The Minimum Size of Qubit Unextendible Product Bases

Nathaniel Johnston

Institute for Quantum Computing, University of Waterloo
Waterloo, Ontario N2L 3G1, Canada
nathaniel.johnston@uwaterloo.ca

Abstract

We investigate the problem of constructing unextendible product bases in the qubit case – that is, when each local dimension equals 2. The cardinality of the smallest unextendible product basis is known in all qubit cases except when the number of parties is a multiple of 4 greater than 4 itself. We construct small unextendible product bases in all of the remaining open cases, and we use graph theory techniques to produce a computer-assisted proof that our constructions are indeed the smallest possible.

1998 ACM Subject Classification G.2.3 Applications

Keywords and phrases unextendible product basis, quantum entanglement, graph factorization

Digital Object Identifier 10.4230/LIPIcs.TQC.2013.93

1 Introduction

Unextendible product bases play a rather diverse and important role in quantum information theory [7]. While their original motivation was for the construction of bound entangled states [5, 12, 13], they have also been used to build indecomposible positive maps [14], to demonstrate Bell inequalities without a quantum violation [3], and demonstrate the existence of nonlocality without entanglement [4].

Furthermore, in the qubit case (i.e., the case where each local space has dimension 2), it has been shown that unextendible product bases can be used to construct tight Bell inequalities with no quantum violation [2] and subspaces of small dimension that are locally indistinguishable [8]. It is the qubit case that we focus on in the present paper. In particular, we consider the question of how small a qubit unextendible product basis can be.

The minimum cardinality of a qubit unextendible product basis on p qubits is well-known to equal $p+1$ when p is odd [1]. When p is even, however, the problem is more difficult. It was shown in [9] that the minimum cardinality equals $p+2$ when $p=4$ or $p \equiv 2 \pmod 4$. Our contribution is to solve the remaining cases (i.e., when $p \geq 8$ and $p \equiv 0 \pmod 4$ – more specifically, we show that the minimum cardinality is $p+3$ when $p=8$ and $p+4$ in all other cases.

Our approach is as follows: we formally introduce the mathematical preliminaries and graph theory techniques that we make use of in Section 2. We construct unextendible product bases of the claimed cardinality in Section 3. Finally, Section 4 is devoted to the proof that there does not exist a smaller unextendible product basis in these cases.

2 Unextendible Product Bases and Orthogonality Graphs

A pure quantum state is represented by a unit vector $|v\rangle \in \mathbb{C}^{d_1} \otimes \cdots \otimes \mathbb{C}^{d_p}$ (and in our setting, $d_1 = \cdots = d_p = 2$ always). We say that $|v\rangle$ is a *product state* if we can write it in

© Nathaniel Johnston;
licensed under Creative Commons License CC-BY
8th Conference on Theory of Quantum Computation, Communication and Cryptography.
Editors: Simone Severini and Fernando Brandao; pp. 93–105
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

the form

$$|v\rangle = |v_1\rangle \otimes \cdots \otimes |v_p\rangle \quad \text{with} \quad |v_j\rangle \in \mathbb{C}^2 \ \forall\, j.$$

An *unextendible product basis (UPB)* is an orthonormal set $\mathcal{S} \subseteq (\mathbb{C}^2)^{\otimes p}$ of product states such that there is no product state orthogonal to every member of $\mathcal{S}$. It is clear that every UPB in $(\mathbb{C}^2)^{\otimes p}$ contains at least $p+1$ states – if it contained only p product states $|v_0\rangle, \ldots, |v_{p-1}\rangle$ then we could construct another product state that is, for each $0 \leq j < p$, orthogonal to $|v_j\rangle$ on the $(j+1)$-th party and thus violate unextendibility.

It turns out that the trivial lower bound of $p+1$ states can be attained when p is odd, and can almost be attained when p is even, as indicated by our main result:

▶ **Theorem 1.** *Let $f(p)$ be the smallest possible number of states in a UPB in $(\mathbb{C}^2)^{\otimes p}$. Then:*
(a) *if p is odd then $f(p) = p+1$;*
(b) *if $p = 4$ or $p \equiv 2 \,(mod\ 4)$ then $f(p) = p+2$;*
(c) *if $p = 8$ then $f(p) = p+3$;*
(d) *otherwise, $f(p) = p+4$.*

Case (a) of Theorem 1 is demonstrated by the "GenShifts" UPB constructed in [7]. Case (b) of Theorem 1 was proved in [9], and in general our techniques and presentation are similar to those of that paper. Our contribution is to prove cases (c) and (d) and hence complete the characterization. It is worth pointing out that cases (c) and (d) of Theorem 1 are the first known cases (qubit or otherwise) where the minimum cardinality of a UPB exceeds the trivial lower bound $1+\sum_j(d_j-1)$ by more than 1 (see [6, 9] for several examples where the trivial lower bound is exceeded by exactly 1).

Orthogonality graphs provide a very useful tool when dealing with unextendible product bases, particularly in the qubit case. Given a set of product states $\mathcal{S} = \{|v_0\rangle, \ldots, |v_{s-1}\rangle\} \subseteq (\mathbb{C}^2)^{\otimes p}$ with $|\mathcal{S}| = s$, we say that the *orthogonality graph of $\mathcal{S}$* is the graph on s vertices $V := \{v_0, \ldots, v_{s-1}\}$ such that there is an edge (v_i, v_j) of color ℓ if and only if $|v_i\rangle$ and $|v_j\rangle$ are orthogonal to each other on party ℓ. Rather than actually using p colors to color the edges of the orthogonality graph, for ease of visualization we instead draw p different graphs on the same set of vertices – one for each party (see Figure 1).

The requirement that $\mathcal{S}$ is an orthonormal set is equivalent to requiring that every edge is present on at least one party in its orthogonality graph. In order to help us visualize the unextendibility requirement, we make a few more observations. In particular,

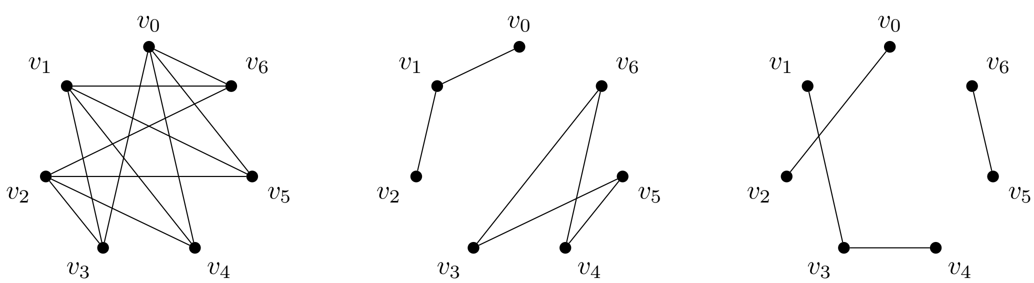

Figure 1 The orthogonality graph of a set of 7 product states in $(\mathbb{C}^2)^{\otimes 3}$. This set of states is a product basis, since every edge is present in at least one of the three graphs, but it is extendible, since we can find a product state that is orthogonal to the states associated with v_3, v_4, v_5, v_6 on the first subsystem, v_0, v_2 on the second subsystem, and v_1 on the third subsystem.

if $|w_0\rangle, |w_1\rangle, |w_2\rangle \in \mathbb{C}^2$ are such that $\langle w_0|w_1\rangle = \langle w_0|w_2\rangle = 0$, then it is necessarily the case that $|w_1\rangle = |w_2\rangle$ (up to irrelevant complex phase). It follows that the orthogonality graph associated with any qubit in a product basis is the disjoint union of complete bipartite graphs. For example, in Figure 1 the left graph is $K_{3,4}$, the center graph is the disjoint union of $K_{1,2}$ and $K_{2,2}$, and the right graph is the disjoint union of $K_{1,2}$ and two copies of $K_{1,1}$.

Furthermore, not only does every set of product states have an orthogonality graph that can be decomposed into the disjoint union of complete bipartite graphs, but the converse is also true: every graph that is built from complete bipartite graphs in this way is the orthogonality graph of some set of product states. To see this, on each party assign to each complete bipartite graph a distinct basis of $\mathbb{C}^2$ in the obvious way. For example, one set of product states giving rise to the orthogonality graph depicted in Figure 1 is as follows:

$$|v_0\rangle := |0\rangle \otimes |0\rangle \otimes |0\rangle, \qquad |v_1\rangle := |0\rangle \otimes |1\rangle \otimes |+\rangle, \qquad |v_2\rangle := |0\rangle \otimes |0\rangle \otimes |1\rangle,$$
$$|v_3\rangle := |1\rangle \otimes |+\rangle \otimes |-\rangle, \qquad |v_4\rangle := |1\rangle \otimes |+\rangle \otimes |+\rangle, \qquad |v_5\rangle := |1\rangle \otimes |-\rangle \otimes |b\rangle,$$
$$|v_6\rangle := |1\rangle \otimes |-\rangle \otimes |b^\perp\rangle,$$

where $|+\rangle := \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $|-\rangle := \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, and $\{|b\rangle, |b^\perp\rangle\}$ is any orthonormal basis of $\mathbb{C}^2$ not equal to $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$.

It is often useful to draw orthogonality graphs of sets of qubit product states in a form that makes their decomposition in terms of complete bipartite graphs more transparent – we draw shaded regions indicating which vertices are equal to each other (up to complex phase) on the given party, and lines between shaded regions indicate that all states in one of the regions are orthogonal to all states in the other region on that party (see Figure 2).

It now becomes straightforward to see whether or not a product basis is unextendible just by looking at its orthogonality graph. A set of product states is unextendible if and only if there is no way to choose one shaded region on each party such that every vertex $v_0, v_1, \ldots, v_{s-1}$ is contained within at least one of the shaded regions. For example, the set of product states described by Figure 2 is extendible because we can choose the shaded region containing v_3, v_4, v_5, v_6 on the first subsystem, v_0, v_2 on the second subsystem, and v_1, v_4 on the third subsystem.

The following simple lemma shows that, in an orthogonality graph of a UPB, every shaded region must be connected to exactly one other shaded region via an edge.

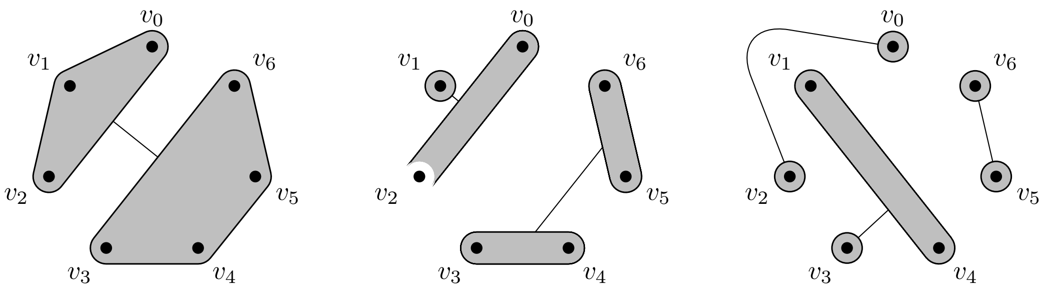

Figure 2 A representation of the same orthogonality graph as that of Figure 1. Vertices within the same shaded region represent states that are equal to each other on that party. Lines between shaded regions indicate that every state within one of the regions is orthogonal to every state within the other region.

▶ **Lemma 2.** *If $\mathcal{S} \subseteq (\mathbb{C}^2)^{\otimes p}$ is a UPB, then for all $|v\rangle \in \mathcal{S}$ and all integers $1 \leq j \leq p$ there is another product state $|w\rangle \in \mathcal{S}$ such that $|v\rangle$ and $|w\rangle$ are orthogonal on the j-th subsystem.*

Proof. Suppose that there exists $1 \leq j \leq p$ and $|v\rangle := |v_{(1)}\rangle \otimes \cdots \otimes |v_{(p)}\rangle \in \mathcal{S}$ such that $|v\rangle$ is not orthogonal to any other member of $\mathcal{S}$ on the j-th subsystem. Because $\mathcal{S}$ is a product basis, $|v\rangle$ must be orthogonal to every member of $\mathcal{S}$ on the remaining $p-1$ subsystems. It follows that if $|v_{(j)}^{\perp}\rangle$ is orthogonal to $|v_{(j)}\rangle$ then the product state $|v_{(1)}\rangle \otimes \cdots |v_{(j-1)}\rangle \otimes |v_{(j)}^{\perp}\rangle \otimes |v_{(j+1)}\rangle \otimes \cdots \otimes |v_{(p)}\rangle$ is orthogonal to every element of $\mathcal{S}$, which shows that $\mathcal{S}$ is extendible. ◀

An obvious corollary of Lemma 2 is that, in the orthogonality graph of a UPB, every party must have an even number of distinct shaded regions – a fact that will be very useful in Section 4.

3 Construction of Small UPBs

Recall that our goal is to show that the smallest UPB in $(\mathbb{C}^2)^{\otimes 8}$ consists of 11 states and the smallest UPB in $(\mathbb{C}^2)^{\otimes 4k}$ consists of $4k+4$ states when $k \geq 3$. Our first step toward this goal is to construct a UPB of the desired size in these cases.

▶ **Lemma 3.** *There exists a UPB in $(\mathbb{C}^2)^{\otimes 8}$ consisting of 11 states.*

Proof. The result follows simply from demonstrating an orthogonality graph on 11 vertices that satisfies the product basis and unextendibility requirements described in Section 2. Such an orthogonality graph is provided in Figure 3.

Indeed, it is straightforward (albeit tedious) to check that the 8 graphs depicted in Figure 3 contain all 55 possible edges between 11 vertices, so the corresponding product states are mutually orthogonal. Unextendibility follows from the (also straightforward but tedious) fact that there is no way to choose a shaded region containing 2 vertices on 3 different parties without at least 2 of them containing the same vertex. ◀

We note that the UPB of Lemma 3 was found by a combination of computer search and tweaking by hand, and it does not seem to generalize to other values of p in any natural way. On the other hand, the UPBs that we now construct of cardinality $4k+4$ are much "tidier".

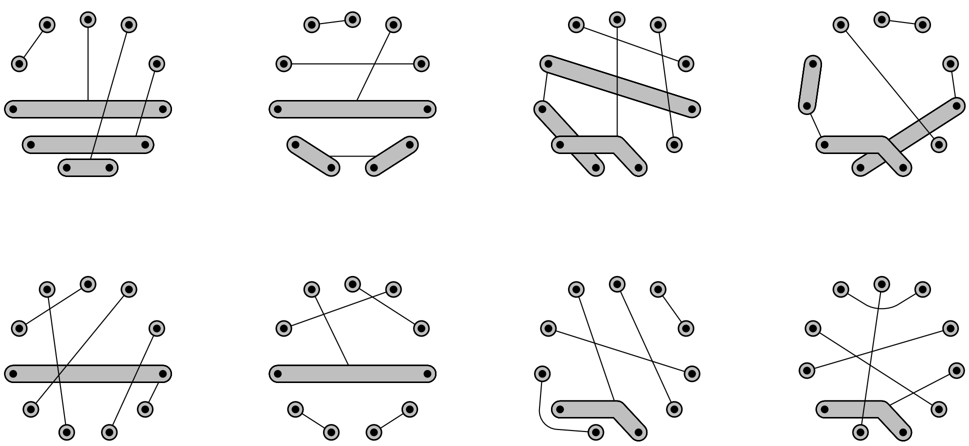

Figure 3 Orthogonality graphs demonstrating that there exists an 11-state UPB in $(\mathbb{C}^2)^{\otimes 8}$.

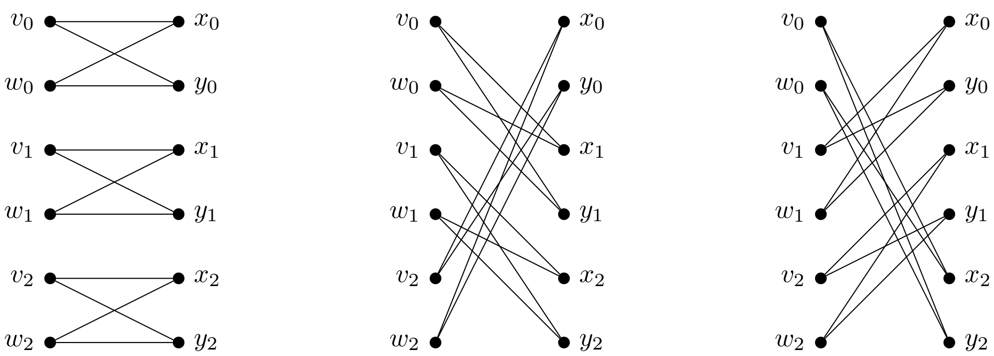

Figure 4 The graphs $B_{0,2}$ (left), $B_{1,2}$ (center), and $B_{2,2}$ (right), used in the construction of a UPB of size 12 in $(\mathbb{C}^2)^{\otimes 8}$.

▶ **Lemma 4.** *If $k \geq 2$ then there exists a UPB in $(\mathbb{C}^2)^{\otimes 4k}$ consisting of $4k+4$ states.*

Proof. We begin by defining a family of $k+1$ graphs $B_{j,k} := (V, E_j)$ for $0 \leq j \leq k$, each on the same set of $4k+4$ vertices $V := \{v_i, w_i, x_i, y_i, : 0 \leq i \leq k\}$. The set of edges E_j in the graph $B_{j,k}$ is defined as follows:

$$\begin{aligned} E_j := \big\{ &(v_i, x_{(i+j)(\mathrm{mod}\ (k+1))}), (v_i, y_{(i+j)(\mathrm{mod}\ (k+1))}), \\ &(w_i, x_{(i+j)(\mathrm{mod}\ (k+1))}), (w_i, y_{(i+j)(\mathrm{mod}\ (k+1))}) : 0 \leq i \leq k \big\}. \end{aligned}$$

The three graphs $B_{0,2}$, $B_{1,2}$, and $B_{2,2}$ in the $k = 2$ case are depicted in Figure 4. It is clear that the graph obtained by taking the union of all edges in all sets $B_{j,k}$ for $0 \leq j \leq k$ is $K_{2k+2,2k+2}$, the complete bipartite graph on two sets of $2k+2$ vertices.

We now define three sets of states $S^{(j)} = \{|v_i^{(j)}\rangle, |w_i^{(j)}\rangle, |x_i^{(j)}\rangle, |y_i^{(j)}\rangle : 0 \leq i \leq k\} \subseteq \mathbb{C}^2$ that have orthogonality graphs $B_{j,k}$ for $0 \leq j \leq 2$ respectively. To this end, let $\{|b_i\rangle, |b_i^\perp\rangle\}_{i=0}^{2k+1}$ be distinct orthonormal bases of $\mathbb{C}^2$ (i.e., $\langle b_i | b_i^\perp \rangle = 0$ for all i, but $|\langle b_i | b_j \rangle|, |\langle b_i | b_j^\perp \rangle|, |\langle b_i^\perp | b_j^\perp \rangle| \notin \{0,1\}$ whenever $i \neq j$). Then let

$$|v_i^{(j)}\rangle := |w_i^{(j)}\rangle := |b_i\rangle \quad \text{and} \quad |x_i^{(j)}\rangle := |y_i^{(j)}\rangle := |b^\perp_{(i-j)(\mathrm{mod}\ (k+1))}\rangle,$$

for $0 \leq j \leq 2$, which clearly results in the desired orthogonality graphs. Furthermore, each set $S^{(j)}$ has the property that any state $|z\rangle \in \mathbb{C}^2$ can be orthogonal to at most two elements of $S^{(j)}$ – a fact that we will use later when discussing unextendibility.

For each of the remaining $k-2$ graphs $B_{j,k}$ $(3 \leq j \leq k)$, we construct sets of product states $S^{(2j-3,2j-2)} = \{|v_i^{(2j-3,2j-2)}\rangle, |w_i^{(2j-3,2j-2)}\rangle, |x_i^{(2j-3,2j-2)}\rangle, |y_i^{(2j-3,2j-2)}\rangle : 0 \leq i \leq k\} \subseteq \mathbb{C}^2 \otimes \mathbb{C}^2$ that have orthogonality graphs $B_{j,k}$ for $3 \leq j \leq k$. To this end, define

$$\begin{aligned} |v_i^{(2j-3,2j-2)}\rangle &:= |b_i\rangle \otimes |b_i\rangle \\ |w_i^{(2j-3,2j-2)}\rangle &:= |b_{i+(k+1)}\rangle \otimes |b_{i+(k+1)}\rangle \\ |x_i^{(2j-3,2j-2)}\rangle &:= |b^\perp_{(i-j)(\mathrm{mod}\ (k+1))}\rangle \otimes |b^\perp_{(i-j)(\mathrm{mod}\ (k+1))+(k+1)}\rangle \\ |y_i^{(2j-3,2j-2)}\rangle &:= |b^\perp_{(i-j)(\mathrm{mod}\ (k+1))+(k+1)}\rangle \otimes |b^\perp_{(i-j)(\mathrm{mod}\ (k+1))}\rangle, \end{aligned}$$

which results in the desired orthogonality graphs.

We now turn our attention to the complement graph of $K_{2k+2,2k+2}$, which is simply the disjoint union of two disjoint copies of K_{2k+2}, the complete graph on $2k+2$ vertices. We

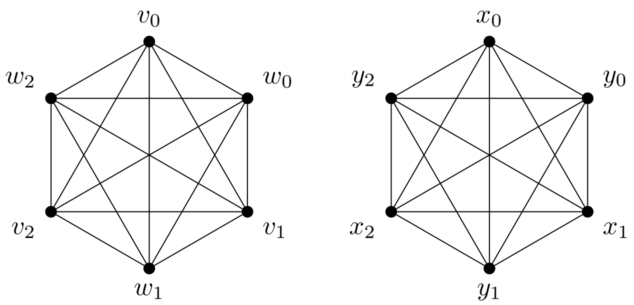

Figure 5 The graph K_6^2 that is the disjoint union of two copies of K_6.

denote this graph by K_{2k+2}^2, and it is depicted in the $k=2$ case in Figure 5. The graph K_{2k+2}^2 will be the orthogonality graph of the remaining $4k-(3+2(k-2))=2k+1$ parties.

Our goal now is to define sets of states $S^{(j)}=\{|v_i^{(j)}\rangle,|w_i^{(j)}\rangle,|x_i^{(j)}\rangle,|y_i^{(j)}\rangle : 0\le i\le k\}\subseteq\mathbb{C}^2$ for $2k-1\le j\le 4k-1$ such that their orthogonality graphs, when taken together, contain all edges of K_{2k+2}^2. To this end, we recall that it is well-known that K_{2k+2} always has a 1-factorization [10, Theorem 9.1], so K_{2k+2}^2 clearly has a 1-factorization as well (see Figure 6). This 1-factorization decomposes K_{2k+2}^2 into $2k+1$ distinct 1-regular spanning subgraphs, and any such graph is clearly the orthogonality graph of the set of states $\{|b_0\rangle,|b_0^\perp\rangle,\ldots,|b_{2k+1}\rangle,|b_{2k+1}^\perp\rangle\}\subset\mathbb{C}^2$ (under an appropriate labelling of the vertices).

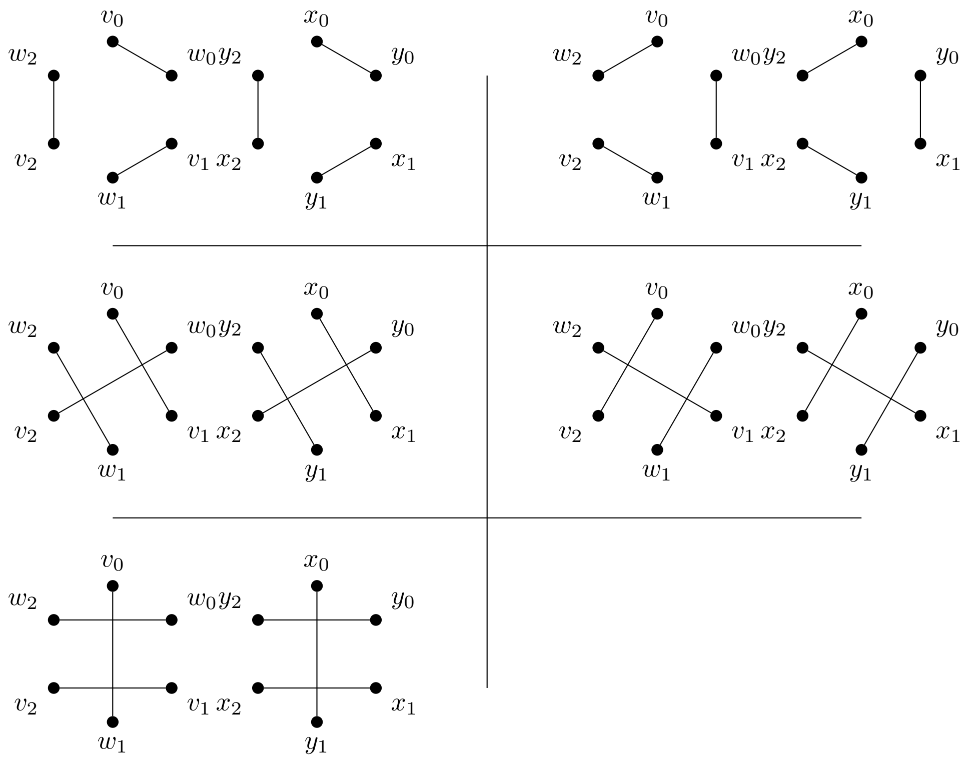

Figure 6 A 1-factorization of K_6^2, which is useful for constructing a UPB of size 12 in $(\mathbb{C}^2)^{\otimes 8}$.

Since the union of the sets of edges present in all of the graphs considered so far is the complete graph K_{4k+4}, we know that the states in the set

$$\mathcal{S} := \left\{ \bigotimes_{j=1}^{4k} |v_i^{(j)}\rangle, \bigotimes_{j=1}^{4k} |w_i^{(j)}\rangle, \bigotimes_{j=1}^{4k} |x_i^{(j)}\rangle, \bigotimes_{j=1}^{4k} |y_i^{(j)}\rangle : 0 \leq i \leq k \right\}$$

are mutually orthogonal. To see why this set is unextendible, recall that any non-zero product state can be orthogonal to at most 2 states on each of the first 3 subsystems, and at most 1 state on each of the remaining $4k-3$ subsystems. It follows that any nonzero product state can be orthogonal to at most $2 \cdot 3 + 1 \cdot (4k-3) = 4k+3$ of these product states. Since no nonzero product state can be orthogonal to all $4k+4$ members of $\mathcal{S}$, it is unextendible, which completes the proof. ◀

4 Proof of Minimality

We now turn our attention to the problem of proving that the UPBs constructed in Section 3 are the smallest possible. Because the main result of [1] tells us that the minimum cardinality of a UPB in $(\mathbb{C}^2)^{\otimes 4k}$ is at least $4k+2$, we only have to prove that there is no UPB of cardinality $4k+2$ when $k \geq 2$ and no UPB of cardinality $4k+3$ when $k \geq 3$. While the proof that there is no UPB of cardinality $4k+2$ is relatively straightforward, the proof that there is no UPB of cardinality $4k+3$ is more involved and consists of many cases and sub-cases. We make use of a C script to solve some of the messier cases, while we solve the simpler cases by hand.

For the entirety of this section, we make use of *partial orthogonality graphs*, which are the same as orthogonality graphs, except perhaps with some conditions unspecified. For example, in Figure 7 the lack of lines indicating orthogonality between shaded regions does not signify that there are no regions orthogonal to each other, but rather that we just don't care *which* regions are orthogonal to each other. Similarly, in Figure 8 there are vertices that are drawn outside of any shaded region. This is intended to mean that we don't care what the shaded region involving that vertex looks like. In general, we only specify the pieces of the orthogonality graphs that are relevant for our proofs.

It will be convenient for us to let $P_1, \ldots, P_{4k}$ denote the $4k$ different parties. We also let M_j denote the maximum number of vertices contained within a single shaded region on party P_j (which is equal to the maximum number of states in the UPB that are equal to each other on party P_j), and let $C_{n,j}$ denote the number of distinct shaded regions containing exactly n vertices on party j (i.e., $C_{n,j}$ is the number of distinct group of exactly n states in the UPB that are equal to each other on party P_j). For example, in Figure 2, if the graphs correspond to parties P_1, P_2 and P_3, then $M_1 = 4$, $M_2 = M_3 = 2$, $C_{3,1} = 1$, $C_{4,1} = 1$, $C_{1,2} = 1$, $C_{2,2} = 3$, $C_{1,3} = 5$, and $C_{2,3} = 1$.

▶ **Lemma 5.** *There is no UPB in* $(\mathbb{C}^2)^{\otimes 4k}$ *of cardinality* $4k+2$ *when* $k \geq 2$.

Proof. Suppose for a contradiction that there exists a UPB of cardinality $4k+2$ in $(\mathbb{C}^2)^{\otimes 4k}$. If it were the case that $M_j \geq 3$ for some j, then we could find a product state that is orthogonal to the 3 corresponding states on that party and to any 1 of the product states on each of the remaining $4k-1$ parties, for a total of all $4k+2$ elements of the UPB, which violates unextendibility. Hence $M_j \leq 2$ for all $1 \leq j \leq 4k$. We now split into two cases.

Case 1: There is at most one party P_j with $M_j = 2$.

Between the $4k$ parties, there must be a total of $(4k+2)(4k+1)/2 = 8k^2+6k+1$ edges in the union of their orthogonality graphs. The $4k-1$ parties other than P_j must be the

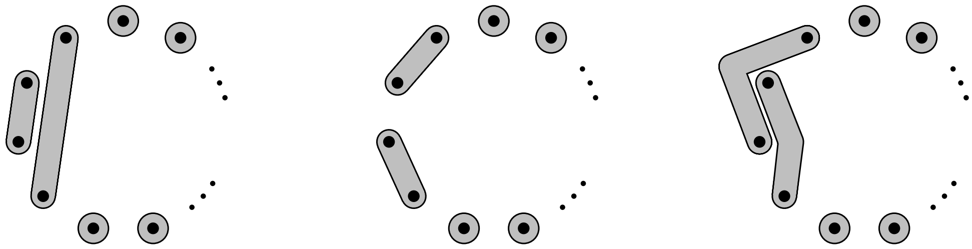

Figure 7 Partial orthogonality graphs of three parties that each have two sets of two equal states, used in the proof of case 2 of Lemma 5. There is no way to add another pair of equal states on any party without violating unextendibility.

disjoint union of $2k+1$ copies of $K_{1,1}$, for a total of at most $(4k-1)(2k+1) = 8k^2+2k-1$ edges. The remaining party P_j then needs at least $(8k^2+6k+1)-(8k^2+2k-1) = 4k+2$ edges. It is easily seen, however, that the largest number of edges that the orthogonality graph of party P_j can have is obtained when it is the disjoint union of k copies of $K_{2,2}$ and one copy of $K_{1,1}$, which results in only $4k+1$ edges, which gives the desired contradiction.
Case 2: There are two (or more) parties $P_i \neq P_j$ with $M_i = M_j = 2$.

It is not difficult to see that $C_{2,\ell} \in \{0,2\}$ for all ℓ or else either Lemma 2 or unextendibility is violated. Furthermore, it is not difficult to see that the unique (up to repositioning vertices and parties) way to have $C_{2,\ell} = 2$ for 3 distinct values of ℓ is given in Figure 7, and there is no way to have $C_{2,\ell}$ for a fourth value of ℓ without violating unextendibility. A simple calculation reveals that the maximum number of edges that can be obtained from the orthogonality graphs of these 3 parties is $(2k+3)+2(2k+2) = 6k+7$. The orthogonality graphs of the remaining $4k-3$ parties are the disjoint union of $2k+1$ copies of $K_{1,1}$, so they each have $2k+1$ edges. Thus the total number of edges among the orthogonality graphs of all $4k$ parties is at most $(6k+7)+(4k-3)(2k+1) = 8k^2+4k+4$. This quantity is smaller than the $8k^2+6k+1$ required edges when $k \geq 2$, which gives the desired contradiction.

◀

Note that the hypothesis of Lemma 5 that $k \geq 2$ really is required, since we have $8k^2+4k+4 \geq 8k^2+6k+1$ in case 2 of the proof of the lemma when $k=1$, so it may be possible to fit all of the required edges into the orthogonality graphs. Indeed, it was shown in [9] that a UPB consisting of $4k+2$ states in $(\mathbb{C}^2)^{\otimes 4k}$ exists in the $k=1$ case.

We now turn our attention to proving that there is no UPB of cardinality $4k+3$ when $k \geq 3$. The idea and techniques used in the proof of this statement are quite similar to the $4k+2$ case, but there are more cases to consider.

▶ **Lemma 6.** *There is no UPB in $(\mathbb{C}^2)^{\otimes 4k}$ of cardinality $4k+3$ when $k \geq 3$.*

Proof. Suppose for a contradiction that there exists a UPB of cardinality $4k+3$ in $(\mathbb{C}^2)^{\otimes 4k}$. If there exists $1 \leq j \leq p$ such that $M_j \geq 4$, then we can find a product state that is orthogonal to at least 4 corresponding states on party P_j and to 1 of the product states on each of the remaining $4k-1$ parties, for a total of $4k+3$ elements of the UPB, which violates unextendibility. Hence $M_j \leq 3$ for all j. Furthermore, this same argument shows that if there exists $i \geq 1$ such that we can choose a single shaded region on each of i parties so that together they contain at least $i+3$ vertices, then unextendibility will be violated. Finally, note that since $4k+3$ is odd, Lemma 2 implies that $M_j \geq 2$ for all j.

We now split into 4 cases, depending on the value of $\max_j\{C_{3,j}\}$ (i.e., the maximum number of sets of 3 equal states on any party).

Case 1: $\max_j\{C_{3,j}\} \geq 3$.

Because $M_j \geq 2$ for all j, it easily follows that we can find shaded regions on two parties that contain $3+2=5$ distinct vertices, which contradicts unextendibility.

Case 2: $\max_j\{C_{3,j}\} = 2$.

Suppose without loss of generality that party P_1 is such that $C_{3,1}=2$. Unextendibility immediately implies that $C_{3,j}=0$ for $j \geq 2$. Since there are $4k-3$ left over vertices on party P_1, which is odd, there must be a copy of $K_{2,1}$ on this party, as in Figure 8. Since v_1 is connected to only one other state on party P_1, it must be connected to 2 states on each of 2 other parties. These sets of 2 vertices must be disjoint and must each contain one of v_2, v_3, v_4 and one of v_5, v_6, v_7. Thus parties P_2 and P_3, without loss of generality, are as in Figure 8, which clearly implies extendibility and rules out this case.

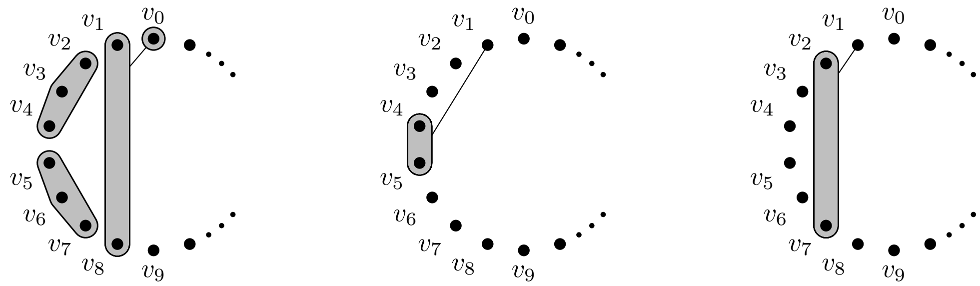

Figure 8 The (essentially unique) partial orthogonality graphs of parties P_1 (left), P_2 (center) and P_3 (right) in case 2 of Lemma 6. Such a product basis is necessarily extendible, as we can find a product state that is orthogonal to the states corresponding to v_1 and v_8 on party P_1, v_4 and v_5 on party P_2, v_2 and v_7 on party P_3, and one of the $4k-3$ remaining states on each of the remaining $4k-3$ parties.

Case 3: $\max_j\{C_{3,j}\} = 0$.

Since $M_j = 2$ for all j, simple parity arguments show that $C_{2,j} \in \{1,3,5,\ldots\}$ for every j. We now split into two sub-cases, depending on the value of $\max_j\{C_{2,j}\}$ (i.e., the maximum number of sets of 2 equal states on any party).

Case 3(a): $\max_j\{C_{2,j}\} \geq 5$.

Suppose that party P_1 has $C_{2,1} \geq 5$. We first argue that there must be at least one other party P_2 with $C_{2,2} \geq 3$. To see this, suppose the contrary – suppose that $C_{2,j}=1$ for all $j \geq 2$. Then each of these $4k-1$ parties contributes at most $2k+2$ edges to the orthogonality graph, for a total of $(4k-1)(2k+2) = 8k^2+6k-2$ edges. The party P_1 contributes no more than $4k+2$ edges, for a total of $8k^2+10k$ edges among all $4k$ parties. However, the complete graph on $4k+3$ vertices has $(4k+3)(4k+2)/2 = 8k^2+10k+3$ edges, so there are at least 3 pairs of non-orthogonal product states in our set, which contradicts the assumption that we are working with a UPB.

We now pick an arbitrary party $P_3 \neq P_1, P_2$. Because $C_{2,3} \geq 1$, we are now able to choose one shaded region on each of parties P_1, P_2, P_3 such that 6 vertices are contained within these regions, which shows that unextendibility is violated. To this end, we choose any shaded region on party P_3 that contains two vertices, then we pick any shaded region on party P_2 that is disjoint from the two vertices we chose on party P_3, and finally we choose any shaded region on party P_1 that is disjoint from all four of the previously-chosen vertices (see Figure 9).

Case 3(b): $\max_j\{C_{2,j}\} \leq 3$.

We begin by noting that the brute-force computer search shows that there can be no more

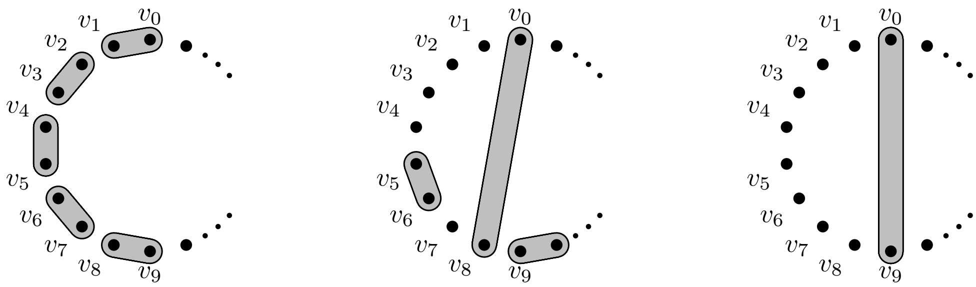

Figure 9 An example of a partial orthogonality graph in case 3(a) of Lemma 6. Such a product basis is necessarily extendible, as we can choose the shaded region containing v_0 and v_9 on party P_3, the disjoint shaded region (i.e., the one containing v_5 and v_6) on party P_2, and the disjoint shaded region (i.e., the one containing v_2 and v_3) on party P_1, for a total of 6 vertices on 3 parties.

than 4 distinct parties P_j for which $C_{2,j} \geq 3$ [11]. Each of these four parties has at most $2k+4$ edges in its orthogonality graph, and each of the remaining $4k-4$ parties has at most $2k+2$ edges on its orthogonality graph, for a total of at most $4(2k+4)+(4k-4)(2k+2) = 8k^2+8k+8$ edges. The complete graph on $4k+3$ vertices has $(4k+3)(4k+2)/2 = 8k^2+10k+3$ edges, so when $k \geq 3$ there are not enough edges in the orthogonality graph, so the set of states does not form a product basis, which contradicts our assumption that we are working with a UPB. Note that this is the case in which the UPB of Lemma 3 arises if $k = 2$, so the fact that we require $k \geq 3$ here is not surprising.

Case 4: $\max_j\{C_{3,j}\} = 1$.

By parity arguments, we see that every party P_j with $C_{3,j} = 1$ must also have $C_{2,j} \in \{1, 3, 5, \ldots\}$. Furthermore, if there exist two (or more) parties P_1, P_2 such that $M_1 = M_2 = 3$, then unextendibility is violated unless $C_{2,j} = 1$ whenever $M_j = 3$.

Case 4(a): There exist three (or more) parties P_1, P_2, P_3 such that $M_1 = M_2 = M_3 = 3$.

Because there must exist a shaded region containing exactly 2 vertices on each party P_1, P_2, P_3, it is easily verified that the only possible configuration of shaded regions on those parties (up to repositioning vertices and parties) that doesn't break unextendibility is the one depicted in Figure 10.

The parties P_1, P_2, P_3 can have no more than $(2k+5)+2(2k+3) = 6k+11$ distinct edges among them (since there will be a lot of overlap at the left edge of the graphs if we make each group of 3 equal states orthogonal to the group of 2 equal states). It is straightforward to see that none of the remaining $4k-3$ parties P_j can have $M_j \geq 3$ or $C_{2,j} \geq 2$ without breaking unextendiblity. Thus those $4k-3$ parties can produce no more than $2k+2$ edges each, for a total of $6k+11+(4k-3)(2k+2) = 8k^2+8k+5$ edges. Since $8k^2+8k+5 < 8k^2+10k+3$ when

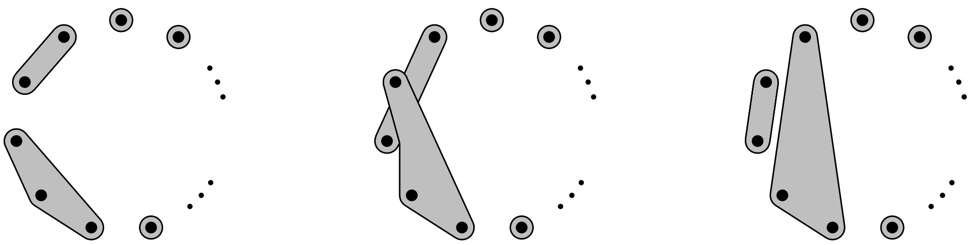

Figure 10 The (essentially unique) partial orthogonality graph that does not violate unextendibility in case 4(a).

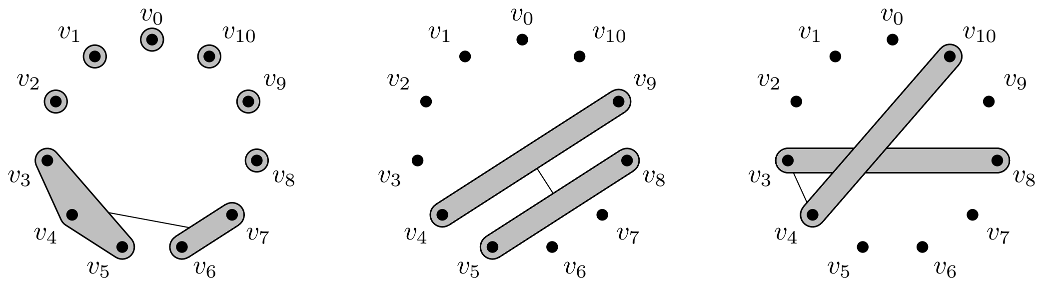

Figure 11 An example of a partial orthogonality graph in case 4(b).

$k \geq 2$, there are some edges missing from the orthogonality graphs, which is a contradiction.

Case 4(b): There exists a party P_1 such that $M_1 = 3$, but $M_j \leq 2$ for $j \geq 2$.

Party P_1 contributes at most $2k+5$ edges to the orthogonality graph, and the unextendibility requirement implies that $C_{2,j} \leq 3$ for $j \geq 2$. Suppose that there are m indices $2 \leq j_1, j_2, \ldots, j_m \leq 4k$ such that $C_{2,j_i} = 3$ for $1 \leq i \leq m$ and $C_{2,j} = 1$ for all other values of j. Then there are at most $(2k+5) + m(2k+4) + (4k-m-1)(2k+2) = 8k^2 + 8k + 2m + 3$ total edges between all $4k$ parties. As in the previous cases, we need a total of $8k^2 + 10k + 3$ edges, which implies that $m \geq k$. We already saw via brute-force search in case 3(b) that we can't have $m \geq 5$, so we only need to rule out the $3 \leq k \leq 4$ cases.

If the group of 3 identical states on party P_1 is represented by vertices v_3, v_4, and v_5 (see Figure 11), then each one of the 3 groups of 2 identical states on the other parties must contain exactly one of v_3, v_4, or v_5. By refining our brute-force computer search to take this restriction into account, we find that there is no configuration of shaded regions that does not violate unextendibility when $m \geq 3$ [11], so no such UPB exists when $k \geq 3$.

Case 4(c): There exist two parties P_1, P_2 such that $M_1 = M_2 = 3$, but $M_j \leq 2$ for $j \geq 3$.

In this case, there are (up to relabelling vertices and parties) only two possible configurations of parties P_1 and P_2, which are depicted in Figures 12 and 13. Notice that in Figure 12, the shaded region on party P_1 that contains exactly two vertices *does not* share any common vertices with the shaded region on party P_2 that contains exactly two vertices, while in Figure 13 those two regions contain the common vertex v_1.

Suppose for now that parties P_1 and P_2 have a total of at most $4k+8$ distinct edges on their orthogonality graphs. If there are m parties P_j ($j \geq 3$) for which $C_{2,j} = 3$, then we have a total of at most $(4k+8) + m(2k+4) + (4k-m-2)(2k+2) = 8k^2 + 8k + 2m + 4$ edges. In all of these m parties, we require that one of the shaded regions contains v_2 and v_3

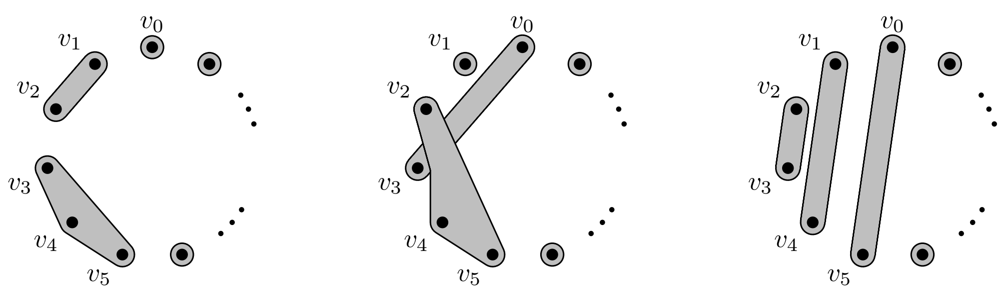

Figure 12 One of two possible partial orthogonality graphs of parties P_1, P_2, and P_3 that does not violate unextendibility in case 4(c).

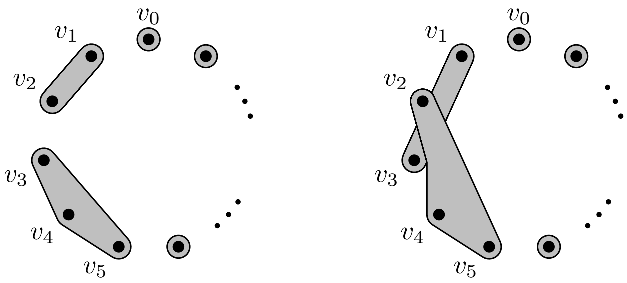

Figure 13 The other possible partial orthogonality graph of parties P_1, P_2 that does not violate unextendibility in case 4(c).

and the other shaded regions containing two vertices each contain one of v_4 or v_5. Thus, the brute-force search described in case 4(b) applies here as well and shows that $m \leq 2$. However, when $m = 2$ we have $8k^2 + 8k + 2m + 4 = 8k^2 + 8k + 8 < 8k^2 + 10k + 3$ when $k \geq 3$, which shows that there can not possibly be enough edges on the orthogonality graphs in this case.

The only remaining possibility is that the parties P_1 and P_2 have a total of at least $4k+9$ distinct edges (and hence *exactly* $4k+9$ distinct edges). In this case, parties P_1 and P_2 must be as in Figure 12, and on both of the parties P_1 and P_2 the set of 3 equal states must be orthogonal to the set of 2 equal states. Furthermore, it is not difficult to show that in this case, any party P_j with $C_{2,j} = 3$ can have at most $2k+4$ edges, but if it has $2k+4$ edges then at least one of those edges must already be present on either party P_1 or P_2. It follows that each party P_j $(j \geq 3)$ can introduce at most $2k+3$ new edges that have not already been counted. Thus, if there are m parties P_j $(j \geq 3)$ for which $C_{2,j} = 3$, we have a total of at most $(4k+9) + m(2k+3) + (4k-m-2)(2k+2) = 8k^2 + 8k + m + 5$ edges. Since $m \leq 2$ (as before) and $k \geq 3$, it follows that $8k^2 + 8k + m + 5 < 8k^2 + 10k + 3$, which again shows that there can not possibly be enough edges on the orthogonality graphs in this case. ◀

Acknowledgements. Thanks are extended to Gus Gutoski for suggesting a computer search to fill in the gaps in the proof of Lemma 6. The author was supported by the Natural Sciences and Engineering Research Council of Canada and the Mprime Network.

References

1. N. Alon and L. Lovász. Unextendible product bases. *J. Combinatorial Theory, Ser. A*, 95:169–179, 2001.
2. R. Augusiak, T. Fritz, M. Kotowski, M. Kotowski, M. Pawłowski, M. Lewenstein, and A. Acín. Tight Bell inequalities with no quantum violation from qubit unextendible product bases. *Phys. Rev. A*, 85:042113, 2012.
3. R. Augusiak, J. Stasinska, C. Hadley, J. K. Korbicz, M. Lewenstein, and A. Acín. Bell inequalities with no quantum violation and unextendible product bases. *Phys. Rev. Lett.*, 107:070401, 2011.
4. C. H. Bennett, D. P. DiVincenzo, C. A. Fuchs, T. Mor, E. Rains, P. W. Shor, J. A. Smolin, and W. K. Wootters. Quantum nonlocality without entanglement. *Phys. Rev. A*, 59:1070–1091, 1999.
5. C. H. Bennett, D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, and B. M. Terhal. Unextendible product bases and bound entanglement. *Phys. Rev. Lett.*, 82:5385–5388, 1999.
6. J. Chen and N. Johnston. The minimum size of unextendible product bases in the bipartite case (and some multipartite cases). E-print: arXiv:1301.1406 [quant-ph], 2013.

7 D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, and B. M. Terhal. Unextendible product bases, uncompletable product bases and bound entanglement. *Commun. Math. Phys.*, 238:379–410, 2003.

8 R. Duan, Y. Xin, and M. Ying. Locally indistinguishable subspaces spanned by three-qubit unextendible product bases. *Phys. Rev. A*, 81:032329, 2010.

9 K. Feng. Unextendible product bases and 1-factorization of complete graphs. *Discrete Appl. Math.*, 154:942–949, 2006.

10 F. Harary. *Graph Theory.* Addison-Wesley, Reading, Mass., 1969.

11 N. Johnston. Code for proving that no UPB of size $4k+3$ exists on $4k$ qubits. Published electronically at `http://www.njohnston.ca/publications/qubit-upbs/code/`, 2013.

12 J. M. Leinaas, P. Ø. Sollid, and J. Myrheim. Unextendible product bases and extremal density matrices with positive partial transpose. E-print: arXiv:1104.1318 [quant-ph], 2011.

13 Ł. Skowronek. Three-by-three bound entanglement with general unextendible product bases. *J. Math. Phys.*, 52:122202, 2011.

14 B. M. Terhal. A family of indecomposable positive linear maps based on entangled quantum states. *Linear Algebra Appl.*, 323:61–73, 2001.