Local distinguishability of generic unentangled orthonormal bases

Jiří Lebl, Asif Shakeel, and Nolan Wallach

Phys. Rev. A **93**, 012330 — Published 20 January 2016

DOI: 10.1103/PhysRevA.93.012330

Local Distinguishability of Generic Unentangled Orthonormal Bases

Jiří Lebl*
Department of Mathematics, Oklahoma State University, Stillwater, OK 74078, USA

Asif Shakeel† and Nolan Wallach‡
Department of Mathematics, University of California, San Diego, La Jolla, CA 92093-0112, USA

An orthonormal basis consisting of unentangled (pure tensor) elements in a tensor product of Hilbert spaces is an Unentangled Orthogonal Basis (UOB). In general, for n qubits, we prove that in its natural structure as a real variety, the space of UOB is a bouquet of products of Riemann spheres parametrized by a class of edge colorings of hypercubes. Its irreducible components of maximum dimension are products of $2^n - 1$ two-spheres. Using a theorem of Walgate and Hardy, we observe that the UOB whose elements are distinguishable by local operations and classical communication (called *locally distinguishable* or *LOCC distinguishable* UOB) are exactly those in the maximum dimensional components. Bennett et al, in their in-depth study of quantum nonlocality without entanglement, include a specific 3 qubit example UOB which is not LOCC distinguishable; we construct certain generalized counterparts of this UOB in n qubits.

I. INTRODUCTION

Quantum nonlocality through entanglement plays a key role as a resource in quantum teleportation, cryptography and error-correcting codes. There exists, however, another nonlocal phenomenon: quantum nonlocality without entanglement, studied at length by Bennett, DiVincenzo, Fuchs, Mor, Rains, Shor, Smolin, and Wootters in [1]. Locality in this sense refers to the elements of an unentangled orthogonal basis (UOB) being distinguishable by a protocol using only local operations by participants (each holding one tensor factor) and classical communication (LOCC) among them, hence such a UOB is *locally distinguishable* or *LOCC distinguishable*. In [1], the authors provide examples of sets of unentangled states that are not LOCC (locally) distinguishable and therefore exhibit nonlocality, give measurement protocols for their optimal distinguishability, state preparation protocols to obtain them, relation to quantum cryptography, and measures to quantify their nonlocality. This form of nonlocality is connected with construction of entangled states [2], but stands on its own as well [1, 3, 4]. Under protocols in which various parties can only measure their own systems (local measurements) and classically communicate, distinguishing among certain unentangled states is impossible. Thus, such states encode quantum nonlocality. It is demonstrably useful in quantum key distribution (QKD), as first observed by Goldenberg and Vaidman [5], and since used in other schemes for secure communication [6, 7].

The converse is to find sets of states that are identifiable through LOCC. A significant body of work is involved with the criteria for recognizing and constructing such states, particularly pertaining the Unextendible Product Basis (UPB) [1–3, 8], but there have also been some characterizations of Unentangled Orthogonal Basis (UOB) and of the form of nonlocality in unentangled settings in higher dimensions [9, 10]. In this paper we analyze the set of orthonormal bases consisting of unentangled states (UOB) in n qubits. We show that in the natural structure of UOB as an algebraic variety over $\mathbb{R}$, the ones that can be distinguished by LOCC are precisely those belonging to the irreducible components of highest dimension.

The organization of this paper is as follows. In Section II, we motivate and give an initial set of definitions that connect the orthognality condition of a UOB to a set of colorings of a hypercube that we call *admissible*. In Section III, we prove the main result that relates maximum number of colors in an admissible coloring of a hypercube to the maximum dimensional component in the set of UOB, and describe its implications. Section IV discusses the LOCC distinguishability of the UOB, and through the theorem of Walgate and Hardy [4], shows that the maximum dimensional component is the unique such set. In Section V we construct UOB not distinguishable by LOCC, hence exhibiting the said nonlocality, and important from the secure communication point of view. Section VI discusses the directions for further research and certain open questions.

II. ADMISSIBLE COLORINGS AND ORTHOGONALITY

We denote by $\mathcal{H}_n$ the space of n qubits that is $\otimes^n \mathbb{C}^2$ with the tensor product Hilbert structure, $\langle \dots | \dots \rangle$. A state in $\mathcal{H}_n$ is called a product state or unentangled state if it is a tensor product of unit vectors in each $\mathbb{C}^2$. We note that two product states $v_1 \otimes v_2 \otimes \cdots \otimes v_n$ and $w_1 \otimes$

* Jiří Lebl was partially supported by NSF grant DMS-1362337 and Oklahoma State University's DIG and ASR grants.; lebl@math.okstate.edu
† Asif Shakeel was partially supported by NSF award PHY-0955518.; ashakeel@ucsd.edu
‡ Nolan Wallach was partially supported by NSF grant DMS-0963035.; nwallach@ucsd.edu

$w_2 \otimes \cdots \otimes w_n$ satisfy

$$\langle v_1 \otimes v_2 \otimes \cdots \otimes v_n | w_1 \otimes w_2 \otimes \cdots \otimes w_n \rangle = 0$$

if and only if there is at least one i with $\langle v_i | w_i \rangle = 0$. Since states are determined up to phase, to think about them unambiguously we must consider them to be elements of the corresponding projective space. If $z \in \mathbb{C}^2$ is non-zero then we assign to z the complex line $[z]$ through 0 and z. The totality of elements $[z]$, $z \in \mathbb{C}^2 - \{0\}$ is denoted (as usual) as $\mathbb{P}^1$ (one-dimensional projective space over $\mathbb{C}$). Up to phase, the element $v_1 \otimes v_2 \otimes \cdots \otimes v_n$ is considered to be $[v_1] \otimes [v_2] \otimes \cdots \otimes [v_n]$. On $\mathbb{P}^1$ we define a real analytic fixed point free involution:

$$[v] \longmapsto [\hat{v}],$$

which assigns to $[v]$ the line $[\hat{v}]$ perpendicular to it (i.e. $\langle v | \hat{v} \rangle = 0$). If S is a subset of $\mathbb{P}^1$ then $\hat{S}$ denotes the set of $[\hat{s}]$ for $[s]$ in S.

Our first goal is to turn the determination of all UOB into a combinatorial problem on the hypercube Q_n. We think of the vertices of the hypercube as the vectors in $\mathbb{R}^n$ with coordinates in the set $\{0,1\}^n$, and consider this to be binary expansions of numbers $0, 1, \ldots, 2^{n-1}$. We also view Q_n as a graph with vertices $0, 1, \ldots, 2^{n-1}$; its edges are the pairs of numbers whose binary expansions differ in exactly one digit (i.e. pairs with Hamming distance 1).

Let $u_0, u_1, \ldots, u_{2^n-1}$ be a UOB, and write its states as

$$[u_j] = [u_{1j}] \otimes [u_{2j}] \otimes \cdots \otimes [u_{nj}].$$

As observed above, if $i \neq j$ then at least one pair $\{[u_{ki}], [u_{kj}]\}$ must be of the form $\{[v], [\hat{v}]\}$. We consider the subset of $\mathbb{P}^1$ that is the set $\mathcal{T} = \{[u_{kj}] | k = 1, \ldots, n, j = 0, \ldots, 2^n - 1\}$. We divide $\mathcal{T}$ into two disjoint pieces $\mathcal{T}_0$ and $\mathcal{T}_1$ such that $\hat{\mathcal{T}}_i \cap \mathcal{T}_i = \emptyset$, $i = 0, 1$. This implies that if $[t] \in \mathcal{T}_0$ and if $[\hat{t}] \in \mathcal{T}$ then $[\hat{t}] \in \mathcal{T}_1$ and vice-versa. To each $[u_j]$ we assign a vector $s_j \in \mathbb{R}^n$ such that its k–th coordinate is 0 if $[u_{kj}] \in \mathcal{T}_0$ or 1 if $[u_{kj}] \in \mathcal{T}_1$. We note that if we assign to s_j the corresponding element

$$[s_j\rangle = [s_{1j} s_{2j} \ldots s_{nj}\rangle\,,$$

then by its very definition $\{[s_j\rangle \,| j = 0, \ldots, 2^n - 1\}$ is an orthonormal set. This implies that the two sets $\mathcal{T}_0$ and $\mathcal{T}_1$ each consist of exactly half of the elements of $\mathcal{T}$ and that $\mathcal{T}_1 = \hat{\mathcal{T}}_0$. Reordering $\mathcal{T}$, let $\mathcal{T}_0 = \{t_1, \ldots, t_r\}$, such that s_j is just the binary expansion of j. Assume a palette of colors $c_1, c_2, \ldots, c_r, \ldots$ is available. From this palette, we assign to each vertex of Q_n an n–tuple of colors taken from c_j with $1 \leq j \leq r$, such that if the i–factor of u_j is t_j or $\hat{t}_j$, we assign to it the color c_j. This is equivalent to coloring the edges of Q_n. Indeed, let a——b be an edge, so a and b differ in exactly one component, which, by orthonormality, has the same color in both a and b. We give the edge a——b that color. Conversely, given an edge-coloring of Q_n, we can assign an n-tuple of colors to each vertex as follows. For the vertex a and component i, let a^i be the unique vertex with all its components the same as those of a except for the i–th which is opposite. We assign the i–th component of vertex a the color of edge a——a^i.

Definition 1 *A coloring of Q_n is said to be admissible if for every pair of vertices there is a component, i, so that one vertex has a 0 in the i–th position and the other has a 1 and both are assigned the same color in that position.*

If we have a coloring of Q_n with colors $c_1, \ldots, c_k$ and $[u_1], \ldots, [u_k]$ are elements of $\mathbb{P}^1$ then we assign to each vertex $s = s_1 s_2 \ldots s_n$ a product state (up to phase): if the i–component has color c_r and $s_i = 0$ then put $[u_r]$ in the i–th position; if $s_i = 1$ put $[\hat{u}_r]$ in the i–th position. For example, for $n = 3$ we have the admissible coloring given in FIG. 1.

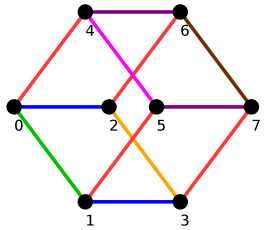

FIG. 1. (Color online) Admissible coloring with 7 colors. The edges 0-4, 1-5, 3-7, 2-6 are red, the edges 0-2, 1-3 are blue, the edges 4-6, 5-7 are violet, the edges 0-1, 4-5, 6-7, and 2-3 are respectively green, purple, brown, and orange.

Here c_1 = green, c_2 = blue, c_3 = red, c_4 = orange, c_5 = purple, c_6 = violet and c_7 = brown. The procedure assigns the UOB:

$$\begin{array}{ll} [u_3] \otimes [u_2] \otimes [u_1], & [u_3] \otimes [u_2] \otimes [\hat{u}_1], \\ [u_3] \otimes [\hat{u}_2] \otimes [u_4], & [u_3] \otimes [\hat{u}_2] \otimes [\hat{u}_4], \\ [\hat{u}_3] \otimes [u_5] \otimes [u_6], & [\hat{u}_3] \otimes [u_5] \otimes [\hat{u}_6], \\ [\hat{u}_3] \otimes [\hat{u}_5] \otimes [u_7], & [\hat{u}_3] \otimes [\hat{u}_5] \otimes [\hat{u}_7]. \end{array} \tag{1}$$

We give the set of UOB of $\mathcal{H}_n$, $\mathcal{U}_n$, its subspace topology in the set of 2^n–tuples of elements of the projective space on $\mathcal{H}_n$, $\mathbb{P}(\mathcal{H}_n)$.

III. MAXIMUM DIMENSIONAL COMPONENT AND MAXIMAL COLORINGS

In this section, we obtain an interesting connection between the admissible colorings and the maximum dimensional component. This comes about through an elegant structure of the admissible colorings when viewed as a combinatorial forest.

Proposition 2 *Fix a pallette of colors $c_1, \ldots, c_k, \ldots$ To each admissible coloring, C, of Q_n with k colors the procedure above yields an injective, continuous mapping*

$$\Phi_C \colon \left(\mathbb{P}^1\right)^k \to \mathcal{U}_n.$$

The union of the images of Φ_C running through all admissible colorings is all of $\mathcal{U}_n$.

For each coloring C the map Φ_C is a homeomorphism onto its image. Thus $\mathcal{U}_n$ is a finite union of smooth manifolds diffeomorphic with $\left(\mathbb{P}^1\right)^k$ for k running through the cardinalities of admissible colorings of Q_n. We introduce a partial order on the set of colorings of Q_n.

Definition 3 *If C_1, C_2 are colorings of Q_n then $C_1 \prec C_2$ if the colors used in C_1 form a subset, S, of those used in C_2 and the set of edges that were colored in C_2 by color $c \notin S$ all have their color replaced by a color in S.*

Lemma 4 *Up to changing the names of the admissible colors $C_1 \prec C_2$ if and only if the image of Φ_{C_1} is contained in that of Φ_{C_2}.*

We make some observations about this ordering. If C is a coloring of Q_n let $C(i)$ denote the colors of the edges with vertices that differ in the i–th position. We change the colors of each $C(i)$ so that $C(i) \cap C(j) = \emptyset$ if $i \neq j$. Thus in a maximal coloring every vertex has n distinct colors. There is a unique minimal coloring (up to changing the names of the colors): the coloring with one color. This coloring yields the tensor product of the standard orthogonal bases of $\mathbb{C}^2$.

We will see in Theorem 6 below that the admissible coloring of Q_3 above is maximal and has the maximum number of colors, 7. This implies that $\mathcal{U}_3$ can be thought of as a bouquet of some fourteen dimensional real manifolds and some lower dimensional ones corresponding to maximal colorings with less than 7 colors. In FIG. 2 is an example of a maximal coloring of Q_3 with 6 colors.

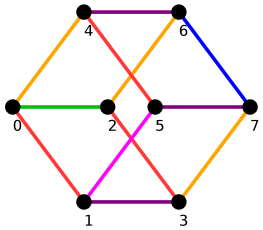

FIG. 2. (Color online) Admissible coloring with 6 colors. The edges 0-4, 3-7, 2-6 are orange, the edges 0-1, 4-5, 2-3 are red, the edges 4-6, 5-7, 1-3 are violet, and the edges 1-5, 0-2, and 6-7 are respectively purple, green, and blue.

The figure corresponds to the UOB:

$$\begin{array}{ll} [u_3]\otimes[u_2]\otimes[u_1], & [u_5]\otimes[u_4]\otimes[\hat{u}_1], \\ [u_3]\otimes[\hat{u}_2]\otimes[u_1], & [u_3]\otimes[\hat{u}_4]\otimes[\hat{u}_1], \\ [\hat{u}_3]\otimes[u_4]\otimes[u_1], & [\hat{u}_5]\otimes[u_4]\otimes[\hat{u}_1], \\ [\hat{u}_3]\otimes[\hat{u}_4]\otimes[u_6], & [\hat{u}_3]\otimes[\hat{u}_4]\otimes[\hat{u}_6]. \end{array}$$

With specific choices of $u_1, \ldots, u_6$, this example appears in [1].

In preparation for our main theorem we give a recursive algorithm for admissibly coloring Q_n with $2^n - 1$ colors, which the theorem asserts is the maximum number. Also Theorem 7 implies this is the only way, up to permuting indices, to color Q_n admissibly with $2^n - 1$ colors.

Lemma 5 *Let C_0 and C_1 be admissible colorings of Q_{n-1}. Writing Q_n as $0 \times Q_{n-1} \cup 1 \times Q_{n-1}$ and choosing a new color c then we color Q_n as follows: all first coordinates are colored with color c if the first index is 0 (respectively 1) then the rest of the indices are colored as in C_0 (resp. C_1). This recipe yields an admissible coloring. In particular, if C_0 and C_1 both use $2^{n-1} - 1$ colors without any repetitions between the colors, then the number of colors is $2^n - 1$ for the coloring of Q_n.*

In FIG. 3 is an example of this method for Q_5 (it uses the algorithm starting with the Q_3 example above with 7 colors to get a Q_4 coloring with 15 colors and then another application to get 31 colors).

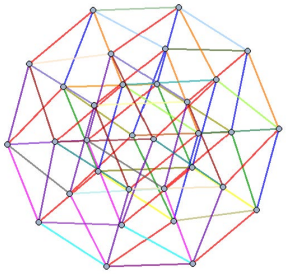

FIG. 3. (Color online) Admissible coloring of Q_5 with 31 colors.

In the proof of the following result we will only use the admissibility of every 2-face of an admissible coloring.

Theorem 6 *(i) Let Q_n be admissibly colored. Then there exists a subforest F (i.e. a subgraph with no circuits) of Q_n that has edges of every possible color in Q_n.*

(ii) The maximum number of colors in an admissible coloring of Q_n is $2^n - 1$.

(iii) Q_n is admissibly colored with $2^n - 1$ colors if and only if some forest in Q_n containing all of its colors each exactly once is a tree that contains all the vertices of Q_n.

(iv) If Q_n is admissibly colored with $2^n - 1$ colors then every subcube Q_m where $m < n$ is also admissibly colored with $2^m - 1$ colors.

Proof. We first show how one can derive (ii) and (iii) from (i). To prove (ii), we note that if a forest consists of k disjoint trees and m vertices then the number of edges is at most $m - k$. Thus if F is the forest asserted in (i) then $m \leq 2^n$. As the number of colors is at most the number of its edges, we have that the number of

colors is at most $2^n - k$, with k the number of connected components (disjoint trees). This proves (ii).

To prove (iii), consider F, a subforest of Q_n containing $2^n - 1$ edges. Then it must contain at least 2^n vertices and the number of connected components is 1. If Q_n is admissibly colored and if F is a tree containing all of its colors each exactly once and all of the vertices of Q_n then since the number of edges is $2^n - 1$, that must be the number of colors.

We now prove (i) by induction on n. If $n = 1, 2$, the result is obvious. So we assume (i) for $n - 1 \geq 2$ and prove the result for n. Let Q_n^j be the set of elements of Q_n with first coordinate j with $j = 0$ or 1. We take each to be an $n-1$ subcube and give each the coloring that it inherits from Q_n. The inductive hypothesis implies that for each of these cubes there is respectively a sub-forest $F \subset Q_n^0$ and $G \subset Q_n^1$ as in (i). From G we delete all the edges with colors that are in F. We now take H to be $F \cup G$ with a subset of edges not in the Q_n^j (we call such edges vertical) adjoined that contain all of the colors of Q_n not contained in $F \cup G$ each exactly once. If we show that H has no cycles then (i) is proved. Suppose on the contrary there is a cycle in H. Then it cannot stay in F and verticle edges or in G and vertical edges. Thus we may assume that it starts in F at p_1 immediately goes vertical along v_1 then passes through $q_1, q_2, \ldots, q_k$ in G and then goes vertical along the edge v_2 which connects to $q \in F$. The circuit may not be as yet closed but we now show that this is enough for a contradiction. In fact, we show that v_1 and v_2 must have the same color. Indeed, consider the following diagram:

$$\begin{array}{ccccccccccc} & q_1 & \to & q_2 & \to & q_3 & \cdots & \cdots & q_{k-1} & \to & q_k \\ v_1 & \uparrow & w_1 & \uparrow & w_2 & \uparrow & \cdots & w_{k-2} & \uparrow & v_2 & \uparrow \\ & p_1 & \to & p_2 & \to & p_3 & \cdots & \cdots & p_{k-1} & \to & q \end{array}.$$

In this diagram only the q_i, p_1, q_1 are guaranteed to be vertices in H and only v_1 and v_2 are vertical edges in H. However, each of the

$$\begin{array}{ccccc} q_i & \to & q_{i+1} & & \\ \uparrow & w_i & \uparrow & & w_{i+1} \\ p_i & \to & p_{i_{+1}} & & \end{array}$$

is a 2 dimensional subcube of Q_n. Since the edge $q_i \to q_{i+1}$ is in G and $p_i \to p_{i+1}$ is an edge of Q_n^0, the two edges have different colors. this implies that w_i and w_{i+1}have the same color (by admissibility). The argument applies to the first and last square also so we see that v_1 and v_2 have the same color contrary to the choice of edges to include.

Before we prove (iv) we recall a property of the forest T that was found in the proof of (iii). There is no path in T that starts in F continues in G and returns to F. We now prove (iv). We note that it is enough to prove this for codimension one subcubes with the inherited coloring. If we choose one such subcube we rotate it so that it is Q_n^0. We now consider the forests T and F. Since Q_n has $2^n - 1$ colors T must be connected. According to (iii) we will be done if we show that F is connected. To prove this we consider x, y vertices in F. Since T is connected there must be a path from x to y in T. This path cannot leave F and return to F. Thus it stays in F. ■

Theorem 7 *Let Q_n be admissibly colored with $2^n - 1$ distinct colors. Then there exists a direction for which all 2^{n-1} edges in that direction have the same color.*

Proof. We first note that the theorem can be proved directly for $n = 2, 3$. We also observe that if Q_3 is colored admissibly with 7 colors then if 3 out of 4 of the edges in the same direction have the same color then so does the fourth. The proof is by induction. Suppose $n \geq 4$ and the lemma is true for Q_{n-1}. We suppose that we have a maximal coloring of Q_n with $2^n - 1$ distinct colors. As before, let us split the Q_n into two $n-1$ dimensional subcubes, the top and the bottom. Let us call them $Q^{(0)}$ for the bottom and $Q^{(1)}$ for the top. The edges between them we call vertical. If all the vertical edges are of the same color, we are done. So suppose that there are at least two distinct colors on the vertical edges. Let us call the vertical direction the x_n-*direction*, taking the naming convention as if the cube was embedded in $\mathbb{R}^n$ with vertices $\{0, 1\}^n$.

The inductive hypothesis implies that there exists some direction, let us call it the x_1-*direction*, in which all the edges in $Q^{(0)}$ are of the same color, let us say the color *red*. We wish to show that all the edges in the x_1-direction in $Q^{(1)}$ are also red. Since not all vertical edges are of the same color, there must exist some 3 dimensional subcube Q' of Q_n, which has edges in the x_1-direction, the vertical x_n-direction, and some other third direction x_j, such that not all vertical edges in Q' are of the same color. The cube Q' has the maximum, 7, colors, therefore one of its directions has all edges of the same color. It cannot be the x_j-direction because the x_1-direction bottom edges are red, so we cannot have the two bottom x_j-direction edges also of the same color by Theorem 6 (iv). (we would have a face with only 2 colors on a maximally colored 3-cube). Our choice of Q' implies that it is not the vertical x_n-direction that has all the same color. Hence all the x_1-direction edges in Q' are of the same color, and so they are all red.

Next pick an "adjacent" cube Q'' with edges in the x_1-direction, x_n-direction and x_k-direction for some k, such that Q'' and Q' share an (x_1, x_n)-face. The two bottom edges in the x_1-direction in Q'' are red, and also the two edges in the x_1-direction on the face it shares with Q' are red. So Q'' has at least 3 red edges in the x_1-direction, and as it is colored with the maximum, 7, colors, all edges in the x_1-direction in Q'' are red. We repeat this procedure until we have shown that all edges in the x_1-direction in the top cube $Q^{(1)}$ are red completing the proof. ■

At this point we see that up to permuting the components of Q_n (and then putting them back in order of the algorithm), Lemma 5 yields all colorings with a maximum number of colors. Thus in our description of the

set of all UOB as a bouquet of products of $\mathbb{P}^1$ given by the maps Φ_C for an admissible coloring of Q_n the components of highest dimension $(2^{n+1}-2)$ are described up to permutation of factors and order as the images of Φ_C with C given by the algorithm. Thus we have

Theorem 8 *The irreducible components of maximum dimension of the variety of UOB are up to permutation of factors the images of Φ_C with C given by the algorithm in Lemma 5. In fact, after reordering factors we can write such a component as*

$$\mathcal{B} = \{[a] \otimes \mathcal{B}_1, [\hat{a}] \otimes \mathcal{B}_2\},$$

where $\mathcal{B}_i, i = 1, 2$ are images of $\Phi_{C_i, i=1,2}$ respectively with C_1, C_2 colorings of Q_{n-1} given by the algorithm in Lemma 5.

IV. DISTINGUISHABILITY BY LOCAL OPERATIONS AND CLASSICAL COMMUNICATION

We now consider LOCC distinguishability of elements of an n–qubit UOB. We are given an unknown n–qubit state in a UOB, and allowed a protocol in which we can perform a sequence of local operations, that is, unitary transformations and local measurements on qubits, where the choice of which qubit to measure at each step can depend on the outcomes of the previous measurements (classical communication). We ask if this LOCC information can determine with certainty which basis element was presented. Let us consider the two families of UOB in three qubits corresponding to the first two displayed colorings above. The first is an example of a coloring, C, with the maximum, 7, colors. We consider the corresponding bases, of the form $\Phi_C([u_1], \ldots, [u_7])$, as in eq. (1), and look at the basis state $[u_3] \otimes [\hat{u}_2] \otimes [u_4]$. We note that if the first measurement is in the first qubit (after applying the local unitary transformation taking $|0\rangle$ and $|1\rangle$ to $[u_3]$ and $[\hat{u}_3]$ respectively), then the outcome is $[u_3]$ with certainty. From a second measurement in the second qubit (after applying the local unitary transformation taking $|0\rangle$ and $|1\rangle$ to $[u_2]$ and $[\hat{u}_2]$ respectively), the outcome is $[\hat{u}_2]$ with certainty. Similarly the measurement in the third qubit must be $[u_4]$ with certainty. We therefore have the correct state with certainty. Notice that the order of measurement is critical. We now consider the second example which is a maximal coloring of Q_3 using 6 colors. This example appears in [1], where it is shown that there is no ordered set of local transformations and measurements for the UOB of the form $\Phi_C(u_1, \ldots, u_6)$, with $[u_i] \neq [u_j]$, that will determine a basis element with certainty.

Theorem 8 implies that the discussion above for $\Phi_C(u_1, \ldots, u_{2^n-1})$ for an admissible coloring of Q_n with $2^n - 1$ colors will work as long as the order is adapted to the algorithm, in Lemma 5, that is used to construct the coloring. Theorem 1 of Walgate and Hardy [4] now implies that if C is a maximal coloring of Q_n with $k < 2^n - 1$ colors then there is no such ordered set of measurements that will identify with certainty a specific state in $\Phi_C(u_1, \ldots, u_k)$, if all of the u_i that appear in a given factor are distinct.

Distinguishability by LOCC is also called *local* distinguishability [4]. We formally define it in the spirit of [4].

Definition 9 *A UOB is locally distinguishable if there exists an ordering of tensor factors $(1, \ldots, n)$, and a sequence of measurements on respective tensor factors $\{M_1, \ldots, M_n\}$ such that:*

1. *M_i for $i > 1$ is a function of the outcomes of previous measurement results $\{r_j\}_{j=1,\ldots,i-1}$ from respective measurements $\{M_j\}_{j=1,\ldots,i-1}$.*
2. *The results $(r_1, \ldots, r_n)$ identify the basis element of the UOB on which the measurement is performed.*

We restate Theorem 1 in [4] (with slight notational change). In this theorem, "going first" refers to the party (tensor factor) performing the first measurement.

Theorem 10 (Walgate and Hardy) *Alice and Bob share a quantum system $\mathbb{C}^2 \otimes \mathbb{C}^n$: Alice has a qubit, and Bob an n-dimensional system that may be entangled with that qubit. If Alice goes first, a set of l orthogonal states $\{\psi_i\}_{i=1\ldots l}$ is exactly locally distinguishable if and only if there is an orthogonal basis $\{a, \hat{a}\}$ for Alice's qubit, and orthonormal sets, $\{\eta_a^i\}_{i=1\ldots l}$ and $\{\eta_{\hat{a}}^i\}_{i=1\ldots l}$, in Bob's system $\mathbb{C}^n$, such that:*

$$\psi_i = a \otimes \eta_a^i + \hat{a} \otimes \eta_{\hat{a}}^i \tag{2}$$

Corollary 11 *A UOB is locally distinguishable if and only if it is from the family of UOB with maximal dimension.*

Proof. Let the UOB be $\mathcal{B}$. An element of $b \in \mathcal{B}$ only has one term in the sum in (2), either $b = a \otimes \eta_a^i$, or $b = \hat{a} \otimes \eta_{\hat{a}}^i$.

Assume $\mathcal{B}$ is from the family of UOB with maximal dimension. Let us show local distinguishability of $\mathcal{B}$. By Theorem 8, the form of $\mathcal{B}$ is

$$\mathcal{B} = \{[a] \otimes \mathcal{B}_1, [\hat{a}] \otimes \mathcal{B}_2\},$$

where $\mathcal{B}_1$ and $\mathcal{B}_2$ are from the maximal dimensional family of UOB in $(\mathbb{C}^2)^{\otimes(n-1)}$. By induction then, we can assume that $\mathcal{B}_1$ and $\mathcal{B}_2$ are locally distinguishable, i.e., the conclusion is true for $n-1$. Then local distinguishability of $\mathcal{B}$ (for n) follows by Theorem 10.

For the converse, assume local distinguishability of the UOB $\mathcal{B}$. Then by Theorem 10, the form of $\mathcal{B}$ is

$$\mathcal{B} = \{[a] \otimes \mathcal{B}_1, [\hat{a}] \otimes \mathcal{B}_2\}, \tag{3}$$

where $[a]$ is in the factor measured first, and $\mathcal{B}_1$ and $\mathcal{B}_2$ are some UOB in the factors, $(\mathbb{C}^2)^{\otimes(n-1)}$, measured afterwards . Local distinguishability of $\mathcal{B}$ implies that of $\mathcal{B}_1$ and $\mathcal{B}_2$. By induction, $\mathcal{B}_1$ and $\mathcal{B}_2$ are from the the

maximal dimensional family of UOB. Then by dimension count in (3), $\mathcal{B}$ is also from the maximal dimensional family of UOB in $(\mathbb{C}^2)^{\otimes n}$. ■

This can also be seen as a direct consequence of Theorem 6 in [11] and substantiates our claims. A sightly stronger result on *asymptotic* distinguishability is obtained from [12], which allows the parties to have infinite resources and arbitrarily long times in their LOCC protocol. Proposition 2 of [12] implies that even under asymptotic LOCC, perfect discrimination is only possible for the UOB that belong to the maximum dimensional family.

V. CONSTRUCTIONS OF MAXIMAL UOB NOT DISTINGUISHABLE BY LOCC

By now, we know that the only UOB that are LOCC distinguishable belong to the maximum dimensional family, and we know which UOB belong to this family. Next we turn to constructions of maximal UOB for n qubits, that are not from the maximum dimensional family. Such UOB give us families that are not distinguishable by LOCC, and therefore are the ones most useful in secure communication protocols like QKD.

Equivalently we are looking for maximally colored cubes with less than the maximum number of colors. We saw the maximally colored Q_3 with 6 colors. Let us construct an analogous coloring on Q_n for $n \geq 4$.

First, we color Q_n with only two colors, and call them 'dominant' and 'non-dominant'. We color according to the rule that every 2-face has to have 3 edges 'dominant' and 1 edge 'non-dominant'. It is not hard to prove that once we pick a single 'non-dominant' edge, then the coloring of an n-cube is forced up to mirror symmetry. Each direction in the 3-cube has 1 'non-dominant' and 3 'dominant' edges. In the 4-cube, each direction has 2 'non-dominant' and 6 'dominant' edges, and this process can be continued for higher n. We now replace the 'dominant' color with n distinct colors, one for each direction. The edges previously colored with 'non-dominant', we color each with a distinct color, and it can be checked the resulting coloring is admissible. We obtain a maximal coloring, which can be shown just by considering the 2-faces: Changing a proper subset of the 'dominant' colors in a single direction to a new color would break the admissibility condition for some 2-face. We obtain $n(2^{n-3}+1)$ colors, which is less than the maximal number of colors possible. Therefore we obtain a family of UOB not distinguishable by LOCC for every n. Following the procedure for Q_4 we obtain the a UOB of the form:

$$
\begin{array}{ll}
[u_4]\otimes[u_3]\otimes[u_2]\otimes[u_1], & [u_4]\otimes[u_6]\otimes[u_5]\otimes[\hat{u}_1],\\
[u_4]\otimes[u_3]\otimes[\hat{u}_2]\otimes[u_1], & [u_7]\otimes[u_3]\otimes[\hat{u}_5]\otimes[\hat{u}_1],\\
[u_8]\otimes[\hat{u}_3]\otimes[u_5]\otimes[u_1], & [u_4]\otimes[\hat{u}_6]\otimes[u_5]\otimes[\hat{u}_1],\\
[u_4]\otimes[\hat{u}_3]\otimes[\hat{u}_5]\otimes[u_9], & [u_4]\otimes[\hat{u}_3]\otimes[\hat{u}_5]\otimes[\hat{u}_9],\\
[\hat{u}_4]\otimes[u_3]\otimes[u_5]\otimes[u_{10}], & [\hat{u}_4]\otimes[u_3]\otimes[u_5]\otimes[\hat{u}_{10}],\\
[\hat{u}_4]\otimes[u_{11}]\otimes[\hat{u}_5]\otimes[u_1], & [\hat{u}_7]\otimes[u_3]\otimes[\hat{u}_5]\otimes[\hat{u}_1],\\
[\hat{u}_8]\otimes[\hat{u}_3]\otimes[u_5]\otimes[u_1], & [\hat{u}_4]\otimes[\hat{u}_3]\otimes[u_{12}]\otimes[\hat{u}_1],\\
[\hat{u}_4]\otimes[\hat{u}_{11}]\otimes[\hat{u}_5]\otimes[u_1], & [\hat{u}_4]\otimes[\hat{u}_3]\otimes[\hat{u}_{12}]\otimes[\hat{u}_1].
\end{array}
$$

This 4-qubit UOB is similar to the 3-qubit example in FIG. 2; it has 3 colors in each direction distributed so that there are 6 edges of one color and 1 edge each of the other 2 colors.

We can, in fact, construct a large supply of maximal families. Let us start with a generalization of the construction we already used to construct the maximal dimensional component. Start with two UOBs $\{b_1,\ldots,b_N\}$ and $\{c_1,\ldots,c_N\}$ where $N=2^{n-1}$, with m and k distinct vectors (colors) respectively. Let a be any unit vector in $\mathbb{C}^2$, and construct the UOB

$$a\otimes b_1,\ldots,a\otimes b_N,\hat{a}\otimes c_1,\ldots,\hat{a}\otimes c_N.$$

This UOB uses $m+k+1$ distinct vectors (colors). If we start with at least one of the UOBs being not LOCC distinguishable, that is, not part of the maximal dimensional family, we again obtain a non-distinguishable family.

In terms of cubes, the above construction colors the Q_n so that one direction has a unique color. Conversely it is not hard to see that if one direction has a unique color, the two Q_{n-1} which this direction separates are then colored with distinct colors if the coloring is to be maximal.

We can also reverse the idea. Instead of making the new factor use only one vector, we can also use as many distinct vectors as possible in the new factor. Take a single UOB $\{b_1,\ldots,b_N\}$ with m distinct vectors, $N=2^{n-1}$. Then take N distinct vectors $a_1,\ldots,a_N\in\mathbb{C}^2$ and construct a new UOB

$$a_1\otimes b_1,\ldots,a_N\otimes b_N,\hat{a}_1\otimes b_1,\ldots,\hat{a}_N\otimes b_N.$$

The number of distinct vectors used is then $m+N=m+2^{n-1}$. Again, if we start with a UOB not in the maximal dimensional component we again obtain a nondistinguishable UOB.

As a remark, one may ask for the minimal number of colors in a maximally colored Q_n. That is, the dimension of the lowest dimensional component of UOB. Let us call this number $C(n)$. Using the constructions above and an induction argument we leave it to the reader to prove:

$$C(2)=3,\qquad C(3)=6,$$
$$2n\leq C(n)\leq 13(2^{n-4})-1\quad(\text{if } n\geq 4).$$

VI. DISCUSSION

In this paper, we presented several ideas and results pertaining UOB for systems of n qubits. To systematize our search for UOB, we began with drawing a connection between UOB and colorings of an n-dimensional hypercube. This led us to the definition of an *admissible* coloring and a partial order on such colorings. The maximal elements of this order define families of UOB of dimensions corresponding to their number of colors. Each coloring defines a forest of colors, such that the maximum dimensional family corresponds to a single tree of $2^n - 1$ colors (dimension of the family). This gave us a complete characterization of the maximum dimensional family, and its structure. Knowing the structure it is apparent through a result of Walgate and Hardy [4] that the only LOCC distinguishable UOB belong to this family.

From the perspective of secure communication, like the QKD protocols, it is the UOB that are *not* LOCC distinguishable that exhibit the nonlocality requisite in the success of the protocols. The generic UOB being LOCC distinguishable, we constructed examples of maximal families of UOB of dimensions less that the maximum. We generalized the earliest examples of such UOB (for $n = 3$) in [1] to arbitrary number n of qubits, and described other constructions that build maximal families from known ones.

This leaves open certain immediate questions. A complete characterization of all the families of UOB is the strongest of them. Short of that, it would be interesting to know what is the lower bound on the dimension of a maximal UOB. In the domain of applications, perhaps more interesting secure communication protocols may be possible by employing these results. It would be very useful if the ideas we have presented could be extended directly as tools to analyze UOB for systems of qudits. Unfortunately given $[u] \in \mathbb{P}^{d-1}$ there is not a unique orthogonal $[\hat{u}] \in \mathbb{P}^{d-1}$ if $d > 2$. To address this ambiguity would require encoding further structure.

ACKNOWLEDGMENTS

The authors thank Gilad Gour for pointing out the work of [1] and [3] on nonlocality without entanglement and for his patient explanation of LOCC to the third named author. They also thank Nathaniel Johnston for his comments, particularly for making them aware of asymptotic distinguishability from [12].

[1] C. H. Bennett, D. P. DiVincenzo, C. A. Fuchs, T. Mor, E. Rains, P. W. Shor, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **59**, 1070 (1999).
[2] D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, and B. M. Terhal, Communications in Mathematical Physics **238**, 379 (2003).
[3] S. Bandyopadhyay, A. Cosentino, N. Johnston, V. Russo, J. Watrous, and Y. Nengkun, arXiv:1408.6981 [quant-ph] (2014).
[4] J. Walgate and L. Hardy, Phys. Rev. Lett. **89**, 147901 (2002).
[5] L. Goldenberg and L. Vaidman, Phys.Rev.Lett. **75**, 1239 (1995).
[6] G. P. Guo, C. F. Li, B. S. Shi, J. Li, and G. C. Guo, Phys. Rev. A **64**, 042301 (2001).
[7] G. He, J. Phys. A: Math. Theor. **44** (2011), 10.1088/1751-8113/44/44/445305.
[8] J. Chen and N. Johnston, Comm. Math. Phys. **333**, 351 (2015).
[9] Z. C. Zhang, F. Gao, G. J. Tian, T. Q. Cao, and Q. Y. Wen, Phys. Rev. A **90**, 022313 (2014).
[10] Y. Feng and Y. Shi, Information Theory, IEEE Transactions on **55**, 2799 (2009).
[11] N. R. Wallach, Contemp. Math. **305**, 291 (2002).
[12] M. Kleinmann, H. Kampermann, and D. Bruß, Phys. Rev. A **84**, 042326 (2011).