

$$\mathbb{E} := \{|A\rangle|B\rangle : [A] = U, [B] = \overline{U}, U \text{ is a unitary matrix}\} \subseteq \mathbb{V}. \tag{84}$$

In the following, we prove that $\mathrm{span}(\mathbb{E}) = \hat{\mathcal{P}}(d)(\subseteq \mathrm{span}(\mathbb{V}))$, which completes the proof. To do that, we show that

$$\mathrm{range}\left(\int dU|A\rangle\langle A|\otimes|B\rangle\langle B|\right) = \hat{\mathcal{P}}(d), \tag{85}$$

where we regard vectors and subspaces as residing in a complex vector space, set $[A] = \overline{[B]} = U$, and compute the integral with respect to the Haar measure. From now on, we will use the matrix representation in the calculation.

$$\int dU S(|A\rangle\langle A|\otimes|B\rangle\langle B|)S^\dagger \tag{86}$$

$$= \int dU S\left(\sum_{ijkl}(U|i\rangle\langle k|U^\dagger)\otimes|i\rangle\langle k|\otimes|j\rangle\langle l|\otimes(\overline{U}|j\rangle\langle l|\overline{U}^\dagger)\right)S^\dagger \tag{87}$$

$$= \int dU \sum_{ijkl}|ij\rangle\langle kl|\otimes\left((U\otimes\overline{U})|ij\rangle\langle kl|(U\otimes\overline{U})^\dagger\right) \tag{88}$$

$$= \sum_{ijkl}|ij\rangle\langle kl|\otimes\left(\int dU(U\otimes U)|il\rangle\langle kj|(U\otimes U)^\dagger\right)^{T_2}, \tag{89}$$

where $S = \sum_{ijk}|ijk\rangle\langle kij|\otimes I$ is a permutation operator and T_2 represents the partial transpose acting on the second system.

For a d^2 by d^2 matrix X and d-dimensional unitary matrix U, it is known that $Y := \int dU(U\otimes U)X(U\otimes U)^\dagger$ can be decomposed as $Y = \alpha I + \beta P$, where $P = \sum_{ij}|ij\rangle\langle ji|$ is the swap matrix [48, Theorem 7.15]. Since $\mathrm{tr}[Y] = \mathrm{tr}[X] = \alpha d^2 + \beta d$ and $\mathrm{tr}[PY] = \mathrm{tr}[PX] = \alpha d + \beta d^2$, we obtain

$$\int dU(U\otimes U)X(U\otimes U)^\dagger = \frac{d\mathrm{tr}[X] - \mathrm{tr}[PX]}{d(d^2-1)}I + \frac{d\mathrm{tr}[PX] - \mathrm{tr}[X]}{d(d^2-1)}P. \tag{90}$$

By using this equation, we can proceed as follows.

$$Eq.~(89) = \frac{dI - |I_d\rangle\langle I_d|}{d(d^2-1)}\otimes I + \frac{d|I_d\rangle\langle I_d| - I}{d(d^2-1)}\otimes P^{T_2} \tag{91}$$

$$= \frac{1}{d(d^2-1)}\left(dI\otimes I + d|I_d\rangle\langle I_d|\otimes|I_d\rangle\langle I_d| - |I_d\rangle\langle I_d|\otimes I - I\otimes|I_d\rangle\langle I_d|\right) \tag{92}$$

$$= \phi_d^+\otimes\phi_d^+ + \frac{1}{d^2-1}(I-\phi_d^+)\otimes(I-\phi_d^+). \tag{93}$$

This proves Eq. (85). □

C.1 Twisted canonical subspace

Let $|\tau\rangle = I^{(R_A)}\otimes L_1^{(R_B)}|I_d\rangle_{R_AR_B}$ and $|L_2\rangle = I^{(A)}\otimes L_2^{(B)}|I_d\rangle_{AB}$ with full rank operators $L_1 \in \mathbf{L}(\mathcal{H}_{R_B})$ and $L_2 \in \mathbf{L}(\mathcal{H}_B)$. We consider a subspace $\mathcal{W}$ defined by

$$\mathcal{W} := \{|\Xi\rangle\in\mathcal{A}\otimes\mathcal{B} : \langle\tau|_{R_AR_B}|\Xi\rangle \in \mathrm{span}(\{|L_2\rangle\})\} \tag{94}$$

$$= \{|\Xi\rangle\in\mathcal{A}\otimes\mathcal{B} : \langle I_d|_{R_AR_B}L_1^\dagger\otimes L_2^{-1}|\Xi\rangle \in \mathrm{span}(\{|I_d\rangle_{AB}\})\} \tag{95}$$

$$= \left(L_1^\dagger\right)^{-1}\otimes L_2\{|\Xi\rangle\in\mathcal{A}\otimes\mathcal{B} : \langle I_d|_{R_AR_B}|\Xi\rangle \in \mathrm{span}(\{|I_d\rangle_{AB}\})\} \tag{96}$$

$$= \left(\left(L_1^\dagger\right)^{-1}\otimes L_2\right)\mathcal{V}_d. \tag{97}$$

We also define a subspace $\mathcal{W}^\circ$ as follows:

$$\mathcal{W}^\circ := \{|\Xi\rangle \in \mathcal{A}\otimes\mathcal{B} : \langle\tau|_{R_AR_B}|\Xi\rangle = 0\} \tag{98}$$
$$= \left(L_1^\dagger\right)^{-1} \otimes L_2\{|\Xi\rangle \in \mathcal{A}\otimes\mathcal{B} : \langle I_d|_{R_AR_B}|\Xi\rangle = 0\} \tag{99}$$
$$= \left(\left(L_1^\dagger\right)^{-1} \otimes L_2\right)\mathcal{V}_d^\circ. \tag{100}$$

Since

$$\mathbb{S}\left(\mathcal{A}:\mathcal{B}\right)\cap\mathcal{W} = \left(\left(L_1^\dagger\right)^{-1} \otimes L_2\right)\left(\mathbb{S}\left(\mathcal{A}:\mathcal{B}\right)\cap\mathcal{V}_d\right), \tag{101}$$
$$\left(\mathbb{S}\left(\mathcal{A}:\mathcal{B}\right)\cap\mathcal{W}\right)\setminus\mathcal{W}^\circ = \left(\left(L_1^\dagger\right)^{-1} \otimes L_2\right)\left(\left(\mathbb{S}\left(\mathcal{A}:\mathcal{B}\right)\cap\mathcal{V}_d\right)\setminus\mathcal{W}^\circ\right), \tag{102}$$

the three propositions shown in this section remain valid if we replace $\mathcal{V}_d$, $\mathcal{V}_d^\circ$ and $\hat{\mathcal{P}}(d)$ with $\mathcal{W}$, $\mathcal{W}^\circ$ and $\left(I^{(AR_A)}\otimes\left(L_1^\dagger\right)^{-1}\otimes L_2\right)\hat{\mathcal{P}}(d)$, respectively.

C.2 Extended canonical subspace

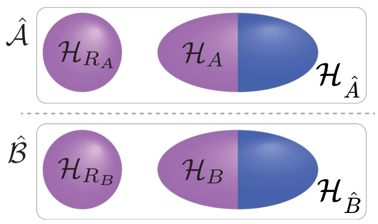

Fig. 8 Hilbert spaces where the extended canonical subspace is defined. We consider the product vectors between $\hat{\mathcal{A}}$ and $\hat{\mathcal{B}}$.

Suppose that the Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ are embedded in an extended Hilbert space, $\mathcal{H}_A \subseteq \mathcal{H}_{\hat{A}}$ and $\mathcal{H}_B \subseteq \mathcal{H}_{\hat{B}}$ (see Fig. 8), and define two subspaces

$$\hat{\mathcal{V}} := \{|\Xi\rangle \in \hat{\mathcal{A}}\otimes\hat{\mathcal{B}} : \langle I_d|_{R_AR_B}|\Xi\rangle \in \mathrm{span}\left(\{|I_d\rangle_{AB}\}\right)\}, \tag{103}$$
$$\hat{\mathcal{V}}^\circ := \{|\Xi\rangle \in \hat{\mathcal{A}}\otimes\hat{\mathcal{B}} : \langle I_d|_{R_AR_B}|\Xi\rangle = 0\}, \tag{104}$$

where $\hat{\mathcal{A}} = \mathcal{H}_{\hat{A}}\otimes\mathcal{H}_{R_A}$, $\hat{\mathcal{B}} = \mathcal{H}_{R_B}\otimes\mathcal{H}_{\hat{B}}$.

Since we can verify that

$$\mathbb{S}\left(\hat{\mathcal{A}}:\hat{\mathcal{B}}\right)\cap\hat{\mathcal{V}} = \{|\hat{A}\rangle|\hat{B}\rangle : [\hat{A}][\hat{B}]^T \in \{0, I_d\oplus 0\}\} \tag{105}$$
$$= \{|\hat{A}\rangle|\hat{B}\rangle : [\hat{A}][\hat{B}]^T = 0\} \cup \{|\hat{A}\rangle|\hat{B}\rangle : [\hat{A}][\hat{B}]^T = I_d\oplus 0\}, \tag{106}$$

where $|\hat{A}\rangle_{AR_A} = (\hat{A}\otimes I^{(R_A)})|I_d\rangle_{R_AR_A}$ and $|\hat{B}\rangle_{R_BB} = (I^{(R_B)}\otimes\hat{B})|I_d\rangle_{R_BR_B}$ for $\hat{A}\in\mathbf{L}\left(\mathcal{H}_{R_A}:\mathcal{H}_A\right)$ and $\hat{B}\in\mathbf{L}\left(\mathcal{H}_{R_B}:\mathcal{H}_B\right)$, and $[\hat{A}]$ and $[\hat{B}]$ are matrix representations of $\hat{A}$ and $\hat{B}$ with respect to the computational basis defining the maximally entangled states and an orthonormal basis of the orthogonal complement $\mathcal{H}_A^\perp$ (or $\mathcal{H}_B^\perp$) of $\mathcal{H}_A$ (or $\mathcal{H}_B$) within $\mathcal{H}_{\hat{A}}$ (or $\mathcal{H}_{\hat{B}}$). Here, I_d represents the d by d identity matrix, which acts on a subspace $\mathcal{H}_A$ (or $\mathcal{H}_B$) in $\mathcal{H}_{\hat{A}}$ (or $\mathcal{H}_{\hat{B}}$). Since $[\hat{A}][\hat{B}]^T = I_d\oplus 0$ implies that $[\hat{A}]$ and $[\hat{B}]$ can be decomposed as

$$[\hat{A}] = \begin{pmatrix}[A]\\0\end{pmatrix}, \quad [\hat{B}] = \begin{pmatrix}[B]\\0\end{pmatrix} \tag{107}$$

by using d by d matrices $[A]$ and $[B]$ satisfying $[A][B]^T = I$, we obtain

$$\{|\hat{A}\rangle|\hat{B}\rangle : [\hat{A}][\hat{B}]^T = I_d\oplus 0\} = (V_A\otimes I^{(R_AR_B)}\otimes V_B)\{|A\rangle|B\rangle : [A][B]^T = I\}, \tag{108}$$

where $V_A : \mathcal{H}_A \to \mathcal{H}_{\hat{A}}$ and $V_B : \mathcal{H}_B \to \mathcal{H}_{\hat{B}}$ are isometry operators that can be represented by $V_A = V_B = \sum_{i=0}^{d-1}|i\rangle\langle i|$ with the computational basis $\{|i\rangle\}_{i=0}^{d-1}$ of $\mathcal{H}_A$ or $\mathcal{H}_B$ defining the maximally entangled state in $\mathcal{H}_A\otimes\mathcal{H}_B$.

By using Eq. (106) and Eq. (108), we can verify that Proposition 6 remains valid if we replace $\mathcal{V}_d$, $\mathcal{V}_d^\circ$ and $\hat{\mathcal{P}}(d)$ with $\hat{\mathcal{V}}$, $\hat{\mathcal{V}}^\circ$ and $(V_A \otimes I^{(R_A R_B)} \otimes V_B)\hat{\mathcal{P}}(d)$, respectively. Since

$$\begin{aligned} \hat{\mathbb{V}} &:= \left(\mathbb{S}\left(\hat{\mathcal{A}} : \hat{\mathcal{B}}\right) \cap \hat{\mathcal{V}}\right) \setminus \hat{\mathcal{V}}^\circ && (109) \\ &= (V_A \otimes I^{(R_A R_B)} \otimes V_B)\{|A\rangle|B\rangle : [A][B]^T = I\}, && (110) \end{aligned}$$

we find that Proposition 7 and Proposition 8 remain valid if we replace $\mathbb{V}$ and $\hat{\mathcal{P}}(d)$ with $\hat{\mathbb{V}}$ and $(V_A \otimes I^{(R_A R_B)} \otimes V_B)\hat{\mathcal{P}}(d)$, respectively.

C.3 Extended and twisted canonical subspace

Let $|\tau\rangle = I^{(R_A)} \otimes L_1^{(R_B)}|I_d\rangle_{R_A R_B}$ and $|L_2\rangle = I^{(A)} \otimes L_2^{(B)}|I_d\rangle_{AB}$ with full-rank operators $L_1^{(R_B)} \in \mathbf{L}(\mathcal{H}_{R_B})$ and $L_2^{(B)} \in \mathbf{L}(\mathcal{H}_B)$.

Consider two Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ that are embedded in an extended Hilbert space as $\mathcal{H}_A \subseteq \mathcal{H}_{\hat{A}}$ and $\mathcal{H}_B \subseteq \mathcal{H}_{\hat{B}}$, and define two subspaces

$$\begin{aligned} \hat{\mathcal{W}} &:= \{|\Xi\rangle \in \hat{\mathcal{A}} \otimes \hat{\mathcal{B}} : \langle\tau|_{R_A R_B}|\Xi\rangle \in \mathrm{span}\left(\{|L_2\rangle\}\right)\}, && (111) \\ \hat{\mathcal{W}}^\circ &:= \{|\Xi\rangle \in \hat{\mathcal{A}} \otimes \hat{\mathcal{B}} : \langle\tau|_{R_A R_B}|\Xi\rangle = 0\}, && (112) \end{aligned}$$

where $\hat{\mathcal{A}} = \mathcal{H}_{\hat{A}} \otimes \mathcal{H}_{R_A}$, $\hat{\mathcal{B}} = \mathcal{H}_{R_B} \otimes \mathcal{H}_{\hat{B}}$. By using a similar calculation to those in the previous cases, we can show that the MFLC of $\mathbb{S}\left(\hat{\mathcal{A}} : \hat{\mathcal{B}}\right) \cap (\hat{\mathcal{W}} \setminus \hat{\mathcal{W}}^\circ)$ is

$$\mathcal{P} := \left(V_A \otimes I^{(R_A)} \otimes \left(L_1^\dagger\right)^{-1} \otimes (V_B L_2)\right)\hat{\mathcal{P}}(d). \qquad (113)$$

D Independence of the success probability from the input state

In general, we say a family of CP maps $\{\mathcal{E}'_m : \mathbf{L}(\mathcal{H}_1) \to \mathbf{L}(\mathcal{H}_2)\}_{m\in\Sigma}$ probabilistically implements an instrument $\{\mathcal{E}_m : \mathbf{L}(\mathcal{H}_1) \to \mathbf{L}(\mathcal{H}_2)\}_{m\in\Sigma}$ if there is a function $p : \mathbf{D}(\mathcal{H}_1) \to [0,1]$ such that

$$\mathcal{E}'_m(\rho) = p(\rho)\mathcal{E}_m(\rho), \qquad (\forall\rho \in \mathbf{D}(\mathcal{H}_1),\ \forall m \in \Sigma). \qquad (114)$$

In this appendix, we show that if the instrument $\{\mathcal{E}_m\}$ is taken from the list in Table 2, then the above p must be a constant function for any probabilistic implementation $\{\mathcal{E}'_m\}$ of $\{\mathcal{E}_m\}$ (The precise statement will be given in Theorem 4).

In the case of entanglement-assisted implementation of quantum operations considered in the main text, the separable instrument $\{\mathcal{S}_m : \mathbf{L}((\mathcal{H}_{A_1} \otimes \mathcal{H}_{R_A}) \otimes (\mathcal{H}_{B_1} \otimes \mathcal{H}_{R_B})) \to \mathbf{L}(\mathcal{H}_2)\}_{m\in\Sigma\cup\{\texttt{fail}\}}$ induces a family of CP maps $\{\mathcal{E}'_m : \mathbf{L}(\mathcal{H}_1) \to \mathbf{L}(\mathcal{H}_2)\}_{m\in\Sigma}$ defined by

$$\mathcal{E}'_m(A) := \mathcal{S}_m(A \otimes \tau). \qquad (\forall A \in \mathbf{L}(\mathcal{H}_1), \forall m \in \Sigma) \qquad (115)$$

(Note that the index `fail` no longer appears in the family.) The argument in this section does not depend on the form of $\{\mathcal{E}'_m\}$, whether it is given by the entanglement-assisted form or not.

Lemma 2 *Let $\mathcal{E} : \mathbf{L}(\mathcal{H}_1) \to \mathbf{L}(\mathcal{H}_2)$ be a CPTP map and $\mathcal{E}' : \mathbf{L}(\mathcal{H}_1) \to \mathbf{L}(\mathcal{H}_2)$ be its probabilistic implementation, that is, a function $p : \mathbf{D}(\mathcal{H}_1) \mapsto [0,1]$ exists and satisfies $\mathcal{E}'(\rho) = p(\rho)\mathcal{E}(\rho)$ for any ρ. If there is a state $\rho_* \in \mathbf{D}(\mathcal{H}_1)$ such that $\mathcal{E}(\rho) \neq \mathcal{E}(\rho_*)$ whenever $\rho \neq \rho_*$, then p is a constant function.*

Proof Let $\rho \in \mathbf{D}(\mathcal{H}_1)$ be a state distinct from ρ_*. We have

$$\mathcal{E}'(\rho + \rho_*) = \mathcal{E}'(\rho) + \mathcal{E}'(\rho_*) = p(\rho)\mathcal{E}(\rho) + p(\rho_*)\mathcal{E}(\rho_*), \qquad (116)$$

from the linearity of $\mathcal{E}'$. On the other hand, we also have

$$\begin{aligned} \mathcal{E}'(\rho + \rho_*) &= 2\mathcal{E}'\left(\frac{\rho + \rho_*}{2}\right) = 2p\left(\frac{\rho + \rho_*}{2}\right)\mathcal{E}\left(\frac{\rho + \rho_*}{2}\right) && (117) \\ &= p\left(\frac{\rho + \rho_*}{2}\right)\mathcal{E}(\rho) + p\left(\frac{\rho + \rho_*}{2}\right)\mathcal{E}(\rho_*), && (118) \end{aligned}$$

by the linearity of $\mathcal{E}$. By equating these two expressions, we arrive at

$$\left(p(\rho) - p\left(\frac{\rho + \rho_*}{2}\right)\right)\mathcal{E}(\rho) = -\left(p(\rho_*) - p\left(\frac{\rho + \rho_*}{2}\right)\right)\mathcal{E}(\rho_*). \qquad (119)$$

Since $\mathcal{E}$ is a trace preserving map, by taking the trace of both sides, we have

$$p(\rho) - p\left(\frac{\rho + \rho_*}{2}\right) = -p(\rho_*) + p\left(\frac{\rho + \rho_*}{2}\right). \qquad (120)$$

Because $\mathcal{E}(\rho)$ and $\mathcal{E}(\rho_*)$ are different by assumption, both sides of the above equality must be zero, which implies

$$p(\rho) = p\left(\frac{\rho+\rho_*}{2}\right) = p(\rho_*). \tag{121}$$

Since this holds for any state ρ ($\neq \rho_*$), the function p takes the constant value $p(\rho_*)$. □

Lemma 3 *Let $\{\mathcal{E}_m : \mathbf{L}(\mathcal{H}_1) \to \mathbf{L}(\mathcal{H}_2)\}_{m\in\Sigma}$ be any instrument from the list in Table 2. Define a linear map $\mathcal{E} : \mathbf{L}(\mathcal{H}_1) \to \mathcal{L}(\mathcal{H}_2 \otimes \mathbb{C}^\Sigma)$ by*

$$\mathcal{E}(\rho) = \sum_m \mathcal{E}_m(\rho) \otimes |m\rangle\langle m|. \tag{122}$$

Then there exists a state $\rho_* \in \mathbf{D}(\mathcal{H}_1)$ such that $\mathcal{E}(\rho) \neq \mathcal{E}(\rho_*)$ whenever $\rho \neq \rho_*$.

Proof The instruments in the list in Table 2 that have an input state are unitary channels, rank-1 POVMs, and verification of pure states.

unitary channel For unitary channels, Σ is a singleton, and $\mathcal{E}(\rho) = U\rho U^\dagger$. Any state in $\mathbf{D}(\mathcal{H}_1)$ can play the role of ρ_* since unitary channels are bijective.

rank-1 POVM Let $\{|M_m\rangle\langle M_m|\}_{m=1,\dots,n}$ be a rank-1 POVM. The CPTP map (122) is defined by $\mathcal{E}(\rho) = \sum_m \langle M_m|\rho|M_m\rangle|m\rangle\langle m|$. In this case, we can take, e.g., $\rho_* = |M_1\rangle\langle M_1|/\langle M_1|M_1\rangle$. This is the unique state that makes $\langle 1|\mathcal{E}(\rho_*)|1\rangle = \langle M_1|\rho_*|M_1\rangle$ equal to its maximum value $\langle M_1|M_1\rangle$, so we have $\langle 1|\mathcal{E}(\rho_*)|1\rangle > \langle 1|\mathcal{E}(\rho)|1\rangle$ and hence $\mathcal{E}(\rho) \neq \mathcal{E}(\rho_*)$ whenever $\rho \neq \rho_*$.

verification of pure state The pure state verification is described by a POVM $\{M_{\texttt{accept}} := q\phi,\ M_{\texttt{reject}} := I - q\phi\}$, with some $q \in [0,1]$ and pure state $\phi \in \mathbf{D}(\mathcal{H}_1)$. The CPTP map (122) is defined by $\mathcal{E}(\rho) = q\mathrm{tr}\,[\phi\rho]\,|a\rangle\langle a| + (1 - q\mathrm{tr}\,[\phi\rho])|r\rangle\langle r|$. Since $\langle a|\mathcal{E}(\rho)|a\rangle = q\mathrm{tr}\,[\phi\rho]$ reaches its maximum value q if and only if $\rho = \phi$, we have $\mathcal{E}(\rho) \neq \mathcal{E}(\phi)$ whenever $\rho \neq \phi$.

□

Theorem 4 *Let $\{\mathcal{E}_m : \mathbf{L}(\mathcal{H}_1) \to \mathbf{L}(\mathcal{H}_2)\}_{m\in\Sigma}$ be any instrument from the list in Table 1. If $\{\mathcal{E}'_m : \mathbf{L}(\mathcal{H}_1) \to \mathbf{L}(\mathcal{H}_2)\}_{m\in\Sigma}$ probabilistically implements $\{\mathcal{E}_m : \mathbf{L}(\mathcal{H}_1) \to \mathbf{L}(\mathcal{H}_2)\}_{m\in\Sigma}$ in the sense that a function $p : \mathbf{D}(\mathcal{H}_1) \to [0,1]$ exists and satisfies $\mathcal{E}'_m(\rho) = p(\rho)\mathcal{E}_m(\rho)$ for all $m \in \Sigma$, then p must be a constant function.*

Proof Define linear maps $\mathcal{E}, \mathcal{E}' : \mathbf{L}(\mathcal{H}_1) \to \mathcal{L}(\mathcal{H}_2 \otimes \mathbb{C}^\Sigma)$ by Eq. (122) and by

$$\mathcal{E}'(\rho) := \sum_m \mathcal{E}'_m(\rho) \otimes |m\rangle\langle m| \tag{123}$$

respectively. $\mathcal{E}$ is a CPTP map. From $\mathcal{E}'_m(\rho) = p(\rho)\mathcal{E}_m(\rho)$ $(\forall m \in \Sigma)$ we obtain

$$\mathcal{E}'(\rho) = \sum_m p(\rho)\mathcal{E}_m(\rho) \otimes |m\rangle\langle m| = p(\rho)\sum_m \mathcal{E}_m(\rho) \otimes |m\rangle\langle m| = p(\rho)\mathcal{E}(\rho). \tag{124}$$

From Lemma 3, there exists a state ρ_* such that $\mathcal{E}(\rho) \neq \mathcal{E}(\rho_*)$ whenever $\rho \neq \rho_*$. So Lemma 2 applies to the CPTP map $\mathcal{E}$ and its probabilistic implementation $\mathcal{E}'$, and implies that p is a constant function.

□

E Extraction of range constraint

Lemma 4 *Let $S \in \mathbf{Pos}(\mathcal{H} \otimes \mathcal{H}_R)$, $\tau \in \mathbf{Pos}(\mathcal{H}_R)$ and $E \in \mathbf{Pos}(\mathcal{H})$. If there exists $p \in \mathbb{R}$ such that $tr_R[S\tau] = pE$, then* $\mathrm{range}(S) \subseteq \mathcal{W}$, *where*

$$\mathcal{W} := \{|\Xi\rangle \in \mathcal{H} \otimes \mathcal{H}_R : \forall|\eta\rangle \in \mathrm{range}(\tau), \langle\eta|\Xi\rangle \in \mathrm{range}(E)\}. \tag{125}$$

Moreover, if $\mathrm{rank}(E) = 1$, *the converse holds.*

In the proof of this lemma, we use the following auxiliary lemma. Although this fact is standard in matrix analysis, we include a proof for completeness.

Lemma 5 $\mathrm{range}\left(\sum_{i\in I}|\Theta_i\rangle\langle\Theta_i|\right) = \mathrm{span}\left(\{|\Theta_i\rangle\}_{i\in I}\right)$ *for any finite set $\{|\Theta_i\rangle\}_{i\in I} \subseteq \mathcal{H}$ of vectors.*

Proof Since $\mathrm{range}\left(\sum_{i\in I}|\Theta_i\rangle\langle\Theta_i|\right) \subseteq \mathrm{span}\left(\{|\Theta_i\rangle\}_{i\in I}\right)$ is trivial, we show the converse by contradiction. Assume that $\mathrm{range}\left(\sum_{i\in I}|\Theta_i\rangle\langle\Theta_i|\right) \subsetneq \mathrm{span}\left(\{|\Theta_i\rangle\}_{i\in I}\right)$. Then, there exists a unit vector $|\phi\rangle \in \mathcal{H}$ such that $|\phi\rangle \in \mathrm{span}\left(\{|\Theta_i\rangle\}_{i\in I}\right)$ and $\langle\phi|\sum_{i\in I}|\Theta_i\rangle\langle\Theta_i||\phi\rangle = 0$. Since the second condition implies $\forall i, \langle\phi|\Theta_i\rangle = 0$, this contradicts the first condition. This completes the proof. □

Proof of Lemma 4 Let S and τ be diagonalized as $S = \sum_x |\Xi_x\rangle\langle\Xi_x|$ and $\tau = \sum_y p_y|\eta_y\rangle\langle\eta_y|$ $(p_y > 0)$, respectively. Since $pE = \mathrm{tr}_R[S\tau] = \sum_{x,y} p_y\langle\eta_y|\Xi_x\rangle\langle\Xi_x|\eta_y\rangle$, we obtain

$$\mathrm{span}\left(\{\langle\eta_y|\Xi_x\rangle\}_{x,y}\right) = \mathrm{range}\,(pE) \subseteq \mathrm{range}\,(E) \tag{126}$$

by using Lemma 5 with $|\Theta_i\rangle = \langle\eta_y|\Xi_x\rangle(\in \mathcal{H})$. This implies that $\langle\eta|\Xi_x\rangle \in \mathrm{range}\,(E)$ for any x and $|\eta\rangle \in \mathrm{range}\,(\tau)$. This proves that $\mathrm{range}\,(S) \subseteq \mathcal{W}$.

Conversely, $\mathrm{range}\,(S) \subseteq \mathcal{W}$ implies that $\langle\eta_y|\Xi_x\rangle \in \mathrm{range}\,(E)$ for all x and y. Since $\mathrm{tr}_R[S\tau] = \sum_{x,y} p_y\langle\eta_y|\Xi_x\rangle\langle\Xi_x|\eta_y\rangle$, we obtain $\exists p \in \mathbb{R}, \mathrm{tr}_R[S\tau] = pE$ if $\mathrm{rank}(E) = 1$. □

F Computing a lower bound based on ϵ-net

Here, we provide an algorithm to obtain a lower bound on Eq. (19). First, we show that for any finite set $\left\{|\Pi_x^{(m)}\rangle \in \mathbb{E}_m\right\}_x$ of product vectors,

$$\text{Eq. (19)} \geq \max\left\{\min_{m\in\Sigma}\frac{\mathrm{tr}[S_m\overline{\tau}]}{\||E_m\rangle\|_2^2(1+\delta)} : \begin{array}{l}\forall m \in \Sigma, x, p_x^{(m)} \geq 0,\\ \forall m \in \Sigma, S_m = \sum_x p_x^{(m)}|\Pi_x^{(m)}\rangle\langle\Pi_x^{(m)}|,\\ \Delta = I - \sum_{m\in\Sigma}\mathrm{tr}_2[S_m],\\ \min_{S\in\mathbf{SEP}(\mathcal{H}_{A_1}\otimes\mathcal{H}_{R_A}:\mathcal{H}_{R_B}\otimes\mathcal{H}_{B_1})}\|\Delta - S\|_1 \leq \delta\end{array}\right\}, \tag{127}$$

where $\|X\|_p := \mathrm{tr}\left[(XX^\dagger)^{\frac{p}{2}}\right]^{\frac{1}{p}}$ is the Schatten p-norm. This is because we can show $\frac{1}{1+\delta}\{S_m\}_{m\in\Sigma}$ is a feasible solution of the optimization problem given in the right-hand side of Eq. (19) when $\{p_x^{(m)}, S_m, \Delta, \delta\}$ is the one given in the right-hand side of Eq. (127) as follows:

- Since $\mathbb{E}_m \subseteq \mathbb{S}\left(\hat{\mathcal{A}} : \hat{\mathcal{B}}\right) \cap \mathcal{W}_m$, we can verify $\frac{1}{1+\delta}S_m \in \mathbf{SEP}\left(\hat{\mathcal{A}} : \hat{\mathcal{B}}\right)$ and $\mathrm{range}\left(\frac{1}{1+\delta}S_m\right) \subseteq \mathcal{W}_m$.
- Let $S^* \in \mathbf{SEP}(\mathcal{H}_{A_1}\otimes\mathcal{H}_{R_A} : \mathcal{H}_{R_B}\otimes\mathcal{H}_{B_1})$ achieve the minimum, i.e., $\|\Delta - S^*\|_1 = \min_S\|\Delta - S\|_1$ in Eq. (127). Since $\|\Delta - S^*\|_1 \leq \delta$ implies that $\delta I + (\Delta - S^*)$ is an element of the separable cone [86], $I - \sum_m \frac{1}{1+\delta}\mathrm{tr}_2[S_m] = \frac{1}{1+\delta}(\delta I + \Delta - S^* + S^*)$ is also an element of the separable cone.

Next, we can verify, by definition, that for any finite subsets $\{\phi_x \in \mathbf{P}(\mathcal{H}_{A_1}\otimes\mathcal{H}_{R_A})\}_x$ and $\{B_x \in \mathbf{Pos}(\mathcal{H}_{R_B}\otimes\mathcal{H}_{B_1})\}_x$,

$$\min_{S\in\mathbf{SEP}(\mathcal{H}_{A_1}\otimes\mathcal{H}_{R_A}:\mathcal{H}_{R_B}\otimes\mathcal{H}_{B_1})}\|\Delta - S\|_1 \leq \left\|\Delta - \sum_x \phi_x\otimes B_x\right\|_1. \tag{128}$$

Moreover, since $\|X\|_1 = \min_{P\geq 0, P\geq X} 2\mathrm{tr}[P] - \mathrm{tr}[X]$ for any Hermitian operator X,

$$\left\|\Delta - \sum_x \phi_x\otimes B_x\right\|_1 \leq 2\mathrm{tr}[P] + \sum_x \mathrm{tr}[B_x] - \mathrm{tr}[\Delta] \tag{129}$$

for any $P \geq 0$ such that $P + \sum_x \phi_x\otimes B_x \geq \Delta$.

Thus, we obtain the following lower bound:

$$\text{Eq. (19)} \geq \max\left\{\min_{m\in\Sigma}\frac{\mathrm{tr}[S_m\overline{\tau}]}{\||E_m\rangle\|_2^2(1+\delta)} : \begin{array}{l}\forall m \in \Sigma, x, p_x^{(m)} \geq 0,\\ \forall m \in \Sigma, S_m = \sum_x p_x^{(m)}|\Pi_x^{(m)}\rangle\langle\Pi_x^{(m)}|,\\ \Delta = I - \sum_{m\in\Sigma}\mathrm{tr}_2[S_m],\\ \delta = 2\mathrm{tr}[P] + \sum_x \mathrm{tr}[B_x] - \mathrm{tr}[\Delta],\\ P \geq 0, P + \sum_x \phi_x\otimes B_x \geq \Delta, B_x \geq 0\end{array}\right\}. \tag{130}$$

This is because $\{p_x^{(m)}, S_m, \Delta, \delta\}$ is a feasible solution of the optimization problem given in the right-hand0side of Eq. (127) when $\{p_x^{(m)}, S_m, \Delta, \delta, P, B_x\}$ is the one given in the right-hand side of Eq. (130). Note that the right-hand side converges to Eq. (19) if we use finer ϵ-nets $\left\{|\Pi_x^{(m)}\rangle\right\}_x$ of $\mathbb{E}_m$ and $\{\phi_x\}_x$ of $\mathbf{P}(\mathcal{H}_{A_1}\otimes\mathcal{H}_{R_A})$. However, the right-hand side cannot be computed by an SDP directly since the target function is not linear.

Alternatively, our algorithm solves the following SDP

$$\max\left\{\min_{m\in\Sigma}\frac{\mathrm{tr}[S_m\overline{\tau}]}{\||E_m\rangle\|_2^2} - \delta : \begin{array}{l}\forall m \in \Sigma, x, p_x^{(m)} \geq 0,\\ \forall m \in \Sigma, S_m = \sum_x p_x^{(m)}|\Pi_x^{(m)}\rangle\langle\Pi_x^{(m)}|,\\ \Delta = I - \sum_{m\in\Sigma}\mathrm{tr}_2[S_m],\\ \delta = 2\mathrm{tr}[P] + \sum_x \mathrm{tr}[B_x] - \mathrm{tr}[\Delta],\\ P \geq 0, P + \sum_x \phi_x\otimes B_x \geq \Delta, B_x \geq 0\end{array}\right\}, \tag{131}$$

and compute $r(\tau) := \min_{m\in\Sigma} \frac{\mathrm{tr}[S_m^* \overline{\tau}]}{\||E_m\rangle\|_2^2 (1+\delta^*)}$ by using S_m^* and δ^* attaining the maximum of Eq. (131). We can find that $r(\tau)$ is a lower bound on the right-hand side of Eq. (130).

By using lower bounds $\{r(\tau_\lambda)\}_\lambda$ for finite resource states $\{\tau_\lambda\}_\lambda$, we can obtain lower bounds $r(\tau)$ for any τ as follows: Assume we can transform τ into an ensemble $\{(p_\lambda, \tau_\lambda)\}_\lambda$ by using an LOCC instrument $\{\mathcal{L}_\lambda\}_\lambda$, i.e., $\mathcal{L}_\lambda(\tau) = p_\lambda \tau_\lambda$ for all λ. Let $\{\mathcal{S}_m^{(\lambda)}\}_m$ be a separable instrument satisfying $\mathcal{S}_m^{(\lambda)}(\rho \otimes \tau_\lambda) = p(\{\mathcal{E}_m\}_m, \tau_\lambda)\mathcal{E}_m(\rho)$ for all λ, ρ, and $m \in \Sigma$. Then, we can verify that $\{\mathcal{S}_m = \sum_\lambda \mathcal{S}_m^{(\lambda)} \circ \mathcal{L}_\lambda\}_m$ is a separable instrument and satisfies

$$\mathcal{S}_m(\rho \otimes \tau) = \sum_\lambda p_\lambda \mathcal{S}_m^{(\lambda)}(\rho \otimes \tau_\lambda) = \sum_\lambda p_\lambda p(\{\mathcal{E}_m\}_m, \tau_\lambda)\mathcal{E}_m(\rho) \tag{132}$$

for all ρ and $m \in \Sigma$. Thus, $p(\{\mathcal{E}_m\}_m, \tau) \geq \sum_\lambda p_\lambda p(\{\mathcal{E}_m\}_m, \tau_\lambda) \geq \sum_\lambda p_\lambda r(\tau_\lambda)$.

Accordingly, we can show the following proposition.

Proposition 9 *Let $|\tau(s)\rangle = \sqrt{1-s}|00\rangle + \sqrt{s}|11\rangle$, where $s \in [0, \frac{1}{2}]$. Then, $f(s) = p(\{\mathcal{E}_m\}_m, \tau(s))$ is concave, where $p(\{\mathcal{E}_m\}_m, \tau)$ is defined in Eq. (19).*

Proof For any $s_1, s_2 \in [0, \frac{1}{2}]$ and $p \in [0,1]$, Theorem 1 in [87] implies that $\tau(ps_1 + (1-p)s_2)$ can be transformed into $\{(p, \tau(s_1)), (1-p, \tau(s_2))\}$ by using an LOCC instrument. Thus,

$$\begin{aligned} f\left(ps_1 + (1-p)s_2\right) &= p\left(\{\mathcal{E}_m\}_m, \tau\left(ps_1 + (1-p)s_2\right)\right) && (133)\\ &\geq pp(\{\mathcal{E}_m\}_m, \tau(s_1)) + (1-p)p(\{\mathcal{E}_m\}_m, \tau(s_2)) && (134)\\ &= pf(s_1) + (1-p)f(s_2). && (135)\end{aligned}$$

This completes the proof. □

Utilizing this proposition, we take the convex hull of the set $\{r(\tau_x)\}_x$, which are numerically obtained lower bounds for finite resource states $\{\tau_x\}_x$, to serve as a lower bound on $p(\{\mathcal{E}_m\}_m, \tau)$ presented in Fig. 5.

G SDPs in numerical experiments

Here, we summarize the SDPs used in the numerical experiments. We wrote the SDPs using Python and utilized the PICOS [88] and QICS [89] packages to solve them.

G.1 Non-local unitary channels

In Fig. 5 (b), we compute three upper bounds on the success probability $p(\mathcal{U}, \tau)$ to implement nonlocal unitary channel $\mathcal{U}$ by SEP channels with a resource state $|\tau\rangle$, given in Eq. (35) and Eq. (36). Each upper bound is computed by solving the following SDPs:

- **PPT + MFLC**:

$$\begin{aligned} &\max \frac{\mathrm{tr}\left[S\overline{\tau}_\theta\right]}{d_A d_B} && (136)\\ &s.t.\ S \in \mathbf{PPT}\left(\hat{\mathcal{A}} : \hat{\mathcal{B}}\right), \mathrm{range}\left(S\right) \subseteq \mathcal{P} && (137)\\ &\quad I - \mathrm{tr}_2\left[S\right] \in \mathbf{PPT}\left(\mathcal{H}_{A_1} \otimes \mathcal{H}_{R_A} : \mathcal{H}_{R_B} \otimes \mathcal{H}_{B_1}\right), && (138)\end{aligned}$$

  where $\mathcal{P}$ is defined in Section 5.1.
- **PPT (DPS 1st Lv.)**:

$$\begin{aligned} &\max \frac{\mathrm{tr}\left[S\overline{\tau}_\theta\right]}{d_A d_B} && (139)\\ &s.t.\ S \in \mathbf{PPT}\left(\hat{\mathcal{A}} : \hat{\mathcal{B}}\right), \mathrm{range}\left(S\right) \subseteq \hat{\mathcal{W}} && (140)\\ &\quad I - \mathrm{tr}_2\left[S\right] \in \mathbf{PPT}\left(\mathcal{H}_{A_1} \otimes \mathcal{H}_{R_A} : \mathcal{H}_{R_B} \otimes \mathcal{H}_{B_1}\right), && (141)\end{aligned}$$

  where $\hat{\mathcal{W}}$ is defined in subsection 5.1.
- **DPS 2nd Lv.**:

$$\max \frac{\mathrm{tr}\left[S\overline{\tau}_\theta\right]}{d_A d_B} \tag{142}$$

$$s.t.\ S_{ext} \in \mathbf{PPT}\left(\hat{\mathcal{A}} : \hat{\mathcal{A}}' : \hat{\mathcal{B}}\right), \mathrm{range}\,(S_{ext}) \subseteq \vee_{n=1}^{2}\hat{\mathcal{A}} \otimes \hat{\mathcal{B}}, \tag{143}$$

$$S = \mathrm{tr}_{\hat{\mathcal{A}}'}\left[S_{ext}\right], \mathrm{range}\,(S) \subseteq \hat{\mathcal{W}}, \tag{144}$$

$$\mathrm{range}\,(S) \subseteq \mathrm{range}\,(V_A) \otimes \mathcal{H}_{R_A} \otimes \mathcal{H}_{R_B} \otimes \mathrm{range}\,(V_B)\,, \tag{145}$$

$$R \in \mathbf{PPT}\left(\mathcal{H}_{A_1} \otimes \mathcal{H}_{R_A} : \mathcal{H}_{A_1'} \otimes \mathcal{H}_{R_A'} : \mathcal{H}_{R_B} \otimes \mathcal{H}_{B_1}\right), \tag{146}$$

$$\mathrm{range}\,(R) \subseteq \vee_{n=1}^{2}(\mathcal{H}_{A_1} \otimes \mathcal{H}_{R_A}) \otimes (\mathcal{H}_{R_B} \otimes \mathcal{H}_{B_1}), \tag{147}$$

$$I - \mathrm{tr}_2\left[S\right] = \mathrm{tr}_{R_A' A_1'}\left[R\right], \tag{148}$$

where $\hat{\mathcal{W}}$ is defined in subsection 5.1 and we consider $\vee_{n=1}^{2}\hat{\mathcal{A}}$ and $\vee_{n=1}^{2}(\mathcal{H}_{A_1} \otimes \mathcal{H}_{R_A})$ are embedded in $\hat{\mathcal{A}} \otimes \hat{\mathcal{A}}'$ and $(\mathcal{H}_{A_1} \otimes \mathcal{H}_{R_A}) \otimes (\mathcal{H}_{A_1'} \otimes \mathcal{H}_{R_A'})$, respectively. Note that the original second level of the DPS hierarchy does not impose Eq. (145). We impose Eq. (145) since we can assume $\mathrm{range}\,(S) \subseteq \mathcal{P}(\subset \mathrm{range}\,(V_A) \otimes \mathcal{H}_{R_A} \otimes \mathcal{H}_{R_B} \otimes \mathrm{range}\,(V_B))$. Thus, this optimization problem can be regarded as a second level of the DPS hierarchy partially strengthened by the MFLC. This modification significantly reduces the size of the SDP.

G.2 Non-local measurement

In Fig. 5 (c), we compute three upper bounds on the success probability to implement the SJM by SEP channels with a resource state $|\tau\rangle$, given in Eq. (39) and Eq. (40). Each upper bound is computed by solving the following SDPs:

- **PPT* + MFLC**:

$$\max \min_m \mathrm{tr}\left[S_m \tau_\theta\right] \tag{149}$$

$$s.t.\ \forall m, S_m \in \mathbf{PPT}\left(\hat{\mathcal{A}} : \hat{\mathcal{B}}\right), \mathrm{range}\,(S_m) \subseteq \mathcal{P}_m, \tag{150}$$

$$R \in \mathbf{PPT}\left(\hat{\mathcal{A}} : \hat{\mathcal{A}}' : \hat{\mathcal{B}}\right), \mathrm{range}\,(R) \subseteq \vee_{n=1}^{2}\hat{\mathcal{A}} \otimes \hat{\mathcal{B}}, \tag{151}$$

$$I - \sum_m S_m = \mathrm{tr}_{\hat{\mathcal{A}}'}\left[R\right], \tag{152}$$

where $\mathcal{P}_m$ is defined in Section 5.2 and we consider $\vee_{n=1}^{2}\hat{\mathcal{A}}$ is embedded in $\hat{\mathcal{A}} \otimes \hat{\mathcal{A}}'$. Note that we partially used a condition resulting from the second level of the DPS hierarchy to improve the upper bound.

- **PPT (DPS 1st Lv.)**:

$$\max \min_m \mathrm{tr}\left[S_m \tau_\theta\right] \tag{153}$$

$$s.t.\ \forall m, S_m \in \mathbf{PPT}\left(\hat{\mathcal{A}} : \hat{\mathcal{B}}\right), \mathrm{range}\,(S_m) \subseteq \hat{\mathcal{W}}_m, \tag{154}$$

$$I - \sum_m S_m \in \mathbf{PPT}\left(\hat{\mathcal{A}} : \hat{\mathcal{B}}\right), \tag{155}$$

where $\hat{\mathcal{W}}_m$ is defined in Section 5.2.

- **DPS 2nd Lv.**:

$$\max \min_m \mathrm{tr}\left[S_m \tau_\theta\right] \tag{156}$$

$$s.t.\ \forall m, S_{ext,m} \in \mathbf{PPT}\left(\hat{\mathcal{A}} : \hat{\mathcal{A}}' : \hat{\mathcal{B}}\right), \tag{157}$$

$$\forall m, \mathrm{range}\,(S_{ext,m}) \subseteq \vee_{n=1}^{2}\hat{\mathcal{A}} \otimes \hat{\mathcal{B}}, \tag{158}$$

$$\forall m, S_m = \mathrm{tr}_{\hat{\mathcal{A}}'}\left[S_{ext,m}\right], \mathrm{range}\,(S_m) \subseteq \hat{\mathcal{W}}_m, \tag{159}$$

$$R \in \mathbf{PPT}\left(\hat{\mathcal{A}} : \hat{\mathcal{A}}' : \hat{\mathcal{B}}\right), \mathrm{range}\,(R) \subseteq \vee_{n=1}^{2}\hat{\mathcal{A}} \otimes \hat{\mathcal{B}}, \tag{160}$$

$$I - \sum_m S_m = \mathrm{tr}_{\hat{\mathcal{A}}'}\left[R\right], \tag{161}$$

where $\hat{\mathcal{W}}_m$ is defined in Section 5.2 and we consider $\vee_{n=1}^{2}\hat{\mathcal{A}}$ are embedded in $\hat{\mathcal{A}} \otimes \hat{\mathcal{A}}'$.

G.3 State verification

In Fig. 5 (d), we compute three upper bounds on the maximum parameter $q(\phi, \tau)$ to deterministically implement a state verification of ϕ by SEP channels with a resource state $|\tau\rangle$, given in Eq. (47) and Eq. (48). Each upper bound is computed by solving the following SDPs:

- **PPT + MFLC**:

$$\max \operatorname{tr}[S\tau_\theta] \tag{162}$$
$$s.t.\ S \in \mathbf{PPT}\left(\hat{\mathcal{A}} : \hat{\mathcal{B}}\right), \operatorname{range}(S) \subseteq \mathcal{P}, \tag{163}$$
$$I - S \in \mathbf{PPT}\left(\hat{\mathcal{A}} : \hat{\mathcal{B}}\right), \tag{164}$$

  where $\mathcal{P}$ is defined in Section 5.3.
- **PPT (DPS 1st Lv.)**:

$$\max \operatorname{tr}[S\tau_\theta] \tag{165}$$
$$s.t.\ S \in \mathbf{PPT}\left(\hat{\mathcal{A}} : \hat{\mathcal{B}}\right), \operatorname{range}(S) \subseteq \hat{\mathcal{W}}, \tag{166}$$
$$I - S \in \mathbf{PPT}\left(\hat{\mathcal{A}} : \hat{\mathcal{B}}\right), \tag{167}$$

  where $\hat{\mathcal{W}}$ is defined in Section 5.3.
- **DPS 2nd Lv.**:

$$\max \operatorname{tr}[S\tau_\theta] \tag{168}$$
$$s.t.\ S_{ext} \in \mathbf{PPT}\left(\hat{\mathcal{A}} : \hat{\mathcal{A}}' : \hat{\mathcal{B}}\right), \operatorname{range}(S_{ext}) \subseteq \vee_{n=1}^{2}\hat{\mathcal{A}} \otimes \hat{\mathcal{B}}, \tag{169}$$
$$S = \operatorname{tr}_{\hat{\mathcal{A}}'}[S_{ext}], \operatorname{range}(S) \subseteq \hat{\mathcal{W}}, \tag{170}$$
$$R \in \mathbf{PPT}\left(\hat{\mathcal{A}} : \hat{\mathcal{A}}' : \hat{\mathcal{B}}\right), \tag{171}$$
$$I - S = \operatorname{tr}_{\hat{\mathcal{A}}'}[R], \tag{172}$$

  where $\hat{\mathcal{W}}$ is defined in Section 5.3 and we consider $\vee_{n=1}^{2}\hat{\mathcal{A}}$ are embedded in $\hat{\mathcal{A}} \otimes \hat{\mathcal{A}}'$.

G.4 Entanglement distillation

In Fig. 5 (a), we compute three upper bounds on the success probability $p(\psi_\theta, \tau)$ to distill a pure entangled state ψ_θ from a mixed state τ by SEP channels, given in Eq. (50) and Eq. (52). Each upper bound is computed by solving the following SDPs:

- **PPT + MFLC**:

$$\max \operatorname{tr}[S\overline{\tau}] \tag{173}$$
$$s.t.\ S \in \mathbf{PPT}(\mathcal{A} : \mathcal{B}), \operatorname{range}(S) \subseteq \mathcal{P}, \tag{174}$$
$$I - \operatorname{tr}_{AB}[S] \in \mathbf{PPT}(\mathcal{H}_{R_A} : \mathcal{H}_{R_B}), \tag{175}$$

  where $\mathcal{P}$ is defined in Proposition 4.
- **PPT (DPS 1st Lv.)**:

$$\max \operatorname{tr}[S\overline{\tau}] \tag{176}$$
$$s.t.\ S \in \mathbf{PPT}(\mathcal{A} : \mathcal{B}), \operatorname{range}(S) \subseteq \mathcal{W}, \tag{177}$$
$$I - \operatorname{tr}_{AB}[S] \in \mathbf{PPT}(\mathcal{H}_{R_A} : \mathcal{H}_{R_B}), \tag{178}$$

  where $\mathcal{W}$ is defined in Section 5.4.
- **PPT (DPS 2nd Lv.)**:

$$\max \operatorname{tr}[S\overline{\tau}] \tag{179}$$
$$s.t.\ S_{ext} \in \mathbf{PPT}(\mathcal{A} : \mathcal{A}' : \mathcal{B}), \operatorname{range}(S_{ext}) \subseteq \vee_{n=1}^{2}\mathcal{A} \otimes \mathcal{B}, \tag{180}$$
$$S = \operatorname{tr}_{\mathcal{A}'}[S_{ext}], \operatorname{range}(S) \subseteq \mathcal{W}, \tag{181}$$
$$I - \operatorname{tr}_{AB}[S] \in \mathbf{PPT}(\mathcal{H}_{R_A} : \mathcal{H}_{R_B}), \tag{182}$$

  where $\mathcal{W}$ is defined in Section 5.4 and we consider $\vee_{n=1}^{2}\mathcal{A}$ are embedded in $\mathcal{A} \otimes \mathcal{A}'$.

H Distillation protocol

H.1 From a mixed state τ in $\mathbf{D}\left(\mathbb{C}^3 \otimes \mathbb{C}^3\right)$ into a pure state ψ_θ

Here, we construct a SEP channel $\mathcal{S} : \mathbf{L}\left(\mathcal{H}_{R_A} \otimes \mathcal{H}_{R_B}\right) \to \mathbf{L}\left(\mathcal{H}_A \otimes \mathcal{H}_B\right)$ for distilling a pure entangled state $|\psi_\theta\rangle = \cos\theta|00\rangle + \sin\theta|11\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ from a mixed state $\tau = \sum_{i=1}^3 q_i\tau_i \in \mathbf{D}\left(\mathcal{H}_{R_A} \otimes \mathcal{H}_{R_B}\right)$, where $\theta \in (0, \frac{\pi}{4}]$, $\forall q_i > 0$, and

$$|\tau_1\rangle = \frac{1}{\sqrt{2}}(|01\rangle + e^{i\theta_1}|10\rangle), |\tau_2\rangle = \frac{1}{\sqrt{2}}(|02\rangle + e^{i\theta_2}|20\rangle), |\tau_3\rangle = \frac{1}{\sqrt{2}}(|12\rangle + e^{i\theta_3}|21\rangle). \tag{183}$$

We can find a Kraus representation $\mathcal{S}(\rho) = \sum_{i,j} E_{i,j}\rho E_{i,j}^\dagger$ for the distillation by modifying the proof of Theorem 2 (b) in [7].

$$\begin{aligned}
E_{1,1} &= \sqrt{p}(\sqrt{\cos\theta}|0\rangle_A\langle 0|_{R_A} + \sqrt{\sin\theta}|1\rangle_A\langle 1|_{R_A}) \\
&\quad \otimes(\sqrt{\cos\theta}|0\rangle_B\langle 1|_{R_B} + e^{-i\theta_1}\sqrt{\sin\theta}|1\rangle_B\langle 0|_{R_B}) && (184)\\
E_{1,2} &= \sqrt{p}(\sqrt{\cos\theta}|0\rangle_A\langle 1|_{R_A} + \sqrt{\sin\theta}|1\rangle_A\langle 0|_{R_A}) \\
&\quad \otimes(e^{-i\theta_1}\sqrt{\cos\theta}|0\rangle_B\langle 0|_{R_B} + \sqrt{\sin\theta}|1\rangle_B\langle 1|_{R_B}) && (185)\\
E_{2,1} &= \sqrt{p}(\sqrt{\cos\theta}|0\rangle_A\langle 0|_{R_A} + \sqrt{\sin\theta}|1\rangle_A\langle 2|_{R_A}) \\
&\quad \otimes(\sqrt{\cos\theta}|0\rangle_B\langle 2|_{R_B} + e^{-i\theta_2}\sqrt{\sin\theta}|1\rangle_B\langle 0|_{R_B}) && (186)\\
E_{2,2} &= \sqrt{p}(\sqrt{\cos\theta}|0\rangle_A\langle 2|_{R_A} + \sqrt{\sin\theta}|1\rangle_A\langle 0|_{R_A}) \\
&\quad \otimes(e^{-i\theta_2}\sqrt{\cos\theta}|0\rangle_B\langle 0|_{R_B} + \sqrt{\sin\theta}|1\rangle_B\langle 2|_{R_B}) && (187)\\
E_{3,1} &= \sqrt{p}(\sqrt{\cos\theta}|0\rangle_A\langle 1|_{R_A} + \sqrt{\sin\theta}|1\rangle_A\langle 2|_{R_A}) \\
&\quad \otimes(\sqrt{\cos\theta}|0\rangle_B\langle 2|_{R_B} + e^{-i\theta_3}\sqrt{\sin\theta}|1\rangle_B\langle 1|_{R_B}) && (188)\\
E_{3,2} &= \sqrt{p}(\sqrt{\cos\theta}|0\rangle_A\langle 2|_{R_A} + \sqrt{\sin\theta}|1\rangle_A\langle 1|_{R_A}) \\
&\quad \otimes(e^{-i\theta_3}\sqrt{\cos\theta}|0\rangle_B\langle 1|_{R_B} + \sqrt{\sin\theta}|1\rangle_B\langle 2|_{R_B}). && (189)
\end{aligned}$$

Through a straightforward calculation, we can show that $E_{i,1}|\tau_i\rangle = E_{i,2}|\tau_i\rangle = \frac{\sqrt{p}}{\sqrt{2}}|\psi_\theta\rangle$ for all i and $E_{i,1}|\tau_j\rangle = E_{i,2}|\tau_j\rangle = 0$ for $i \neq j$. This implies $\mathcal{S}(\tau) = p\psi_\theta$. Thus, we can obtain the maximum success probability p of the distillation by maximizing p under the constraint $I - \sum_{i,j} E_{i,j}^\dagger E_{i,j} \in \mathbf{SEP}\left(\mathbb{C}^3 : \mathbb{C}^3\right)$. By a straightforward calculation, we obtain

$$\begin{aligned}
E_{1,1}^\dagger E_{1,1} &= p(\cos\theta|0\rangle\langle 0| + \sin\theta|1\rangle\langle 1|) \otimes (\sin\theta|0\rangle\langle 0| + \cos\theta|1\rangle\langle 1|) && (190)\\
E_{1,2}^\dagger E_{1,2} &= p(\sin\theta|0\rangle\langle 0| + \cos\theta|1\rangle\langle 1|) \otimes (\cos\theta|0\rangle\langle 0| + \sin\theta|1\rangle\langle 1|) && (191)\\
E_{2,1}^\dagger E_{2,1} &= p(\cos\theta|0\rangle\langle 0| + \sin\theta|2\rangle\langle 2|) \otimes (\sin\theta|0\rangle\langle 0| + \cos\theta|2\rangle\langle 2|) && (192)\\
E_{2,2}^\dagger E_{2,2} &= p(\sin\theta|0\rangle\langle 0| + \cos\theta|2\rangle\langle 2|) \otimes (\cos\theta|0\rangle\langle 0| + \sin\theta|2\rangle\langle 2|) && (193)\\
E_{3,1}^\dagger E_{3,1} &= p(\cos\theta|1\rangle\langle 1| + \sin\theta|2\rangle\langle 2|) \otimes (\sin\theta|1\rangle\langle 1| + \cos\theta|2\rangle\langle 2|) && (194)\\
E_{3,2}^\dagger E_{3,2} &= p(\sin\theta|1\rangle\langle 1| + \cos\theta|2\rangle\langle 2|) \otimes (\cos\theta|1\rangle\langle 1| + \sin\theta|2\rangle\langle 2|). && (195)
\end{aligned}$$

This implies

$$\sum_{i,j} E_{i,j}^\dagger E_{i,j} = p \times \mathrm{diag}(2\sin 2\theta, 1, 1, 1, 2\sin 2\theta, 1, 1, 1, 2\sin 2\theta). \tag{196}$$

Therefore, the maximum success probability of this protocol is $p = \min\left\{1, \frac{1}{2\sin 2\theta}\right\}$.

I Proof for Proposition 4

Before presenting the proof, we show the following lemma.

Lemma 6 *The MFLC of* $\mathbb{S}(\mathcal{A} : \mathcal{B}) \cap (\mathcal{V} \setminus \mathcal{V}^\circ)$ *is* $\vee_{n=1}^2(\mathcal{H}_A \otimes \mathcal{H}_{R_A})$*, where* $\mathcal{A} = \mathcal{H}_A \otimes \mathcal{H}_{R_A}$, $\mathcal{B} = \mathcal{H}_{R_B} \otimes \mathcal{H}_B$, $\dim\mathcal{H}_A = \dim\mathcal{H}_B = 2$, $\dim\mathcal{H}_{R_A} = \dim\mathcal{H}_{R_B} = d$,

$$\begin{aligned}
\mathcal{V} &= \left\{|\Xi\rangle \in \mathcal{A} \otimes \mathcal{B} : \forall|\psi\rangle \in \wedge_2\mathbb{C}^d, \langle\psi|_{R_AR_B}|\Xi\rangle \in \mathrm{span}\left(\{|01\rangle - |10\rangle\}\right)\right\}, && (197)\\
\mathcal{V}^\circ &= \{|\Xi\rangle \in \mathcal{A} \otimes \mathcal{B} : \forall|\psi\rangle \in \wedge_2\mathbb{C}^d, \langle\psi|_{R_AR_B}|\Xi\rangle = 0\}, && (198)
\end{aligned}$$

and we regard the symmetric subspace $\vee_{n=1}^2(\mathcal{H}_A \otimes \mathcal{H}_{R_A})$ *as being embedded in* $\mathcal{H}_A \otimes \mathcal{H}_{R_A} \otimes \mathcal{H}_B \otimes \mathcal{H}_{R_B}$ *by the isomorphism* $\mathcal{H}_B \otimes \mathcal{H}_{R_B} \simeq \mathcal{H}_A \otimes \mathcal{H}_{R_A}$.

Proof For any $|A\rangle|B\rangle \in \mathbb{S}(\mathcal{A}:\mathcal{B}) \cap \mathcal{V}$, it holds that for any $0 \le i < j \le d-1$,

$$\exists \alpha_{ij} \in \mathbb{C},\ \langle i|_{R_A}|A\rangle\langle j|_{R_B}|B\rangle - \langle j|_{R_A}|A\rangle\langle i|_{R_B}|B\rangle = \alpha_{ij}(|01\rangle_{AB} - |10\rangle_{AB}). \tag{199}$$

By defining, $[A_{ij}] = \begin{pmatrix} (\langle i|_{R_A}\langle 0|_A)|A\rangle & (\langle i|_{R_A}\langle 1|_A)|A\rangle \\ (\langle j|_{R_A}\langle 0|_A)|A\rangle & (\langle j|_{R_A}\langle 1|_A)|A\rangle \end{pmatrix}$, $[B_{ij}] = \begin{pmatrix} (\langle i|_{R_B}\langle 0|_B)|B\rangle & (\langle i|_{R_B}\langle 1|_B)|B\rangle \\ (\langle j|_{R_B}\langle 0|_B)|B\rangle & (\langle j|_{R_B}\langle 1|_B)|B\rangle \end{pmatrix}$, Eq. (199) is equivalent to

$$\exists \alpha_{ij} \in \mathbb{C},\ [A_{ij}]^T \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} [B_{ij}] = \alpha_{ij} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{200}$$

By straightforward calculation, we find that Eq. (199) is equivalent to either of the following cases:

1. $\exists \alpha_{ij} \in \mathbb{C}^\times,\ [B_{ij}] = \alpha_{ij}[A_{ij}] \wedge \det(A) \neq 0$
2. $[A_{ij}] = 0$
3. $\exists \begin{pmatrix} a \\ b \end{pmatrix} \in \mathbb{C}^2 \setminus \{0\}, \exists \begin{pmatrix} c \\ d \end{pmatrix} \in \mathbb{C}^2,\ [A_{ij}] = \begin{pmatrix} 0 & 0 \\ a & b \end{pmatrix}, [B_{ij}] = \begin{pmatrix} 0 & 0 \\ c & d \end{pmatrix}$
4. $\exists \beta \in \mathbb{C}, \exists \begin{pmatrix} a \\ b \end{pmatrix} \in \mathbb{C}^2 \setminus \{0\}, \exists \begin{pmatrix} c \\ d \end{pmatrix} \in \mathbb{C}^2,\ [A_{ij}] = \begin{pmatrix} a & b \\ \beta a & \beta b \end{pmatrix}, [B_{ij}] = \begin{pmatrix} c & d \\ \beta c & \beta d \end{pmatrix}$

Note that except for the first case, $[A_{ij}]^T \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} [B_{ij}] = 0$ holds.

Thus, for any $|A\rangle|B\rangle \in \mathbb{S}(\mathcal{A}:\mathcal{B}) \cap (\mathcal{V} \setminus \mathcal{V}^\circ)$, there exists i and j such that the first case holds. We let

$$[A_{ij}] = \begin{pmatrix} (\langle i|_{R_A}\langle 0|_A)|A\rangle & (\langle i|_{R_A}\langle 1|_A)|A\rangle \\ (\langle j|_{R_A}\langle 0|_A)|A\rangle & (\langle j|_{R_A}\langle 1|_A)|A\rangle \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix},\ [B_{ij}] = \begin{pmatrix} (\langle i|_{R_B}\langle 0|_B)|B\rangle & (\langle i|_{R_B}\langle 1|_B)|B\rangle \\ (\langle j|_{R_B}\langle 0|_B)|B\rangle & (\langle j|_{R_B}\langle 1|_B)|B\rangle \end{pmatrix} = \alpha_{ij}[A_{ij}], \tag{201}$$

where $\alpha_{ij} \in \mathbb{C}^\times$ and $\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} \neq 0$. Observe that for all integers k such that $i < k \le d-1$, the matrices $[A_{ik}]$ and $[B_{ik}]$, associated with the pair (i,k) satisfy either the first or the fourth case. This implies $[B_{ik}] = \alpha_{ij}[A_{ik}]$. On the other hand, observe that for all integers k such that $0 \le k < j$, the matrices $[A_{kj}]$ and $[B_{kj}]$, associated with the pair (k,j), satisfy either the first, the third, or the fourth case. This also implies $[B_{kj}] = \alpha_{ij}[A_{kj}]$. Therefore, we obtain $\exists \alpha \in \mathbb{C}^\times, |B\rangle = \alpha|A\rangle$. This completes the proof.

□

Proof of Proposition 4 First, by following the argument in the twisted canonical subspace in Section C.1, we can show that

$$\begin{aligned} \mathcal{W} &= \left\{|\Xi\rangle \in \mathcal{A}\otimes\mathcal{B} : \forall i, \langle \overline{\tau}_i|_{R_A R_B}(\sigma_Y L^{-1})^{(B)}|\Xi\rangle \in \mathrm{span}\left(\{|01\rangle - |10\rangle\}\right)\right\} && (202)\\ &= (L\sigma_Y)^{(B)}\mathcal{V}, && (203)\\ \mathcal{W}^\circ &= (L\sigma_Y)^{(B)}\mathcal{V}^\circ, && (204) \end{aligned}$$

where

$$\begin{aligned} \mathcal{V} &= \{|\Xi\rangle \in \mathcal{A}\otimes\mathcal{B} : \forall i, \langle \overline{\tau}_i|_{R_A R_B}|\Xi\rangle \in \mathrm{span}\left(\{|01\rangle - |10\rangle\}\right)\}, && (205)\\ \mathcal{V}^\circ &= \{|\Xi\rangle \in \mathcal{A}\otimes\mathcal{B} : \forall i, \langle \overline{\tau}_i|_{R_A R_B}|\Xi\rangle = 0\}. && (206) \end{aligned}$$

This implies that the MFLC of $\mathbb{S}(\mathcal{A}:\mathcal{B}) \cap (\mathcal{W} \setminus \mathcal{W}^\circ)$ is $(L\sigma_Y)^{(B)}\mathcal{P}'$, where $\mathcal{P}'$ is the MFLC of $\mathbb{S}(\mathcal{A}:\mathcal{B}) \cap (\mathcal{V} \setminus \mathcal{V}^\circ)$. Applying Lemma 6 completes the proof. □