Complete hierarchy of linear systems for certifying quantum entanglement of subspaces

Nathaniel Johnston, Benjamin Lovitz, and Aravindan Vijayaraghavan

Phys. Rev. A **106**, 062443 — Published 29 December 2022

DOI: 10.1103/PhysRevA.106.062443

A Complete Hierarchy of Linear Systems for Certifying Quantum Entanglement of Subspaces

Nathaniel Johnston*
Department of Mathematics and Computer Science, Mount Allison University, Sackville, New Brunswick, Canada
Department of Mathematics & Statistics, University of Guelph, Guelph, ON, Canada

Benjamin Lovitz†
Department of Mathematics, Northeastern University, Boston, Massachusetts, USA

Aravindan Vijayaraghavan‡
Department of Computer Science, Northwestern University, Evanston, Illinois, USA

We introduce a hierarchy of linear systems for showing that a given subspace of pure quantum states is entangled (i.e., contains no product states). This hierarchy outperforms known methods already at the first level, and it is complete in the sense that every entangled subspace is shown to be so at some finite level of the hierarchy. It generalizes straightforwardly to the case of higher Schmidt rank, as well as the multipartite cases of completely and genuinely entangled subspaces. These hierarchies work extremely well in practice even in very large quantum systems, as they can be implemented via elementary linear algebra techniques rather than the semidefinite programming techniques that are required by previously-known hierarchies.

PACS numbers: 03.65.Ud, 03.67.Bg

INTRODUCTION

Quantum entanglement is one of the central features of modern physics, and the problem of determining when entanglement is present in a quantum system is one of its most active research areas [1, 2]. Of particular interest in this area is the problem of determining whether or not a given subspace is entangled. That is, the problem of determining whether or not every pure state in the subspace is entangled (i.e., not a product state) [3, 4].

In the bipartite setting of two quantum systems, one of the standard uses of certifying entanglement in subspaces is that any mixed quantum state supported on an entangled subspace is necessarily entangled [5, 6], but numerous other applications have appeared in recent years. For example, entangled subspaces can be used to construct entanglement witnesses [7, 8] and to perform quantum error correction [9, 10]. Further applications of this problem and its robust variants include determining the performance of QMA(2) protocols, computing the geometric measure of entanglement, and determining the ground-state energy of mean-field Hamiltonians as examples [11]. (For yet more applications, the reference [11] contains a compendium of 21 equivalent or closely related problems in quantum information and computer science!)

In the multipartite setting of three or more quantum systems, there are different notions of entanglement of a subspace. A completely entangled subspace in one containing no product states [6], while a genuinely entangled subspace is one containing no states that are product across any bipartition (genuine entanglement is a stricter requirement than complete entanglement) [12, 13]. Completely entangled subspaces are useful for locally discriminating pure quantum states [14, 15], while genuinely entangled subspaces have been shown to have applications in quantum cryptography [16].

Determining whether or not a subspace is entangled is a difficult problem (see [17] or [11, Corollary 14], for example). To certify that a subspace is not entangled, it suffices to present a product vector in that subspace, but it is hard to actually find such a product vector in the first place. In the other direction, it is not known how to efficiently show that a given subspace *is* entangled, even with the help of a certificate. To date, the only practical methods known for solving this problem work in very limited situations, such as when the subspace's dimension is smaller than the local dimensions [18–20], or when the dimensions are small enough that separability hierarchies based on semidefinite programming can be employed [21–23].

We solve this problem by presenting a hierarchy of linear systems that can be used to certify that a given subspace is entangled. Our hierarchy is distinct from other hierarchies commonly used in quantum information theory; known semidefinite programming hierarchies are based on symmetric extensions and/or the sum of squares hierarchies [21], while our hierarchy is based on Hilbert's projective Nullstellensatz from algebraic geometry [24]. As a result, our hierarchy terminates (i.e., detects every entangled subspace) at a finite level that depends only on the local dimensions; something that is known not to be possible for separability-based hierarchies like symmetric extensions [25].

Our hierarchy works extremely well in practice, with even its first level being able to certify entanglement in subspaces that are much larger (quadratic in the local dimensions) than can be handled by other known techniques. The hierarchy also generalizes straightforwardly to r-entangled subspaces (i.e., subspaces in which every pure state has large Schmidt rank [26]), as well as to multipartite completely entangled subspaces and genuinely entangled subspaces. It also provides, as an immediate corollary, a new separability criterion that works well at detecting entanglement in low-rank mixed quantum states; even ones whose entanglement cannot be detected by

the partial transpose [27] (i.e., bound entangled states [28]). We provide MATLAB code that implements all of our methods [29].

THE FIRST LEVEL OF THE HIERARCHY

We use $\mathcal{H}_A$ and $\mathcal{H}_B$ to denote finite-dimensional complex Hilbert spaces (which can be thought of as $\mathbb{C}^{d_A}$ and $\mathbb{C}^{d_B}$) of dimension d_A and d_B, respectively. A pure state $|x\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ (i.e., a unit column vector) is said to be a *product state* if it can be written in the form $|x\rangle = |v\rangle \otimes |w\rangle$ for some $|v\rangle \in \mathcal{H}_A$ and $|w\rangle \in \mathcal{H}_B$, and it is said to have *Schmidt rank r* (denoted by $\mathrm{SR}(|x\rangle) = r$) if it can be written as a linear combination (i.e., superposition) of r product states but not fewer. A subspace of $\mathcal{H}_A \otimes \mathcal{H}_B$ is called *r-entangled* (or just *entangled* if $r = 1$) if every pure state in it has Schmidt rank $r + 1$ or larger.

The starting point of our hierarchy for certifying that a given subspace is r-entangled is the observation that, for $|x\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$, we have $\mathrm{SR}(|x\rangle) \leq r$ if and only if

$$(P^{\wedge}_{A,r+1} \otimes P^{\wedge}_{B,r+1})(|x\rangle^{\otimes(r+1)}) = 0, \tag{1}$$

where $P^{\wedge}_{A,r+1}$ is the projection onto the antisymmetric subspace of $\mathcal{H}_A^{\otimes(r+1)}$ (and similarly for the "B" subscripts). This is a classical result in algebraic geometry (see e.g., [30]), and it has been used in a variety of contexts. For example, it appeared in a tensor decomposition algorithm in [31], and a similar observation was made in [32], where antisymmetric projections were used to create a semidefinite programming hierarchy for computing the Schmidt number of a mixed state.

For brevity, we define

$$\Phi^1_r \stackrel{\text{def}}{=} P^{\wedge}_{A,r+1} \otimes P^{\wedge}_{B,r+1}, \tag{2}$$

and for completeness, we formally state and prove the observation that we just made about Φ^1_r:

Proposition 1. *Suppose $|x\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ and let Φ^1_r be the linear map from Equation* (2)*. Then $\mathrm{SR}(|x\rangle) \leq r$ if and only if $\Phi^1_r(|x\rangle^{\otimes(r+1)}) = 0$.*

Proof. Write $|x\rangle$ in its Schmidt decomposition $|x\rangle = \sum_{j=1}^{s} \lambda_j |v_j\rangle \otimes |w_j\rangle$ with $s = \mathrm{SR}(|x\rangle)$. Then

$$\begin{aligned}\Phi^1_r(|x\rangle^{\otimes(r+1)}) &= (P^{\wedge}_{A,r+1} \otimes P^{\wedge}_{B,r+1})(|x\rangle^{\otimes(r+1)}) \\ &= \sum_{j_1,\ldots,j_{r+1}=1}^{s} \lambda_{j_1} \cdots \lambda_{j_{r+1}} P^{\wedge}_{A,r+1}\Big(|v_{j_1}\rangle \otimes \cdots \otimes |v_{j_{r+1}}\rangle\Big) \otimes P^{\wedge}_{B,r+1}\Big(|w_{j_1}\rangle \otimes \cdots \otimes |w_{j_{r+1}}\rangle\Big).\end{aligned}$$

If $s \leq r$ then $\{|v_{j_1}\rangle, \ldots, |v_{j_{r+1}}\rangle\}$ is a set containing r or fewer members, so $P^{\wedge}_{A,t}(|v_{j_1}\rangle \otimes \cdots \otimes |v_{j_{r+1}}\rangle) = 0$, so $\Phi^1_r(|x\rangle^{\otimes(r+1)}) = 0$.

On the other hand, if $s > r$ then for any $1 \leq \widetilde{j_1} < \cdots < \widetilde{j_{r+1}} \leq s$ we have

$$\begin{aligned}&(\langle v_{\widetilde{j_1}}| \otimes \cdots \otimes \langle v_{\widetilde{j_{r+1}}}|)P^{\wedge}_{A,r+1}(|v_{j_1}\rangle \otimes \cdots \otimes |v_{j_{r+1}}\rangle) \\ &= (\langle w_{\widetilde{j_1}}| \otimes \cdots \otimes \langle w_{\widetilde{j_{r+1}}}|)P^{\wedge}_{B,r+1}(|w_{j_1}\rangle \otimes \cdots \otimes |w_{j_{r+1}}\rangle),\end{aligned}$$

and this quantity is non-zero if and only if $\{\widetilde{j_1}, \ldots, \widetilde{j_{r+1}}\} = \{j_1, \ldots, j_{r+1}\}$. It follows that

$$\Big(\langle v_{\widetilde{j_1}}| \otimes \cdots \otimes \langle v_{\widetilde{j_{r+1}}}| \otimes \langle w_{\widetilde{j_1}}| \otimes \cdots \otimes \langle w_{\widetilde{j_{r+1}}}|\Big)\Phi^1_r(|x\rangle^{\otimes(r+1)})$$

is non-zero (in fact, strictly positive). In particular, this means that $\Phi^1_r(|x\rangle^{\otimes(r+1)}) \neq 0$, completing the proof. □

The superscript "1" in the notation Φ^1_r refers to the fact that this map gives us the first level of our hierarchy for certifying that a subspace of $\mathcal{H}_A \otimes \mathcal{H}_B$ is r-entangled:

Theorem 2. *Let $\mathcal{S} \subseteq \mathcal{H}_A \otimes \mathcal{H}_B$ be a subspace with basis $\{|x_1\rangle, \ldots, |x_{d_S}\rangle\}$. If the set*

$$\Big\{\Phi^1_r(|x_{j_1}\rangle \otimes \cdots \otimes |x_{j_{r+1}}\rangle) : 1 \leq j_1 \leq \cdots \leq j_{r+1} \leq d_S\Big\} \tag{3}$$

is linearly independent then $\mathcal{S}$ is r-entangled.

We provide a brief proof of this theorem here, even though it is a special case of the upcoming Theorem 4. The reason for this is that Theorem 2 is rather straightforward to prove, and it is instructive to see where this base of the hierarchy comes from, whereas the proof of the more general Theorem 4 is quite long and technical (and thus left to the appendix).

Proof of Theorem 2. By Proposition 1, the subspace $\mathcal{S}$ is r-entangled if and only if

$$\Phi^1_r\left(\Big(\sum_{i=1}^{d_S} c_i |x_i\rangle\Big)^{\otimes(r+1)}\right) \neq 0 \tag{4}$$

for all non-zero $c_1, \ldots, c_{d_S} \in \mathbb{C}$.

By linearity and symmetry of Φ^1_r, it holds that

$$\begin{aligned}&\Phi^1_r\left(\Big(\sum_{i=1}^{d_S} c_i |x_i\rangle\Big)^{\otimes(r+1)}\right) \\ &\quad= \sum_{i_1,\ldots,i_{r+1}=1}^{d_S} c_{i_1} \cdots c_{i_{r+1}} \Phi^1_r(|x_{i_1}\rangle \otimes \cdots \otimes |x_{i_{r+1}}\rangle) \\ &\quad= \sum_{i_1 \leq \cdots \leq i_{r+1}} \mu^{\ell,r+1}_{i_1,\ldots,i_{r+1}} c_{i_1} \cdots c_{i_{r+1}} \Phi^1_r(|x_{i_1}\rangle \otimes \cdots \otimes |x_{i_{r+1}}\rangle),\end{aligned} \tag{5}$$

where $\mu^{\ell,r+1}_{i_1,\ldots,i_{r+1}}$ is some multinomial coefficient that counts how many times the term $c_{i_1}\cdots c_{i_{r+1}}\Phi^1_r(|x_{i_1}\rangle\otimes\cdots\otimes|x_{i_{r+1}}\rangle)$ appears in the second line of Equation (5).

If Equation (4) does *not* hold then it follows from Equation (5) that there is some linear combination of the vectors of the form $\Phi^1_r(|x_{i_1}\rangle\otimes\cdots\otimes|x_{i_{r+1}}\rangle)$ that equals 0 (i.e., the set (4) is linearly dependent). The theorem is simply the contrapositive of this statement. □

Since the set (3) consists of $\binom{d_S+r}{r+1}$ vectors, each living inside the $\binom{d_A}{r+1}\binom{d_B}{r+1}$-dimensional range of Φ^1_r, Theorem 2 can be implemented by determining whether or not a homogeneous $\binom{d_A}{r+1}\binom{d_B}{r+1}\times\binom{d_S+r}{r+1}$ linear system has a non-zero solution. Despite just being the first level of the hierarchy, this linear system can already certify r-entanglement of subspaces that are significantly larger than the local dimensions d_A and d_B; a fact that we now illustrate with several examples and an additional proposition.

We say that a property holds for a *generic d_S-dimensional subspace of $\mathcal{H}_A\otimes\mathcal{H}_B$* if it holds with probability one for a Haar-random d_S-dimensional subspace of $\mathcal{H}_A\otimes\mathcal{H}_B$ (see e.g., [14, Definition 2.2] for the definition of a Haar-random subspace) [33]. It is known that the maximum dimension of an r-entangled subspace is $(d_A-r)(d_B-r)$ [26]. For $r=1$, the following proposition shows that the first level of the hierarchy already certifies entanglement of a generic subspace of dimension up to a constant multiple of this maximum. This is surprising, given that the best-known algorithm in the worst case for determining whether a subspace is entangled or not runs in time exponential in $\sqrt{d_A}$ when $d_A=d_B$ [34].

Proposition 3. *In the notation of Theorem 2, if $r=1$ then the set* (3) *is linearly independent for a generic subspace of dimension $d_S<(d_A-1)(d_B-1)/4$.*

We defer the proof of this proposition to the appendix.

Proposition 3 gives a sufficient condition for a generic subspace of dimension d_S to be certified by the first level of our hierarchy. In the opposite direction, by just considering the size of the linear system that Theorem 2 describes, we know that

$$\binom{d_S+r}{r+1}\leq\binom{d_A}{r+1}\binom{d_B}{r+1} \tag{6}$$

is necessary.

The following pair of examples show that this bound is in fact tight in many cases, i.e., the first level of our hierarchy certifies entanglement of any subspace $\mathcal{S}$ for which d_S satisfies Inequality (6).

Example 1. *When $d_A=d_B=4$ and $r=1$, Inequality* (6) *holds exactly when $d_S\leq 8$, so the largest subspace that we can hope to certify is entangled via Theorem 2 has dimension* 8. *It indeed works all the way up to dimension* 8*, getting quite close to the maximum dimension of entangled subspaces of $(d_A-r)(d_B-r)=9$ in this case.*

For example, following the construction of large entangled subspaces from [26], consider the subspace

$$\mathcal{S}=\text{span}\{|x_1\rangle,\ldots,|x_8\rangle\}\subset\mathcal{H}_A\otimes\mathcal{H}_B,$$

where (here we omit normalization factors for brevity, and we use $|j\rangle$ to denote the j-th standard basis vector of $\mathcal{H}_A$ and $\mathcal{H}_B$)

$$\begin{aligned}
|x_1\rangle &= |0\rangle\otimes|0\rangle+|1\rangle\otimes|1\rangle+|2\rangle\otimes|2\rangle+|3\rangle\otimes|3\rangle,\\
|x_2\rangle &= |0\rangle\otimes|0\rangle-|1\rangle\otimes|1\rangle+|2\rangle\otimes|2\rangle-|3\rangle\otimes|3\rangle,\\
|x_3\rangle &= |0\rangle\otimes|1\rangle+|1\rangle\otimes|2\rangle+|2\rangle\otimes|3\rangle,\\
|x_4\rangle &= |1\rangle\otimes|0\rangle+|2\rangle\otimes|1\rangle+|3\rangle\otimes|2\rangle,\\
|x_5\rangle &= |0\rangle\otimes|1\rangle+2|1\rangle\otimes|2\rangle+3|2\rangle\otimes|3\rangle,\\
|x_6\rangle &= |1\rangle\otimes|0\rangle+2|2\rangle\otimes|1\rangle+3|3\rangle\otimes|2\rangle,\\
|x_7\rangle &= |0\rangle\otimes|2\rangle+|1\rangle\otimes|3\rangle, \quad \textit{and}\\
|x_8\rangle &= |2\rangle\otimes|0\rangle+|3\rangle\otimes|1\rangle.
\end{aligned}$$

To show that $\mathcal{S}$ is entangled, it suffices to solve the $\binom{d_A}{r+1}\binom{d_B}{r+1}\times\binom{d_S+r}{r+1}=36\times 36$ linear system described by Theorem 2. Doing so reveals that the set (3) *is indeed linearly independent, so $\mathcal{S}$ is entangled.*

Similarly, we generated 10^5 Haar-random 8-dimensional subspaces of $\mathcal{H}_A\otimes\mathcal{H}_B$, and Theorem 2 detected their entanglement every single time (we will show in the upcoming Theorem 4 that this behavior is expected).

Example 2. *When $d_A=d_B=4$ and $r=2$, Inequality* (6) *holds exactly when $d_S\leq 3$, so the largest subspace that we can hope to certify is 2-entangled via Theorem 2 has dimension* 3*. Many subspaces of this dimension are indeed certified, such as the span of the states $|x_1\rangle$, $|x_3\rangle$, and $|x_4\rangle$ from Example 1. Performing this certification simply requires us to solve a $\binom{d_A}{r+1}\binom{d_B}{r+1}\times\binom{d_S+r}{r+1}=16\times 10$ linear system.*

Similarly, we generated 10^5 Haar-random 3-dimensional subspaces of $\mathcal{H}_A\otimes\mathcal{H}_B$, and Theorem 2 detected their 2-entanglement every single time.

Table I provides some numerics that show the maximum dimension of an r-entangled subspace that can be certified by Theorem 2 (which, in all cases displayed, is equal to the largest value of d_S for which Inequality (6) holds) in various local dimensions, as well as the amount of time that it takes our code to certify such a subspace on a standard desktop computer. The subspaces that we checked to obtain these timings have a form that is similar to that of the subspace from Example 1. We note that the $r=2$ timings are significantly higher than the $r=1$ timings since the dimensions of the linear system that must be solved ($\binom{d_A}{r+1}\binom{d_B}{r+1}\times\binom{d_S+r}{r+1}$) grows quickly with r.

THE REST OF THE HIERARCHY

For an integer $k\geq 1$, the k-th level of our hierarchy is based on the following linear map acting on $(\mathcal{H}_A\otimes\mathcal{H}_B)^{\otimes(r+k)}$:

$$\Phi^k_r \stackrel{\text{def}}{=} (P^{\wedge}_{A,r+1}\otimes P^{\wedge}_{B,r+1}\otimes I_{AB,k-1})P^{\vee}_{AB,r+k}, \tag{7}$$

	$r = 1$		$r = 2$	
$d_A = d_B$	max. d_S	time	max. d_S	time
3	3	0.01 s	1	0.03 s
4	8	0.03 s	3	0.19 s
5	13	0.08 s	7	0.65 s
6	20	0.20 s	12	2.38 s
7	29	0.49 s	18	8.17 s
8	39	1.06 s	25	27.46 s
9	50	2.24 s	33	1.78 min
10	63	5.56 s	43	14.62 min

Table I. The maximum dimension d_S of a subspace of $\mathcal{H}_A \otimes \mathcal{H}_B$ that can be certified to be r-entangled by the first level of the hierarchy (i.e., Theorem 2), as well as the time required to do the certification, for small values of $d_A = d_B$ and r. In all cases shown here, the maximum dimension is the largest d_S for which Inequality (6) holds.

where $I_{AB,k-1}$ is the identity on $(\mathcal{H}_A \otimes \mathcal{H}_B)^{\otimes(k-1)}$ and $P^{\vee}_{AB,r+k}$ is the projection onto the $\binom{d_A d_B + r + k - 1}{r+k}$-dimensional symmetric subspace of $(\mathcal{H}_A \otimes \mathcal{H}_B)^{\otimes(r+k)}$ (i.e., the symmetrization is performed between the $r + k$ copies of $\mathcal{H}_A \otimes \mathcal{H}_B$, but not between $\mathcal{H}_A$ and $\mathcal{H}_B$).

In the $k = 1$ case, Φ^k_r is exactly the same as the linear map Φ^1_r from Equation (2), which can be seen by noting that $\text{range}(P^{\wedge}_{A,r+1} \otimes P^{\wedge}_{B,r+1}) \subseteq \text{range}(P^{\vee}_{AB,r+1})$. Theorem 2 still works if Φ^1_r is replaced by Φ^k_r, but we now furthermore get a converse that completely characterizes *all* r-entangled subspaces:

Theorem 4. *Let $\mathcal{S} \subseteq \mathcal{H}_A \otimes \mathcal{H}_B$ be a subspace with basis $\{|x_1\rangle, \ldots, |x_{d_S}\rangle\}$. Then $\mathcal{S}$ is r-entangled if and only if there exists an integer $1 \leq k \leq (\max\{r, 2\} + 1)^{d_A d_B} - r$ such that the set*

$$\left\{\Phi^k_r(|x_{j_1}\rangle \otimes \cdots \otimes |x_{j_{r+k}}\rangle) : 1 \leq j_1 \leq \cdots \leq j_{r+k} \leq d_S\right\} \qquad (8)$$

is linearly independent. Furthermore, if a subspace $\mathcal{S}$ is certified to be r-entangled at the k-th level of the hierarchy (i.e., if the set (8) is linearly independent), then a generic d_S-dimensional subspace will be certified at the k-th level.

The proof of Theorem 4 is rather long and technical, so we defer it to the appendix, but the rough idea behind it is as follows. The set of pure states in $\mathcal{H}_A \otimes \mathcal{H}_B$ with Schmidt rank at most r is an algebraic variety (i.e., can be defined via polynomial equations), since $\text{SR}(|x\rangle) \leq r$ if and only if every $(r + 1) \times (r + 1)$ submatrix of the matricization of $|x\rangle$ has determinant zero. Numerous tools from algebraic geometry are thus at our disposal for this problem, and in particular we use Hilbert's nullstellensatz to establish the hierarchy.

Theorem 4 really does establish a *hierarchy* for detecting r-entanglement in a subspace: if the set (8) is linearly independent for a particular value of k, then it is linearly independent for all larger values of k as well. While this hierarchy is only guaranteed to detect *all* r-entangled subspaces at its very high $k = (\max\{r, 2\} + 1)^{d_A d_B} - r$ level, it is remarkable that a bound that does not depend on $\mathcal{S}$ exists at all (after all, no analogous bound can exist for semidefinite programming hierarchies for the separability problem [25]). Furthermore, the last sentence of the theorem allows us to show in practice that a much lower level (i.e., smaller value of k) suffices to detect most r-entangled subspaces, simply by finding a single r-entangled subspace of the maximal dimension $(d_A - r)(d_B - r)$ that is detected at that low level.

We have found such examples already at the $k = 2$ level of the hierarchy in many low-dimensional cases. Example 3 illustrates how such a certification at the 2nd level of the hierarchy works, and Table II provides some numerics to show how long it takes this 2nd level of the hierarchy to certify r-entanglement of a maximum-dimensional subspace for some small values of the local dimensions and r.

Example 3. *Suppose $d_A = d_B = 4$, $r = 1$, and $|x_1\rangle, \ldots, |x_8\rangle$ are as in Example 1. If*

$$|x_9\rangle = \frac{1}{2}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle - |2\rangle \otimes |2\rangle - |3\rangle \otimes |3\rangle)$$

then $\mathcal{S} := \text{span}\{|x_1\rangle, \ldots, |x_9\rangle\}$ cannot possibly be shown to be entangled by the first level of the hierarchy, since its dimension is too large. However, solving the $\binom{d_A}{r+1}\binom{d_B}{r+1}(d_A d_B)^{k-1} \times \binom{d_S + r + k - 1}{r+k} = 576 \times 165$ linear system described by the second level of the hierarchy (i.e., Theorem 4 when $k = 2$) verifies that it is indeed entangled.

As a bit of a side note, we observe that the number of rows in this linear system could be taken to be slightly less than $\binom{d_A}{r+1}\binom{d_B}{r+1}(d_A d_B)^{k-1}$, since $\text{rank}(\Phi^k_r)$ is actually smaller than $\text{rank}(P^{\wedge}_{A,r+1} \otimes P^{\wedge}_{B,r+1} \otimes I_{AB,k-1}) = \binom{d_A}{r+1}\binom{d_B}{r+1}(d_A d_B)^{k-1}$. However, indexing the range of Φ^k_r so as to take advantage of this (or even computing its rank exactly) is quite difficult.

	$r = 1, k = 2$		$r = 2, k = 2$	
$d_A = d_B$	max. d_S	time	max. d_S	time
3	4	0.11 s	1	0.58 s
4	9	0.47 s	4	7.39 s
5	16	1.38 s	9	22.01 s
6	25	8.04 s	16	2.59 min
7	36	48.42 s	25	33.18 min

Table II. A summary of how long it takes the 2nd level of the hierarchy (i.e., Theorem 4 with $k = 2$) to certify r-entanglement of a subspace of $\mathcal{H}_A \otimes \mathcal{H}_B$ with dimension $(d_A - r)^2$ (i.e., the maximum dimension), for small values of $d_A = d_B$ and r.

The size of the linear system described by Theorem 4 increases exponentially with k. However, it is also very sparse, so it can typically be solved even if it has hundreds of thousands of rows and columns.

CERTIFYING SCHMIDT NUMBER OF LOW-RANK MIXED STATES

The Schmidt number [35] of a mixed quantum state ρ acting on $\mathcal{H}_A \otimes \mathcal{H}_B$, denoted by $\mathrm{SN}(\rho)$, is the least integer r such that ρ is a convex combination of projectors onto Schmidt-rank-r pure states from $\mathcal{H}_A \otimes \mathcal{H}_B$:

$$\rho = \sum_j p_j |v_j\rangle\langle v_j|, \tag{9}$$

where $\{p_j\}$ is a probability distribution and each $|v_j\rangle$ has Schmidt rank at most r. If $\mathrm{SN}(\rho) = 1$ then ρ is called separable, and it is called entangled otherwise [36].

Determining whether a given mixed state is separable or entangled (or more generally, determining a state's Schmidt number) is a hard problem [37, 38], so in practice numerous one-sided tests are used. One such test is the range criterion [5], which says that if $\mathrm{range}(\rho)$ is not spanned by members of $\mathcal{H}_A \otimes \mathcal{H}_B$ with Schmidt rank at most r, then $\mathrm{SN}(\rho) \geq r + 1$ (a fact that follows immediately from the decomposition (9) of ρ).

While the range criterion is simple to state and prove, actually making use of it is difficult, since it is difficult to show that a given subspace of $\mathcal{H}_A \otimes \mathcal{H}_B$ is not spanned by pure states with small Schmidt rank. Theorem 4 helps solve this problem, and immediately gives us the following result:

Corollary 1. *Let ρ be a mixed state acting on $\mathcal{H}_A \otimes \mathcal{H}_B$ with $d = \mathrm{rank}(\rho)$, and let $\{|x_1\rangle, \ldots, |x_d\rangle\} \subseteq \mathcal{H}_A \otimes \mathcal{H}_B$ be a basis of* $\mathrm{range}(\rho)$*. If there exists an integer $k \geq 1$ such that*

$$\left\{\Phi_r^k(|x_{j_1}\rangle \otimes \cdots \otimes |x_{j_{r+k}}\rangle) : 1 \leq j_1 \leq \cdots \leq j_{r+k} \leq d\right\} \tag{10}$$

is linearly independent, then $\mathrm{SN}(\rho) \geq r + 1$.

This corollary works best when applied to low-rank mixed states, and in particular we expect the first (i.e., $k = 1$) level of the hierarchy to detect most states' Schmidt number when $d_S = \mathrm{rank}(\rho)$ satisfies Inequality (6). Higher levels of the hierarchy allow for the certification of Schmidt number of higher-rank states, even ones whose entanglement cannot be detected by the celebrated positive partial transpose (PPT) criterion [27].

Example 4. *Recall that if $U \subseteq \mathcal{H}_A \otimes \mathcal{H}_B$ is an unextendible product basis [6], then the density matrix*

$$\rho_U := \frac{1}{d_A d_B - |U|}\left(I - \sum_{|v\rangle \in U} |v\rangle\langle v|\right)$$

is a PPT entangled state. For example, let $d_A = d_B = 3$ and consider the 5-state "Tiles" UPB [39] (here we omit normalization factors for brevity):

$$\begin{aligned} U_{\text{tiles}} := \{&|0\rangle \otimes (|0\rangle - |1\rangle), |2\rangle \otimes (|1\rangle - |2\rangle) \\ &(|0\rangle - |1\rangle) \otimes |2\rangle, (|1\rangle - |2\rangle) \otimes |0\rangle, \\ &(|0\rangle + |1\rangle + |2\rangle) \otimes (|0\rangle + |1\rangle + |2\rangle)\} \subset \mathcal{H}_A \otimes \mathcal{H}_B. \end{aligned}$$

The associated PPT entangled state $\rho_{U_{\text{tiles}}}$ has $d = \mathrm{rank}(\rho_{U_{\text{tiles}}}) = 4$, which is too high-rank for the $k = 1$ level of Corollary 1 to be able to detect entanglement in.

However, we can apply the second level of that hierarchy by picking a basis of $\mathrm{range}(\rho)$ *and then solving the $\binom{d_A}{r+1}\binom{d_B}{r+1}(d_A d_B)^{k-1} \times \binom{d+r+k-1}{r+k} = 81 \times 20$ linear system described by Corollary 1. Doing so certifies (in about* 0.1 *seconds) that $\rho_{U_{\text{tiles}}}$ is entangled.*

The above example is not a fluke: the map Φ_1^k detects entanglement in most low-rank states. For example, repeating the above example with the "Tiles" UPB replaced by any of the "Pyramid" [6], "QuadRes", or "GenTiles2" UPBs [39] yields the exact same conclusions: Φ_1^2 detects the entanglement in the associated PPT entangled state.

The following example shows how the same method can be used to show that a low-rank mixed state isn't just entangled, but has Schmidt number strictly larger than 2:

Example 5. *Let $d_A = d_B = 4$ and consider the mixed state*

$$\rho = \frac{1}{3}\sum_{j=1}^{3} |x_j\rangle\langle x_j| \in \mathcal{H}_A \otimes \mathcal{H}_B,$$

where (we again omit normalization factors for brevity)

$$\begin{aligned} |x_1\rangle &= |0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle + |2\rangle \otimes |2\rangle + |3\rangle \otimes |3\rangle, \\ |x_2\rangle &= |0\rangle \otimes |1\rangle + |1\rangle \otimes |2\rangle + |2\rangle \otimes |3\rangle + |3\rangle \otimes |0\rangle, \\ |x_3\rangle &= |0\rangle \otimes |2\rangle + |1\rangle \otimes |3\rangle + |2\rangle \otimes |0\rangle - |3\rangle \otimes |1\rangle. \end{aligned}$$

The PPT criterion readily shows that ρ is entangled (i.e., $\mathrm{SN}(\rho) \geq 2$*), but we can say more by making use of Φ_2^1. In particular, ρ has rank $d = 3$, and solving the $\binom{d_A}{r+1}\binom{d_B}{r+1} \times \binom{d+r}{r+1} = 16 \times 4$ system of linear equations described by Corollary 1 shows that* $\mathrm{SN}(\rho) \geq 3$.

MULTIPARTITE COMPLETELY ENTANGLED SUBSPACES

Our hierarchy generalizes straightforwardly to the multipartite scenario (i.e., the tensor product of three or more Hilbert spaces). For example, a completely entangled subspace (CES) $\mathcal{S}$ of $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$ is one containing no product vector (i.e., no vector of the form $|u\rangle \otimes |v\rangle \otimes |w\rangle$) [3, 4]. We define P_{ABC}^{CES} to be the orthogonal projection onto

$$\wedge^2\mathcal{H}_A \otimes \wedge^2(\mathcal{H}_B \otimes \mathcal{H}_C) + \wedge^2(\mathcal{H}_A \otimes \mathcal{H}_B) \otimes \wedge^2\mathcal{H}_C, \tag{11}$$

where $\wedge^2\mathcal{H}$ denotes the antisymmetric (i.e., wedge) tensor product of two copies of $\mathcal{H}$. We emphasize that the subspace (11) is a sum of subspaces of $(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C)^{\otimes 2}$, but it is not a *direct* sum of subspaces.

Since $|x\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$ is a product vector if and only if it is product across each of the $\mathcal{H}_A \otimes (\mathcal{H}_B \otimes \mathcal{H}_C)$ and $(\mathcal{H}_A \otimes \mathcal{H}_B) \otimes \mathcal{H}_C$ bipartitions, we have $|x\rangle$ being a product vector if and only if $P_{ABC}^{\text{CES}}(|x\rangle^{\otimes 2}) = 0$. If we define the linear map

$$\Phi_{\text{CES}}^k \stackrel{\text{def}}{=} (P_{ABC}^{\text{CES}} \otimes I_{ABC,k-1})P_{ABC,k+1}^{\vee}, \tag{12}$$

then we have the following theorem that is directly analogous to the bipartite hierarchy provided by Theorem 4:

Theorem 5. *Let $\mathcal{S} \subseteq \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$ be a subspace with basis $\{|x_1\rangle, \ldots, |x_{d_S}\rangle\}$. Then $\mathcal{S}$ is completely entangled if and only if there exists an integer $1 \leq k \leq 3^{d_A d_B d_C} - r$ such that the set*

$$\left\{\Phi^k_{\text{CES}}(|x_{j_1}\rangle \otimes \cdots \otimes |x_{j_{k+1}}\rangle) : 1 \leq j_1 \leq \cdots \leq j_{k+1} \leq d_S\right\} \quad (13)$$

is linearly independent. Furthermore, if a subspace $\mathcal{S}$ is detected to be completely entangled at the k-th level of the hierarchy (i.e., if (13) is linearly independent), then a generic d_S-dimensional subspace will be detected at the k-th level.

The above theorem follows from Theorem 6 via analogous arguments to those used in the proof of Theorem 4, in the appendix.

Example 6. *The largest possible dimension of a completely entangled subspace of $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$ is $d_A d_B d_C - d_A - d_B - d_C + 2$, and one particular example of such a subspace is [4]*

$$\begin{aligned}\mathcal{S} := \text{span}\Big\{&|i_A\rangle \otimes |i_B\rangle \otimes |i_C\rangle - |j_A\rangle \otimes |j_B\rangle \otimes |j_C\rangle : \\ &i_A + i_B + i_C = j_A + j_B + j_C \\ &0 \leq i_A, j_A < d_A, 0 \leq i_B, j_B < d_B, 0 \leq i_C, j_C < d_C\Big\}.\end{aligned}$$

Our method is able to certify this maximal-dimension CES for several small values of d_A, d_B, and d_C, as summarized in Table III.

(d_A, d_B, d_C)	max. d_S	level k	time
(2, 2, 2)	4	2	0.12 s
(2, 2, 3)	7	2	0.30 s
(2, 2, 4)	10	2	0.67 s
(2, 2, 5)	13	2	1.21 s
(2, 2, 6)	16	2	3.47 s
(2, 2, 7)	19	2	6.05 s
(2, 2, 8)	22	2	18.90 s
(2, 2, 9)	25	2	38.40 s
(2, 3, 3)	12	3	19.58 s
(2, 3, 4)	17	3	8.24 min
(2, 3, 5)	22	3	2.50 h
(3, 3, 3)	20	4	14.68 h

Table III. A summary of which level k of the hierarchy from Theorem 5 can be used to detect entanglement in the maximum-dimension completely entangled subspace of $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$ from Example 6, for small values of d_A, d_B, and d_C, as well as the computational time taken to do the certification.

Theorem 5 generalizes straightforwardly to the case of $p > 3$ parties using the fact that a multipartite vector $|x\rangle$ is product if and only if it is product across $p - 1$ of its single-party bipartitions, and redefining P^{CES}_{ABC} accordingly. For example, if $p = 4$ then we would define P^{CES}_{ABCD} to be the orthogonal projection onto the (non-direct) sum

$$\begin{aligned}\wedge^2\mathcal{H}_A \otimes \wedge^2(\mathcal{H}_B \otimes \mathcal{H}_C \otimes \mathcal{H}_D) + \wedge^2\mathcal{H}_B \otimes \wedge^2(\mathcal{H}_A \otimes \mathcal{H}_C \otimes \mathcal{H}_D) \\ + \wedge^2\mathcal{H}_C \otimes \wedge^2(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_D)\end{aligned}$$

and then define $\Phi^k_{\text{CES}} = (P^{\text{CES}}_{ABCD} \otimes I_{ABCD,k-1})P^{\vee}_{ABCD,k+1}$. This map, if substituted into Theorem 5, provides a complete hierarchy for detecting completely entangled subspaces in 4-party systems.

MULTIPARTITE GENUINELY ENTANGLED SUBSPACES

Another notion of multipartite entanglement of a subspace is that of a genuinely entangled subspace, which is a subspace in which no pure state is a product state across any bipartition [12, 13]. Genuine entanglement is a stricter requirement than complete entanglement, since pure states can be separable across one or more bipartitions without being a product vector.

Our hierarchy can be applied directly to the case of genuinely entangled subspaces simply by applying Theorem 4 across every bipartition. For example, when trying to certify genuine entanglement of a subspace of $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$, we consider the map Φ^k_1 from Equation (7) with respect to a particular bipartition of $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$. That is, we define

$$\Phi^k_{AB,C} \stackrel{\text{def}}{=} (P^{\wedge}_{AB,2} \otimes P^{\wedge}_{C,2} \otimes I_{ABC,k-1})P^{\vee}_{ABC,k+1},$$

and similarly for $\Phi^k_{AC,B}$ and $\Phi^k_{BC,A}$. Theorem 4 then immediately implies the following corollary:

Corollary 2. *Let $\mathcal{S} \subseteq \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$ be a subspace with basis $\{|x_1\rangle, \ldots, |x_{d_S}\rangle\}$. Then $\mathcal{S}$ is genuinely entangled if and only if there exists an integer $1 \leq k \leq 3^{d_A d_B d_C} - 1$ such that the sets*

$$\begin{aligned}&\left\{\Phi^k_{AB,C}(|x_{j_1}\rangle \otimes \cdots \otimes |x_{j_{1+k}}\rangle) : 1 \leq j_1 \leq \cdots \leq j_{1+k} \leq d_S\right\}, \\ &\left\{\Phi^k_{AC,B}(|x_{j_1}\rangle \otimes \cdots \otimes |x_{j_{1+k}}\rangle) : 1 \leq j_1 \leq \cdots \leq j_{1+k} \leq d_S\right\}, \\ &\left\{\Phi^k_{BC,A}(|x_{j_1}\rangle \otimes \cdots \otimes |x_{j_{1+k}}\rangle) : 1 \leq j_1 \leq \cdots \leq j_{1+k} \leq d_S\right\}\end{aligned}$$

are all linearly independent.

Example 7. *Let $d_A = d_B = d_C = 3$ and consider the 5-dimensional genuinely entangled subspace of $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$ that was introduced in [13] (see Proposition 2 of that paper, and the discussion afterwards). To certify that this subspace is genuinely entangled, we can apply the $k = 1$ case of Corollary 2, which requires us to solve three 108×15 linear systems. Doing so verifies (in about 0.4 seconds) that it is indeed genuinely entangled.*

The above corollary generalizes straightforwardly to any number of parties by similarly applying the map Φ^k_1 from Equation (7) to all $2^{p-1} - 1$ bipartitions of the p parties.

CONCLUSIONS

We have introduced a hierarchy of systems of linear equations for certifying that a given subspace is entangled. This hierarchy is complete in the sense that every entangled subspace is certified to be so at a finite level that is independent

of the subspace being checked. Since the hierarchy only depends on solving a linear system, it can be implemented much more easily, and it runs much quicker, than methods based on semidefinite programming. The hierarchy works extremely well in practice, with many entangled subspaces of interest being detected already at the first or second level, and it generalizes straightforwardly to higher Schmidt rank and the multipartite setting.

ACKNOWLEDGEMENTS

N.J. was supported by NSERC Discovery Grant RGPIN-2022-04098. B.L. acknowledges that this material is based upon work supported by the National Science Foundation under Award No. DMS-2202782. A.V. was supported by the National Science Foundation under grants Grant No. CCF-1652491, CCF 1934931.

* njohnston@mta.ca
† benjamin.lovitz@gmail.com
‡ aravindv@northwestern.edu

[1] O. Gühne and G. Tóth, "Entanglement detection," Physics Reports **474**, 1–75 (2009).
[2] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, "Quantum entanglement," Reviews of Modern Physics **81**, 865–942 (2009).
[3] K. R. Parthasarathy, "On the maximal dimension of a completely entangled subspace for finite level quantum systems," Proc. Indian Acad. Sci. (Math. Sci.) **114**, 365–374 (2004).
[4] B. V. R. Bhat, "A completely entangled subspace of maximal dimension," International Journal of Quantum Information **4**, 325–330 (2006).
[5] P. Horodecki, "Separability criterion and inseparable mixed states with positive partial transposition," Physics Letters A **232**, 333–339 (1997).
[6] C. H. Bennett, D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, and B. M. Terhal, "Unextendible product bases and bound entanglement," Physical Review Letters **82**, 5385–5388 (1999).
[7] R. Augusiak1, J. Tura, and M. Lewenstein, "A note on the optimality of decomposable entanglement witnesses and completely entangled subspaces," Journal of Physics A: Mathematical and Theoretical **44**, 212001 (2011).
[8] D. Chruściński and G. Sarbicki, "Entanglement witnesses: construction, analysis and classification," Journal of Physics A: Mathematical and Theoretical **47**, 483001 (2014).
[9] G. Gour and N. R. Wallach, "Entanglement of subspaces and error-correcting codes," Physical Review A **76**, 042309 (2007).
[10] F. Huber and M. Grassl, "Quantum codes of maximal distance and highly entangled subspaces," Quantum **4**, 284 (2020).
[11] Aram W. Harrow and Ashley Montanaro, "An efficient test for product states with applications to quantum merlin-arthur games," in *2010 IEEE 51st Annual Symposium on Foundations of Computer Science* (2010) pp. 633–642.
[12] M. Demianowicz and R. Augusiak, "From unextendible product bases to genuinely entangled subspaces," Physical Review A **98**, 012313 (2018).
[13] S. Agrawal, S. Halder, and M. Banik, "Genuinely entangled subspace with all-encompassing distillable entanglement across every bipartition," Physical Review A **99**, 032335 (2019).
[14] J. Walgate and A. J. Scott, "Generic local distinguishability and completely entangled subspaces," Journal of Physics A: Mathematical and Theoretical **41**, 375305 (2008).
[15] B. Lovitz and N. Johnston, "Entangled subspaces and generic local state discrimination with pre-shared entanglement," Quantum **6**, 760 (2022).
[16] A. H. Shenoy and R. Srikanth, "Maximally nonlocal subspaces," Journal of Physics A: Mathematical and Theoretical **52**, 095302 (2019).
[17] Jonathan F Buss, Gudmund S Frandsen, and Jeffrey O Shallit, "The computational complexity of some problems of linear algebra," Journal of Computer and System Sciences **58**, 572–596 (1999).
[18] N. Linden, S. Popescu, and J. A. Smolin, "Entanglement of superpositions," Physical Review Letters **97**, 100502 (2006).
[19] G. Gour and A. Roy, "Entanglement of subspaces in terms of entanglement of superpositions," Physical Review A **77**, 012336 (2008).
[20] M. Demianowicz, G. Rajchel-Mieldzioć, and R. Augusiak, "Simple sufficient condition for subspace to be completely or genuinely entangled," New Journal of Physics **23**, 103016 (2021).
[21] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri, "A complete family of separability criteria," Physical Review A **69**, 022308 (2004).
[22] M. Navascués, M. Owari, and M. B. Plenio, "Complete criterion for separability detection," Physical Review Letters **103**, 160404 (2009).
[23] A. W. Harrow, A. Natarajan, and X. Wu, "An improved semidefinite programming hierarchy for testing entanglement," Communications in Mathematical Physics **352**, 881–904 (2017).
[24] J. Harris, *Algebraic Geometry: A First Course*, Graduate Texts in Mathematics (Springer New York, 2013).
[25] H. Fawzi, "The set of separable states has no finite semidefinite representation except in dimension 3×2," Communications in Mathematical Physics **386**, 1319–1335 (2021).
[26] T. S. Cubitt, A. Montanaro, and A. Winter, "On the dimension of subspaces with bounded Schmidt rank," Journal of Mathematical Physics **49**, 022107 (2008).
[27] A. Peres, "Separability criterion for density matrices," Physical Review Letters **77**, 1413–1415 (1996).
[28] M. Horodecki, P. Horodecki, and R. Horodecki, "Mixed-state entanglement and distillation: Is there a "bound" entanglement in nature?" Physical Review Letters **80**, 5239–5242 (1998).
[29] See `http://www.njohnston.ca/publications/entanglement-of-sub` or the supplementary material of the arXiv version of this paper for MATLAB code.
[30] Joseph M. Landsberg, *Tensors: Geometry and Applications*, Graduate studies in mathematics (American Mathematical Society, 2012).
[31] Jean-François Cardoso, "Super-symmetric decomposition of the fourth-order cumulant tensor. blind identification of more sources than sensors." in *ICASSP*, Vol. 91 (Citeseer, 1991) pp. 3109–3112.
[32] G. Tóth, T. Moroder, and O. Gühne, "Evaluating convex roof entanglement measures," Physical Review Letters **114**, 160501 (2015).
[33] All of the genericity statements made here also hold more generally under the algebraic-geometric definition of generic pre-

sented in [15].
[34] Boaz Barak, Pravesh K Kothari, and David Steurer, "Quantum entanglement, sum of squares, and the log rank conjecture," in *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing* (2017) pp. 975–988.
[35] B. M. Terhal and P. Horodecki, "Schmidt number for density matrices," Physical Review A **61**, 040301(R) (2000).
[36] R. F. Werner, "Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model," Physical Review A **40**, 4277–4281 (1989).
[37] S. Gharibian, "Strong NP-hardness of the quantum separability problem," Quantum Information and Computation **10**, 343–360 (2010).
[38] L. Gurvits, "Classical deterministic complexity of Edmonds' problem and quantum entanglement," in *Proceedings of the Thirty-Fifth Annual ACM Symposium on Theory of Computing* (2003) pp. 10–19.
[39] D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, and B. M. Terhal, "Unextendible product bases, uncompletable product bases and bound entanglement," Communications in Mathematical Physics **238**, 379–410 (2003).
[40] J. Kollár, "Sharp effective nullstellensatz," Journal of the American Mathematical Society , 963–975 (1988).

APPENDIX: PROOF OF THEOREM 4 AND PROPOSITION 3

We now prove our main result—Theorem 4, which Theorem 2 occurs as a special case of. We require the following result, which essentially amounts to a translation of Hilbert's projective Nullstellensatz.

Theorem 6. *Let r be a positive integer and let $\Psi_r^1 : \mathcal{H}_X^{\otimes(r+1)} \to \mathcal{H}_Y$ be a linear map that is invariant under all permutations of the $r+1$ copies of $\mathcal{H}_X$, i.e., $\Psi_r^1 P_{X,r+1}^{\vee} = \Psi_r^1$. Then the following statements are equivalent:*

1. *$\Psi_r^1(|x\rangle^{\otimes(r+1)}) \neq 0$ for all pure states $|x\rangle \in \mathcal{H}_X$.*
2. *There exists a positive integer $1 \leq k \leq (\max\{r,2\}+1)^{d_X} - r$ for which $\operatorname{range}(P_{X,r+k}^{\vee}) \cap \ker(\Psi_r^k) = \{0\}$, where $\Psi_r^k := (\Psi_r^1 \otimes I_{X,k-1}) P_{X,r+k}^{\vee}$.*

Proof. For $2 \Rightarrow 1$, if $\operatorname{range}(P_{X,r+k}^{\vee}) \cap \ker(\Psi_r^k) = \{0\}$, then for all pure states $|x\rangle \in \mathcal{H}_X$ it holds that

$$0 \neq \Psi_r^k(|x\rangle^{\otimes(r+k)}) = \Psi_r^1(|x\rangle^{\otimes(r+1)}) \otimes |x\rangle^{\otimes(k-1)},$$

so $\Psi_r^1(|x\rangle^{\otimes(r+1)}) \neq 0$. The converse $1 \Rightarrow 2$ is more difficult, and is obtained by translating Statement 1 to a statement about zeroes of homogeneous polynomials, invoking Hilbert's projective Nullstellensatz, and then translating back.

In more details, first observe that the coordinates of $\Psi_r^1(|x\rangle^{\otimes(r+1)})$ as $|x\rangle$ ranges over the unit vectors in $\mathcal{H}_X$ can be written as homogeneous d_X-variate polynomials $p_1, \ldots, p_{d_Y}$ in $|x\rangle$ of degree $r+1$, so Statement 1 is equivalent to there being no unit vector $|x\rangle$ (or equivalently, by scaling, no nonzero vector $|x\rangle$) for which $p_1(|x\rangle) = \cdots = p_{d_Y}(|x\rangle) = 0$. By Hilbert's projective Nullstellensatz and a degree bound due to Kollár, this is equivalent to the existence of a positive integer $1 \leq k \leq (\max\{r,2\}+1)^{d_X} - r$ for which every degree $r+k$ monomial $x_{j_1} \cdots x_{j_{r+k}}$ can be written as a linear combination of the polynomials $q_{i_1,\ldots,i_{k-1},j} \stackrel{\text{def}}{=} x_{i_1} \cdots x_{i_{k-1}} p_\ell$, where $i_1, \ldots, i_{k-1}$ range from 1 to d_X, and ℓ ranges from 1 to d_Y [24, 40].

As with $\Psi_r^1(|x\rangle^{\otimes(r+1)})$, the coordinates of $\Psi_r^k(|x\rangle^{\otimes(r+k)})$ as $|x\rangle$ ranges over the unit vectors in $\mathcal{H}_X$ can be written as homogeneous d_X-variate polynomials of degree $r+k$. Direct calculation shows that these polynomials are precisely $q_{i_1,\ldots,i_{k-1},j}$ (the identity map $I_{X,k-1}$ that appears in the definition of Ψ_r^k produces the monomials $x_{i_1} \cdots x_{i_{k-1}}$). Since every monomial $x_{j_1} \cdots x_{j_{r+k}}$ can be written as a linear combination of the polynomials $q_{i_1,\ldots,i_{k-1},j}$, there exists a linear map $\Xi : \mathcal{H}_Y \otimes \mathcal{H}_X^{\otimes(k-1)} \to \mathcal{H}_X^{\otimes(r+k)}$ for which $\Xi \circ \Psi_r^k(|x\rangle^{\otimes(r+k)}) = |x\rangle^{\otimes(r+k)}$ for all $|x\rangle \in \mathcal{H}_X$. It follows that

$$\ker(\Psi_r^k) \cap \operatorname{span}\{|x\rangle^{\otimes(r+k)} : |x\rangle \in \mathcal{H}_X\} = \{0\}.$$

This completes the proof, since $\operatorname{span}\{|x\rangle^{\otimes(r+k)} : |x\rangle \in \mathcal{H}_X\} = \operatorname{range}(P_{X,r+k}^{\vee})$. □

In the following proof of Theorem 4, we make use of Theorem 6 in the special case where $\mathcal{H}_X = \mathcal{H}_A \otimes \mathcal{H}_B$ and $\mathcal{H}_Y = (\mathcal{H}_A \otimes \mathcal{H}_B)^{\otimes(r+1)} \oplus (\mathcal{H}_A \otimes \mathcal{H}_B)^{\otimes(r+1)}$.

Proof of Theorem 4. Let $P_{\mathcal{S}}^{\perp}$ be the projection onto the orthogonal complement of $\mathcal{S}$. Then $\mathcal{S}$ is r-entangled if and only if there does not exist $|x\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ for which $\Psi_r^1(|x\rangle^{\otimes(r+1)}) = 0$, where we define

$$\Psi_r^1 : (\mathcal{H}_A \otimes \mathcal{H}_B)^{\otimes(r+1)} \to (\mathcal{H}_A \otimes \mathcal{H}_B)^{\otimes(r+1)} \oplus (\mathcal{H}_A \otimes \mathcal{H}_B)^{\otimes(r+1)}$$

by

$$\Psi_r^1 \stackrel{\text{def}}{=} \begin{bmatrix} \Phi_r^1 \\ (P_{\mathcal{S}}^{\perp} \otimes I_{AB,r}) P_{AB,r+1}^{\vee} \end{bmatrix}.$$

Indeed, by Proposition 1, $\mathcal{S}$ is r-entangled if and only if for every $|x\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ for which $P_{\mathcal{S}}^{\perp}|x\rangle = 0$, it holds that $\Phi_r^1(|x\rangle^{\otimes(r+1)}) \neq 0$, which is easily seen to be equivalent to the above statement about Ψ_r^1.

By Theorem 6, this is in turn equivalent to the existence of a positive integer $1 \leq k \leq (\max\{r,2\}+1)^{d_A d_B} - r$ for which $\operatorname{range}(P_{AB,r+k}^{\vee}) \cap \ker(\Psi_r^k) = \{0\}$, where

$$\Psi_r^k \stackrel{\text{def}}{=} (\Psi_r^1 \otimes I_{AB,k-1}) P_{AB,r+k}^{\vee} = \begin{bmatrix} \Phi_r^k \\ (P_{\mathcal{S}}^{\perp} \otimes I_{AB,r+k-1}) P_{AB,r+k}^{\vee} \end{bmatrix}.$$

Now, $\operatorname{range}(P_{AB,r+k}^{\vee}) \cap \ker(\Psi_r^k) = \{0\}$ if and only if $\operatorname{range}(P_{AB,r+k}^{\vee}) \cap \operatorname{range}(P_{\mathcal{S}} \otimes I_{AB,r+k-1}) \cap \ker(\Phi_r^k) = \{0\}$, where $P_{\mathcal{S}}$ denotes the projection onto $\mathcal{S}$. Observe that

$$\begin{aligned}\operatorname{range}(P^{\vee}_{AB,r+k}) \cap \operatorname{range}(P_{\mathcal{S}} \otimes I_{AB,r+k-1}) &= \operatorname{range}(P^{\vee}_{AB,r+k}) \cap \operatorname{range}(P_{\mathcal{S}}^{\otimes(r+k)}) \\ &= \operatorname{range}(P^{\vee}_{AB,r+k} P_{\mathcal{S}}^{\otimes(r+k)}) \\ &= \operatorname{span}\{P^{\vee}_{AB,r+k}(|x_{j_1}\rangle \otimes \cdots \otimes |x_{j_{r+k}}\rangle) : 1 \le j_1, \ldots, j_{r+k} \le d_S\} \\ &= \operatorname{span}\{P^{\vee}_{AB,r+k}(|x_{j_1}\rangle \otimes \cdots \otimes |x_{j_{r+k}}\rangle) : 1 \le j_1 \le \cdots \le j_{r+k} \le d_S\},\end{aligned}$$

where the first line follows from permutation invariance, the second follows from the fact that the projections $P^{\vee}_{AB,r+k}$ and $P_{\mathcal{S}}^{\otimes(r+k)}$ commute, the third is clear, and the fourth follows from the fact that

$$P^{\vee}_{AB,r+k}(|x_{j_1}\rangle \otimes \cdots \otimes |x_{j_{r+k}}\rangle) = P^{\vee}_{AB,r+k}(|x_{j_{\sigma(1)}}\rangle \otimes \cdots \otimes |x_{j_{\sigma(r+k)}}\rangle)$$

for every permutation σ of $\{1, 2, \ldots, r+k\}$ (i.e., permutation invariance again). By permutation invariance of Φ^k_r, $\mathcal{S}$ is r-entangled if and only if

$$\operatorname{span}\{|x_{j_1}\rangle \otimes \cdots \otimes |x_{j_{r+k}}\rangle : 1 \le j_1 \le \cdots \le j_{r+k} \le d_S\} \cap \ker(\Phi^k_r) = \{0\},$$

i.e., the set in Equation (8) is linearly independent.

For the statement beginning with "Furthermore...," observe that linear independence of the set in Equation (8) is equivalent to the non-vanishing of some $\binom{d_S+r+k-1}{d_S-1} \times \binom{d_S+r+k-1}{d_S-1}$-minor of the matrix formed by taking the vectors in the set as columns. Since this determinant is a polynomial in the entries of $|x_1\rangle, \ldots, |x_{d_S}\rangle$, and any polynomial that is not identically zero vanishes on a set of Haar measure zero, this completes the proof. □

Proof of Proposition 3. A generic subspace $\mathcal{S} \subset \mathcal{H}_A \otimes \mathcal{H}_B$ of dimension d_S can be chosen by picking d_S generic vectors $|x_1\rangle, \ldots, |x_{d_S}\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ for the basis that spans $\mathcal{S}$. Let $G = \{P^{\vee}_{AB,2}(|x_{j_1}\rangle \otimes |x_{j_2}\rangle) : 1 \le j_1 \le j_2 \le d_S\}$. We need to show that with probability 1,

$$\ker(\Phi^1_1) \cap \operatorname{span}(G) = \{0\}. \tag{14}$$

We remark that the above condition is invariant under scaling of the vectors $|x_1\rangle, \ldots, |x_{d_S}\rangle$. Hence, we will ignore the unit vector requirement for $|x_1\rangle, \ldots, |x_{d_S}\rangle$ (and all the vectors) for the purposes of this proof.

We now prove (14). In the set G, the indices j_1, j_2 could be equal. We will partition the $\binom{d_S+1}{2}$ vectors in G into subsets $G_{\text{eq}} = \{P^{\vee}_{AB,2}(|x_j\rangle \otimes |x_j\rangle) : 1 \le j \le d_S\}$ and $G_{\text{neq}} = G \setminus G_{\text{eq}}$ has the terms with unequal indices. To establish (14), it suffices to prove the following claim.

Claim. *With probability* 1 *over the choice of* $|x_1\rangle, \ldots, |x_{d_S}\rangle$, *we have for all* $1 \le j_1 < j_2 \le d_S$, *and all* $1 \le j \le d_S$,

$$P^{\vee}_{AB,2}(|x_{j_1}\rangle \otimes |x_{j_2}\rangle) \notin \operatorname{span}\Big(\ker(\Phi^1_1) \cup G_{\text{neq}} \setminus \{P^{\vee}_{AB,2}(|x_{j_1}\rangle \otimes |x_{j_2}\rangle)\}\Big), \tag{15}$$

and

$$|x_j\rangle^{\otimes 2} \notin \operatorname{span}\Big(\ker(\Phi^1_1) \cup G_{\text{neq}} \cup G_{\text{eq}} \setminus \{|x_j\rangle^{\otimes 2}\}\Big). \tag{16}$$

To prove the claim, we first define the following subspaces. For each $i \in [d_S]$, let

$$\mathcal{U}_i := \operatorname{span}\Big\{P^{\vee}_{AB,2}(|x_i\rangle \otimes |z\rangle) \;:\; |z\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B\Big\}.$$

Note that $\dim(\mathcal{U}_i) \le d_A d_B$ and $\dim(\ker(\Phi^1_1)) = (d_A d_B)^2 - \binom{d_A}{2}\binom{d_B}{2}$.

Consider $P^{\vee}_{AB,2}(|x_{j_1}\rangle \otimes |x_{j_2}\rangle)$ for some $1 \le j_1 \le j_2 \le d_S$, and let $J^* = \{j_1\} \cup \{j_2\}$ representing the distinct indices involved. We observe that if $\mathcal{U}_{-J^*} := \bigcup_{i \in [d_S] \setminus J^*} \mathcal{U}_i$, then

$$\text{If } j_1 < j_2, \;\; G_{\text{neq}} \setminus \{P^{\vee}_{AB,2}(|x_{j_1}\rangle \otimes |x_{j_2}\rangle)\} \subseteq \mathcal{U}_{-J^*}, \tag{17}$$

$$\text{else if } j_1 = j_2, \;\; G_{\text{neq}} \cup G_{\text{eq}} \setminus \{|x_{j_1}\rangle^{\otimes 2}\} \subseteq \mathcal{U}_{-J^*}. \tag{18}$$

This is because when $j_1 < j_2$, every other vector in G_{neq} involves at least one vector $|x_j\rangle$ with $j \in [d_S] \setminus J^*$. Hence (17) is true. Similarly when $j_1 = j_2$, we have (18) since every other vector in both G_{eq} and G_{neq} involves at least one vector $|x_j\rangle$ with $j \in [d_S] \setminus J^*$.

The rest of the argument is the same for both (15) and (16). Let $\mathcal{V}_{-J^*} := \operatorname{im}(P^{\vee}_{AB,2}) \cap \ker(\Phi^1_1) + \mathcal{U}_{-J^*}$. Then

$$\begin{aligned}\dim(\mathcal{V}_{-J^*}) &\le \binom{d_A d_B + 1}{2} - \binom{d_A}{2} \cdot \binom{d_B}{2} + d_S(d_A d_B) \\ &< \binom{d_A d_B + 1}{2},\end{aligned}$$

since $d_S \cdot (d_A d_B) < \binom{d_A}{2}\binom{d_B}{2}$ by our assumption on d_S. It follows that $\mathcal{V}_{-J^*} \subsetneq \operatorname{im}(P^{\vee}_{AB,2})$. Hence $P^{\vee}_{AB,2}(|x_{j_1}\rangle \otimes |x_{j_2}\rangle) \notin \mathcal{V}_{-J^*}$ for a generic choice of $|x_{j_1}\rangle, |x_{j_2}\rangle$ (note that $\mathcal{V}_{-J^*}$ does not depend on $|x_{j_1}\rangle, |x_{j_2}\rangle$). This establishes both (15) and (16), and completes the proof of Proposition 3. □