LA-UR-02-1333
Approved for public release;
distribution is unlimited.

Title: **Quantum Matching Theory (with new complexity-theoretic, combinatorial and topological insights on the nature of the Quantum Entanglement)**

Author(s): Leonid Gurvits

Submitted to:

Quantum Matching Theory (with new complexity-theoretic , combinatorial and topological insights on the nature of the Quantum Entanglement)

Leonid Gurvits
Los Alamos National Laboratory
Los Alamos, NM 87545
email: gurvits@lanl.gov

Abstract

Classical matching theory can be defined in terms of matrices with nonnegative entries. The notion of Positive operator , central in Quantum Theory , is a natural generalization of matrices with nonnegative entries. Based on this point of view , we introduce a definition of perfect Quantum (operator) matching . We show that the new notion inherits many "classical" properties , but not all of them . This new notion goes somewhere beyound matroids . For separable bipartite quantum states this new notion coinsides with the full rank property of the intersection of two corresponding geometric matroids . In the classical situation , permanents are naturally associated with perfects matchings. We introduce an analog of permanents for positive operators, called Quantum Permanent and show how this generalization of the permanent is related to the Quantum Entanglement. Besides many other things , Quantum Permanents provide new rational inequalities necessary for the separability of bipartite quantum states . Using Quantum Permanents , we give deterministic poly-time algorithm to solve Hidden Matroids Intersection Problem and indicate some "classical" complexity difficulties associated with the Quantum Entanglement. Finally , we prove that the weak membership problem for the convex set of separable bipartite density matrices is NP-HARD.

1 Introduction and Main Definitions

The (classical) Matching Theory is an important , well studied but still very active part of the Graph Theory (Combinatorics) . The Quantum Entanglement is one of the central topics in Quantum Information Theory . We quote from [31] : "An understanding of entanglement seems to be at the heart of theories of quantum computations and quantum cryptography , as it has been at the heart of quantum mechanics itself . "
We would like to stress that our paper does not contain explicit connections to Quantum Computing (though they might arise sooner or later) . It rather aims to study the Quantum Entanglement from the point of view of classical computational complexity and computational geometry and to use some ideas/structures from Quantum Information Theory to construct and analyse classical algorithms.
We will introduce in this paper a Quantum generalization of the Matching Theory and will show that this generalization gives new and surprising insights on the nature of the Quantum Entanglement . Of course , there already exist several "bipartite" generalizations of (classical) bipartite matching theory . The most relevant to our paper is the Theory of Matroids , namely its part analyzing properties of intersections of two geometric matroids .

Definition 1.1: Intersection of two geometric matroids $MI(X,Y) = \{(x_i, y_i), 1 \leq i \leq K\}$ is a finite family of distinct 2-tuples of nonzero N-dimensional complex vectors , i.e. $x_i, y_i \in C^N$.
The rank of $MI(X,Y)$ is the largest integer m such that there exist $1 \leq i_1 < ... < i_m \leq K$ with both sets $\{x_{i_1}, ..., x_{i_m}\}$ and $\{y_{i_1}, ..., y_{i_m}\}$ being linearly independent. If $Rank(MI(X,Y))$ is equal to N then $MI(X,Y)$ is called matching . The matroidal permanent $MP_{(X,Y)}$ is defined as follows :

$$MP_{(X,Y)} =: \sum_{1 \leq i_1 < i_2 < ... < i_N \leq K} \det(\sum_{1 \leq k \leq N} x_{i_k} x_{i_k}^\dagger) \det(\sum_{1 \leq k \leq N} y_{i_k} y_{i_k}^\dagger) \quad (1)$$

∎

Remark 1.2: Let us denote linear space (over complex numbers) of $N \times N$ complex matrices as $M(N)$. It is clear from this definition that $MI(X,Y)$ is matching iff $MP_{(X,Y)} > 0$. Moreover , $MI(X,Y)$ is matching iff the linear subspace $Lin(X,Y) \subset M(N)$ generated by the matrices $\{x_i y_i^\dagger, 1 \leq i \leq K\}$ contains a nonsingular matrix and , in general , $Rank(MI(X,Y))$ is equal to the maximal matrix rank achieved in $Lin(X,Y)$. The following equality generalizes Barvinok's ([10]) unbiased estimator for mixed discriminants :

$$MP_{(X,Y)} = E(|\det(\sum_{1 \leq i \leq K} \xi_i x_i y_i^\dagger)|^2) \quad (2)$$

where $\{\xi_i, 1 \leq i \leq K\}$ are zero mean independent (or even $2N$-wise independent) complex valued random variables such that $E(|\xi_i|^2 = 1, 1 \leq i \leq K$. It is not clear whether the analysis from [9] can be applied to $MP_{(X,Y)}$. ∎

Example 1.3: Suppose that $x_i \in \{e_1, ..., e_N\}, 1 \leq i \leq K$, where $\{e_1, ..., e_N\}$ is a standard basis in C^N. Define the following positive semidefinite $N \times N$ matrices :

$$Q_i = \sum_{(e_i, y_j) \in (X,Y)} y_j y_j^\dagger, 1 \leq i \leq N.$$

Then it is easy to see that in this case matroidal permanent coinsides with the mixed discriminant , i.e. $MP_{(X,Y)} = M(Q_1, \cdots, Q_N)$ where the mixed discriminant defined as follows :

$$M(Q_1, ...Q_N) = \frac{\partial^n}{\partial x_1 ... \partial x_n} \det(x_1 Q_1 + ... + x_N Q_N). \quad (3)$$

We will also use the following equivalent definition :

$$M(Q_1,...Q_N) = \sum_{\sigma,\tau \in S_N} (-1)^{sign(\sigma\tau)} \prod_{i=1}^{N} Q_i(\sigma(i),\tau(i)), \quad (4)$$

where S_n is the symmetric group, i.e. the group of all permutations of the set $\{1,2,\cdots,N\}$. If matrices $Q_i, 1 \leq i \leq N$ are diagonal then their mixed discriminant is equal to the corresponding permanent ([30]). ∎

Let us pose , before moving to Quantum generalizations , the following "classical" desision problem . We will call it Hidden Matroids Intersection Problem (**HMIP**) :

Problem 1.4: Given linear subspace $L \subset M(N)$ and a promise that L has a (hidden) basis consisting of rank one matrices. Is there exists poly-time deterministic algorithm to decide whether L contains a nonsingular matrix ? Or more generally , to compute maximum matrix rank achieved in L ? ∎

Below in the paper we will assume that linear subspace $L \subset M(N)$ in (**HMIP**) is given as a some rational basis in it. If this basis consists of rank one matrices then there is nothing "hidden" and one can just apply standard poly-time deterministic algorithm computing rank of intersection of two matroids. A natural (trivial) way to attack (**HMIP**) would be to exract a (hidden) basis consisting of rank one matrices. We are not aware about the complexity of this extraction . The following example shows that there exist linear subspaces $L \subset M(N)$ having a rational real basis and a "rank one" basis but without rational "rank one" basis :
Consider the following 2×2 matrix

$$A = \begin{pmatrix} 0 & -2 \\ 1 & 0 \end{pmatrix},$$

and define linear subspace $IR \subset M(2)$ generated by A and the identity I .
It is easy to see that
$Rank(bA + aI) \leq 1$ iff $a^2 + 2b^2 = 0$.
Therefore there are no rank one rational (complex) matrices in IR . From the other hand rank one matrices

$$C = \sqrt{2}I + iA, D = \sqrt{2}I - iA$$

form a basis in IR .
One of the main results of our paper is a positive answer to the nonsingularity part of (**HMIP**) . Moreover our algorithm is rather simple and does not require to work with algebraic numbers .
And , of course , we are aware about randomized poly-time algorithms , based on Scwartz's lemma , to solve this part of (**HMIP**) . But for general linear subspaces , i.e. without extra promise , poly-time deterministic algorithms are not known and the problem is believed to be "HARD" . To move to Quantum generalization , we need to recall several , standard in Quantum Information literature , notions .

1.1 Positive and completely positive operators ; bipartite density matrices and Quantum Entanglement

Definition 1.5: A positive semidefinite matrix $\rho_{A,B} : C^N \otimes C^N \to C^N \otimes C^N$ is called bipartite unnormalized density matrix (**BUDM**) , if $tr(\rho_{A,B}) = 1$ then this $\rho_{A,B}$ is called bipartite density matrix .
It is convinient to represent bipartite $\rho_{A,B} = \rho(i_1,i_2,j_1,j_2)$ as the following block matrix :

$$\rho_{A,B} = \begin{pmatrix} A_{1,1} & A_{1,2} & \dots & A_{1,N} \\ A_{2,1} & A_{2,2} & \dots & A_{2,N} \\ \dots & \dots & \dots & \dots \\ A_{N,1} & A_{N,2} & \dots & A_{N,N} \end{pmatrix}, \quad (5)$$

where $A_{i_1,j_1} =: \{\rho(i_1,i_2,j_1,j_2) : 1 \leq i_2,j_2 \leq N\}, 1 \leq i_1,j_1 \leq N$.
A (**BUDM**) ρ called **separable** if

$$\rho = \rho_{(X,Y)} =: \sum_{1 \leq i \leq K} x_i x_i^\dagger \otimes y_i y_i^\dagger, \quad (6)$$

and **entangled** otherwise .
If vectors $x_i, y_i; 1 \leq i \leq K$ in (6) are real then ρ is called **real separable** .
Quantum marginals defined as $\rho_A = \sum_{1 \leq i \leq N} A_{i,i}$ and $\rho_B(i,j) = tr(A_{i,j}); 1 \leq i,j \leq N$.

We will call (**BUDM**) ρ weakly separable if there exists a separable $\rho'_{(X,Y)}$ with the same Image as $\rho : Im(\rho) = Im(\rho'_{(X,Y)})$.
(Recall that in this finite dimensional case $Im(\rho)$ is a linear subspace formed by all linear combinations of columns of matrix ρ .)
A linear operator $T : M(N) \to M(N)$ called positive if $T(X) \succeq 0$ for all $X \succeq 0$, and strictly positive if $T(X) \succeq \alpha tr(X) I$ for all $X \succeq 0$ and some $\alpha > 0$. A positive operator T is called completely positive if

$$T(X) = \sum_{1 \leq i \leq N^2} A_i X A_i^\dagger; A_i, X \in M(N) \quad (7)$$

Choi's representation of linear operator $T : M(N) \to M(N)$ is a block matrix $CH(T)_{i,j} =: T(e_i e_j^\dagger)$. Dual to T respect to the inner product $< X,Y >= tr(XY^\dagger)$ is denoted as T^*. Very usefull and easy Choi's result states that T is completely positive iff $CH(T)$ is (**BUDM**) . Using this natural (linear) correspondence between completely positive operators and (**BUDM**) , we will freely "transfer" properties of (**BUDM**) to completely positive operators . For example , a linear operator T is called separable iff $CH(T)$ is separable , i.e.

$$T(Z) = T_{(X,Y)}(Z) = \sum_{1 \leq i \leq K} x_i y_i^\dagger Z y_i x_i^\dagger \quad (8)$$

Notice that $CH(T_{(X,Y)}) = \rho_{(\bar{Y},X)}$ and $T^*_{(X,Y)} = T_{(Y,X)}$.
(Components of vector $\bar{y}$ are complex conjugates of corresponding components of y) . ∎

Remark 1.6: In light of definition (1.5) , we will represent linear subspaces $L \subset M(N) \cong C^N \otimes C^N$ in (**HMIP**) as images of weakly separable (**BUDM**) ρ . And as the complexity measure we will use the number of bits of (rational) entries of ρ. ∎

The next definition introduces the quantum permanent $QP(\rho)$, the main tool to solve (**HMIP**) . Though it was not our original intention , it happened that $QP(\rho_{(X,Y)}) = MP_{(X,Y)}$.

Definition 1.7: We define quantum permanent, $QP(\rho)$, by the following equivalent formulas :

$$QP(\rho) =: \sum_{\sigma \in S_N} (-1)^{sign(\sigma)} M(A_{1,\sigma(1)},...,A_{N,\sigma(N)}); \quad (9)$$

$$QP(\rho) = \sum_{\tau_1,\tau_2,\tau_3 \in S_N} (-1)^{sign(\tau_1\tau_2\tau_3)} \prod_{i=1}^{N} rho(i,\tau_1(i),\tau_2(i),\tau_3(i)); \quad (10)$$

$$QP(\rho) = \frac{1}{N!} \sum_{\tau_1,\tau_2,\tau_3,\tau_4 \in S_N} (-1)^{sign(\tau_1\tau_2\tau_3)\tau_4} \prod_{i=1}^{N} rho(\tau_1(i),\tau_2(i),\tau_3(i),\tau_4(i)). \quad (11)$$

Remark 1.8: The representation (6) is not unique , it follows directly from the Caratheodory Theorem that one always can choose $K \leq N^4$ in (6) . Thus , the set of separable (**BUDM**) , denoted by $Sep(N,N)$, is a convex closed set . As it is known that $Sep(N,N)$ has non-empty interiour , it follows from straigthforward dimensions counting that for the "most" separable (**BUDM**) at least $K \geq \frac{N^4}{2N-1}$. ∎

In the next proposition we summarize the properties of the quantum permanents we will need later in the paper .

Proposition 1.9:

1.
$$QP(\rho_{(X,Y)}) = MP_{(X,Y)} \tag{12}$$

2.
$$QP(\rho) = < \rho^{\otimes N} Z, Z >, \tag{13}$$
where $\rho^{\otimes N}$ stands for a tensor product of N copies of ρ , $< .,. >$ is a standard inner product and
$Z(j_1^{(1)}, j_2^{(1)}; ...; j_1^{(N)}, j_2^{(N)}) = \frac{1}{N! \frac{1}{2}}(-1)^{sign(\tau_1 \tau_2)}$
if $j_k^{(i)} = \tau_k(i)(1 \leq i \leq N); \tau_k \in S_N(k = 1,2)$ and zero otherwise .
(The equality (13) implies that if $\rho_1 \succeq \rho_2 \succeq 0$ then $QP(\rho_1) \geq QP(\rho_2) \geq 0$.)

3.
$$QP((A_1 \otimes A_2)\rho(A_3 \otimes A_4) = \det(A_1 A_2 A_3 A_4) QP(\rho) \tag{14}$$

4.
$$QP(\rho_{A,B}) = QP(\rho_{B,A}) \tag{15}$$

Example 1.10: Let us present a few cases when Quantum Permanents can be computed "exactly ". They will also illustrate how universal is this new notion .

1. Let $\rho_{A,B}$ be a product state , i.e. $\rho_{A,B} = C \otimes D$. Then $QP(C \otimes D) = Det(C) Det(D)$.
2. Let $\rho_{A,B}$ be a pure state , i.e. there exists a matrix $(R = R(i,j) : 1 \leq i,j \leq N)$ such that $\rho_{A,B}(i_1, i_2, j_1, j_2) = R(i_1, i_2)\overline{R(j_1, j_2)}$. In this case $QP(\rho_{A,B}) = N! |Det(R)|^2$.
3. Define blocks of $\rho_{A,B}$ as $A_{i,j} = R(i,j) e_i e_i^{\dagger}$. Then $QP(\rho_{A,B}) = Per(R)$.

∎

The next definition introduces Quantum Perfect Matching.

Definition 1.11: Let us consider a positive (linear) operator $T : M(N) \to M(N)$, a map $G : C^N \to C^N$, and the following three conditions :

1. $G(x) \in Im(T(xx^{\dagger}))$.
2. If $\{x_1, ..., x_N\}$ is a basis in C^N then $\{G(x_1), ..., G(x_N)\}$ is also a basis, i.e. the map G preserves linear independence.
3. If $\{x_1, ..., x_N\}$ is an orthogonal basis in C^N then $\{G(x_1), ..., G(x_N)\}$ is a basis .

. We say that map G is Quantum Perfect Matching for T if it satisfies conditions (1,2) above ; say map G is Quantum Semi-Perfect Matching for T if it satisfies conditions (1,3) above .
(As notion of positive linear operator as well notions of Quantum Perfect (Semi - Perfect) Matching can be similarly defined for a real numbers case .) ∎

In the rest of the paper we will address the following topics :

1. Characterization of Quantum Perfect Matchings in spirits of Hall's theorem .
2. Topological and algebraic properties of Quantum Perfect Matchings , i.e. properties of maps G in Definition (1.11).
3. Compelexity of checking whether given positive operator has Quantum Perfect Matching . For weakly separable operators this problem is equivalent to the nonsingularity part of (**HMIP**) .
4. Quantum (or Operator) generalizations of Sinkhorn's iterations (in the spirit of [24] , [32] , [30]).
5. van der Waerden Conjecture for Quantum Permanents.
6. Connections between topics above and the Quantum Entanlement .
7. Complexity to check the separability .

2 Necessary and sufficient conditions for Quantum Perfect Matchings

Definition 2.1: A positive linear operator $T : M(N) \to M(N)$ called rank non-decreasing iff
$$Rank(T(X)) \geq Rank(X) \text{ if} X \succeq 0; \tag{16}$$
and called indecomposable iff
$$Rank(T(X)) > Rank(X) \text{ if} X \succeq 0 \text{ and} 1 \leq Rank(X) < N. \tag{17}$$
A positive linear operator $T : M(N) \to M(N)$ called doubly stochastic iff $T(I) = I$ and $T^*(I) = I$; called ϵ - doubly stochastic iff $DS(T) =: tr((T(I) - I)^2) + tr((T^*(I) - I)^2) \leq \epsilon^2$. ∎

The next conjectures generalize Hall's theorem to Quantum Perfect Matchings .

Conjecture 2.2: Assuming that the Axiom of Choice and the Continium Hypothesis hold, a positive linear operator T has Quantum Perfect Matching iff it is rank non-decreasing . ∎

Conjecture 2.3: Assuming that the Axiom of Choice and the Continium Hypothesis hold, a positive linear operator T has Quantum Semi-Perfect Matching iff it is rank non-decreasing . ∎

Remark 2.4: We realize that the presence of the Axiom of Choice and the Continium Hypothesis in linear finite dimensional result might look a bit weird . But we will illustrate below in this section that for some completely positive entangled operators corresponding Quantum semi-perfect matching maps G are necessary quite complicated , for instance necessary discontinuos . Moreover Conjecture 1 is plain wrong , even for doubly stochastic indecomposable completely positive operators . In separable and even weakly separable cases one does not need "exotic axioms" and one can realize Quantum perfect matching map it it exists as a linear nonsingular transformation through a rather simple use of Edmonds-Rado theorem . ∎

The next Proposition(2.5) is a slight generalization of the corresponding result in [24] .

Proposition 2.5: *Doubly stochastic operators are rank non-decreasing . If either $T(I) = I$ or $T^*(I) = I$ and $DS(T) \leq N^{-1}$ then T is rank non-decreasing . If $DS(T) \leq (2N+1)^{-1}$ then T is rank non-decreasing .*

Example 2.6: Consider the following completely positive doubly stochastic operator $Sk_3 : M(3) \to M(3)$:

$$Sk_3(X) = \frac{1}{2}A_{(1,2)}XA^{\dagger}_{(1,2)} + A_{(1,3)}XA^{\dagger}_{(1,3)} + A_{(2,3)}XA^{\dagger}_{(2,3)} \tag{18}$$

Here $\{A_{(i,j)}, 1 \leq i < j \leq 3\}$ is a standard basis in a linear subspace of $M(3)$ consisting of all skew-symmetric matrices , i.e. $A_{(i,j)} =: e_ie_j^{\dagger} - e_ie_i^{\dagger}$ and $\{e_i, 1 \leq i \leq 3\}$ is a standard orthonormal basis in C^3 . It is easy to see that for a non-zero 3-dimensional column vector x vector $y \in ImSk_3(xx^{\dagger})$ iff $y_1x_1+y_2x_2+y_3x_3 = 0$ or in other words $\bar{y} \in x^{\perp}$, where $x^{\perp}$ stands for orthogonal complement of x . Notice that $Dim(x^{\perp}) = 2$.
Suppose that G is Quantum semi-perfect matching map ,
then $\overline{G(x)} \in x^{\perp}$ and , at least , $G(x)$ is nonzero for nonzero vectors x. By the well known topological result , impossibility to comb the unit sphere in C^3 , none of Quantum semi- perfect matchings for Sk_3 is continuous. It is not difficult to show that the operator Sk_3 is entangled . A direct computation shows that

$$QP(CH(Sk_3)) = 0 \tag{19}$$

An easy "lifting" of this construction allows to get a similar example for all $N \geq 3$. From the other hand , for $N = 2$ all rank non-decreasing positive operators have linear nonsingular Quantum perfect matchings .

Proposition 2.7: *Assuming that the Axiom of Choice and the Continium Hypothesis hold, Sk_3 has a Quantum semi-perfect matching .*

Proof: (Sketch) Let us well order the projective unit sphere PS_2 in C^3 : $PS_2 = (t_{\alpha}; \alpha \in \Gamma)$ in such way that for any $\beta \in \Gamma$ the interval $(t_{\alpha} : \alpha \leq \beta)$ is at most countable . As complex conjugation does not affect linear independence , our goal is to build $(g_{\alpha} \in PS_2; \alpha \in \Gamma : g_{\alpha} \neq 0, g_{\alpha} \in t_{\alpha}^{\perp})$ such that if $(t_{\alpha_1}, t_{\alpha_2}, t_{\alpha_3})$ is orthogonal basis then $(g_{\alpha_1}, g_{\alpha_2}, g_{\alpha_3})$ are independent .
As it usually happens in inductive constructions , we will inductively force an additional property : $g_{\alpha} \neq t_{\beta}$ if $\alpha > \beta$.
Notice if this condition satisfied then the linear space $L(g_{\alpha}, g_{\beta})$ generated by (g_{α}, g_{β}) is not equal to $L(t_{\alpha}, t_{\beta})$ if $< t_{\alpha}, t_{\beta} >= 0$ and $\alpha > \beta$. Using the countability assumption , it is easy to show that at each step of trasfinite induction the set of 'bad" candidates has measure zero , which allows always to choose a "good" guy g_{γ} without changing already constructed $(g_{\alpha}; \alpha < \gamma)$. ∎

The next Proposition shows that Sk_3 does not have Quantum perfect matchings !

Proposition 2.8: *Sk_3 does not have Quantum perfect matchings*

Proof: Suppose that $G(.)$ is Quantum perfect matching for Sk_3 .
Take any non-zero x and an orthogonal basis $\{y, z\}$ in $x^{\perp}$ such that $G(x) = (0, a_1, a_2)$ in $\{x, y, z\}$ basis and $a_1 \neq 0, a_2 \neq 0$.
Let $G(y) = (b_1, 0, b_2), G(z) = (c_1, c_2, 0)$ (Recall that $\overline{G(x)} \in x^{\perp}$).
Suppose that $z \in L(G(x), G(y))$, and $y \in L(G(x), G(z))$.
Then $b_1 = 0$ and $c_1 = 0$. This contradicts
to $((G(x), G(y), G(z))$ being a basis . Thus there exists an orthogonal basis (O_1, O_2, O_3) such that O_3
does not belong to $L(G(O_1), G(O_2))$.
Take non-zero vector v such that $v^{\perp} = L(G(O_1), G(O_2))$.
As $O(3) \notin L(G(O_1), G(O_2))$ thus $< v, O_3 > \neq 0$ and (O_1, O_2, v) is a basis . But , clearly , there is no basis $(G(O_1), G(O_2), d)$ with $d \in v^{\perp} = L(G(O_1), G(O_2))$.
We got a contradiction , hence there are no Quantum perfect matching for Sk_3 . ∎

Next result shows that for weakly separable (and thus for separable) operators the situation is very different.

Theorem 2.9: *Suppose that $T : M(N) \to M(N)$ is linear positive weakly separable operator , i.e. there exists a a family of rank one matrices $\{x_1y_1^{\dagger}, ..., x_ly_l^{\dagger}\} \subset M(N)$ such that for positive semidefinite matrices $X \succeq 0$ the following identity holds :*

$$Im(T(X)) = Im(\sum_{i=1}^{l} x_iy_i^{\dagger}Xy_ix_i^{\dagger}) \tag{20}$$

Then the following conditions are equivalent :

1. *T is rank non-decreasing .*
2. *The rank of intersection of two geometric matroids $MI(X, Y)$ is equal to N.*
3. *The exists a nonsingular matrix A such that $Im(AXA^{\dagger}) \subset Im(T(X)), X \succeq 0$.*

If , additionaly , T is completely positive then these conditions are equivalent to existence of nonsingular matrix A such that operator $T'(X) = T(X) - AXA^{\dagger}$ is completely positive .
In this case $QP(CH(T)) \geq N!|Det(A)|^2 > 0$.

Proof: Recall Edmonds-Rado Theorem for $MI(X, Y)$:
Rank of $MI(X, Y)$ is equal N iff

$$\dim(L(x_i; i \in A) + \dim(L(y_j; j \in \bar{A}) \geq N, \tag{21}$$

where $A \subset \{1, 2, ..., l\}$ and $\bar{A}$ is a complement of A.
Suppose that rank of $MI(X, Y)$ is equal to N. Then

$$RankT(X) = \dim(L(x_i; i \in A)) \text{ where } A =: \{i : y_i^{\dagger}Xy_i \neq 0\}$$

As $\dim(L(y_j; j \in \bar{A}) \leq dim(Ker(X)) = N - Rank(X)$ hence , from Edmonds-Rado Theorem we get that $RankT(X) \geq N - (N - Rank(X)) = Rank(X)$.
Suppose that T is rank non-decreasing and for any $A \subset \{1, 2, ..., l\}$ consider an orthogonal projector $P \succeq 0$ on $L(y_j; j \in \bar{A})^{\perp}$. Then

$$\dim(L(x_i : i \in A)) \geq RankT(P) \geq Rank(P) =$$

$$= N - \dim(L(y_j; j \in \bar{A})).$$

It follows from Edmonds-Rado Theorem that rank of $MI(X, Y)$ is equal to N .
All "equivalencies" follow now directly .
The inequality $QP(CH(T)) \geq N!|Det(A)|^2 > 0$ follows from monotonicity of Quantum Permanents (Part 2 of Prop. 1.9) and Part 2 of Example 1.10 ∎

Remark 2.10: Let us explain why Conjectures (2.2 - 2.3) generalize Hall's theorem . Consider a square weighted incidence matrix A_{Γ} of a bipartite graph Γ , i.e. $A_{\Gamma}(i, j) > 0$ if i from the first part is adjacent to j from the second part and equal to zero otherwise. Then Hall's theorem can be immediately reformulated as follows : A perfect matching , which is just a permutation in this bipartite case , exists iff $|A_{\Gamma}x|_+ \geq |x|_+$ for any vector x with nonnegative entries , where $|x|_+$ stands for a number of positive entries of a vector x . One also can look at Theorem(2.9) as a Hall's like reformulation of Edmonds-Rado theorem . ∎

2.1 A pleminary summary

So far , we got necessary and sufficient conditions for the existence of Quantum Perfect Matchings for weakly separable operators and presented an example of completely positive doubly stochastic entangled operator which has a Quantum Semi-Perfect Matching (which is necessary discontinuous) , but does not have Quantum Perfect Matchings .
These results provide new combinatorial - topological insights on the nature of the Quantum Entanglement and hint that even the notion of rank non-decreasing operator is beyound Matroids Theory for entangled operators.
It is not clear to us how crucial are "logical" assumptions
in Proposition (2.7) . As conditions in Definition 1.11 are semi-algebraic , it seems possible to try to apply powerfull Tarski theory .
Theorem(2.9) shows that in separable (even weakly separable) case these assumptions are not needed . The next question , which we study in the next sections , is about efficient , i.e. polynomial time , deterministic algorithms to check the existence of Quantum Perfect Matchings . We will describe and analyse below in the paper a "direct" deterministic polynomial time algorithm for weakly separable case (which also solves the nonsigularity part of (**HMIP**)) . A complexity bound for a separable case is slightly better than for just weakly separable case . Our algorithm is an operator generalization of Sinkhorn's iterative scaling . We conjecture that without some kind of separability promise checking whether given positive operator is rank non-decreasing is "HARD" even for completely positive operators.

3 Operator Sinkhorn's iterative scaling

Recall that for a square matrix $A = \{a_{ij} : 1 \leq i, j \leq N\}$ row scaling is defined as

$$R(A) = \{\frac{a_{ij}}{\sum_j a_{ij}}\} ,$$

column scaling as $C(A) = \{\frac{a_{ij}}{\sum_i a_{ij}}\}$ assuming that all denominators are nonzero.

The iterative process $...CRCR(A)$ is called *Sinkhorn's iterative scaling* (SI). There are two main , well known , properties of this iterative process , which we will generalize to positive Operators.

Proposition 3.1:

1. *Suppose that $A = \{a_{i,j} \geq 0 : 1 \leq i,\ j \leq N\}$. Then (SI) convergess iff A is matching, i.e., there exists a permutation π such that $a_{i,\pi(i)} > 0$ $(1 \leq i \leq N)$.*
2. *If A is indecomposable, i.e., A has a doubly-stochastic pattern and is fully indecomposable in the usual sense , then (SI) converges exponentially fast. Also in this case there exist unique positive diagonal matrices $D_1, D_2, \det(D_2) = 1$ such that the matrix $D_1^{-1}AD_2^{-1}$ is doubly stochastic.*

Definition 3.2: [Operator scaling] Consider linear positive operator $T : M(N) \to M(N)$. Define a new positive operator , Operator scaling , $S_{C_1,C_2}(T)$ as :

$$S_{C_1,C_2}(T)(X) =: C_1T(C_2^\dagger XC_2)C_1^\dagger \tag{22}$$

Assuming that both $T(I)$ and $T^*(I)$ are nonsingular we define analogs of row and column scalings :

$$R(T) = S_{T(I)^{-\frac{1}{2}},I}(T), C(T) = S_{I,T^*(I)^{-\frac{1}{2}}}(T) \tag{23}$$

Operator Sinkhorn's iterative scaling (OSI) is the iterative process $...CRCR(T)$ ∎

Remark 3.3: Using Choi's representation of the operator T in Definition(1.5) , we can define analogs of operator scaling (which are exactly so called local transformations in Quantum Information Theory) and (OSI) in terms of (**BUDM**) :

$$\begin{aligned} S_{C_1,C_2}(\rho_{A,B}) &= C_1 \otimes C_2(\rho_{A,B})C_1^\dagger \otimes C_2^\dagger; \\ R(\rho_{A,B}) &= \rho_A^{-\frac{1}{2}} \otimes I(\rho_{A,B})\rho_A^{-\frac{1}{2}} \otimes I, \\ C(\rho_{A,B}) &= I \otimes \rho_B^{-\frac{1}{2}}(\rho_{A,B})I \otimes \rho_B^{-\frac{1}{2}}. \end{aligned} \tag{24}$$

∎

Let us introduce a class of locally scalable functionals (**LSF**) defined on a set of positive linear operators , i.e. functionals satisfying the following identity :

$$\varphi(S_{C_1,C_2}(T)) = Det(C_1C_1^\dagger)Det(C_2C_2^\dagger)\varphi(T) \tag{25}$$

We will call (**LSF**) bounded if there exists a function f such that $|\varphi(T)| \leq f(tr(T(I))$. It is clear that bounded (**LSF**) are natural "potentials" for analyzing (OSI) . Indeed , Let $T_n, T_0 = T$ be a trajectory of (OSI) , T is a positive linear operator . Then $T_i(I) = I$ for odd i and $T_{2i}(I)^* = I, i \geq 1$. Thus if $\varphi(.)$ is (**LSF**) then

$$\begin{aligned} \varphi(T_{i+1}) = a(i)\varphi(T_i), a(i) = Det(T_i^*(I))^{-1} \text{ if } i \text{ is odd }, \\ a(i) = Det(T_i(I))^{-1} \text{ if } i > 0 \text{ is even.} \end{aligned} \tag{26}$$

As $tr(T_i(I)) = tr(T_i^*(I)) = N, i > 0$, thus by the ariphmetic/geometric means inequality we have that $|\varphi(T_{i+1})| \geq |\varphi(T_i)|$ and if $\varphi(.)$ is bounded and $|\varphi(T)| \neq 0$ then $DS(T_n)$ converges to zero .

To prove a generalization of Statement 1 in Prop.(3.1) we need to "invent" a bounded (**LSF**) $\varphi(.)$ such that $\varphi(T) \neq 0$ iff operator T is rank non-decreasing . We call such functionals responsible for matching . It is easy to prove that $QP(CH(T))$ is a bounded (**LSF**) . Thus if $QP(CH(T)) \neq 0$ then $DS(T_n)$ converges to zero and , by Prop. (2.5) , T is rank non-decreasing . From the other hand , $QP(CH(Sk_3)) = 0$ and Sk_3 is rank non-decreasing (even indecomposable). This is another "strangeness" of entangled operators , we wonder if it is possible to have "nice" , say polynomial with integer coefficients , responsible for matching (**LSF**) ? We introduce below responsible for matching bounded (**LSF**) which is continuous but non-differentiable .

Definition 3.4: For a positive operator $T : M(N) \to M(N)$, we define its capacity as

$$Cap(T) = \inf\{Det(T(X)) : X \succ 0, Det(X) = 1\} . \tag{27}$$

∎

It is easy to see that $Cap(T)$ is (**LSF**) .
Since $Cap(T) \leq Det(T(I)) \leq (\frac{tr(T(I))}{N})^N$,
hence $Cap(T)$ is bounded (**LSF**) .

Lemma 3.5: *A positive operator $T : M(N) \to M(N)$ is rank non-decreasing iff $Cap(T) > 0$.*

Proof: Let us fix an orthonormal basis (unitary matrix) $U = \{u_1, ..., u_N\}$ in C^N and associate with positive operator T the following positive operator :

$$T_U(X) =: \sum_{1 \leq i \leq N} T(u_iu_i^\dagger)tr(X\, u_iu_i^\dagger). \tag{28}$$

(In physics words , T_U is a decohorence respect to the basis U , i.e. in this basis applying T_U to matrix X is the same as applying T to the diagonal restriction of X.)
It is easy to see that a positive operator T is rank non-decreasing iff operators T_U are rank non-decreasing for all unitary U .
And for fixed U all properties of T_U are defined by the following N-tuple of $N \times N$ positive semidefinite matrices :

$$\mathbf{A}_{T,U} =: (T(u_1 u_1^\dagger), ..., T(u_N u_N^\dagger). \tag{29}$$

Importantly for us , T_U is rank non-decreasing iff the mixed discriminant $M(T(u_1 u_1^\dagger), ..., T(u_N u_N^\dagger)) > 0$.
Define capacity of $\mathbf{A}_{T,U}$,

$$Cap(\mathbf{A}_{T,U}) =:$$
$$\inf\{Det(\sum_{1\le i\le N} T(u_i u_i^\dagger)\gamma_i) : \gamma_i > 0, \prod_{1\le i\le N} \gamma_i = 1\}.$$

It is clear from the definitions that $Cap(T)$ is equal to infimum of $Cap(\mathbf{A}_{T,U})$ over all unitary U.
One of the main results of [30] states that

$$M(\mathbf{A}_{T,U}) =: M(T(u_1 u_1^\dagger), ..., T(u_N u_N^\dagger)) \le Cap(\mathbf{A}_{T,U}) \le \le \frac{N^N}{N!} M(T(u_1 u_1^\dagger), ..., T(u_N u_N^\dagger)). \tag{30}$$

As the mixed discriminant is a continuous (analytic) functional and the group $SU(N)$ of unitary matrices is compact , we get the next inequality :

$$\min_{U\in SU(N)} M(\mathbf{A}_{T,U}) \le Cap(T) \le \frac{N^N}{N!} \min_{U\in SU(N)} M(\mathbf{A}_{T,U}) \tag{31}$$

The last inequality proves that $Cap(T) > 0$ iff positive operator$T$ is rank non-decreasing. ∎

So , the capacity is a bounded (**LSF**) responsible for matching , which proves the next theorem :

Theorem 3.6:

1. *Let $T_n, T_0 = T$ be a trajectory of (OSI) , T is a positive linear operator . Then $DS(T_n)$ converges to zero iff T is rank non-decreasing .*
2. *Positive linear operator T is rank non-decreasing iff for all $\epsilon > 0$ there exists ϵ-doubly stochastic operator scaling of T .*

The next theorem generalizes second part of Prop. (3.1) and is proved on almost the same lines as Lemmas 24,25,26,27 in [30] .

Theorem 3.7:

1. *There exist nonsingular matrices C_1, C_2 such that $S_{C_1,C_2}(T)$ is doubly stochastic iff the infimum in (26) is attained .*
   Moreover , if $Cap(T) = Det(T(C))$ where $C \succ 0, Det(C) = 1$
   then $S_{T(C)^{\frac{-1}{2}}, C^{\frac{1}{2}}}(T)$ is doubly stochastic .
   Positive operator T is indecomposable iff the infimum in (27) is attained and unique .
2. *Doubly stochastic operator T is indecomposable iff $tr(T(X))^2 \le a\, tr(X)^2$ for some $0 \le a < 1$ and all traceless hermitian matrices X.*
3. *If Positive operator T is indecomposable then $DS(T_n)$ converges to zero with the exponential rate , i.e. $DS(T_n) \le K a^n$ for some K and $0 \le a < 1$.*

4 Lower and upper bounds on Quantum Permanents

The next proposition follows fairly directly from the second part of Prop.(1.9) and Cauchy-Schwarz inequality

Proposition 4.1: *Suppose that $\rho_{A,B}$ is (***BUDM** *). Then*

$$\max_{\sigma\in S_N} |M(A_{1,\sigma(1)}, ..., A_{N,\sigma(N)})| = M(A_{1,1}, ..., A_{N,N}) \tag{32}$$

Corollary 4.2: *If $\rho_{A,B}$ is (***BUDM** *) then*

$$QP(\rho_{A,B}) \le N! M(A_{1,1}, ..., A_{N,N}) \le N! Det(\rho_A). \tag{33}$$

Permanental part of Example(1.10) shows that $N!$ is exact constant in both parts of (32) , i.e. if blocks $A_{i,j} = e_i e_j^\dagger, 1 \le i, j \le N$ then $QP(\rho_{A,B}) = N!$ and $M(A_{1,1}, ..., A_{N,N}) = Det(\rho_A) = 1$.

The next proposition follows from the Hadamard's inequality : if $X \succ 0$ is $N \times N$ matrix then $Det(X) \le \prod_{i=1}^N X(i,i)$.

Proposition 4.3: *If $X \succ 0$ then the following inequality holds :*

$$Det(\sum_{i=1}^K x_i y_i^\dagger X y_i x_i^\dagger) \ge Det(X) MP_{(X,Y)}. \tag{34}$$

Corollary 4.4: *Suppose that separable (***BUDM** *) $\rho_{A,B}$ is Choi's representation of completely positive operator T .*
Then for all $X \succ 0$ the next inequality holds :

$$Det(T(X)) \ge QP(\rho_{A,B}) Det(X) \tag{35}$$

Since $\rho_A = T(I)$, hence $QP(\rho_{A,B}) \le Det(\rho_A)$ in separable case .
*(Notice that Corollary 4.2 provides an example of entangled (***BUDM** *) which does not satisfy (35) .)*

Call (**BUDM**) $\rho_{A,B}$ doubly stochastic if it is Choi's representation of completely positive doubly stochastic operator T . I.e. (**BUDM**) $\rho_{A,B}$ is doubly stochastic iff $\rho_A = \rho_B = I$. As we already explained , the set of separable (**BUDM**) is convex and closed . Thus the set of doubly stochastic separable (**BUDM**) , $DSEP(N,N)$, is a convex compact . Define

$$\beta(N) = \min_{\rho\in DSEP(N,N)} QP(\rho).$$

Then it follows that $\beta(N) > 0$ for all integers N . The next conjecture is , in a sense , a third generation of the famous van der Waerden conjecture . First generation is a permanental conjecture proved by Falikman and Egorychev ([15] , [14]) in 1980 and second generation is Mixed discriminants conjecture posed by R.Bapat [4] in 1989 and proved by the author in 1999 [19]. Mixed discriminants conjecture corresponds to block-diagonal doubly stochastic (**BUDM**) . Any good lower bound on $\beta(N)$ will provide similarly to [30] deterministic poly-time approximations for Matroidal permanents and new sufficient conditions for the Quantum Entanglement.

Conjecture 4.5:

$$\beta(N) = \frac{N!}{N^N}? \tag{36}$$

It is true for $N = 2$. ∎

5 Polynomial time deterministic algorithm for (HMIP)

We introduced Hidden Matroids Intersection Problem (**HMIP**) as a well posed computer science problem , which , seemingly , requires no "Quantum" background . Also , we explained that (**HMIP**) can be formulated in terms of weakly separable (**BUDM**) . Let us consider the following three properties of (**BUDM**) $\rho_{A,B}$. (We will view this $\rho_{A,B}$ as Choi's representation of completely positive operator T , i.e. $\rho_{A,B} = CH(T)$.)

P1 $Im(\rho_{A,B})$ contains a nonsingular matrix .

P2 The Quantum permanent $QP(\rho_{A,B}) > 0$.

P3 Operator T is rank non-decreasing .

We proved already that $P1 \longrightarrow P2 \longrightarrow P3$ and illustrated that that the implication $P2 \longrightarrow P3$ is strict . In fact the implication $P1 \longrightarrow P2$ is also strict. But , our Theorem (2.9), which is just an easy adoptation of Edmonds-Rado theorem , shows that for weakly separable (**BUDM**) the three properties $P1, P2, P3$ are equivalent . Recall that to check $P1$ without the weak separability promise is the same as to check whether given linear subspace of $M(N)$ contains a nonsingular matrix and it is very unlikely that this desision problem can be solved in Polynomial Deterministic time . Next , we will desribe and analyze Polynomial time deterministic algorithm to check whether $P3$ holds provided that it is promised that $\rho_{A,B}$ is weakly separable .
In terms of Operator Sinkhorn's iterative scaling (OSI) we need to check if there exists n such that $DS(T_n) \leq \frac{1}{N}$. If $L =: \min\{n : DS(T_n) \leq \frac{1}{N}\}$ is bounded by a polynomial in N and number of bits of $\rho_{A,B}$ then we have a Polynomial time Deterministic algorithm to solve (**HMIP**) . Algorithms of this kind for "classical" matching problem appeared independently in [24] and [32] . In the "classical" case they are just another , conseptually simple , but far from optimal , poly-time algorithms to check whether a perfect matching exists . But for (**HMIP**) , our , Operator Sinkhorn's iterative scaling based approach seems to be the only possibility ?
Assume that , without loss of generality , that all entries of $\rho_{A,B}$ are integer numbers and their maximum magnitude is Q. Then $Det(\rho_A) \leq (QN)^N$ by the Hadamard's inequality . If $QP(\rho_{A,B}) > 0$ then necessary $QP(\rho_{A,B}) \geq 1$ for it is an integer number. Thus

$$QP(CH(T_1)) = \frac{QP(CH(T))}{Det(\rho_A)} \geq (QN)^{-N}.$$

Each nth iteration ($n \leq L$) after the first one will multiply the Quantum permanent by $Det(X)^{-1}$, where $X \succ 0, tr(X) = N$ and $tr((X-I)^2) > \frac{1}{N}$. Using results from [24] , $Det(X)^{-1} \geq (1 - \frac{1}{3N})^{-1} =: \delta$. Putting all this together , we get the following upper bound on L , the number of steps in (OSI) to reach the "boundary" $DS(T_n) \leq \frac{1}{N}$:

$$\delta^L \leq \frac{QP(CH(T_L))}{(QN)^{-N}} \tag{37}$$

It follows frm Prop.(4.2) and Cor.(4.4) that in weakly separable case $QP(CH(T_L)) \leq N!$
and in separable case $QP(CH(T_L)) \leq 1$.
Taking logarithms we get that in weakly separable case

$$L \leq\approx 3N(N\ln(N) + N(\ln(N) + \ln(Q)); \tag{38}$$

and in separable case

$$L \leq\approx 3N(N(\ln(N) + \ln(Q)). \tag{39}$$

In any case , L is polynomial in the dimension N and the number of bits $\log(Q)$.

To finish our analysis , we need to evaluate a complexity of each step of (OSI) .
Recall that $T_n(X) = L_n(T(R_n^\dagger X R_n))L_n^\dagger$
for some nonsingular matrices L_n and R_n,
$T_n(I) = L_n(T(R_n^\dagger R_n))L_n^\dagger$ and $T_n^*(I) = R_n(T^*(L_n^\dagger L_n))R_n^\dagger$.
To evaluate $DS(T_n)$ we need to compute $tr((T_n^*(I)-I)^2)$ for odd n and $tr((T_n(I)-I)^2)$ for even n .
Define $P_n = L_n^\dagger L_n, Q_n = R_n^\dagger R_n$. It is easy to see that the matrix $T_n(I)$ is similar to $P_n T(Q_n)$, and $T_n^*(I)$ is similar to $Q_n T^*(P_n)$.
As traces of similar matrices are equal , therefore to evaluate $DS(T_n)$ it is sufficient to compute matrices P_n, Q_n.
But , $P_{n+1} = (T(Q_n))^{-1}$ and $Q_{n+1} = (T^*(P_n))^{-1}$.
And this leads to standard , rational , matrix operations with $O(N^3)$ per one iteration in (OSI) .
Notice that our original definition of (OSI) requires computation of an operator square root . It can be replaced by the Cholesky factorization , which still requires computing scalar square roots . But our final algorithm is rational !

6 Weak Membership Problem for a convex compact set of normalized bipartite separable density matrices is NP-HARD

One of the main research activities in Quantum Information Theory is a search for "operational" criterium for the separability . We will show in this section that , in a sense defined below , the problem is NP-HARD even for bipartite normalized density matrices provided that each part is large (each "particle" has large number of levels). First , we need to recall some basic notions from computational convex geometry.

6.1 Algorithmic aspects of convex sets

We will follow [18].

Definition 6.1: A proper (i.e. with nonempty interior) convex set $K \subset R^n$ called well-bounded a-centered if there exist rational vector $a \in K$ and positive (rational) numbers r, R such that $B(a,r) \subset K$ and $K \subset B(a,R)$ (here $B(a,r) = \{x : \|x-a\| \leq r\}$ and $\|.\|$ is a standard eucleadian norm in R^n) . Encoding length of such convex set K is

$$< K >= n + < r > + < R > + < a >,$$

where $< r >, < R >, < a >$ are the number of bits of corresponding rational numbers and rational vector .
Following [18] we define $S(K,\delta)$ as a union of all δ-balls with centers belonging to K ; and $S(K,-\delta) = \{x \in K : B(x,\delta) \subset K\}$.
∎

Definition 6.2: The Weak Membership Problem ($WMEM(K,y,\delta)$) is defined as follows :
Given a rational vector $y \in R^n$ and a rational number $\delta > 0$ either
(i) assert that $y \in S(K,\delta)$, or
(ii) assert that $y \notin S(K,-\delta)$.

The Weak Validity Problem ($WVAL(K,c,\gamma,\delta)$) is defined as follows :
Given a rational vector $y \in R^n$, rational number γ and a rational number $\delta > 0$ either
(i) assert that $< c,x >=: c^T x \leq \gamma + \delta$ for all $x \in S(K,-\delta)$, or
(ii) assert that $c^T x \geq \gamma - \delta$ for some $x \in S(K,\delta)$.
∎

Remark 6.3: Define $M(K,c) =: \max_{x \in K} < c,x >$. It is easy to see that

$$M(K,c) \geq M(S(K,-\delta),c) \geq M(K,c) - \|c\|\delta\frac{R}{r};$$
$$M(K,c) \leq M(S(K,\delta),c) \leq M(K,c) + \|c\|\delta$$

∎

Recall that seminal Yudin - Nemirovskii theorem ([7], [18]) implies that if there exists a deterministic algorithm solving $WMEM(K, y, \delta)$ in $Poly(< K > + < y > + < \delta >)$ steps then there exists a deterministic algorithm solving $WVAL(K, c, \gamma, \delta)$ in $Poly(< K > + < c > + < \delta > + < \gamma >)$ steps.
Let us denote as $SEP(M, N)$ a compact convex set of separable density matrices $\rho_{A,B} : C^M \otimes C^N \to C^M \otimes C^N$, $tr(\rho_{A,B}) = 1$, $M \geq N$. Recall that

$$SEP(M, N) = CO(\{xx^\dagger \otimes yy^\dagger : x \in C^M, y \in C^N; \|x\| = \|y\| = 1\}),$$

where $CO(X)$ stands for a convex hull generated by a set X.
Our goal is to prove that Weak Membership Problem for $SEP(M, N)$ is NP-HARD . As we are going to use Yudin - Nemirovskii theorem , it is sufficient to prove that $WVAL(SEP(M, N), c, \gamma, \delta)$ is NP-HARD respect to the complexity measure $(M + < c > + < \delta > + < \gamma >)$ and to show that $< SEP(M, N) >$ is polynomial in M.

6.2 Geometry of $SEP(M, N)$

First , $SEP(M, N)$ can be viewed as a compact convex subset of the hyperplane in R^D, $D =: N^2M^2$. The standard euclidean norm in $R^{N^2M^2}$ corresponds to the Frobenius norm for density matrices , i.e. $\|\rho\|_F = tr(\rho\rho^\dagger)$. The matrix $\frac{1}{NM}I \in SEP(M, N)$ and $\|\frac{1}{N^2}I - xx^\dagger \otimes yy^\dagger\|_F = \sqrt{\frac{D}{D-1}} < 1$ for all norm one vectors x, y. Thus $SEP(M, N)$ is covered by the ball $B(\frac{1}{NM}I, \sqrt{\frac{D}{D-1}})$.
The following result was recently proved in [34] .

Theorem 6.4: *Let Δ be a block hermitian matrix as in (5) . If $tr(\Delta) = 0$ and $\|\Delta\|_F \leq \sqrt{\frac{1}{D(D-1)}}$ then the the block matrix $\frac{1}{D}I + \Delta$ is separable.*

Summarizing , we get that for $D = MN$

$$B(\frac{1}{D}I, \sqrt{\frac{1}{D(D-1)}}) \subset SEP(M, N) \subset B(\frac{1}{D}I, \sqrt{\frac{D}{D-1}}),$$

(balls are restricted to the corresponding hyperplane) and conclude that $< SEP(M, N) > \leq Poly(MN)$. It is left to prove that $WVAL(SEP(M, N), c, \gamma, \delta)$ is NP-HARD respect to the complexity measure $(MN + < c > + < \delta > + < \gamma >)$.

6.3 Proof of Hardness

Let us consider the following hermitian block matrix :

$$C = \begin{pmatrix} 0 & A_1 & \dots & A_{M-1} \\ A_1 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ A_{M-1} & 0 & \dots & 0 \end{pmatrix}, \qquad (40)$$

i.e. (i, j) blocks are zero if either $i \neq 1$ or $j \neq 1$ and $(1, 1)$ block is also zero ; $A_1, ..., A_{M-1}$ are real symmetric $N \times N$ matrices .

Proposition 6.5:

$$\max_{\rho \in SEP(M,N)} tr(C\rho) = \max_{y \in R^N, \|y\|=1} \sum_{1 \leq i \leq M-1} (y^T A_i y)^2.$$

Proof: First , by linearity and the fact that the set of extreme points

$$Ext(SEP(M, N)) = \{xx^\dagger \otimes yy^\dagger : x \in C^M, y \in C^N; \|x\| = \|y\| = 1\}$$

we get that

$$\max_{\rho \in SEP(M,N)} tr(C\rho) = \max_{xx^\dagger \otimes yy^\dagger : x \in C^M, y \in C^N; \|x\| = \|y\| = 1} tr(C(xx^\dagger \otimes yy^\dagger)).$$

But $tr(C(yy^\dagger \otimes xx^\dagger)) = tr(A(y)xx^\dagger)$, where real symmetric $M \times M$ matrix $A(y)$ is defined as follows :

$$A(y) = \begin{pmatrix} 0 & a_1 & \dots & a_{M-1} \\ a_1 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ a_{M-1} & 0 & \dots & 0 \end{pmatrix}; a_i = tr(A_i yy^\dagger), 1 \leq i \leq M-1.$$

Thus

$$\max_{\rho \in SEP(M,N)} tr(C\rho) = \max_{yy^\dagger \otimes xx^\dagger : x \in C^M, y \in C^N; \|x\| = \|y\| = 1} tr(C\rho) = \max_{\|y\|=1} \lambda_{max} A(y).$$

(Above $\lambda_{max} A(y)$ is a maximum eigenvalue of $A(y)$)
It is easy to see $A(y)$ has only two non-zero eigenvalues $(d, -d)$, where $d = \sum_{1 \leq i \leq M-1} (tr(A_i yy^\dagger))^2$.
As $A_i, 1 \leq i \leq N - 1$ are real symmetric matrices we finally get that

$$\max_{\rho \in SEP(M,N)} tr(C\rho) = \max_{y \in R^N, \|x\|=1} \sum_{1 \leq i \leq N-1} (y^T A_i y)^2.$$

∎

Proposition(6.5) and Remark(6.3) suggest that in order to prove NP-HARDness of
$WVAL(SEP(M, N), c, \gamma, \delta)$ respect to the complexity measure $M + < c > + < \delta > + < \gamma >$ it is sufficient to prove that the following problem of is NP-HARD :

Definition 6.6: (RSDF problem) Given k $l \times l$ real rational symmetric matrices $(A_i, 1 \leq i \leq l)$ and rational numbers (γ, δ) to check whether

$$\gamma + \delta \geq max_{x \in R^l, \|x\|=1} f(x) \geq \gamma - \delta, f(x) =: \sum_{1 \leq i \leq l} (x^T A_i x)^2.$$

respect to the complexity measure
$(lk + \sum_{1 \leq i \leq l} < A_i > + < \delta > + < \gamma >)$. ∎

It was shown in [6], by a reduction to the KNAPSACK , that RSDF problem is NP-HARD provided
$k \geq \frac{l(l-1)}{2} + 1$.
We summarize all this in the following theorem

Theorem 6.7: *The Weak Membership Problem for $SEP(M, N)$ is NP-HARD if $N \leq M \leq \frac{N(N-1)}{2} + 2$.*

Remark 6.8: It is easy exercise to prove that (**BUDM**) $\rho_{A,B}$ written in block form (5) is real separable iff it is separable and all the blocks in (5) are real symmetric matrices . It follows that , with obvious modifications , Theorem 6.7 is valid for the real separability too .
The construction (40) was inspired by Arkadi Nemirovski proof of NP-HARDness to check the positivity of a given operator [2] . ∎

7 Concluding Remarks

Many ideas of this paper were suggested by [30] . The world of mathematical interconnections is very unpredictable (and thus is so exciting) . The main technical result in a very recent breaktrough in Communicational Complexity [33] is a rediscovery of particular , rank one , case of a general , matrix tuples scaling , result proved in [30] with much simpler proof than in [33] . Perhaps this our paper will produce something new in Quantum Communicational Complexity ?

We still don't know whether there is a deterministic poly-time algorithm to check whether given completely positive operator is rank non-decreasing . And this question is related to lower bounds on $Cap(T)$ provided that Choi's representation $CH(T)$ is an integer semidefinite matrix .

Theorem(6.7) together with other results from our paper gives a new , classical complexity based , insight on the nature of the Quantum Entanglement and , in a sense , closes a long line of research in Quantum Information Theory . Still many open questions remained (for the author) , for instance , is it still NP-HARD for (M, N) bipartite systems wnen N is a fixed constant ?

We hope that the constructions introduced in this paper , especially Quantum Permanent , will have a promising future . The "third generation" of van der Waerden conjecture we introduced above will require the "second generation" of Alexandrov-Fenchel inequalities [1]. We think , that in general , mixed discriminants and mixed volumes should be studied (used) more enthusiastically in the Quantum context . After all , they are noncommutative generalizations of the permanent ....

It is my great pleasure to thank my LANL colleagues Manny Knill and Howard Barnum .

Finally , I would like to thank Arkadi Nemirovski for many enlightening discussions .

References

[1] A. Aleksandrov, On the theory of mixed volumes of convex bodies, IV, Mixed discriminants and mixed volumes (in Russian), *Mat. Sb. (N.S.)* 3 (1938), 227-251.

[2] A.Nemirovski , Personal Communication , 2001.

[3] I. Bárány and Z. Furedi, Computing the volume is difficult, *Discrete & Computational Geometry*, 2 (1987), 319-326.

[4] R. B. Bapat, Mixed discriminants of positive semidefinite matrices, *Linear Algebra and its Applications* 126, 107-124, 1989.

[5] S.L. Woronowicz , Positive maps of low dimensional matrix algebras , Rep. Math. Phys. 10, 165 (1976) , 165-183 .

[6] A. Ben-Tal and A.Nemirovski , Robust convex optimization , Mathematics of Operational Research , Vol. 23 , 4 (1998) , 769-805 .

[7] D.B.Yudin and A.S. Nemirovskii , Informational complexity and efficient methods for the solution of convex extremal problems (in Russian) , Ekonomica i Matematicheskie Metody 12 (1976) , 357 -369 .

[8] R. B. Bapat, T. E. S. Raghavan, **Nonnegative matrices and applications**, Cambridge University Press, 1997.

[9] A. I. Barvinok, Computing Mixed Discriminants, Mixed Volumes, and Permanents, *Discrete & Computational Geometry*, 18 (1997), 205-237.

[10] A. I. Barvinok, Polynomial time algorithms to approximate permanents and mixed discriminants within a simply exponential factor, *Random Structures & Algorithms* , 14 (1999), 29-61.

[11] M. Dyer and A. Frieze, The complexity of computing the volume of a polyhedron, *SIAM J. Comput.*, 17, 967-994, 1988.

[12] M. Dyer, P. Gritzmann and A. Hufnagel, On the complexity of computing mixed volumes, *SIAM J. Comput.*, 27(2), 356-400, 1998.

[13] J. Edmonds, Submodular functions, matroids, and certain polyhedra, in **Combinatorial structures and their applications**, R. Guy, H. Hanani, N. Sauer and J. Schönheim, eds., Gordon and Breach, New York, 1970, 69-87.

[14] G.P. Egorychev, The solution of van der Waerden's problem for permanents, *Advances in Math.*, 42, 299-305, 1981.

[15] D. I. Falikman, Proof of the van der Waerden's conjecture on the permanent of a doubly stochastic matrix, *Mat. Zametki* 29, 6: 931-938, 957, 1981, (in Russian).

[16] S. Friedland, A lower bound for the permanent of a doubly stochastic matrix, *Annals of Mathematics*, 110(1979), 167-176.

[17] C. D. Godsil, **Algebraic Combinatorics**, Chapman and Hall, 1993.

[18] M. Grötschel, L. Lovasz and A. Schrijver, **Geometric Algorithms and Combinatorial Optimization**, Springer-Verlag, Berlin, 1988.

[19] L. Gurvits, Van der Waerden Conjecture for Mixed Discriminants, submitted, 2000; accepted for publication in *Advances in Mathematics*, 2001.

[20] M. Jerrum and A. Sinclair, Approximating the permanent, *SIAM J. Comput.*, 18, 1149-1178, 1989.

[21] M. Jerrum, A. Sinclair and E. Vigoda, A polynomial-time approximation algorithm for the permanent of a matrix with non-negative entries, *Proc. 33 ACM Symp. on Theory of Computing*, ACM, 2001.

[22] F. John, Extremum problems with inequalities as subsidiary conditions, **Studies and Essays, presented to R. Courant on his 60th birthday**, Interscience, New York, 1948.

[23] B. Kalantari and L Khachian, On the complexity of nonnegative matrix scaling, *Linear Algebra Appl.*, 240, 87-104, 1996.

[24] N. Linial, A. Samorodnitsky and A. Wigderson, A deterministic strongly polynomial algorithm for matrix scaling and approximate permanents, *Proc. 30 ACM Symp. on Theory of Computing*, ACM, New York, 1998.

[25] Y. Nesterov and A. Nemirovskii, **Interior-Point Polynomial Algorithms in Convex Programming**, SIAM, Philadelphia, PA, 1994.

[26] A. Nemirovski and U. Rothblum, On complexity of matrix scaling, *Linear Algebra Appl.* 302/303, 435-460, 1999.

[27] A. Panov, On mixed discriminants connected with positive semidefinite quadratic forms, *Soviet Math. Dokl.* 31 (1985).

[28] R. Schneider, **Convex bodies: The Brunn-Minkowski Theory**, Encyclopedia of Mathematics and Its Applications, vol. 44, Cambridge University Press, New York, 1993.

[29] L. G. Valiant, The complexity of computing the permanent, *Theoretical Computer Science*, 8(2), 189-201, 1979.

[30] L.Gurvits and A. Samorodnitsky , A deterministic polynomial-time algorithm for approximating mised discriminant and mixed volume , *Proc. 32 ACM Symp. on Theory of Computing*, ACM, New York, 2000.

[31] P.Horodecki , J. A. Smolin , B.M.Terhal , A . V. Thapliyal , Rank two Bipartite Bound Entangled States Do not Exist , arXiv:quant-ph/9910122v4 , 2001 .

[32] L.Gurvits and P.Yianilos , The deflation-inflation method for certain semidefinite programming and maximum determinant completion problems , NECI technical report , 1998 .

[33] J. Forster , A Linear Lower Bound on the Unbounded Error Probabilistic Communication Complexity , Sixteenth Annual IEEE Conference on Computational Complexity , 2001 .

[34] L.Gurvits and H.Barnum , Size of the separable neighborhood of the maximally mixed bipartite quantum state , Los Alamos

National Laboratory unclassified technical report LAUR 02-2414 , 2002.