On decomposable correlation matrices

Benjamin Lovitz
Institute for Quantum Computing and Department of Applied Mathematics, University of Waterloo, Waterloo, Canada

ABSTRACT
A correlation matrix is a positive semidefinite matrix with ones on the diagonal. In this work, we introduce and study r-decomposable correlation matrices: those that can be written as the Schur product of correlation matrices of rank at most r. We find that for all $r \geq 2$, every $(r+1) \times (r+1)$ correlation matrix is r-decomposable, and we construct $(2r+1) \times (2r+1)$ correlation matrices that are not r-decomposable. One question this leaves open is whether every $4 \times 4$ correlation matrix is 2-decomposable, which we make partial progress towards resolving. Motivations in quantum information are discussed.

1. Introduction
For a positive integer $n$, let $L(\mathbb{C}^n)$ denote the set of linear operators on $\mathbb{C}^n$, and let $\text{Cor}(\mathbb{C}^n) \subset L(\mathbb{C}^n)$ denote the set of correlation matrices: positive semidefinite matrices with diagonal entries all equal to one. Equivalently, a matrix $P \in L(\mathbb{C}^n)$ is a correlation matrix if there exists a set of unit vectors $\{v_1, \ldots, v_n\} \subset \mathbb{C}^n$ such that $P(a, b) = \langle v_a, v_b \rangle$ for all $a, b \in \{1, \ldots, n\}$, in which case we say $P$ is generated by $\{v_1, \ldots, v_n\}$. We say a correlation matrix $P \in \text{Cor}(\mathbb{C}^n)$ is r-decomposable if it can be written as the Schur product $\otimes$ (also known as the Hadamard product, entrywise product, or pointwise product) of correlation matrices of rank $\leq r$, i.e.

$$P = R_1 \otimes \cdots \otimes R_m$$

for some positive integer $m$ and correlation matrices $R_1, \ldots, R_m \in \text{Cor}(\mathbb{C}^n)$ with rank($R_i$) $\leq r$ for all $i \in \{1, \ldots, m\}$. Equivalently, a correlation matrix is r-decomposable if it is generated by a set of unit product vectors in $(\mathbb{C}^r)^\otimes m$ (i.e. unit vectors of the form $x_1 \otimes \cdots \otimes x_m$ for $x_1, \ldots, x_m \in \mathbb{C}^r$) for some positive integer $m$. We denote the set of r-decomposable correlation matrices as $\text{Cor}_r(\mathbb{C}^n)$.

Our main mathematical results are as follows:

- It is well known that $\text{Cor}(\mathbb{C}^n)$ is a compact and convex set. To our knowledge, it is not known whether $\text{Cor}_r(\mathbb{C}^n)$ is closed, and we leave this question unanswered. We show that $\text{Cor}_r(\mathbb{C}^n)$ is not convex when $r \geq 1$ and $n \geq 2r + 1$. 

It is clear that $\text{Cor}_r(\mathbb{C}^n) = \text{Cor}(\mathbb{C}^n)$ for all $n \leq r$. We prove that $\text{Cor}_{n-1}(\mathbb{C}^n) = \text{Cor}(\mathbb{C}^n)$ for all $n \geq 3$, but $\text{Cor}_r(\mathbb{C}^n) \not\subseteq \text{Cor}(\mathbb{C}^n)$ for all $n \geq 2r + 1$.

The previous point leaves open the question of whether the containment $\text{Cor}_r(\mathbb{C}^n) \subseteq \text{Cor}(\mathbb{C}^n)$ is strict for $n \in \{r + 2, \ldots, 2r\}$, and in particular whether $\text{Cor}_2(\mathbb{C}^4) \subseteq \text{Cor}(\mathbb{C}^4)$ is strict. We reduce the latter to a simpler question of whether every element of a certain subset of $\text{Cor}(\mathbb{C}^4)$ can be written as the Schur product of just two rank-two correlation matrices, which could make the problem more tractable for analytical or numerical approaches.

In Section 2 we motivate the study of $r$-decomposability in the context of quantum information. Our mathematical results do not rely on the material in this section, so it can be safely skipped. In Section 3 we review some mathematical preliminaries, in Section 4 we present our main results on $\text{Cor}_r(\mathbb{C}^n)$, in Section 5 we study the question of whether the containment $\text{Cor}_2(\mathbb{C}^4) \subseteq \text{Cor}(\mathbb{C}^4)$ is strict, and in Section 6 we apply our results to an entanglement detection scenario introduced in Section 2.

2. Motivation in quantum information

The general topic of correlation matrices has received considerable interest in quantum information [1–6]. This interest is due in part to Tsirelson's theorem [7], which reveals an intimate connection between correlation matrices and certain nonlocal correlations that can arise from bipartite quantum systems. Another motivation is the identification of correlation matrices with Schur channels, examples of which include physically relevant channels such as generalized dephasing channels, cloning channels, and the Unruh channel [3].

The particular topic of Schur products of correlation matrices has also been studied in quantum information [8–10]. Let $\{v_1, \ldots, v_n\} \subset \mathbb{C}^s$ and $\{u_1, \ldots, u_n\} \subset \mathbb{C}^t$ be unit vectors with $s \leq t$, and let $P, Q \in \text{Cor}(\mathbb{C}^n)$ be the correlation matrices they generate respectively. It is well known that $P = Q$ if and only if there exists an isometry $U$ such that $Uv_a = u_a$ for all $a \in \{1, \ldots, n\}$. More generally, in [8,9] it is proven that there exists a quantum channel $\Phi$ such that $\Phi(v_a v_a^*) = u_a u_a^*$ for all $a \in \{1, \ldots, n\}$ if and only if there exists a correlation matrix $R \in \text{Cor}(\mathbb{C}^n)$ such that $P = R \circ Q$. Moreover, it is not hard to show (using the Stinespring representation of $\Phi$) that the rank of $R$ is equal to the Choi rank of $\Phi$, which reveals a close relationship between this topic and $r$-decomposability. We note that [8,9] also give results on transformations between sets of general density matrices.

In [10] a topic very similar to ours is studied. A characterization is found of what we call $\text{CS-decomposable}$ correlation matrices: those that can be written as a Schur product of correlation matrices, each of which are generated by a set of coherent states (states of light produced by an ideal laser [11]). Equivalently, CS-decomposable correlation matrices are those that are generated by multi-mode coherent states: unit vectors that are tensor products of coherent states.

We now briefly summarize how the study of CS-decomposability is motivated in [10], as it will also motivate our study of $r$-decomposability. A pressing need in quantum information is to adapt or reinvent existing quantum protocols to be more experimentally realizable. Quantum fingerprinting and appointment scheduling are two examples of tasks for which this need has been recently addressed. The original protocols for these tasks use...
high dimensional entangled states that are difficult to prepare in a lab [12,13], but both protocols have been adapted to use tensor products of coherent states and/or qubits (which are easier to produce experimentally), and simple quantum operations, while attaining similar figures of merit [14–16]. The experimental ease of producing tensor products of coherent states or low-dimensional unit vectors leads us to ask what other protocols can be adapted to use such states. This motivates the study of CS-decomposable and $r$-decomposable correlation matrices. By the discussion of the previous paragraph, protocols that use a fixed set of unit vectors can be adapted to use any other set of unit vectors that generate the same correlation matrix, simply by applying the corresponding isometry. Thus, if a protocol requires a set of unit vectors that generate a CS-decomposable ($r$-decomposable) correlation matrix, then the protocol can be adapted into a protocol that uses tensor products of coherent states (or $r$-dimensional unit vectors), which might be easier to implement than the original protocol. In this way, the study of CS-decomposable and $r$-decomposable correlation matrices could potentially give rise to more experimentally implementable protocols.

We further motivate our study of $r$-decomposability by the following entanglement detection scenario. Say we are given many copies of unknown pure states $v_1 v_1^*, \ldots, v_n v_n^*$, on which we are allowed to perform any of the measurements $\{v_1 v_1^*, 1 - v_1 v_1^*\}, \ldots, \{v_n v_n^*, 1 - v_n v_n^*\}$, and we wish to detect that for any partitioning of the space into subsystems of dimension $\leq r$, at least one of the states must be entangled. This scenario is similar to our $r$-decomposability question, as the only meaningful information to be gained from performing the allowed measurements is precisely the inner products $\langle v_a v_a^*, v_b v_b^* \rangle$ for $a, b \in \{1, \ldots, n\}$. In Proposition 6.1 we find cases of this scenario in which one can indeed detect entanglement.

3. Mathematical preliminaries

Here we review some elementary facts and definitions we use. We often find it convenient to identify a complex Euclidean space by a symbol such as $\mathcal{X}$, $\mathcal{Y}$, or $\mathcal{Z}$, rather than $\mathbb{C}^n$, because it allows us to refer to multiple spaces that could be isomorphic to each other. For any complex Euclidean space $\mathcal{X}$, let $\langle \cdot, \cdot \rangle : \mathcal{X} \times \mathcal{X} \to \mathbb{C}$ be the standard Euclidean inner product that is conjugate-linear in the first argument and linear in the second argument. For linear operators $A, B \in L(\mathcal{X}, \mathcal{Y})$, define $\langle A, B \rangle := \text{Tr}(A^* B)$. Let $\| \cdot \| = \sqrt{\langle \cdot, \cdot \rangle}$ be the Euclidean norm, and define the set of unit vectors $S(\mathcal{X})$ as the set of vectors $x \in \mathcal{X}$ that satisfy $\|x\| = 1$. Let $U(\mathcal{X}, \mathcal{Y}) \subset L(\mathcal{X}, \mathcal{Y})$ be the set of isometries from $\mathcal{X}$ to $\mathcal{Y}$, i.e. the set of operators that preserve the Euclidean norm. For a non-negative integer $a$, let $e_a$ denote the standard basis vector with 1 in the $a$th position and zeros elsewhere. We use the convention $[m] := \{1, \ldots, m\}$ for any positive integer $m$.

For a positive integer $m$ and complex Euclidean spaces $\mathcal{X}_1, \ldots, \mathcal{X}_m$, we say a vector (or tensor)

$$x \in \mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_m$$

is a product vector (or elementary tensor) if it is non-zero and can be written as

$$x = x_1 \otimes \cdots \otimes x_m$$

for some collection of non-zero vectors $x_1 \in \mathcal{X}_1, \ldots, x_m \in \mathcal{X}_m$. If $x$ is not a product vector and is non-zero then we say $x$ is entangled. We use $\text{Prod} (\mathcal{X}_1 : \cdots : \mathcal{X}_m)$ to denote the set
of product vectors in $\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_m$, and Prod$S$ $(\mathcal{X}_1 : \cdots : \mathcal{X}_m)$ to denote the set of unit product vectors. We refer to the spaces $\mathcal{X}_1, \ldots, \mathcal{X}_m$ that compose the space $\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_m$ as subsystems.

For positive integers $n$ and $m$, we frequently define sets of product vectors

$$\{x_a : a \in [n]\} \subset \text{Prod} (\mathcal{X}_1 : \cdots : \mathcal{X}_m)$$

without explicitly defining for each $a \in [n]$ corresponding vectors $x_{a,1}, \ldots, x_{a,m}$ for which

$$x_a = x_{a,1} \otimes \cdots \otimes x_{a,m}.$$  

In this case, we implicitly fix some such set of vectors $x_{a,1}, \ldots, x_{a,m}$ (they are unique up to scalar multiples $\alpha_{a,1}x_{a,1}, \ldots, \alpha_{a,m}x_{a,m}$ such that $\alpha_{a,1} \cdots \alpha_{a,m} = 1$), and refer to the vectors $x_{a,j}$ without further introduction. We use symbols like $a, b, c$ to index vectors, and symbols like $i, j, k$ to index subsystems.

We conclude this section by reviewing some elementary facts about correlation matrices. It is straightforward to verify that a matrix $P \in \text{L}(\mathbb{C}^n)$ is contained in Cor$(\mathbb{C}^n)$ if and only if $P = A^*A$ for some linear operator $A \in \text{L}(\mathbb{C}^n, \mathbb{C}^s)$ (and positive integer $s$), the columns of which form unit vectors. We say $P$ is generated by some set of unit vectors $\{v_a : a \in [n]\} \subset S(\mathbb{C}^s)$ if these vectors can be chosen as the columns of $A$. Note that $P(a, b) = \langle v_a, v_b \rangle$, so $P$ is the matrix of inner products (i.e. the Gram matrix) of any generating set of unit vectors. Recall that two sets of unit vectors $\{v_a : a \in [n]\} \subset S(\mathbb{C}^s)$ and $\{u_a : a \in [n]\} \subset S(\mathbb{C}^t)$ with $s \leq t$ generate the same correlation matrix if and only if there exists an isometry $U \in \text{U}(\mathbb{C}^s, \mathbb{C}^t)$ such that $Uv_a = u_a$ for all $a \in [n]$. This property follows from the standard result that two operators $A \in \text{L}(\mathbb{C}^n, \mathbb{C}^s)$ and $B \in \text{L}(\mathbb{C}^n, \mathbb{C}^t)$ satisfy $A^*A = B^*B$ if and only if $B = UA$ for some isometry $U \in \text{U}(\mathbb{C}^s, \mathbb{C}^t)$. Note that by linearity, the linear dependence of every generating set is the same. The following proposition reveals a straightforward yet important connection between the Schur product of correlation matrices and the tensor product of the unit vectors in their generating sets, which we state without proof.

**Proposition 3.1:** A correlation matrix $P \in \text{Cor}(\mathbb{C}^n)$ is $r$-decomposable if and only if there exists a positive integer $m$, complex Euclidean spaces $\mathcal{X}_1, \ldots, \mathcal{X}_m$ with $\dim \mathcal{X}_i \leq r$ for all $i \in [m]$, and a set of unit product vectors $\{x_a : a \in [n]\} \subset \text{Prod}S (\mathcal{X}_1 : \cdots : \mathcal{X}_m)$ that generate $P$.

### 4. Results on $r$-decomposable correlation matrices

Here we state and prove our main results on $r$-decomposable correlation matrices.

**Theorem 4.1:** For any integers $r \geq 2$ and $n \leq r + 1$, $\text{Cor}_r(\mathbb{C}^n) = \text{Cor}(\mathbb{C}^n)$. More generally, let $\mathcal{X}$ be a complex Euclidean space and $P \in \text{Cor}(\mathcal{X})$ be a correlation matrix. If $\text{rank}(P) \geq 3$ and $P$ is generated by a set of unit vectors that contains a vector that is not in the span of the rest, then $P$ is $(\text{rank}(P) - 1)$-decomposable.

Note that a correlation matrix $P \in \text{Cor}(\mathbb{C}^n)$ with $\text{rank}(P) \leq r$ is trivially contained in Cor$_r(\mathbb{C}^n)$, so the only non-trivial part of the first sentence is that if an $n \times n$ correlation
matrix $P$ has full rank (i.e. it is generated by a linearly independent set of unit vectors), then it is $(n - 1)$-decomposable. The second sentence generalizes this statement to say that if $P$ is generated by a set of unit vectors that contains a vector that is not in the span of the rest, then it is $(\text{rank}(P) - 1)$-decomposable.

**Proof:** We prove the second (more general) statement. Let $\{v_a : a \in [n]\}$ be a set of unit vectors that generate $P$ such that

$$v_c \not\in \text{span}\{v_a : a \in [n] \setminus \{c\}\}$$

for some index $c \in [n]$.

If $v_c$ is orthogonal to every other vector, then the construction is easy: the set of vectors with each $v_a$ replaced by $v_a \otimes e_0$ for $a \neq c$, and $v_c$ replaced by $v'_c \otimes e_1$ for any unit vector $v'_c \in \text{span}\{v_a : a \in [n] \setminus \{c\}\}$ generates $P$. This is a $(\text{rank}(P) - 1)$-decomposition of $P$, since

$$\dim \text{span}\{v_a : a \in [n] \setminus \{c\}\} = \text{rank}(P) - 1$$

and

$$\dim \text{span}\{e_0, e_1\} = 2 \leq \text{rank}(P) - 1.$$

If $v_c$ is not orthogonal to every other vector, then define

$$\Pi := \text{Proj} \left( \text{span}\{v_a : a \in [n] \setminus \{c\}\} \right),$$

and define two correlation matrices $R$ and $Q$ as

$$R(a, b) = \frac{\langle v_a, \Pi v_b \rangle}{\| \Pi v_a \| \| \Pi v_b \|}$$

and

$$Q(a, b) = \begin{cases} \| \Pi v_c \|, & a \neq b \text{ and } c \in \{a, b\} \\ 1, & \text{otherwise.} \end{cases}$$

It is straightforward to verify that $P = R \odot Q$. Indeed, for $c \notin \{a, b\}$,

$$(R \odot Q)(a, b) = \frac{\langle v_a, \Pi v_b \rangle}{\| \Pi v_a \| \| \Pi v_b \|} = \langle v_a, v_b \rangle.$$

Otherwise,

$$(R \odot Q)(a, c) = \frac{\langle v_a, \Pi v_c \rangle}{\| \Pi v_a \| \| \Pi v_c \|} \| \Pi v_c \| = \langle v_a, v_c \rangle,$$

and similarly, $(R \odot Q)(c, a) = \langle v_c, v_a \rangle$. The correlation matrix $R$ has rank($R$) = rank($P$) - 1, and is generated by the unit vectors $\Pi v_a / \| \Pi v_a \|$. The correlation matrix $Q$ has rank($Q$) = 2, and is generated by the set of unit vectors $\{u_a : a \in [n]\} \subset \mathcal{S}(\mathbb{C}^2)$, where

$$u_a = \begin{cases} e_0, & a \neq c \\ \| \Pi v_c \| e_0 + \sqrt{1 - \| \Pi v_c \|^2} e_1, & a = c. \end{cases}$$

This completes the proof.
Now we find cases in which Cor$_r (\mathbb{C}^n) \subsetneq \text{Cor} (\mathbb{C}^n)$. We require the following lemma, which we reference without proof. We note that this lemma holds more generally over an arbitrary field.

**Lemma 4.2** ([17,18], Corollary 10 in [19]): Let $m \geq 1$ be an integer, let $\mathcal{X}_1, \ldots, \mathcal{X}_m$ be complex Euclidean spaces, and let $x_1, x_2 \in \text{Prod} (\mathcal{X}_1 : \cdots : \mathcal{X}_m)$ be product vectors. Then the following statements are equivalent:

1. For all scalars $\alpha_1, \alpha_2 \in \mathbb{C}$, it holds that $\alpha_1 x_1 + \alpha_2 x_2 \in \text{Prod} (\mathcal{X}_1 : \cdots : \mathcal{X}_m) \cup \{0\}$.
2. For some non-zero scalars $\alpha_1, \alpha_2 \in \mathbb{C} \setminus \{0\}$, it holds that $\alpha_1 x_1 + \alpha_2 x_2 \in \text{Prod} (\mathcal{X}_1 : \cdots : \mathcal{X}_m) \cup \{0\}$.
3. There exists at most a single index $j \in [m]$ for which $\dim \text{span}\{x_{1,j}, x_{2,j}\} = 2$.

**Theorem 4.3:** For all integers $r \geq 1$ and $n \geq 2r + 1$, Cor$_r (\mathbb{C}^n) \subsetneq \text{Cor} (\mathbb{C}^n)$.

**Proof:** For $r = 1$, the statement follows easily from the fact that the Schur product of any two rank-one correlation matrices is again rank one (see the proof of Lemma 5.5). Assume $r \geq 2$. We find a correlation matrix $P \in \text{Cor} (\mathbb{C}^{2r+1})$ that is not contained in Cor$_r (\mathbb{C}^{2r+1})$. This will prove the claim, as it implies that any correlation matrix in Cor$_r (\mathbb{C}^n)$ with principal submatrix $P$ is not $r$-decomposable.

Let $v_1, \ldots, v_{r+1}$ be any linearly independent collection of unit vectors for which

$$|\langle v_a, v_{a+2} \rangle| > |\langle v_a, v_{a+1} \rangle| \cdot |\langle v_{a+1}, v_{a+2} \rangle|. \quad (15)$$

For example, one could choose any $p \in (0, 1)$ and let $\langle v_a, v_b \rangle = p$ for all $a \neq b \in [r + 1]$. Let $\alpha_1, \ldots, \alpha_r, \beta_2, \ldots, \beta_{r+1} \in \mathbb{C} \setminus \{0\}$ be any collection of non-zero scalars subject to the constraint that for all $a \in [r]$ it holds that $\|\alpha_a v_a + \beta_{a+1} v_{a+1}\| = 1$, and let $P$ be the correlation matrix generated by

$$\{v_1, \ldots, v_{r+1}, \alpha_1 v_1 + \beta_2 v_2, \alpha_2 v_2 + \beta_3 v_3, \ldots, \alpha_r v_r + \beta_{r+1} v_{r+1}\}. \quad (16)$$

Note that rank($P$) = $r + 1$. For notational convenience, we extend the definition of $v_a$ to denote the $a$th vector in this set for each $a \in [2r + 1]$.

We proceed by contradiction. The existence of an $r$-decomposition of $P$ is equivalent to the existence of a positive integer $m$, complex Euclidean spaces $\mathcal{X}_1, \ldots, \mathcal{X}_m \cong \mathbb{C}^r$, and unit product vectors $\{x_a : a \in [2r + 1]\} \subset \text{ProdS} (\mathcal{X}_1 : \cdots : \mathcal{X}_m)$ such that $\langle x_a, x_b \rangle = \langle v_a, v_b \rangle$ for all $a, b \in [2r + 1]$. By Lemma 4.2, this implies that for each $a \in [r]$,

$$\dim \text{span}\{x_{a,i}, x_{a+1,i}\} = 2 \quad (17)$$

for at most a single index $i \in [m]$. Furthermore, such an index indeed exists for every $a \in [r]$, since for all $a \in [r]$,

$$\dim \text{span}\{x_a, x_{a+1}\} = \dim \text{span}\{v_a, v_{a+1}\} = 2. \quad (18)$$

For each $a \in [r]$, fix $i_a \in [m]$ to denote the unique index that satisfies (17). Since $|\langle x_{a,i}, x_{a+1,i} \rangle| = 1$ for all $i \neq i_a$, it must hold that $|\langle x_{a,i}, x_{a+1,i} \rangle| = |\langle v_a, v_{a+1} \rangle|$ for all $a \in$
Note that
\[ \dim \text{span}\{x_{a,i} : a \in [2r + 1]\} \leq r \]  
(19)
for all \(i \in [m]\), and
\[ \dim \text{span}\{x_1, \ldots, x_{r+1}\} = \dim \text{span}\{v_1, \ldots, v_{r+1}\} = r + 1, \]
(20)
so there must exist an index \(a \in [r - 2]\) such that \(i_a \neq i_{a+1}\). Fix \(a\) to denote one such index. Note that
\[ |\langle x_{a,i_a}, x_{a+1,i_a} \rangle| = |\langle v_{a+1}, v_{a+2} \rangle| \]
(21)
\[ |\langle x_{a+1,i_{a+1}}, x_{a+2,i_{a+1}} \rangle| = |\langle v_{a+1}, v_{a+2} \rangle| \]
(22)
\[ |\langle x_{a,i_{a+1}}, x_{a+1,i_{a+1}} \rangle| = 1 \]
(23)
\[ |\langle x_{a+1,i_a}, x_{a+2,i_a} \rangle| = 1, \]
(24)
from which it follows that
\[ |\langle x_{a,i_a}, x_{a+2,i_a} \rangle| = |\langle v_a, v_{a+1} \rangle| \]
(25)
\[ |\langle x_{a,i_{a+1}}, x_{a+2,i_{a+1}} \rangle| = |\langle v_{a+1}, v_{a+2} \rangle|, \]
(26)
but this implies
\[ |\langle v_a, v_{a+2} \rangle| = |\langle x_a, x_{a+2} \rangle| \]
(27)
\[ = \prod_{i=1}^{m} |\langle x_{a,i}, x_{a+2,i} \rangle| \]
(28)
\[ \leq |\langle x_{a,i_a}, x_{a+2,i_a} \rangle| \cdot |\langle x_{a,i_{a+1}}, x_{a+2,i_{a+1}} \rangle| \]
(29)
\[ = |\langle v_a, v_{a+1} \rangle| \cdot |\langle v_{a+1}, v_{a+2} \rangle|, \]
(30)
a contradiction to (15). This completes the proof. \(\blacksquare\)

**Corollary 4.4:** For all integers \(r \geq 1\) and \(n \geq 2r + 1\), \(\text{Cor}_r(\mathbb{C}^n)\) is not convex.

**Proof:** We first prove that \(\text{Cor}_r(\mathbb{C}^{2r+1})\) is not convex. Let \(P \in \text{Cor}(\mathbb{C}^{2r+1}) \setminus \text{Cor}_r(\mathbb{C}^{2r+1})\) be any correlation matrix constructed in Theorem 4.3. Since \(\text{Cor}(\mathbb{C}^{2r+1})\) is contained in a real affine space of dimension \(2r(2r + 1)\), then by Carathéodory’s theorem \([20]\),
\[ P = \sum_{i=1}^{s} p(i)R_i \]
(31)
for some positive integer \(s \leq 2r(2r + 1) + 1\), probability vector \(p\), and extreme point correlation matrices \(R_i\). By Corollary 2 in \([21]\), \(\text{rank}(R_i) \leq \lfloor \sqrt{2r + 1} \rfloor \leq r\) for all \(i \in [s]\). It follows that \(\text{Cor}_r(\mathbb{C}^{2r+1})\) is not convex, since each \(R_i\) is \(r\)-decomposable and \(P\) is not.
For the general statement, let $n \geq 2r + 1$ be any integer. For each $i \in [s]$, let $R'_i \in \text{Cor}(\mathbb{C}^n)$ be any correlation matrix with rank($R'_i$) = rank($R_i$) $\leq r$ that contains $R_i$ as the upper-left principal submatrix. Then

$$P' := \sum_{i=1}^{s} p(i)R'_i \in \text{Cor}(\mathbb{C}^n)$$

contains $P$ as the upper-left principal submatrix, so $P'$ is not $r$-decomposable. As before, it follows that Cor$_r(\mathbb{C}^n)$ is not convex, since each $R'_i$ is $r$-decomposable and $P'$ is not. ■

5. Is the containment Cor$_2(\mathbb{C}^4) \subseteq \text{Cor}(\mathbb{C}^4)$ strict?

Theorem 4.1 implies Cor$_2(\mathbb{C}^3) = \text{Cor}(\mathbb{C}^3)$, while Theorem 4.3 implies Cor$_2(\mathbb{C}^5) \subsetneq \text{Cor}(\mathbb{C}^5)$. This leaves open the question of whether the containment Cor$_2(\mathbb{C}^4) \subseteq \text{Cor}(\mathbb{C}^4)$ is strict. For a correlation matrix $P \in \text{Cor}(\mathbb{C}^4)$, it might seem possible that a 2-decomposition (1) exists only for large values of $m$, which could make our problem intractable. Theorem 5.1 allows us to restrict our attention to $m = 2$.

**Theorem 5.1:** The following statements are equivalent:

1. Cor$_2(\mathbb{C}^4) \subsetneq \text{Cor}(\mathbb{C}^4)$.
2. There exists a correlation matrix $P \in \text{Cor}(\mathbb{C}^4)$ such that rank($P$) = 3, every vector in a generating set of $P$ is contained in the span of the rest, and $P$ is not 2-decomposable into the Schur product of precisely two correlation matrices of rank 2.

In matroid-theoretic terms, a generating set of any correlation matrix satisfying statement 2 will form a circuit (a minimal linearly dependent set, see [22]). Several statements in this section can be phrased in terms of circuits.

Theorem 5.1 shows that it suffices to consider rank-three correlation matrices for which every vector in a generating set is contained in the span of the rest. In Proposition 5.2, we construct 2-decompositions of an infinite family of such correlation matrices, thus narrowing our question even further. We speculate that perhaps our construction can inspire a more general construction of all such correlation matrices.

**Proposition 5.2:** Let $P \in \text{Cor}(\mathbb{C}^4)$ be any correlation matrix generated by a set of unit vectors $\{v_a : a \in [4]\}$ such that there exists a real number $-1/2 < p < 1$ for which $\langle v_a, v_b \rangle = p$ for all $a \neq b \in [3]$, and there exist non-zero scalars $\alpha_1, \alpha_2 \in \mathbb{C} \setminus \{0\}$ for which $v_4 = \alpha_1(v_1 + v_3) + \alpha_2 v_2$. Then $P \in \text{Cor}_2(\mathbb{C}^4)$.

In the remainder of this section, we prove Theorem 5.1 and Proposition 5.2. For Theorem 5.1, (1 $\Rightarrow$ 2) will follow from Lemma 5.3, and (2 $\Rightarrow$ 1) will follow from Lemma 5.5. We now prove these lemmas.

**Lemma 5.3:** For all integers $n \geq 3$ and $2 \leq r \leq n - 1$, if Cor$_r(\mathbb{C}^n) \subsetneq \text{Cor}(\mathbb{C}^n)$, then there exists a correlation matrix $P \in \text{Cor}(\mathbb{C}^n) \setminus \text{Cor}_r(\mathbb{C}^n)$ such that every vector in a generating set of $P$ is contained in the span of the rest.
Proof: By assumption, there exists $P \in \text{Cor} (\mathbb{C}^n)$ that is not $r$-decomposable. If there exists a vector in a generating set of $P$ that is not contained in the span of the rest, then by the proof of Theorem 4.1 there exists a decomposition $P = Q \odot R$ where rank($Q$) = 2 and rank($R$) = rank($P$) − 1. If there exists a vector in a generating set of $R$ that is not contained in the span of the rest, then this process can be repeated until we have a decomposition

$$P = Q_1 \odot \cdots \odot Q_m \odot R'$$

(33)

for which each $Q_i$ has rank 2 and every vector in a generating set of $R'$ is contained in the span of the rest. Furthermore, $R'$ is not $r$-decomposable, for otherwise $P$ would be $r$-decomposable.

To prove Lemma 5.5, we require the following lemma proven by the author in [19]. We note that this lemma holds more generally over an arbitrary field.

Lemma 5.4 (Corollary 9 in [19]): Let $n$ and $m$ be positive integers, let $\mathcal{X}_1, \ldots, \mathcal{X}_m$ be complex Euclidean spaces, and let $\{x_a : a \in [n]\} \subset \text{Prod} (\mathcal{X}_1 : \cdots : \mathcal{X}_m)$ be a set of linearly independent product vectors. If there exist non-zero scalars $\alpha_1, \ldots, \alpha_n \in \mathbb{C} \setminus \{0\}$ such that

$$\sum_{a \in [n]} \alpha_a x_a \in \text{Prod} (\mathcal{X}_1 : \cdots : \mathcal{X}_m),$$

(34)

then the vectors $x_1, \ldots, x_n$ are non-parallel in at most $n-1$ subsystems, i.e. dim span$\{x_{a,j} : a \in [n]\} > 1$ for at most $n-1$ indices $j \in [m]$.

Lemma 5.5: For any integer $n \geq 3$, let $P \in \text{Cor} (\mathbb{C}^n)$ be any correlation matrix of rank $n-1$ generated by a set of unit vectors $\{v_a : a \in [n]\}$ for which

$$v_n = \sum_{a \in [n-1]} \alpha_a v_a$$

(35)

for some non-zero scalars $\alpha_1, \ldots, \alpha_{n-1} \in \mathbb{C} \setminus \{0\}$. For any integer $2 \leq r \leq n-1$, if $P \in \text{Cor}_r (\mathbb{C}^n)$, then $P$ is $r$-decomposable as the Schur product of $n-2$ correlation matrices of rank $\leq r$.

Proof: By assumption, there exists a positive integer $m \geq 2$, complex Euclidean spaces $\mathcal{X}_1, \ldots, \mathcal{X}_m$, and unit product vectors $\{u_a : a \in [n]\} \subset \text{Prod}_S (\mathcal{X}_1 : \cdots : \mathcal{X}_m)$ that generate $P$ and satisfy

$$u_n = \sum_{a \in [n-1]} \alpha_a u_a,$$

(36)

where the vectors $\{u_a : a \in [n-1]\}$ are linearly independent by the condition rank($P$) = $n-1$. By Lemma 5.4, this implies dim span$\{u_{a,j} : a \in [n]\} > 1$ for at most $n-2$ indices $i \in [m]$. For each $i \in [m]$, let $R_i$ be the correlation matrix generated by $\{u_{a,i} : a \in [n]\}$, so that

$$P = R_1 \odot \cdots \odot R_m.$$

(37)

Then rank $R_i > 1$ for at most $n-2$ indices $i \in [m]$. 
We conclude by showing that for any correlation matrix $R$ and rank-one correlation matrix $R'$, $R \odot R'$ is a correlation matrix with $\text{rank}(R \odot R') = \text{rank}(R)$. This will complete the proof, since all the rank-one correlation matrices in the $r$-decomposition (37) can be absorbed into the $\leq n - 2$ correlation matrices of rank $> 1$ to construct the desired decomposition.

It follows from Schur's product theorem that $R \odot R'$ is a correlation matrix [23]. Since $R'$ is positive semidefinite and rank-one, then $R' = xx^*$ for some vector $x$. Furthermore, since $R'$ has ones on the diagonal, each element of $x$ has unit modulus. It follows that

$$R \odot R' = R \odot xx^* = \text{Diag}(x) R \text{Diag}(x)^*, \quad (38)$$

where $\text{Diag}(x)$ is the diagonal unitary matrix with $\text{Diag}(x)(a,a) = x(a)$. Since $\text{Diag}(x)$ has full rank, then $\text{rank}(\text{Diag}(x) R \text{Diag}(x)^*) = \text{rank}(R)$, which completes the proof. ■

Theorem 5.1 follows easily from Lemmas 5.3 and 5.5. Now we prove Proposition 5.2.

**Proof of Proposition 5.2:** We have

$$P = \begin{bmatrix} 1 & p & p & \alpha_1 + (\alpha_1 + \alpha_2)p \\ p & 1 & p & \alpha_2 + 2\alpha_1 p \\ p & \alpha_1 + (\alpha_1 + \alpha_2)p & \alpha_2 + 2\alpha_1 p & 1 \\ \alpha_1 + (\alpha_1 + \alpha_2)p & \alpha_2 + 2\alpha_1 p & \alpha_1 + (\alpha_1 + \alpha_2)p & 1 \end{bmatrix}. \quad (39)$$

We construct $P$ as

$$P = Q_1 \odot Q_2, \quad (40)$$

where

$$Q_1 = \begin{bmatrix} 1 & \sqrt{\frac{1+p}{2}} & \sqrt{\frac{1+p}{2}} & p \\ \sqrt{\frac{1+p}{2}} & 1 & \sqrt{\frac{1+p}{2}} & 1 \\ \frac{1+p}{2} & 1 & \sqrt{\frac{1+p}{2}} & 1 \\ \frac{1+p}{2} & 1 & \sqrt{\frac{1+p}{2}} & \sqrt{\frac{1+p}{2}} \end{bmatrix}, \quad (41)$$

$$Q_2 = \begin{bmatrix} 1 & \sqrt{\frac{2}{1+p}} & \frac{\alpha_1 + (\alpha_1 + \alpha_2)p}{\sqrt{1+p}} \\ \frac{2}{1+p} & 1 & \sqrt{\frac{2}{1+p}} & \alpha_2 + 2\alpha_1 p \\ \frac{2}{1+p} & 1 & \frac{\alpha_1 + (\alpha_1 + \alpha_2)p}{\sqrt{1+p}} & 1 \\ \frac{2}{1+p} & \frac{\alpha_1 + (\alpha_1 + \alpha_2)p}{\sqrt{1+p}} & \frac{2}{1+p} & 1 \end{bmatrix}. \quad (42)$$

The equality is clear; it only remains to show that $Q_1$ and $Q_2$ are positive semidefinite and rank two.
First, it is easily verified that $Q_1$ is the correlation matrix generated by the unit vectors

\begin{align*}
q_{1,1} &= e_0 \\ q_{1,2} &= \sqrt{\frac{1+p}{2}}e_0 + \sqrt{\frac{1-p}{2}}e_1 \\ q_{1,3} &= pe_0 + \sqrt{1-p^2}e_1 \\ q_{1,4} &= q_{1,2},
\end{align*}

which implies $Q_1$ is positive semidefinite. Furthermore, $\text{rank}(Q_1) \leq 2$, since these vectors span at most a two-dimensional space.

Second, we verify that $Q_2$ is the correlation matrix of the unit vectors

\begin{align*}
q_{2,1} &= p\sqrt{\frac{2}{1+p}}e_0 + \frac{\alpha_1}{|\alpha_1|}\sqrt{\frac{1+p-2p^2}{1+p}}e_1 \\ q_{2,2} &= e_0 \\ q_{2,3} &= q_{2,1} \\ q_{2,4} &= (\alpha_2 + 2\alpha_1 p)e_0 + |\alpha_1|\sqrt{2(1+p-2p^2)}e_1,
\end{align*}

which will complete the proof, since it implies $\text{rank}(Q_2) \leq 2$ as above. The vectors $q_{2,1}, q_{2,2}, q_{2,3}$ are easily seen to be normalized. For $q_{2,4}$, recall the normalization condition on $v_4$

\[\langle v_4, v_4 \rangle = 2|\alpha_1|^2(p + 1) + |\alpha_2|^2 + (\alpha_1\alpha_2 + \alpha_1\alpha_2)2p = 1,\]

which implies

\[1 - |\alpha_2 + 2\alpha_1 p|^2 = 1 - (|\alpha_2|^2 + 4|\alpha_1|^2p^2 + (\alpha_1\alpha_2 + \alpha_1\alpha_2)2p) = 2|\alpha_1|^2(1 + p - 2p^2).\]

It follows that $q_{2,4}$ is normalized. Now we show that the inner products between $q_{2,1}, \ldots, q_{2,4}$ reproduce $Q_2$. All are easily seen except $\langle q_{2,1}, q_{2,4} \rangle$, which we now verify:

\begin{align*}
\langle q_{2,1}, q_{2,4} \rangle &= p\sqrt{\frac{2}{1+p}}(\alpha_2 + 2\alpha_1 p) + \frac{\alpha_1}{|\alpha_1|}\sqrt{\frac{1+p-2p^2}{1+p}}|\alpha_1|\sqrt{2(1+p-2p^2)} \\
&= \frac{2}{1+p} (p(\alpha_2 + 2\alpha_1 p) + \alpha_1(1 + p - 2p^2)) \\
&= \frac{2}{1+p} (\alpha_1 + (\alpha_1 + \alpha_2)p).
\end{align*}

This completes the proof.
6. Application of our results in an entanglement detection scenario

Here we apply our results to an entanglement detection scenario. Say we are given many copies of unknown pure states
\[ v_1^*, \ldots, v_n^*, w \]
with \( v_1, \ldots, v_n \in S(\mathcal{X}) \) for an unknown complex Euclidean space \( \mathcal{X} \). Suppose further that we are allowed to perform any of the measurements
\[
\{v_1^* v_1^*, \mathbb{I} - v_1^* v_1^*\}, \ldots, \{v_n^* v_n^*, \mathbb{I} - v_n^* v_n^*\}
\]
on any of the states \( v_1^*, \ldots, v_n^*, w \), and we wish to detect entanglement in the following sense. For some positive integer \( r \), we wish to detect that for any complex Euclidean space \( \mathcal{X} \), any set of unit vectors \( v_1, \ldots, v_n \in S(\mathcal{X}) \) that are consistent with the measurement outcomes observed in the above scenario, and any decomposition \( \mathcal{X} = \mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_m \) of \( \mathcal{X} \) into spaces of dimension \( \dim(\mathcal{X}_i) \leq r \), at least one of the vectors \( v_1, \ldots, v_n \) must be entangled.

In the above scenario, the only meaningful information that can be gained from the measurement outcomes is precisely the Gram matrix of \( \{v_1^* v_1^*, \ldots, v_n^* v_n^*\} \) (the matrix of inner products \( \langle v_a v_a^*, v_b v_b^* \rangle \) for \( a, b \in \{1, \ldots, n\} \)). Note that a correlation matrix \( R \) is the Gram matrix of rank-one projectors if and only if \( R = P \odot \overline{P} \) for some correlation matrix \( P \). The above scenario is therefore equivalent to being given some correlation matrix \( R \) that is the Gram matrix of rank-one projectors, and wishing to detect that for any correlation matrix \( P \), if \( R = P \odot \overline{P} \), then \( P \) is not \( r \)-decomposable. In Proposition 6.1 we find examples of such entanglement detection.

**Proposition 6.1:** For any integer \( r \geq 1 \) and real number \( 0 < p < 1 \), there exists a correlation matrix arising from a set of \( 2r + 1 \) unit vectors
\[
\{v_1, \ldots, v_{r+1}, v_{(1,2)}, v_{(2,3)}, \ldots, v_{(r,r+1)}\}
\]
such that for all \( a \neq b \in [r+1] \),
\[
|\langle v_a, v_b \rangle|^2 = p^2,
\]
and for all \( a \in [r] \),
\[
|\langle v_a, v_{(a,a+1)} \rangle|^2 = \frac{1 + p}{2}.
\]
Furthermore, any such correlation matrix with \( 0 < p < \frac{1}{r} \) is not \( r \)-decomposable.

**Proof:** We first prove the existence of such a correlation matrix. The correlation matrix generated by the set of unit vectors
\[
\left\{ v_1, \ldots, v_{r+1}, \frac{1}{\sqrt{2(1+p)}}(v_1 + v_2), \ldots, \frac{1}{\sqrt{2(1+p)}}(v_r + v_{r+1}) \right\},
\]
with \( \langle v_a, v_b \rangle = p \) for all \( a \neq b \in [r+1] \), satisfies the desired conditions. Indeed,
\[
\begin{align*}
\left\langle v_a, \frac{1}{\sqrt{2(1+p)}}(v_a + v_{a+1}) \right\rangle &= \frac{1}{\sqrt{2(1+p)}}(1+p) \\
&= \sqrt{\frac{1+p}{2}},
\end{align*}
\]
and similarly,
\[
\begin{align*}
\left\langle v_{a+1}, \frac{1}{\sqrt{2(1+p)}}(v_a + v_{a+1}) \right\rangle &= \sqrt{\frac{1+p}{2}}.
\end{align*}
\]

Now we prove that any such correlation matrix with \(0 < p < \frac{1}{r}\) is not \(r\)-decomposable. For \(r = 1\), the statement follows easily from the fact that the Schur product of any two rank-one correlation matrices is again rank one (see the proof of Lemma 5.5), and that for all \(0 < p < 1\), any correlation matrix satisfying the conditions of the proposition has rank \(\geq 2\).

Assume \(r \geq 2\). It is clear that \(|\langle v_a, v_{a+2} \rangle| > |\langle v_a, v_{a+1} \rangle| \cdot |\langle v_{a+1}, v_{a+2} \rangle|\) for all \(a \in [r-2]\). Thus, by the proof of Theorem 4.3 it suffices to show that the vectors \(\{v_1, \ldots, v_{r+1}\}\) are linearly independent, and that for all \(a \in [r]\) it holds that \(v_{(a,a+1)} = \alpha_a v_a + \beta_{a+1} v_{a+1}\) for some non-zero scalars \(\alpha_a, \beta_{a+1} \in \mathbb{C} \setminus \{0\}\).

First, by Gershgorin’s circle theorem [23], the condition that \(|\langle v_a, v_b \rangle|^2 = p^2\) for all \(a \neq b \in [r+1]\), along with \(0 < p < \frac{1}{r}\), implies that the vectors \(\{v_1, \ldots, v_{r+1}\}\) are linearly independent. Second, for each \(a \in [r]\) the principal submatrix of \(P\) generated by the vectors \(\{v_a, v_{a+1}, v_{(a,a+1)}\}\) is of the form
\[
P_{(a,a+1)} = \begin{pmatrix}
1 & e^{i\phi_1}p & e^{i\phi_2} \sqrt{\frac{1+p}{2}} \\
e^{-i\phi_1}p & 1 & e^{i\phi_3} \sqrt{\frac{1+p}{2}} \\
e^{i\phi_2} \sqrt{\frac{1+p}{2}} & e^{-i\phi_3} \sqrt{\frac{1+p}{2}} & 1
\end{pmatrix}
\]
for some \(\phi_1, \phi_2, \phi_3 \in [0, 2\pi]\). Note that
\[
\text{Det}(P_{(a,a+1)}) = p(1+p)(-1 + \cos(\phi_1 - \phi_2 + \phi_3)) \leq 0,
\]
and since \(P_{(a,a+1)}\) is positive semidefinite,
\[
\text{Det}(P_{(a,a+1)}) = 0.
\]
This implies that \(P_{(a,a+1)}\) has rank one or two. We can deduce \(\text{rank}(P_{(a,a+1)}) \neq 1\) because \(v_a\) and \(v_{a+1}\) are linearly independent. Thus, \(\text{rank}(P_{(a,a+1)}) = 2\), which implies...
\[ v_{(a,a+1)} = \alpha_a v_a + \beta_{a+1} v_{a+1} \] for some scalars \( \alpha_a, \beta_{a+1} \in \mathbb{C} \), both of which must be non-zero because no entry in \( P^{(a,a+1)} \) has unit magnitude.

**Acknowledgments**

I thank Norbert Lütkenhaus for first proposing this research topic, and for many helpful discussions. I thank John Watrous for helpful discussions and comments on drafts of this manuscript. I thank Chi-Kwong Li, Ashutosh Marwah, and Daniel Puzzuoli for helpful discussions.

**Disclosure statement**

No potential conflict of interest was reported by the author.

**References**

[1] Devetak I, Shor P. The capacity of a quantum channel for simultaneous transmission of classical and quantum information. Commun Math Phys. 2005;256(2):287–303.
[2] Cleve R, Slofstra W, Unger F, et al. Perfect parallel repetition theorem for quantum XOR proof systems. Comput Complex. 2008;17(2):282–299.
[3] K Brádler, P Hayden, D Touchette, et al. Trade-off capacities of the quantum Hadamard channels. Phys Rev A. 2010;81:062312.
[4] Haagerup U, Musat M. Factorization and dilation problems for completely positive maps on von Neumann algebras. Commun Math Phys. 2011;303(2):555–594.
[5] Winter A, Yang D. Potential capacities of quantum channels. IEEE Trans Inf Theory. 2016;62(3):1415–1424.
[6] Yu N, Duan R, Xu Q. Bounds on the distance between a unital quantum channel and the convex hull of unitary channels. IEEE Trans Inf Theory. 2017;63(2):1299–1310.
[7] Tsirelson B. Quantum analogues of the Bell inequalities. The case of two spatially separated domains. J Sov Math. 1987;36(4):557–570.
[8] Chefles A, Jozsa R, Winter A. On the existence of physical transformations between sets of quantum states. Int J Quantum Inf. 2004;2(01):11–21.
[9] Huang Z, Li CK, Poon E, et al. Physical transformations between quantum states. J Math Phys. 2012;53(10):102209.
[10] Marwah AS, Lütkenhaus N. Characterization of gram matrices of multimode coherent states. Phys Rev A. 2019;99:012346.
[11] Born M, Wolf E. Principles of optics: electromagnetic theory of propagation, interference and diffraction of light. Elmsford (New York): Elsevier; 2013.
[12] Buhrman H, Cleve R, Watrous J, et al. Quantum fingerprinting. Phys Rev Lett. 2001;87(16):167902.
[13] Buhrman H, Cleve R, Wigderson A. Quantum vs. classical communication and computation. In: Proceedings of the thirtieth annual ACM symposium on theory of computing. New York, NY: ACM; 1998. p. 63–68; STOC ’98.
[14] Arrazola JM, Lütkenhaus N. Quantum fingerprinting with coherent states and a constant mean number of photons. Phys Rev A. 2014;89:062305.
[15] Lovitz B, Lütkenhaus N. Families of quantum fingerprinting protocols. Phys Rev A. 2018;97:032340.
[16] Touchette D, Lovitz B, Lütkenhaus N. Practical quantum appointment scheduling. Phys Rev A. 2018;97:042320.
[17] Westwick R. Transformations on tensor spaces. Pac J Math. 1967;23(3):613–620.
[18] Johnston N. Characterizing operations preserving separability measures via linear preserver problems. Linear Multilinear Algebra. 2011;59(10):1171–1187.
[19] Lovitz B. Toward an analog of Kruskal’s theorem on tensor decomposition. arXiv preprint. 2018;math.CO/1812.00264.
[20] Rockafellar RT. Convex analysis. Princeton (New Jersey): Princeton University Press; 2015.
[21] Li CK, Tam BS. A note on extreme correlation matrices. SIAM J Matrix Anal Appl. 1994;15(3):903–908.
[22] Oxley J. Matroid theory. Oxford, England: Oxford University Press; 2006.
[23] Horn R, Johnson C. Matrix analysis. New York (New York): Cambridge University Press; 2013.