THE PPT^2 CONJECTURE HOLDS FOR ALL CHOI-TYPE MAPS

SATVIK SINGH AND ION NECHITA

In the rapidly developing field of Quantum technologies, the task of entanglement distribution between two parties occupies a central stage in many important protocols [BBC$^+$93, Eke91]. However, as the distance between the two parties increases, the error probability in any transmission channel gets larger, resulting in degradation of the quality of the distributed entanglement. To overcome this problem, quantum repeater devices are used [BDCZ98]. The basic idea of such a device is to split up the long transmission channel into shorter manageable segments, each of which can be supplied with high fidelity entangled states. Then, the well-known entanglement swapping technique [ZZHE93] can be used to transfer the entanglement from the intermediate segments to the ends of the transmission channel. A key conjecture in this regard was proposed by M. Christandl [Chr12], which states that all PPT (positive under partial transposition) entangled states are useless from the perspective of repeater devices, since the swapping of entanglement in such states inevitably leads to a separable (non-entangled) state. This conjecture has profound implications in the realm of quantum cryptography, where it implies that although PPT states can be employed to distill secret key between two parties in a bipartite setting [HHHO05], the same cannot be done using PPT states in a repeater scenario [BCHW15, CF17]. The conjecture admits an equivalent formulation in terms of linear maps between matrix algebras, where it amounts to saying that the composition of any two PPT maps (these are the maps which are both completely positive and completely copositive) is entanglement breaking.

Conjecture 1. [Chr12] *The composition of two arbitrary* PPT *maps is entanglement breaking.*

In the present submission, our primary contribution is a proof of the PPT^2 conjecture for linear maps between matrix algebras which are (conjugate) *covariant* under the action of the diagonal unitary group. This class of maps is quite rich and includes many notable names like the Choi-type maps, Schur multipliers, classical channels, etc. The ingredients required in the proof are developed in three papers, which appeared in the following chronological order[1]:

(1) Diagonal unitary and orthogonal symmetries in quantum theory [SN20a]
(2) Can entanglement hide behind triangle-free graphs? [Sin20]
(3) The PPT^2 conjecture holds for all Choi-type maps [SN20b]

In [SN20a], we present the general theory of bipartite matrices and linear maps between matrix algebras which are respectively, *invariant* and *covariant*, under the *diagonal unitary* and *orthogonal* groups' actions. Notably, we show that the separability of such bipartite matrices (or the entanglement breaking property of the corresponding covariant maps) admits an equivalent description in terms of the cones of *pairwise* and *triplewise completely positive* matrices, which generalize the well-studied cone of completely positive matrices from combinatorics and optimization theory [BSM03]. Building upon this link, a novel graph theoretic protocol is devised in [Sin20] to detect and construct a new kind of entanglement in bipartite quantum states, which dwells in peculiar *"triangle-free"* distribution of zeros on the states' diagonals. Finally, the ideas used in [Sin20] are more concretely formalized in [SN20b], using a generalization of the matrix-theoretic notion of factor width for pairwise and triplewise completely positive matrices, which turns out to be instrumental in the final proof of the PPT^2 conjecture for the aforementioned class of maps. Hence, in a nutshell, our work proves the unsuitability of a large class of states (corresponding to the diagonal unitary covariant maps) from the perspective of repeater protocols and hence provides significant contribution to the solution of a long-standing open problem in quantum information theory.

1. Diagonal unitary and orthogonal symmetries in quantum theory

Let us describe in more detail the classes of quantum states and channels that we consider. The key insight of our work is to analyze the symmetry induced by the *diagonal unitary* (resp. *orthogonal*) groups, denoted

[1] S. Singh was the main contributor for all the papers, and the sole author of [Sin20]

by $\mathcal{DU}_d$, resp. $\mathcal{DO}_d$. We investigate this symmetry in the realm of bipartite matrices and linear maps between matrix algebras; the equivalence between the two scenarios is given by the Choi-Jamiołkowski isomorphism.

There are three different such classes of matrices and maps, corresponding respectively, to the action of $\mathcal{DU}_d$, the conjugate action of $\mathcal{DU}_d$, and the action of $\mathcal{DO}_d$. We introduce them in the following table, with bipartite matrices and linear maps being segregated to the left and the right, respectively.

Local Diagonal Unitary Invariant (LDUI) $(U \otimes U)X(U^* \otimes U^*) = X \quad \forall U \in \mathcal{DU}_d$	*Diagonal Unitary Covariant (DUC)* $\Phi(U\rho U^*) = U^*\Phi(\rho)U \quad \forall U \in \mathcal{DU}_d$
Conjugate Local Diagonal Unitary Inv. (CLDUI) $(U \otimes U^*)X(U^* \otimes U) = X \quad \forall U \in \mathcal{DU}_d$	*Conjugate Diagonal Unitary Covariant (CDUC)* $\Phi(U\rho U^*) = U\Phi(\rho)U^* \quad \forall U \in \mathcal{DU}_d$
Local Diagonal Orthogonal Invariant (LDOI) $(O \otimes O)X(O \otimes O) = X \quad \forall O \in \mathcal{DO}_d$	*Diagonal Orthogonal Covariant (DOC)* $\Phi(O\rho O) = O\Phi(\rho)O \quad \forall O \in \mathcal{DO}_d$

Notably, we can identify the relevant parametrizations for the objects in each class. For example, CDUC maps are parametrized by a pair of matrices $A, B \in \mathcal{M}_d(\mathbb{C})$ having the same diagonal $\operatorname{diag} A = \operatorname{diag} B$:

$$\Phi_{(A,B)}(\rho) = \operatorname{diag}(A\,|\operatorname{diag}\rho\rangle) + \widetilde{B} \odot \rho,$$

where $\widetilde{B} = B - \operatorname{diag} B$, and $\odot$ denotes the Hadamard product.

We have identified in the literature a plethora of examples of such states and maps, showcasing the fact that the set of diagonal symmetric objects is very rich and significant for quantum information theory. The set of bipartite matrices that we consider contains diagonal states, Werner states [Wer89], isotropic states [HH99], states which are diagonal in the Dicke basis of the symmetric subspace [Yu16, TAQ+18], canonical NPT states [DSS+00], and $\mathbb{C}^3 \otimes \mathbb{C}^3$ edge states [KO12]. Diagonal symmetric linear maps include the identity channel, the transposition, classical channels, Schur multipliers, the Choi map and its many generalizations [Cho75, CMR18], diagonal-preserving maps [Kye95, LW97], and maps related to the characterization of stable subspaces of extremal bistochastic maps [MO15, RSC15].

We provide a complete toolkit to study the above classes of matrices and maps, which allows one to uniformly explore a plethora of relevant questions about a large class of important quantum states and channels.

Theorem 2. *Consider two matrices $A, B \in \mathcal{M}_d(\mathbb{C})$ having the same diagonal. Then, the following statements hold for a CLDUI bipartite matrix X and for the CDUC linear map Φ corresponding to the pair (A, B):*

1. *X is positive semi-definite $\iff$ Φ is completely positive $\iff$ $A \succcurlyeq 0$ and $B \geq 0$*
2. *X^Γ is positive semidefinite $\iff$ Φ is completely copositive $\iff$ $A \succcurlyeq 0, B = B^*, A_{ij}A_{ji} \geq |B_{ij}|^2\ \forall i, j$*
3. *X is PPT $\iff$ the map Φ is PPT $\iff$ $A \succcurlyeq 0$, $B \geq 0$, and $A_{ij}A_{ji} \geq |B_{ij}|^2\ \forall i, j$.*
4. *X is separable $\iff$ Φ is entanglement breaking $\iff$ (A, B) is pairwise completely positive.*

where $A \succcurlyeq 0$ and $B \geq 0$ denote that A is entrywise non-negative and B is positive semi-definite, respectively.

Notice that in the above theorem, the notion of *pairwise completely positivity* [JM19] (as well as its generalization to triples that we introduced) is related to the separability problem; we provide some basic facts about these notions, and study in detail their convex structure. To be precise, given matrices $A, B, C \in \mathcal{M}_d(\mathbb{C})$ with equal diagonals, we say that (A, B) (resp. (A, B, C)) is pairwise completely positive (PCP) (resp. triplewise completely positive (TCP)) if there exist vectors $\{|v_n\rangle, |w_n\rangle\}_{n\in I} \subset \mathbb{C}^d$ (for a finite index set I) such that

$$A = \sum_{n\in I} |v_n \odot \overline{v_n}\rangle\langle w_n \odot \overline{w_n}| \qquad B = \sum_{n\in I} |v_n \odot w_n\rangle\langle v_n \odot w_n|\,.$$

$$\text{resp. } A = \sum_{n\in I} |v_n \odot \overline{v_n}\rangle\langle w_n \odot \overline{w_n}| \qquad B = \sum_{n\in I} |v_n \odot w_n\rangle\langle v_n \odot w_n| \qquad C = \sum_{n\in I} |v_n \odot \overline{w_n}\rangle\langle v_n \odot \overline{w_n}|\,.$$

The well-studied cone of completely positive matrices [BSM03] from combinatorics and optimization theory corresponds to the $A = B = C$ case in the above decompositions.

2. Can entanglement hide behind triangle-free graphs?

We now proceed to briefly describe the ideas used in [Sin20] to establish a link between the entanglement of a bipartite quantum state and the zero-pattern of its diagonal. Given an arbitrary state $\rho \in \mathcal{M}_d(\mathbb{C}) \otimes \mathcal{M}_d(\mathbb{C})$, we define matrices $A, B, C \in \mathcal{M}_d(\mathbb{C})$ entrywise as $A_{ij} = \langle ij|\rho|ij\rangle$, $B_{ij} = \langle ii|\rho|jj\rangle$, and $C_{ij} = \langle ij|\rho|ji\rangle$. A d-vertex graph $G(A)$ can then be associated to A in such a way that for $i \neq j$, $\{i, j\}$ forms an edge in $G(A)$ if both A_{ij}

and A_{ji} are non-zero. We say that ρ is Δ*-free* if $G(A)$ does not contain any triangles. From this definition, it is clear that the Δ-freeness of a state is nothing but a restriction on the zero-pattern of the state's diagonal. Now, by locally projecting ρ into the LDOI subspace: $\rho \mapsto \mathbb{E}_O[(O \otimes O)\rho(O \otimes O)] = \rho_{A,B,C}$, we see that the Δ-free property forces any set of vectors $\{|v_n\rangle, |w_n\rangle\}_{n\in I} \subset \mathbb{C}^d$ forming the TCP decomposition of (A, B, C) (if it exists at all) to have small common support, i.e. $\sigma(v_n \odot w_n) \leq 2$ for each $n \in I$, where $\sigma(v)$ denotes the size of the support of $|v\rangle \in \mathbb{C}^d$. This leads us to a non-trivial necessary condition for the separability of ρ in terms of positivity of the associated comparison matrices $M(B)$ and $M(C)$ [Sin20, Theorem III.2], which can easily be exploited to devise a simple entanglement detection strategy in bipartite states (recall that for $Z \in \mathcal{M}_d(\mathbb{C})$, its comparison matrix $M(Z)$ is defined entrywise as $M(Z)_{ij} = |Z_{ij}|$ for $i = j$ and $M(Z)_{ij} = -|Z_{ij}|$ otherwise).

Theorem 3. *Let ρ be an arbitrary $d \otimes d$ Δ-free state with the associated matrices A, B, C defined as above. Then, ρ is entangled if either $M(B)$ or $M(C)$ is not positive semi-definite.*

Since the conditions stated in the above theorem are very easy to verify in practice (efficient classical algorithms exist to check both the Δ-freeness of a graph and the positivity of a given matrix), one can deduce that Theorem 3 provides a highly non-trivial yet computationally efficient entanglement test. As the number of Δ-free zero patterns increases rather tremendously with the system's dimensions, so does the number of Δ-free entangled families of states. For instance, using the protocol presented in [Sin20, Section IV], one can construct $\sim 10^{10}$ distinct families of PPT-entangled Δ-free states in a paltry $15 \otimes 15$ system.

3. The PPT^2 conjecture holds for all Choi-type maps

In [SN20b], we formalize the idea of PCP/TCP decompositions of matrix pairs/triples having small common supports by introducing the notion of *factor width*. A PCP (resp. TCP) matrix pair (A, B) (resp. triple (A, B, C)) is said to have *factor width* k if it admits a PCP (resp. TCP) decomposition with vectors $\{|v_n\rangle, |w_n\rangle\}_{n\in I} \subset \mathbb{C}^d$ such that $\sigma(v_n \odot w_n) \leq k$ for each $n \in I$. In this terminology, the results of the previous section can be seen to revolve around the properties of PCP/TCP matrices with factor width 2. The primary technical tool required in our proof of the PPT^2 conjecture for (C)DUC maps relies on the following necessary and sufficient condition for matrix pairs (A, B) to be PCP with factor width 2 [SN20b, Theorem 3.10].

Theorem 4. *Let $A, B \in \mathcal{M}_d(\mathbb{C})$ have equal diagonals such that A is entrywise positive, B is positive semi-definite and $A_{ij}A_{ji} \geq |B_{ij}|^2 \; \forall i, j$. Then, (A, B) is* PCP *with factor width 2 $\iff$ $M(B)$ is positive semi-definite.*

It can be shown that the above characterization ceases to hold for TCP matrices due to the added complexity of the third matrix [SN20a, Example 9.2]. Having equipped ourselves with all the necessary machinery, we now present an outline of our proof of the PPT^2 conjecture for (C)DUC maps. Using elementary algebra, one can deduce that the composition of two arbitrary PPT (C)DUC maps with the associated matrix pairs $(A_1, B_1), (A_2, B_2)$ yields another PPT (C)DUC map, which has either one of the following two associated matrix pairs: $(\mathfrak{A}, \mathfrak{B}) = (A_1A_2, B_1 \odot B_2^\top + \text{diag}(A_1A_2 - B_1 \odot B_2))$ or $(\mathfrak{A}', \mathfrak{B}') = (A_1A_2, B_1 \odot B_2 + \text{diag}(A_1A_2 - B_1 \odot B_2))$. The strategy then is to use Theorem 4 to show that both $(\mathfrak{A}, \mathfrak{B})$ and $(\mathfrak{A}', \mathfrak{B}')$ are PCP with factor width 2, which implies that the composition is entanglement breaking (see Theorem 2), thus completing the proof.

Theorem 5. *The composition of two arbitrary PPT (C)DUC maps corresponds to a* PCP *matrix pair with factor width 2; in particular, it is entanglement breaking.*

It should be noted that Theorem 5 contains a *stronger* version of the PPT^2 conjecture for (C)DUC maps, since the cone of all PCP matrices is a strict superset of the cone of PCP matrices with factor width 2. Finally, we expect that the resolution of the PPT^2 conjecture for DOC maps will require stronger separability criteria for the associated Choi matrices, in terms of sufficient conditions for membership in PCP/TCP cones.

In conclusion, we would like to emphasize the diversity of the various realms of physics and mathematics that are spanned by our research. First of all, the core subject lies in the area of *quantum information theory*, pertaining more precisely to entanglement theory. The different classes of invariant bipartite states and covariant linear maps that we study are formulated in the framework of *multi-linear algebra*. *Convexity theory* plays a crucial role in our study because of the focus given to the cones of positive semidefinite, PPT, and separable invariant matrices, which are shown to admit equivalent descriptions in terms of certain associated cones of matrix pairs/triples. The study of Δ-free entanglement borrows crucial concepts from *graph theory*. Finally, the investigations into the notion of factor width entails the use of important techniques from *matrix analysis*, particularly from the *Perron-Frobenious theory* of non-negative matrices.

References

[BBC+93] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Phys. Rev. Lett.*, 70:1895–1899, Mar 1993. 1

[BCHW15] Stefan Bäuml, Matthias Christandl, Karol Horodecki, and Andreas Winter. Limitations on quantum key repeaters. *Nature communications*, 6(1):1–5, 2015. 1

[BDCZ98] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller. Quantum repeaters: The role of imperfect local operations in quantum communication. *Phys. Rev. Lett.*, 81:5932–5935, Dec 1998. 1

[BSM03] Abraham Berman and Naomi Shaked-Monderer. *Completely positive matrices.* World Scientific, 2003. 1, 2

[CF17] Matthias Christandl and Roberto Ferrara. Private states, quantum data hiding, and the swapping of perfect secrecy. *Physical review letters*, 119(22):220506, 2017. 1

[Cho75] Man-Duen Choi. Positive semidefinite biquadratic forms. *Linear Algebra and its Applications*, 12(2):95 – 100, 1975. 2

[Chr12] M. Christandl. PPT square conjecture. *Banff International Research Station Workshop:* Operator Structures in Quantum Information Theory, 2012. 1

[CMR18] Dariusz Chruscinski, Marcin Marciniak, and Adam Rutkowski. Generalizing Choi-like maps. *Acta Mathematica Vietnamica*, 43:661–674, 2018. 2

[DSS+00] David P. DiVincenzo, Peter W. Shor, John A. Smolin, Barbara M. Terhal, and Ashish V. Thapliyal. Evidence for bound entangled states with negative partial transpose. *Phys. Rev. A*, 61:062312, May 2000. 2

[Eke91] Artur K. Ekert. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.*, 67:661–663, Aug 1991. 1

[HH99] Michał Horodecki and Paweł Horodecki. Reduction criterion of separability and limits for a class of distillation protocols. *Phys. Rev. A*, 59:4206–4216, Jun 1999. 2

[HHHO05] Karol Horodecki, Michał Horodecki, Paweł Horodecki, and Jonathan Oppenheim. Secure key from bound entanglement. *Phys. Rev. Lett.*, 94:160502, Apr 2005. 1

[JM19] Nathaniel Johnston and Olivia MacLean. Pairwise completely positive matrices and conjugate local diagonal unitary invariant quantum states. *Electronic Journal of Linear Algebra*, 35:156–180, 2019. 2

[KO12] Seung-Hyeok Kye and Hiroyuki Osaka. Classification of bi-qutrit positive partial transpose entangled edge states by their ranks. *Journal of Mathematical Physics*, 53(5):052201, 2012. 2

[Kye95] Seung-Hyeok Kye. Positive linear maps between matrix algebras which fix diagonals. *Linear Algebra and its Applications*, 216:239 – 256, 1995. 2

[LW97] Chi-Kwong Li and Hugo J. Woerdeman. Special classes of positive and completely positive maps. *Linear Algebra and its Applications*, 255(1):247 – 258, 1997. 2

[MO15] Marek Miller and Robert Olkiewicz. Stable subspaces of positive maps of matrix algebras. *Open Systems & Information Dynamics*, 22(02):1550011, 2015. 2

[RSC15] Adam Rutkowski, Gniewomir Sarbicki, and Dariusz Chruściński. A class of bistochastic positive optimal maps in $M_d(\mathbb{C})$. *Open Systems & Information Dynamics*, 22(03):1550016, 2015. 2

[Sin20] Satvik Singh. Can entanglement hide behind triangle-free graphs? *preprint arXiv:2010.11891*, 2020. 1, 2, 3

[SN20a] Satvik Singh and Ion Nechita. Diagonal unitary and orthogonal symmetries in quantum theory. *preprint arXiv:2010.07898*, 2020. 1, 3

[SN20b] Satvik Singh and Ion Nechita. The PPT^2 conjecture holds for all choi-type maps. *preprint arXiv:2011.03809*, 2020. 1, 3

[TAQ+18] Jordi Tura, Albert Aloy, Ruben Quesada, Maciej Lewenstein, and Anna Sanpera. Separability of diagonal symmetric states: a quadratic conic optimization problem. *Quantum*, 2:45, 2018. 2

[Wer89] Reinhard F. Werner. Quantum states with einstein-podolsky-rosen correlations admitting a hidden-variable model. *Phys. Rev. A*, 40:4277–4281, Oct 1989. 2

[Yu16] Nengkun Yu. Separability of a mixture of dicke states. *Physical Review A*, 94(6):060101, 2016. 2

[ZZHE93] M. Zukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert. "event-ready-detectors" bell experiment via entanglement swapping. *Phys. Rev. Lett.*, 71:4287–4290, Dec 1993. 1