Quantum Discrepancy: A Non-Commutative Version of Combinatorial Discrepancy

Kasra Alishahi
Department of Mathematical Sciences
Sharif University of Technology
Tehran, Iran
alishahi@sharif.ir

Mohaddeseh Rajaee Ali Rajaei
Faculty of Mathematical Sciences
Tarbiat Modares University
Tehran, Iran
{mohaddeseh.rajaee,alirajaei}@modares.ac.ir

Submitted: Jan 3, 2018; Accepted: Dec 3, 2019; Published: May 15, 2020
© The authors. Released under the CC BY-ND license (International 4.0).

Abstract

In this paper, we introduce a notion of quantum discrepancy, a non-commutative version of combinatorial discrepancy which is defined for projection systems, i.e. finite sets of orthogonal projections, as non-commutative counterparts of set systems. We show that besides its natural algebraic formulation, quantum discrepancy, when restricted to set systems, has a probabilistic interpretation in terms of determinantal processes. Determinantal processes are a family of point processes with a rich algebraic structure. A common feature of this family is the local repulsive behavior of points. Alishahi and Zamani (2015) exploit this repelling property to construct low-discrepancy point configurations on the sphere.

We give an upper bound for quantum discrepancy in terms of \( N \), the dimension of the space, and \( M \), the size of the projection system, which is tight in a wide range of parameters \( N \) and \( M \). Then we investigate the relation of these two kinds of discrepancies, i.e. combinatorial and quantum, when restricted to set systems, and bound them in terms of each other.

Mathematics Subject Classifications: 05D40
1 Introduction

1.1 Definition of Quantum Discrepancy

In 1964, Roth proved in [11] that for any blue-red coloring of $[N] := \{1, 2, \ldots, N\}$, there always exists an arithmetic progression, in which the difference between the number of red and blue points is $\Omega(N^{1/4})$. Roth’s theorem was one of the first results in a field that was later named combinatorial discrepancy theory, which is also related to, or has applications in diverse fields of mathematics and theoretical computer science, such as Ramsey theory, hypergraph coloring, arithmetic structures, probabilistic and approximation algorithms, complexity theory, and data structure. For a general introduction to discrepancy theory, its relations to computer science, and recent results in this field see [4, 5, 9].

If we forget the special structure of the family of arithmetic progressions, we can formulate the basic problem of this field in a more general form. Assume that $\Omega$ is a finite set. A 2-coloring or more simply a coloring of $\Omega$ can be modeled by a function $\chi : \Omega \rightarrow \{\pm 1\}$. Assuming $\chi(s) = 1$ and $\chi(s) = -1$ as $s$ is colored red and blue, respectively, the absolute value of $\chi(S) := \sum_{s \in S} \chi(s)$ is a measure of the imbalance between the number of red and blue elements in $S$ due to $\chi$. Now, given a set system $\mathcal{S}$, i.e. a subset of $2^\Omega$, the discrepancy of $\mathcal{S}$ is defined by

$$\text{Disc}(\mathcal{S}) = \min_{\chi: \text{coloring}} \max_{S \in \mathcal{S}} |\chi(S)|. \quad (1)$$

Note that since the structure of a set system remains unaffected if we change the labels of points in the ground set, from now on, we suppose that $\Omega = [N]$ for some $N \in \mathbb{N}$.

Since the combinatorial minimization in (1) has exponentially many feasible values, exhaustive search is not a computationally efficient method for finding a low-discrepancy coloring, i.e. a coloring such as $\chi$ that makes $\max_{S \in \mathcal{S}} |\chi(S)|$ small. Moreover, many of general upper bounds such as Spencer’s bound, mentioned in the next subsection, are based on techniques that are non-constructive, in the sense that they prove the existence of low-discrepancy colorings without any guide to accessing them. Designing efficient algorithms for the construction of colorings with optimal or nearly optimal discrepancy is an active area of research in the theory of combinatorial discrepancy. In recent years, remarkable achievements have been attained in this area (e.g. see [5, Ch. 6] and [12]).

Quantum discrepancy is a non-commutative version of combinatorial discrepancy, which is defined as follows. In what follows, $\mathcal{M}_N(\mathbb{C})$ stands for the set of $N \times N$ matrices with complex entries.

**Definition 1.** Suppose $N$ is a natural number. A finite set $\mathcal{P}$ of orthogonal projections of $\mathbb{C}^N$, i.e. operators such as $P$ with the property that $P^2 = P = P^*$, is called a projection system in $\mathbb{C}^N$. A Hermitian matrix $\chi \in \mathcal{M}_N(\mathbb{C})$ with eigenvalues in $\{\pm 1\}$ is named a quantum coloring (a justification for this denomination is provided at the end of this subsection). We define the quantum discrepancy of a projection system $\mathcal{P}$ to be

$$\text{QDisc}(\mathcal{P}) = \min_{\chi: \text{quantum coloring}} \max_{P \in \mathcal{P}} \left[ \text{tr}^2(\chi P) + \text{tr} (\chi[P][P]) \right]^\frac{1}{2}, \quad (2)$$

Note that $\text{QDisc}(\mathcal{P})$ is a lower bound on the classical discrepancy of $\mathcal{P}$.
where \( [A, B] := AB - BA \) is the commutator of \( A \) and \( B \).

Quantum discrepancy is well-defined for each projection system since the expression \( \text{tr}^2(\chi P) + \text{tr}(\chi[\chi, P]P) \) is real and non-negative. Because \( \chi \) and \( P \) are Hermitian, \( \text{tr}(\chi P) \) is real. Also, it will be seen in Subsection 2.2 that \( \text{tr}(\chi[\chi, P]P) \) is real and non-negative (see Lemma 12).

To a set system \( S \subseteq 2^{[N]} \) we can assign a projection system \( \mathcal{P}_S \) in a natural way: for \( S \in S \) we set \( P_S \) to be the diagonal matrix that for each \( i \in [N] \), its \( i \)-th diagonal entry is equal to 1 if \( i \in S \), and 0 otherwise. Then, we put \( \mathcal{P}_S = \{ P_S : S \in S \} \). Moreover, any coloring \( \chi \) of \([N]\) can be considered as a diagonal matrix with diagonal entries \( \pm 1 \). Thus, projection systems and quantum colorings generalize set systems and colorings, respectively. In addition, for a set \( S \subseteq [N] \), and a (diagonal) coloring \( \chi \), \( \text{tr}(\chi P_S) = \chi(S) \) and since \( \chi \) and \( P_S \) are both diagonal, \( [\chi, P_S] = 0 \). Hence, in this situation,

\[
[\text{tr}^2(\chi P_S) + \text{tr}(\chi[\chi, P_S]P_S)]^{1/2} = |\text{tr}(\chi P_S)| = |\chi(S)|.
\]

It is proved in Subsection 2.2 that, for an orthogonal projection \( P \) and a quantum coloring \( \chi \), it holds that

\[
\text{tr}(\chi[\chi, P]P) = \frac{1}{2} \|[\chi, P]\|_2^2.
\]

Therefore, the second term, i.e. \( \text{tr}(\chi[\chi, P]P) \), has also a simple meaning. The reason for choosing the combination \( \left[ \text{tr}^2(\chi P) + \frac{1}{2} \|[\chi, P]\|_2^2 \right]^{1/2} \) which might look messy, lies in its probabilistic interpretation, when \( \mathcal{P} \) is associated to a set system. In fact, for a quantum coloring \( \chi \) there is a determinantal point process \( \mathcal{X} \) on \([N]\) (see Definition 8) such that for any \( S \subseteq [N] \),

\[
\left[ \text{tr}^2(\chi P_S) + \text{tr}(\chi[\chi, P_S]P_S) \right]^{1/2} = \left[ \mathbb{E} \left[ (2\mathcal{X}(S) - |S|)^2 \right] \right]^{1/2}.
\]

In this formula \( \mathcal{X}(S) \) represents \( |\mathcal{X} \cap S| \), i.e. the number of points of \( \mathcal{X} \) which belong to \( S \). Therefore, if we assume that the set of red points of \([N]\) is determined randomly according to the distribution of \( \mathcal{X} \), the right-hand side of (3) can be considered as the imbalance imposed by the process \( \mathcal{X} \) to \( S \). This probabilistic approach to the combinatorial discrepancy problem (including the proof of (3)) is fully described in Subsection 2.1.

We intend to emphasize the importance of the commutator operator in (2). The appearance of \( [\chi, P] \) reveals the strong non-commutative essence of the quantum discrepancy. This non-commutativity is partially a result of extending the notion of the coloring. Thus, we have a non-commutative concept of discrepancy even for set systems. There is another aspect of non-commutativity which lies in \( \mathcal{P} \). When all projections in \( \mathcal{P} \) commute pairwise, they are simultaneously unitarily diagonalizable since they are Hermitian. Therefore, \( \mathcal{P} \), possibly after a unitary change of the basis, corresponds to a set system, and because of the cyclic property of the trace function, \( \text{QDisc}(\mathcal{P}) \) will be equal to \( \text{QDisc}(\mathcal{P}_S) \) for some set system \( S \). However, this is not the case for a general projection system which
may include non-commuting elements. Hence, the complexity of the notion of quantum discrepancy also lies in the non-commutativity inside $\mathcal{P}$.

Now, let us justify the term “quantum” in “quantum discrepancy”. In classical physics, the phase space of a system is described by a set which is finite if the system has finite states. An observable of this system is a real-valued function on the phase space. In quantum physics, the phase space is replaced by a Hilbert space. If the classical phase space has $N$ elements, the quantum phase space would be $\mathbb{C}^N$. The quantum counterpart of an observable $f$ is a Hermitian operator with the same spectrum as the image of $f$ (see [17] for more explanation). Now, note that in the current quantization process of combinatorial discrepancy, subsets of $[N]$ are replaced by orthogonal projections which are in one-to-one correspondence with subspaces of $\mathbb{C}^N$, and functions of the form $\chi : [N] \rightarrow \{\pm 1\}$ are replaced by Hermitian matrices with eigenvalues in $\{\pm 1\}$.

In the preface of [17] Weaver refers to the two above-mentioned ideas as general principles of quantization. It is worthwhile to see this in his own words:

...We have now reached a point where it is possible to give a simple, unified approach to the general concept of quantization in mathematics.

The fundamental idea of mathematical quantization is that sets are replaced by Hilbert spaces. Thus, we regard lattice operations (join, meet, orthocomplement) on subspaces of a Hilbert space as corresponding to set-theoretic operations (union, intersection, complement) on subsets of a set. This already allows one to determine quantum analogs of some simple structures. But the real breakthrough is the fact that the quantum version of a complex-valued function on a set is an operator on a Hilbert space...

With more work the analogy can be pushed even further. At each step one must formulate the given classical notion in just the right way to obtain a viable quantum version. This sometimes requires significant creativity. However, as it is done in case after case, general quantization principles emerge.

The remaining parts of this paper are organized as follows. The next subsection is dedicated to the statement of the main results. In order to make the current subsection more coherent, discussions about equivalent forms of quantum discrepancy are postponed to Section 2. We prove the main results in Sections 3, and 4. Finally, Section 5 is devoted to some concluding remarks.

1.2 Main Results

The main results of this paper can be divided into two categories: quantum discrepancy of a general projection system, and quantum discrepancy of a set system. Note that, to be more precise, we have to use a phrase like “quantum discrepancy of a projection system which is associated with a set system” instead of “quantum discrepancy of a set system”. But, for more convenience, we use the latter.

In the case of a general projection system, we first investigate upper bounds. For a set system $\mathcal{S}$ of size $M$ in $[N]$, a trivial upper bound for $\text{Disc}(\mathcal{S})$ is $N$. We prove the same bound holds for quantum discrepancy.
Theorem 2 (Trivial Upper Bound). For each projection system \( P \) in \( \mathbb{C}^N \),

\[ \text{QDisc}(P) \leq N. \]

Another general upper bound of Disc(\( S \)) can be obtained by coloring the points of \([N]\), randomly. It can be shown that if \( S \) is a set system consisting of \( M \) subsets of \([N]\), Disc(\( S \)) = \( O(\sqrt{N \log M}) \). In particular for \( M = O(N) \), Disc(\( S \)) = \( O(\sqrt{N \log N}) \).

We recall that for two functions \( f \) and \( g \) on \( \mathbb{N} \times \mathbb{N} \), \( f(m,n) = O(g(m,n)) \) means that there exists a constant \( c > 0 \) independent of \( m \) and \( n \), such that \( |f(m,n)| \leq c|g(m,n)| \) for all but a finite set of values of \((m,n) \in \mathbb{N} \times \mathbb{N}\).

Using random quantum colorings, we obtain an upper bound for QDisc(\( P_S \)) in terms of \( N \) and \( M \).

Theorem 3. Suppose \( P \) is an \( M \)-element projection system in \( \mathbb{C}^N \). Then

\[ \text{QDisc}(P) = O(\sqrt{N + \log M}). \]

The random coloring bound of Disc(\( S \)), i.e. \( O(\sqrt{N \log M}) \), is not tight. Spencer, in [13], obtained another upper bound which is optimal. He proved that when \( M \geq N \),

\[ \text{Disc}(S) = O\left(\sqrt{N \log \left(2M/N\right)}\right). \]

In particular, if \( M = O(N) \), Disc(\( S \)) would be of order \( O(\sqrt{N}) \). A probabilistic proof for the optimality of Spencer’s bound is sketched in [9] (Exercise 1, Section 4.1). It is based on a random set system \( S \) and is designed to prove that if \( c > 0 \) is a sufficiently small constant and \( N \leq M \leq 2^{CN} \), there exists a set system \( S \) on \([N]\) with \( M \) elements such that Disc(\( S \)) \( \geq c\sqrt{N \log(2M/N)} \).

In case of a projection system, its size is not bounded in terms of the dimension of the ground space. Hence, by Theorem 2, the bound given in Theorem 3 can not be tight for all values of \( N \) and \( M \). However, by choosing a random projection system with an appropriate distribution, we prove that this bound is tight in the worst case, provided that \( M \) is neither too large nor too small with respect to \( N \).

Theorem 4. Suppose \( M \) is neither too small nor too large with respect to \( N \), such that

\[ aN \leq M, \quad \log M \leq bN, \]

for appropriate constants \( a, b > 0 \), which are independent of \( M \) and \( N \). There exist an \( M \)-element projection system \( P \) in \( \mathbb{C}^N \) and a constant \( c > 0 \), which depends only on \( b \), with the property that

\[ \text{QDisc}(P) \geq c\sqrt{N + \log M}. \]

In the procedure of proving Theorem 3 it becomes clear that this partially tight bound occurs with probability at least 1/2. Hence, Theorem 3 is of constructive importance. If
we generate multiple samples of the specified random quantum coloring, we have, with high probability, a quantum coloring that satisfies the given bound.

After this general consideration, we focus on a projection system $\mathcal{P}_S$ corresponding to a set system $\mathcal{S}$ of size $M$ in $[N]$. For this special kind of projection systems both $\text{Disc}(\mathcal{S})$ and $\text{QDisc}(\mathcal{P}_S)$ are defined. Since each combinatorial coloring is a quantum coloring,

$$\text{QDisc}(\mathcal{P}_S) \leq \text{Disc}(\mathcal{S}). \tag{4}$$

We prove two other relations between these two quantities. First, we investigate the case where $\text{QDisc}(\mathcal{P}_S) = 0$, and obtain the following result.

**Theorem 5.** Suppose $\mathcal{S}$ is a set system on $[N]$, and $\mathcal{P}_S$ is its corresponding projection system. $\text{QDisc}(\mathcal{P}_S) = 0$ if and only if $\text{Disc}(\mathcal{S}) = 0$.

For the remaining set systems we bound $\text{QDisc}(\mathcal{P}_S)$ and $\text{Disc}(\mathcal{S})$ in terms of each other in a way different from (4).

**Theorem 6.** Suppose $\mathcal{S}$ is a set system with $M \geq 2$ subsets of $[N]$, and $\mathcal{P}_S$ is its corresponding projection system. If $\text{QDisc}(\mathcal{P}_S) \neq 0$, then for some constant $c > 0$, independent of $M$, $N$, and $\mathcal{S}$, it holds that

$$\text{Disc}(\mathcal{S}) < \left(2c \max \left[\sqrt{\log(2M)}, \frac{\log(2M)}{\text{QDisc}(\mathcal{P}_S)}\right] + 1\right) \text{QDisc}(\mathcal{P}_S).$$

This theorem shows that $\text{Disc}(\mathcal{S})$ which is not smaller than $\text{QDisc}(\mathcal{P}_S)$ can not be arbitrarily larger. This illustrates an important aspect of the study of quantum discrepancy to combinatorial discrepancy theory, i.e. an upper bound for $\text{QDisc}(\mathcal{P}_S)$ leads to an upper bound for $\text{Disc}(\mathcal{S})$. The idea of the proof is that a quantum coloring with low quantum discrepancy gives us a low-discrepancy coloring. The next example demonstrates another application of Theorem 6.

**Example 7.** Suppose $\mathcal{S}$ is the set system of all arithmetic progressions in $[N]$. As mentioned before, $\text{Disc}(\mathcal{S}) = \Omega(N^{1/4})$. Thus, $\text{QDisc}(\mathcal{P}_S) \neq 0$. It can be shown that in this special case $M = O(N^3)$, so $\log(2M) = O(\log N)$. From Theorem 6 we conclude that for some $c' > 0$, we have $(c'\sqrt{\log N} + 1)\text{QDisc}(\mathcal{P}_S) = \Omega(N^{1/4})$. Hence,

$$\text{QDisc}(\mathcal{P}_S) = \Omega(N^{\frac{1}{4} - \epsilon}), \quad \forall \epsilon > 0.$$ 

And since $\text{Disc}(\mathcal{S}) = O(N^{1/4})$ (see [10]), it follows that for each $\epsilon > 0$,

$$c_1 N^{\frac{1}{4} - \epsilon} \leq \text{QDisc}(\mathcal{P}_S) \leq c_2 N^{\frac{1}{4}},$$

where $c_1 = c_1(\epsilon)$ and $c_2$ are suitable positive constants.
2 Equivalent Forms of Quantum Discrepancy

2.1 A Probabilistic Approach to Combinatorial Discrepancy

A probabilistic interpretation of quantum discrepancy when restricted to set systems is explained in this subsection. The core idea behind the scenes is to color points of the ground set $[N]$ randomly according to the distribution of a determinantal process.

Note that a coloring of $[N]$ is uniquely determined by a subset of $[N]$, that is the set of, say, its red points. Hence, a random coloring of $[N]$ is, in fact, a random subset of this set. Such a random object, i.e a random subset of $[N]$, is called a simple point process on $[N]$ (the word “simple” indicates that the multiplicity of each point of $[N]$ in any realization is at most one).

Definition 8. A simple point process $X$ on $[N]$ is said to be a determinantal process, if there is a matrix $K \in M_N(\mathbb{C})$ such that for every $\{i_1, i_2, \ldots, i_k\} \subseteq [N]$

$$P[i_1, i_2, \ldots, i_k \in X] = \det \left( (K_{ij})_{i,j \in \{i_1, i_2, \ldots, i_k\}} \right) \cdot (5)$$

$K$ is called the kernel of $X$.

The following proposition provides a necessary and sufficient condition for a Hermitian matrix $K$ to be the kernel of a determinantal process (see e.g. Theorem 4.5.5 in [8]).

Proposition 9. Suppose $K$ is a Hermitian matrix. $K$ is the kernel of a determinantal process if and only if its spectrum is a subset of $[0,1]$.

A determinantal process $X$ with a Hermitian kernel $K$ on $[N]$ has negative correlations since for any distinct values of $i, j \in [N]$

$$P[i, j \in X] = P[i \in X]P[j \in X] - |K_{ij}|^2 \leq P[i \in X]P[j \in X]$$

More generally, using Koteljanskii’s inequality (see e.g. [7], Theorem 7.8.9), it can be proved that any two disjoint sets $I, J \subseteq [N]$ repel each other in the sense that

$$P[I \cup J \subseteq X] \leq P[I \subseteq X]P[J \subseteq X].$$

Therefore, it is expected that determining red points of a coloring according to the law of a determinantal process would prevent them from accumulating in one or more members of a given set system.

Now, suppose $\chi$ is a quantum coloring. Then, $K := (\chi + I)/2$ is a Hermitian matrix with eigenvalues in $\{0,1\}$. In fact, $K$ is an orthogonal projection. On the other hand, for an arbitrary orthogonal projection $K$, the matrix $2K - I$ is a quantum coloring. Hence, by Proposition 9, there is a one-to-one correspondence between the set of $N \times N$ quantum colorings and the set of determinantal projection processes on $[N]$, i.e. determinantal processes that their kernels are orthogonal projections. The mentioned probabilistic interpretation of quantum discrepancy of a set system is based on this correspondence.
Lemma 10. Suppose $\mathcal{P}_S$ is the projection system corresponding to a set system $\mathcal{S}$ in $[N]$. Then,

$$\text{QDisc}(\mathcal{P}_S) = \min_{\chi} \max_{S \in \mathcal{S}} \left[ \mathbb{E} \left[ (2\chi(S) - |S|)^2 \right] \right]^{\frac{1}{2}},$$

while the minimum is taken over all determinantal projection processes on $[N]$.

Proof. According to the explanation given before the lemma, it is enough to prove that for each $S \subseteq [N],$

$$\text{tr}^2(\chi \mathcal{P}_S) + \text{tr}(\chi \chi^T \mathcal{P}_S) = \mathbb{E} \left[ (2\chi(S) - |S|)^2 \right],$$

where $\chi$ is an arbitrary quantum coloring and $\chi$ is the determinantal projection process with kernel $K = (\chi + I)/2$. We start from the right-hand side. By definition of $P_S$, we have $|S| = \text{tr}(P_S)$. Thus,

$$\mathbb{E} \left[ (2\chi(S) - |S|)^2 \right] = 4\mathbb{E} \left[ \chi^2(S) \right] - 4\text{tr}(P_S)\mathbb{E} [\chi(S)] + \text{tr}^2(P_S).$$

We compute $\mathbb{E}[\chi(S)]$ and $\mathbb{E}[\chi^2(S)]$. Suppose that the $i$-th diagonal element of $P_S$ is $p_{ii}$. If $1_E$ represents the indicator function of an arbitrary event $E$, then for any $S \subseteq [N]$ it holds that

$$\chi(S) = \sum_{i \in S} 1_{\{i \in \chi\}}.$$ (8)

Hence,

$$\mathbb{E} [\chi(S)] = \sum_{i \in S} \mathbb{P}[i \in \chi] \quad \text{(by (8), linearity of expectation)}$$

$$= \sum_{i=1}^N \mathbb{P}[i \in \chi]1_{\{i \in S\}}.$$ (by (5))

According to the definition of $P_S$, we have $1_{\{i \in S\}} = p_{ii}$. Thus,

$$\mathbb{E} [\chi(S)] = \sum_{i=1}^N K_{ii}p_{ii}$$

$$= \text{tr}(KP_S).$$ (9)

Using (8) and linearity of the expectation once again, we obtain

$$\mathbb{E} [\chi^2(S)] = \sum_{i \in S} \mathbb{P}[i \in \chi] + \sum_{S \times S \atop i \neq j} \mathbb{P}[i, j \in \chi]$$

$$= \text{tr}(KP_S) + \sum_{S \times S \atop i \neq j} \mathbb{P}[i, j \in \chi].$$ (10)
On the other hand,
\[
\sum_{S \times S, i \neq j} \mathbb{P}[i, j \in X] = \sum_{1 \leq i \neq j \leq N} \mathbb{P}[i, j \in X] \mathbf{1}_{i \in S} \mathbf{1}_{j \in S}
\]
\[
= \sum_{1 \leq i \neq j \leq N} [K_{ii}K_{jj} - K_{ij}K_{ji}] p_{ii}p_{jj} \quad \text{(by (5))}
\]
\[
= \sum_{1 \leq i \neq j \leq N} K_{ii}p_{ii}K_{jj}p_{jj} - \sum_{1 \leq i \neq j \leq N} |K_{ij}|^2 p_{ii}p_{jj} \quad \text{\(K\) is Hermitian}
\]
\[
= \text{tr}^2(KPS) - \sum_{1 \leq i \leq N} K_{ii}^2 p_{ii} - \sum_{1 \leq i \neq j \leq N} |K_{ij}|^2 p_{ii}p_{jj}
\]
\[
= \text{tr}^2(KPS) - \sum_{1 \leq i \leq N} |K_{ii}|^2 p_{ii}p_{jj}
\]
\[
= \text{tr}^2(KPS) - \text{tr}((KPS)^2). \quad (11)
\]
Combining (7), (9), (10), and (11) results in the following equation.
\[
\mathbb{E} \left[ (2X(S) - |S|)^2 \right] = \text{tr}^2(2KPS - P_S) + 4\text{tr} (KPS(I - KPS)). \quad (12)
\]
It is straightforward to check that for \(K = (\chi + I)/2\), and each \(S\),
\[
\text{tr}^2(2KPS - P_S) + 4\text{tr} (KPS(I - KPS)) = \text{tr}^2(\chi P_S) + \text{tr} (\chi [\chi, P_S]P_S),
\]
which together with (12) gives (6). \(\Box\)

Remark 11. By the bias-variance decomposition
\[
\mathbb{E} \left[ (2X(S) - |S|)^2 \right] = \left[ \mathbb{E}[2X(S)] - |S| \right]^2 + \text{Var}[2X(S)].
\]
If \(X\) is the uniform independent coloring of points, and so has kernel \(I/2\) (which is not a projection), the first summand on the right-hand side will be zero. Moreover, for a deterministic coloring \(X\) the second summand vanishes. Lemma 10 indicates that the quantum discrepancy of a set system is small, if there exists a determinantal projection process on the ground set that makes both summands small enough for each member of that set system.

Note that the set of orthogonal projections in \(\mathbb{C}^N\) is the set of extreme points of the convex set of positive semi-definite elements of \(\mathcal{M}_N(\mathbb{C})\) with eigenvalues in \([0, 1]\). In other words, according to Proposition 9, kernels of all determinantal projection processes constitute the extreme points of the set of kernels of all determinantal processes with a Hermitian kernel. This makes a similarity between the set of (combinatorial) colorings and quantum colorings. Each coloring of \([N]\) can be assigned uniquely to an \(N\)-tuple of 0s and 1s which determines its distribution: the \(i\)-th coordinate shows the probability of coloring the element \(i\) red. These tuples are extreme points of the unit cube \([0, 1]^N\) which can be viewed as the set of laws of all methods for coloring points of \([N]\) independently:
in \((p_1, p_2, \ldots, p_N) \in [0, 1]^N\), \(p_i\) is the chance of \(i\) to be colored red. Moreover, just as the number of red points in each coloring is fixed, it can be shown that determinantal projection processes are exactly those determinantal processes with Hermitian kernels that have a fixed number of points (see the second part of Proposition 24 which is a part of Theorem 4.5.3 in [8]).

### 2.2 A Measure of Non-Commutativity

It is explained in Subsection 1.1 that the term \(\text{tr}(\chi|\chi, P|P)\) encodes the non-commutative nature of quantum discrepancy. The following lemma provides an algebraically simple relation between \(\text{tr}(\chi|\chi, P|P)\) and the commutator of \(\chi\) and \(P\), which illustrates the existing non-commutativity more explicitly.

**Lemma 12.** Suppose \(P\) and \(\chi\) are an orthogonal projection and a quantum coloring, respectively. Then,

\[
\text{tr}(\chi|\chi, P|P) = \frac{1}{2} \|\chi, P\|_2^2.
\]

**Proof.** The following calculation results in what we want.

\[
\|\chi, P\|_2^2 = \text{tr}([\chi, P]^*[\chi, P])
= \text{tr}((P\chi - \chi P)(\chi P - P\chi))
= \text{tr}(P\chi^2 P - (P\chi)^2 - (\chi P)^2 + \chi P^2 \chi)
= 2\text{tr}\left(\chi^2 P^2 - (\chi P)^2\right) \quad \text{(trace is cyclic)}
= 2\text{tr}(\chi(\chi P - P\chi)P)
= 2\text{tr}(\chi|\chi, P|P).
\]

**Corollary 13.** Suppose \(\mathcal{P}\) is a projection system in \(\mathbb{C}^N\). Then,

\[
\text{QDisc}(\mathcal{P}) = \min_{\chi} \max_{P \in \mathcal{P}} \left[\text{tr}^2(\chi P) + \frac{1}{2} \|\chi, P\|_2^2\right]^{1/2},
\]

where the minimum is taken over the set of quantum colorings.

Now, quantum discrepancy can be interpreted more simply. As mentioned in Subsection 1.1, for a diagonal projection \(P_S\) and a diagonal coloring \(\chi\), \(\text{tr}(\chi P_S) = \chi(S)\). Therefore, the term \(|\text{tr}(\chi P)|\) is common between the two kinds of discrepancies. The additional term, \(\frac{1}{2} \|\chi, P\|_2^2\), appears as a measure of the non-commutativity arisen as the result of replacing a (diagonal) coloring and a set with a quantum coloring and an orthogonal projection, respectively.

**Remark 14.** The specific combination of \(|\text{tr}(\chi P)|\) and \(\|\chi, P\|_2\) used to define quantum discrepancy, i.e. \(\left[\text{tr}^2(\chi P) + \frac{1}{2} \|\chi, P\|_2^2\right]^{1/2}\), has the advantage of having a probabilistic interpretation as explained in the previous subsection. However, since

\[
\frac{a + b}{\sqrt{3}} \leq \sqrt{a^2 + \frac{1}{2} b^2} \leq a + b, \quad \text{for all } a, b \geq 0,
\]

\[\text{QDisc}(\mathcal{P}) = \min_{\chi} \max_{P \in \mathcal{P}} \left[\text{tr}^2(\chi P) + \frac{1}{2} \|\chi, P\|_2^2\right]^{1/2},\]

where the minimum is taken over the set of quantum colorings.
QDisc(\(P\)) is essentially the same quantity as the simpler and possibly more intuitive formulation \(\min_\chi\max_{P \in \mathcal{P}} \left[ |\text{tr}(\chi P)| + \|\chi, P\|_2 \right]\).

### 3 General Upper Bounds

For a set \(S \subseteq [N]\) and a determinantal process \(\mathcal{X}\), we have \(|2\mathcal{X}(S) - |S|| \leq N\). Hence, QDisc(\(P_S\)) \(\leq N\) for each set system \(S\). Theorem 2 states that this bound also holds for an arbitrary projection system.

**Proof of Theorem 2.** We show that if \(\chi, P \in \mathcal{M}_N(\mathbb{C})\) are a quantum coloring and an orthogonal projection, respectively, then

\[
\text{tr}^2(\chi P) + \text{tr}(\chi[\chi,P]P) \leq N^2,
\]

and this results in what we want. According to the properties of \(\chi\) and \(P\),

\[
\text{tr}(\chi[\chi,P]P) = \text{tr}(P - (\chi P)^2) .
\]

Therefore, we show that

\[
\text{tr}^2(\chi P) + \text{tr}(P - (\chi P)^2) \leq N^2.
\]

Because of the cyclic property of the trace function, it is enough to prove this inequality for a diagonal \(\chi\). To be more precise, consider a spectral decomposition of \(\chi\), i.e. a representation such as \(\chi = UDU^*,\) where \(D\) is diagonal and \(U\) is unitary. Then, for instance, \(\text{tr}(\chi P) = \text{tr}(D(U^*PU))\), and \(U^*PU\) is an orthogonal projection.

By computing diagonal entries of \(\chi P\) and \((\chi P)^2\) it can be shown that

\[
\text{tr}^2(\chi P) - \text{tr}(\chi(\chi P)^2) = 2 \sum_{1 \leq i < j \leq N} \left[ \chi_{ii} \chi_{jj} (P_{ii}P_{jj} - |P_{ij}|^2) \right] .
\]

The orthogonal projection \(P\) is positive semi-definite and its operator norm is equal to 1. Hence, \(P_{ii}P_{jj} - |P_{ij}|^2\) is in \([0,1]\). Diagonal entries of \(\chi\) are \(-1\) or \(1\), and we conclude that

\[
\text{tr}^2(\chi P) - \text{tr}(\chi(\chi P)^2) \leq 2 \sum_{1 \leq i < j \leq N} 1 = N^2 - N.
\]

At last, \(\text{tr}^2(\chi P) + \text{tr}(P - (\chi P)^2) \leq N^2 - N + N = N^2\).

**Remark 15.** With a similar method, the bound given in Theorem 2 can be improved. In fact, it holds that

\[
\text{QDisc}(\mathcal{P}) \leq \max_{P \in \mathcal{P}} \text{rank}(P),
\]

which results in \(\text{QDisc}(\mathcal{P}) \leq N\).
3.1 Proof of Theorem 3

Instead of proving Theorem 3 directly, we prove Theorem 17 which results in the former. Our approach to give an upper bound for the quantum discrepancy of a general projection system \( P \) in \( \mathbb{C}^N \) is to investigate the random variable \( \left[ \text{tr}^2(\chi P) + \text{tr} (\chi [\chi, P]) \right]^{1/2} \), where \( \chi \) is a random quantum coloring with a certain distribution (Definition 16) and \( P \in \mathcal{P} \). For more convenience we name this random variable \( \chi(P) \). As mentioned before,

\[
\chi(P) = \left[ \text{tr}^2(\chi P) + \text{tr} (P - (\chi P)^2) \right]^{1/2}.
\]  

(14)

Definition 16. By a random balanced quantum coloring we mean a random matrix \( \chi = UDU^* \), where \( U \) has Haar distribution on the group of \( N \times N \) unitary matrices, \( \text{U}(N) \), and

\[
D := \begin{bmatrix}
I_{\left\lfloor \frac{N}{2} \right\rfloor} & 0 \\
0 & -I_{\left\lceil \frac{N}{2} \right\rceil}
\end{bmatrix}.
\]

Theorem 17 (Quantum Random Coloring). Suppose \( P \) is an \( M \)-element projection system in \( \mathbb{C}^N \). There exists a constant \( c > 0 \), independent of \( N, M \) and \( P \), such that for

\[
\Delta_P := \sqrt{2} \left[ \sqrt{\frac{1}{c} \log(8M)} + \frac{N^2}{N^2 - 1} \text{rank}(P) - \frac{N}{N^2 - 1} \text{rank}^2(P) + \frac{\text{rank}(P)}{N} \right],
\]

and for large enough values of \( N \), the probability that a random balanced quantum coloring \( \chi \) satisfies simultaneously all inequalities

\[
\chi(P) \leq \Delta_P, \quad P \in \mathcal{P}
\]

is at least \( 1/2 \). In particular, \( \text{QDisc}(\mathcal{P}) = O(\sqrt{N + \log M}) \).

Proof of this theorem is mainly based on the concentration of \( \text{tr}(\chi P) \) and \( \text{tr}(P - (\chi P)^2) \) around their means. We will use the following proposition which is the same as Corollary 4.4.31 in [2] but in our words.

Proposition 18. Assume we are given deterministic matrices \( X_1, \ldots, X_k \in \mathcal{M}_N(\mathbb{C}) \) and a constant \( \sigma \) that controls all singular values of these matrices from above. Let \( p := p(x_1, x_2, \ldots, x_{k+2}) \) be a polynomial of \( k + 2 \) non-commutative variables with complex coefficients. For \( X \in \text{U}(N) \) define \( f(X) = \text{tr} \left( p(X, X^*, X_1, X_2, \ldots, X_k) \right) \). Then, there are positive constants \( N_0 = N_0(p) \) and \( c = c(p, \sigma) \) such that for any \( \delta > 0 \) and \( N > N_0 \),

\[
\mathbb{P} \left[ |f(X) - \mathbb{E}[f(X)]| \geq \delta N \right] \leq 2 \exp \left(-cN^2 \delta^2 \right),
\]

in which, \( \mathbb{P} \) is the unique Haar probability measure on \( \text{U}(N) \) and \( \mathbb{E}[\cdot] \) is the expected value with respect to \( \mathbb{P} \).

Another component of the proof is estimating \( \mathbb{E} \left[ \text{tr}(\chi P) \right] \) and \( \mathbb{E} \left[ \text{tr}(P - (\chi P)^2) \right] \).
Lemma 19. If $\chi$ is a random balanced quantum coloring, and $P$ is an orthogonal projection in $\mathbb{C}^N$, then
\[
\left| \mathbb{E} [\text{tr}(\chi P)] \right| \leq \frac{\text{rank}(P)}{N}, \tag{15}
\]
\[
\mathbb{E} \left[ \text{tr} \left( P - (\chi P)^2 \right) \right] \leq \frac{N^2}{N^2 - 1} \text{rank}(P) - \frac{N}{N^2 - 1} \text{rank}^2(P). \tag{16}
\]

Proof. We compute exact values of $\mathbb{E} [\text{tr}(\chi P)]$ and $\mathbb{E} \left[ \text{tr} \left( P - (\chi P)^2 \right) \right]$. According to the distribution of $\chi$, we assume, without loss of generality, that $P$ is diagonal. More precisely, if $V$ and $\Pi$ are respectively a unitary and a diagonal matrix such that $P = V \Pi V^*$ is a spectral decomposition of $P$, then by the cyclic property of the trace function\[
\text{tr}(\chi P) = \text{tr}(UDU^*V\Pi V^*) = \text{tr} \left( (V^*U)D(V^*U)^*\Pi \right) .
\]
Haar measure is invariant under left multiplication by a unitary matrix, so $(V^*U)D(V^*U)^*$ has the same distribution as $\chi$.

$\mathbb{E} [\text{tr}(\chi P)]$:
\[
(\chi P)_{ii} = \sum_{j=1}^{N} U_{ij} D_{jj} U_{ij} P_{ii} . \tag{D, P are diagonal}
\]
Thus, $\mathbb{E} [(\chi P)_{ii}] = \sum_{j=1}^{N} \mathbb{E} [U_{ij}^2] D_{jj} P_{ii}$. Since Haar measure is invariant under left and right multiplication by a unitary matrix, all entries of $U$ are identically distributed. As a result, $\mathbb{E} [U_{ij}^2] = 1/N$. Therefore,
\[
\mathbb{E} \left[ \text{tr}(\chi P) \right] = \sum_{ij} \frac{1}{N} D_{jj} P_{ii} = \frac{1}{N} \text{tr}(D) \text{tr}(P) = \begin{cases} 0, & \text{even } N \\ \frac{\text{rank}(P)}{N}, & \text{odd } N \end{cases} .
\]

Now, (15) is clear.

$\mathbb{E} \left[ \text{tr} \left( P - (\chi P)^2 \right) \right]$:
According to Lemma 12, and (13), it holds that $\text{tr}(P - (\chi P)^2) = \frac{1}{2} \| [\chi, P] \|_2^2$. Therefore, $\text{tr}(P - (\chi P)^2) = \frac{1}{2} \sum_{i,j} |([\chi, P])_{ij}|^2$. We have
\[
([\chi, P])_{ij} = \chi_{ij} (P_{jj} - P_{ii}) = \begin{cases} \chi_{ij}, & P_{ii} = 0, P_{jj} = 1 \\ -\chi_{ij}, & P_{ii} = 1, P_{jj} = 0 \\ 0, & \text{otherwise} \end{cases} .\]

Therefore, $\| [\chi, P] \|_2^2 = 2 \sum_{i,j:P_{ii}=1,P_{jj}=1} |\chi_{ij}|^2$. We compute $|\chi_{ij}|^2$.
\[
|\chi_{ij}|^2 = \chi_{ij} \cdot \overline{\chi}_{ij} = \sum_{k=1}^{N} U_{ik} D_{kk} U_{jk} \cdot \sum_{l=1}^{N} \overline{U}_{il} D_{ll} U_{jl} \tag{D is diagonal}
\]

THE ELECTRONIC JOURNAL OF COMBINATORICS 27(2) (2020), #P2.19 13
\[
= \sum_{k,l} U_{ik} U_{jl} U_{il} U_{jk} D_{kk} D_{ll}.
\]

Using Proposition 4.2.3 in [6], we know that for \(i \neq j\):

\[
\mathbb{E}[U_{ik} U_{jl} U_{il} U_{jk}] = \begin{cases} 
\mathbb{E}[|U_{ik}|^2 |U_{jk}|^2], & k = l \\
\mathbb{E}[U_{ik} U_{jl} U_{il} U_{jk}], & k \neq l \\
\frac{1}{N(N + 1)}, & k = l \\
-\frac{1}{N(N^2 - 1)}, & k \neq l
\end{cases}
\]

Therefore,

\[
\mathbb{E}[|\chi_{ij}|^2] = \sum_{k=1}^{N} \frac{1}{N(N + 1)} D_{kk}^2 - \sum_{k \neq l} \frac{1}{N(N^2 - 1)} D_{kk} D_{ll}
\]

\[
= \sum_{k=1}^{N} \frac{1}{N(N + 1)} - \frac{1}{N(N^2 - 1)} \sum_{k \neq l} D_{kk} D_{ll} 
= \frac{1}{N + 1} - \frac{1}{N(N^2 - 1)} (\text{tr}^2(D) - N)
\]

\[
= \begin{cases} 
\frac{N}{N^2 - 1}, & \text{even } N \\
\frac{1}{N}, & \text{odd } N
\end{cases}
\]

We obtain

\[
\mathbb{E}[\text{tr} \left( P - (\chi P)^2 \right)] = \frac{1}{2} \mathbb{E}[\|\chi, P\|_2^2]
\]

\[
= \sum_{i,j: P_{ii}=1, P_{jj}=0} \mathbb{E}[|\chi_{ij}|^2]
\]

\[
= \begin{cases} 
\frac{N}{N^2 - 1} \cdot \sum_{i,j: P_{ii}=1, P_{jj}=0} 1, & \text{even } N \\
\frac{1}{N} \cdot \sum_{i,j: P_{ii}=1, P_{jj}=0} 1, & \text{odd } N
\end{cases}
\]

\[
= \begin{cases} 
\frac{N}{N^2 - 1} \cdot \text{rank}(P)(N - \text{rank}(P)), & \text{even } N \\
\frac{1}{N} \cdot \text{rank}(P)(N - \text{rank}(P)), & \text{odd } N
\end{cases}
\]
\[
\leq \frac{N}{N^2 - 1} \cdot \text{rank}(P)(N - \text{rank}(P)) \tag{N \geq 2}
\]
\[
= \frac{N^2}{N^2 - 1} \text{rank}(P) - \frac{N}{N^2 - 1} \text{rank}^2(P).
\]

Hence, (16) holds.

**Proof of Theorem 17.** For any \( P \in \mathcal{P} \),
\[
\mathbb{P}[\chi(P) > \Delta_P] = \mathbb{P}[\text{tr}^2(\chi P) + \text{tr}(P - (\chi P)^2) > \Delta_P^2] 
\leq \mathbb{P}\left[\left|\text{tr}(\chi P)\right| > \frac{\Delta_P}{\sqrt{2}}\right] + \mathbb{P}\left[\text{tr}(P - (\chi P)^2) > \frac{\Delta_P^2}{2}\right]. \tag{17}
\]

We show that for each \( P \in \mathcal{P} \), both \( \mathbb{P}\left[\left|\text{tr}(\chi P)\right| > \Delta_P \sqrt{2}\right] \) and \( \mathbb{P}\left[\text{tr}(P - (\chi P)^2) > \Delta_P^2 / 2\right] \) are at most \( 1/(4M) \). Then, because of (17) we obtain
\[
\mathbb{P}\left[\bigcap_{P \in \mathcal{P}} \{\chi(P) \leq \Delta_P\} \right] = 1 - \mathbb{P}\left[\bigcup_{P \in \mathcal{P}} \{\chi(P) > \Delta_P\} \right] 
\geq 1 - \sum_{P \in \mathcal{P}} \mathbb{P}[\chi(P) > \Delta_P] \quad \text{(the union bound)}
\geq 1 - M \frac{1}{2M} = \frac{1}{2},
\]
which is the first claim of the theorem.

If we put \( p_1(x_1, x_2, x_3, x_4) = x_1 x_3 x_2 x_4 \) and \( p_2(x_1, x_2, x_3, x_4) = x_4 - (x_1 x_3 x_2 x_4)^2 \), then for a random balanced quantum coloring \( \chi = UDU^* \),
\[
f_1(U) := \text{tr}(p_1(U, U^*, D, P)) = \text{tr}(\chi P),
\]
\[
f_2(U) := \text{tr}(p_1(U, U^*, D, P)) = \text{tr}(P - (\chi P)^2).
\]

Since the singular values of \( D \), and each \( P \) are at most 1, by Proposition 18 we have positive constants \( c_1 = c_1(p_1) \), \( c_2 = c_2(p_2) \) and a natural number \( N_0 \) such that for any \( N > N_0 \), \( \delta > 0 \), and \( P \in \mathcal{P} \)
\[
\mathbb{P}\left[\left|\text{tr}(\chi P) - \mathbb{E}[\text{tr}(\chi P)]\right| > \delta N\right] \leq 2 \exp\left(-c_1 N^2 \delta^2\right), \tag{18}
\]
\[
\mathbb{P}\left[\left|\text{tr}(P - (\chi P)^2) - \mathbb{E}[\text{tr}(P - (\chi P)^2)]\right| > \delta N\right] \leq 2 \exp\left(-c_2 N^2 \delta^2\right). \tag{19}
\]

Let \( c = \min(c_1, c_2) \). Since the function \( x \mapsto \exp(-x) \) is decreasing, \( c_1 \), \( c_2 \), and so \( c \) are assumed, without loss of generality, to be in the interval \( (0, 1] \).

\[
\mathbb{P}\left[\left|\text{tr}(\chi P)\right| > \frac{\Delta_P}{\sqrt{2}}\right] \leq \frac{1}{4M}.
\]
Note that $\frac{N^2}{N^2 - 1} \text{rank}(P) - \frac{N}{N^2 - 1} \text{rank}^2(P) \geq 0.

$$
\mathbb{P}\left[|\text{tr}(\chi P)| > \frac{\Delta_P}{\sqrt{2}}\right] \leq \mathbb{P}\left[|\text{tr}(\chi P)| > \sqrt{\frac{1}{c} \log(8M) + \frac{\text{rank}(P)}{N}}\right]
\leq \mathbb{P}\left[|\text{tr}(\chi P)| - \frac{\text{rank}(P)}{N} > \sqrt{\frac{1}{c_1} \log(8M)}\right] \quad (c \leq c_1)
\leq \mathbb{P}\left[|\text{tr}(\chi P)| - |\mathbb{E}[\text{tr}(\chi P)]| > \sqrt{\frac{1}{c_1} \log(8M)}\right] \quad (\text{by (15)})
\leq \mathbb{P}\left[|\text{tr}(\chi P) - \mathbb{E}[\text{tr}(\chi P)]| > \sqrt{\frac{1}{c_1} \log(8M)}\right]
\leq 2 \exp\left[-\log(8M)\right] \quad (\text{for large values of } N, \text{ by (18)})
= \frac{1}{4M}.
$$

$$
\mathbb{P}\left[\text{tr}(P - (\chi P)^2) > \frac{\Delta_P^2}{2}\right] \leq \frac{1}{4M}:
$$

$$
\mathbb{P}\left[\text{tr}(P - (\chi P)^2) > \frac{\Delta_P^2}{2}\right]
\leq \mathbb{P}\left[\text{tr}(P - (\chi P)^2) > \frac{1}{c} \log(8M) + \frac{N^2}{N^2 - 1} \text{rank}(P) - \frac{N}{N^2 - 1} \text{rank}^2(P)\right]
\leq \mathbb{P}\left[\text{tr}(P - (\chi P)^2) - \mathbb{E}[\text{tr}(P - (\chi P)^2)] > \frac{1}{c_2} \log(8M)\right] \quad (c \leq c_2, (16))
\leq \mathbb{P}\left[|\text{tr}(P - (\chi P)^2) - \mathbb{E}[\text{tr}(P - (\chi P)^2)]| > \sqrt{\frac{1}{c_2} \log(8M)}\right] \quad (c_2 \leq 1)
\leq \frac{1}{4M} \quad (\text{by (19)})
$$

To prove the second claim, note that for large values of $N$, $\mathbb{P}\left[\bigcap_{P \in \mathcal{P}} \{\chi(P) \leq \Delta_P\} \right] > 0$, so there exists a realization $\tilde{\chi}$ of $\chi$ for which

$$
\max_{P \in \mathcal{P}} \tilde{\chi}(P) \leq \max_{P \in \mathcal{P}} \Delta_P,
$$

and thus, $Q\text{Disc}(\mathcal{P}) \leq \max_{P \in \mathcal{P}} \Delta_P$. Moreover, since $0 \leq \text{rank}(P) \leq N$, for every $P \in \mathcal{P}$,

$$
\Delta_P \leq \sqrt{2} \left[\sqrt{\frac{1}{c} \log(8M) + \frac{N^3}{N^2 - 1} + 1}\right]
\leq \sqrt{2} \left[\sqrt{\frac{1}{c} \log(8M) + N + 1}\right]. \quad (N \geq 2)
$$

Hence, $Q\text{Disc}(P) = O(\sqrt{N + \log M})$. \hfill \Box
3.2 Proof of Theorem 4

A probabilistic proof of Theorem 4 is given in this subsection. It is based on the behavior of a random projection system. Note that for \( \Pi := \begin{bmatrix} I_{[N/2]} & 0 \\ 0 & 0 \end{bmatrix} \in M_N(\mathbb{C}) \), and a Haar-distributed random element \( U \) of \( U(N) \), the random matrix \( P := U\Pi U^* \) is a random orthogonal projection. In fact, \( P \) is the orthogonal projection onto a random subspace of dimension \( \lfloor N/2 \rfloor \) in \( \mathbb{C}^N \). In this subsection we assume that \( P = \{P_1, \ldots, P_M \} \), where for each \( i \), \( P_i = U_i\Pi U_i^* \) and \( \{U_1, \ldots, U_M \} \) is an independent set of Haar-distributed random elements of \( U(N) \). Moreover, we suppose that \( M \) and \( N \) satisfy the conditions of Theorem 4, i.e. for some \( a, b > 0 \)

\[
aN \leq M, \quad \log M \leq bN. \tag{20}
\]

To prove the theorem, it suffices to show that there exists a constant \( c = c(b) > 0 \) for which

\[
\mathbb{P} \left[ \text{QDisc}(P) \leq c\sqrt{N + \log M} \right] < 1. \tag{21}
\]

Note that for the \( \chi(P) \) given by (14) and any \( c > 0 \),

\[
\mathbb{P} \left[ \text{QDisc}(P) \leq c\sqrt{N + \log M} \right] = \mathbb{P} \left[ \min_{\chi} \max_{P \in \mathcal{P}} \chi(P) \leq c\sqrt{N + \log M} \right] \\
\leq \mathbb{P} \left[ \bigcup_{\chi} \left( \max_{P \in \mathcal{P}} \chi(P) \leq c\sqrt{N + \log M} \right) \right].
\]

If the number of quantum colorings were finite and not too large, using the union bound together with Proposition 18 could be helpful to obtain (21). Although the set of quantum colorings is uncountable, the same idea can be applied in an indirect way. The method is borrowed from Subsection 2.3.1 of [15]. There, an upper bound for the operator norm of a certain family of random matrices is provided using this technique, which is named the epsilon-net argument. The following lemma provides a way to go from the uncountable set of quantum colorings to an appropriate finite subset.

**Lemma 20.** Suppose \( C \subseteq \mathbb{R}^d \) is compact. For any \( \epsilon > 0 \), there exists a finite set \( \Sigma^{(\epsilon)} \subseteq C \) so that for each \( L \)-Lipschitz function \( \varphi : C \to \mathbb{R} \), and \( \Delta \in \mathbb{R} \), if \( \min_{x \in C} \varphi(x) \leq \Delta \), then \( \min_{x \in \Sigma^{(\epsilon)}} \varphi(x) \leq \Delta + \epsilon L \).

**Proof.** Set \( \Sigma^{(\epsilon)} \) to be an \( \epsilon \)-net in \( C \), that is a maximal subset of \( C \) with the property that the distance between each two distinct points is more than \( \epsilon \).

To see that \( \Sigma^{(\epsilon)} \) is finite, suppose \( B(x, r) \) and \( \bar{B}(x, r) \) are open and closed balls with radius \( r > 0 \) and center \( x \in \mathbb{R}^d \), respectively. By compactness, \( C \) is included in \( B(O, r) \) for some \( r > 0 \) (\( O \) is the origin). For any two distinct \( x, y \in \Sigma^{(\epsilon)} \), \( \bar{B}(x, \epsilon/2) \) and \( \bar{B}(y, \epsilon/2) \) are disjoint. Also, each of them is included in \( \bar{B}(O, r + \epsilon/2) \). Thus,

\[
\sum_{x \in \Sigma^{(\epsilon)}} \text{vol}(\bar{B}(x, \epsilon/2)) = \text{vol}(\bigcup_{x \in \Sigma^{(\epsilon)}} \bar{B}(x, \epsilon/2)) \leq \text{vol}(\bar{B}(O, r + \epsilon/2)).
\]
Hence,
\[ \left| \Sigma^{(e)} \right| \leq \frac{\text{vol}(\mathcal{B}(O, r + \frac{\epsilon}{2}))}{\text{vol}(\mathcal{B}(O, \frac{\epsilon}{2}))} = \left( \frac{r + \frac{\epsilon}{2}}{\frac{\epsilon}{2}} \right)^d = \left( \frac{2r + \epsilon}{\epsilon} \right)^d < \infty. \]

For a function \( \varphi \) satisfying the given conditions, if \( \min_{x \in C} \varphi(x) \leq \Delta \), there is some \( x_0 \in C \) such that \( \varphi(x_0) \leq \Delta \). Because of maximality of \( \Sigma^{(e)} \), \( \|x_1 - x_0\| \leq \epsilon \) for at least one point \( x_1 \in \Sigma^{(e)} \). By the Lipschitz property,
\[ \varphi(x_1) - \varphi(x_0) \leq |\varphi(x_1) - \varphi(x_0)| \leq L \|x_1 - x_0\|. \]

Thus, \( \varphi(x_1) \leq \Delta + \epsilon L \), and hence \( \min_{x \in \Sigma^{(e)}} \varphi(x) \leq \Delta + \epsilon L \). \( \square \)

**Corollary 21.** Suppose \( Y \) is a random object and the random function \( \varphi(x, Y) \) has the property that for any realization \( y \) of \( Y \) its value, \( \varphi(x; y) \), is an \( L \)-Lipschitz real-valued function on a compact set \( C \). Then, for any \( \Delta, \epsilon > 0 \)
\[ P \left[ \min_{x \in C} \varphi(x, Y) \leq \Delta \right] \leq \sum_{x \in \Sigma^{(e)}} P[\varphi(x, Y) \leq \Delta + \epsilon L]. \]  
\[ (22) \]

**Proof.** By Lemma 20, the same \( \Sigma^{(e)} \) works for each \( L \)-Lipschitz function \( \varphi(x; y) \). Moreover, for any realization \( y \) of \( Y \), if \( \min_{x \in C} \varphi(x; y) \leq \Delta \), then \( \min_{x \in \Sigma^{(e)}} \varphi(x; y) \leq \Delta + \epsilon L \). Hence,
\[ P \left[ \min_{x \in C} \varphi(x, Y) \leq \Delta \right] \leq P \left[ \min_{x \in \Sigma^{(e)}} \varphi(x, Y) \leq \Delta + \epsilon L \right] \]
\[ = P \left[ \bigcup_{x \in \Sigma^{(e)}} \{ \varphi(x, Y) \leq \Delta + \epsilon L \} \right] \]
\[ \leq \sum_{x \in \Sigma^{(e)}} P[\varphi(x, Y) \leq \Delta + \epsilon L]. \] (the union bound) \( \square \)

Note that appropriate upper bounds on the size of \( \Sigma^{(e)} \), and values of the summands on the right-hand side of (22), would result in controlling the probability of the event \( \min_{x \in C} \varphi(x, Y) \leq \Delta \).

To verify the Lipschitz property of the functions within the proof, a matrix version of Hölder inequality will be used.

**Proposition 22** (Tracial Hölder Inequality). For \( P, Q \in \mathcal{M}_N(\mathbb{C}) \) and \( 1 \leq p, q \leq \infty \) with the property that \( 1/p + 1/q = 1 \),
\[ |\text{tr}(P^*Q)| \leq \|P\|_p \|Q\|_q. \]  
(23)

Here, \( \|\cdot\|_p \) is the Schatten \( p \)-norm which is defined for \( 1 \leq p \leq \infty \) and \( P \in \mathcal{M}_N(\mathbb{C}) \) with singular values \( \sigma_1 \leq \sigma_2 \leq \cdots \leq \sigma_N \) as
\[ \|P\|_p = \left[ \sum_i \sigma_i^p \right]^{1/p} \text{ for } 1 \leq p < \infty, \quad \|P\|_\infty = \sigma_N. \]
This inequality proved in [3] is due to Carlen.

**Proof of Theorem 4.** Suppose \( c > 0 \) and set \( C \subseteq \mathcal{M}_N(\mathbb{C}) \) to be the set of quantum colorings. Put

\[
C_1 = \{ \chi \in C : |\text{tr}(\chi)| > \sqrt{N} \log N \} , \quad C_2 = \{ \chi \in C : |\text{tr}(\chi)| \leq \sqrt{N} \log N \} .
\]

Then,

\[
\mathbb{P} \left[ \text{QDisc}(\mathcal{P}) \leq c\sqrt{N + \log M} \right] = \mathbb{P} \left[ \min_{\chi} \max_{P \in \mathcal{P}} \left[ |\text{tr}^2(\chi P) + \text{tr}(P - (\chi P)^2)| \leq c^2(N + \log M) \right] \right]
\]

\[
\leq \mathbb{P} \left[ \min_{\chi \in C_1} \max_{P \in \mathcal{P}} \left[ |\text{tr}^2(\chi P) + \text{tr}(P - (\chi P)^2)| \leq c^2(N + \log M) \right] \right] + \mathbb{P} \left[ \min_{\chi \in C_2} \max_{P \in \mathcal{P}} \left[ |\text{tr}^2(\chi P) + \text{tr}(P - (\chi P)^2)| \leq c^2(N + \log M) \right] \right] .
\]

Because of the non-negativity of \( \text{tr}^2(\chi P) \) and \( \text{tr}(P - (\chi P)^2) \),

\[
\mathbb{P} \left[ \text{QDisc}(\mathcal{P}) \leq c\sqrt{N + \log M} \right] \leq \mathbb{P} \left[ \min_{\chi \in C_1} \max_{P \in \mathcal{P}} |\text{tr}(\chi P)| \leq c\sqrt{N + \log M} \right] + \mathbb{P} \left[ \min_{\chi \in C_2} \max_{P \in \mathcal{P}} \text{tr}(P - (\chi P)^2) \leq c^2(N + \log M) \right] .
\]

It is enough to prove the existence of a constant \( c > 0 \) which depends only on \( b \), given in (20), and satisfies the following inequalities for all but a finite set of values of \((M, N)\).

\[
\mathbb{P} \left[ \min_{\chi \in C_1} \max_{P \in \mathcal{P}} |\text{tr}(\chi P)| \leq c\sqrt{N + \log M} \right] < \frac{1}{2} ,
\]

\[
\mathbb{P} \left[ \min_{\chi \in C_2} \max_{P \in \mathcal{P}} \text{tr}(P - (\chi P)^2) \leq c^2(N + \log M) \right] < \frac{1}{2} .
\]

To achieve this goal the epsilon-net argument will be applied twice. To be permitted to make use of Lemma 20, the compactness and Lipschitz properties must be checked.

The space \((\mathcal{M}_N(\mathbb{C}), \|\cdot\|_2)\) is isomorphic to \((\mathbb{R}^{N^2}, \|\cdot\|_2)\) as a normed vector space. The subset of Hermitian matrices, \( \mathcal{H}_N \), is actually an \( N^2 \)-dimensional subspace of \( \mathcal{M}_N(\mathbb{C}) \), and so a Euclidean metric space. Eigenvalues of a matrix are continuous functions of its entries. Moreover, \( \|\chi\|_2 = \sqrt{N} \) and \( \text{tr}(\chi) \in \{\pm 1, \pm 2, \ldots, \pm N\} \) for each \( \chi \in C \). Hence, \( C_1 \) and \( C_2 \) are compact sets in \( \mathcal{H}_N \).

The maximum of a family of \( L \)-Lipschitz functions is again \( L \)-Lipschitz. Hence, according to Corollary 21, it suffices to verify the Lipschitz property of the functions \(|\text{tr}(\chi P)|\) and \( \text{tr}(\bar{P} - (\chi \bar{P})^2) \) for \( \bar{P} \), a realization of \( P \in \mathcal{P} \).

\[
|\text{tr}(\chi_1 \bar{P})| - |\text{tr}(\chi_2 \bar{P})| \leq |\text{tr}(\chi_1 - \chi_2) \bar{P}|\]

\[
\]
\[
\begin{align*}
\|\hat{P}\|_2 & \leq \|x_1 - x_2\|_2 & \text{(by (23))} \\
\leq \sqrt{\frac{N}{2}} \|x_1 - x_2\|_2. & \quad \text{(rank}(\hat{P}) = \lfloor \frac{N}{2} \rfloor) \\
\end{align*}
\]

Hence, for any realization $\hat{P}$ of $P$, $\varphi_1(\chi; \hat{P}) := \max_{\hat{P} \in \mathcal{P}} |\text{tr}(\chi\hat{P})|$ is $\sqrt{N}/2$-Lipschitz on $C_1$. On the other hand, since $\|\hat{P}\|_\infty = 1$, and $\|x_1\|_1 = \|x_2\|_1 = N$,

\[
\begin{align*}
\left|\text{tr}(\hat{P} - (\chi_1 \hat{P})^2) - \text{tr}(\hat{P} - (\chi_2 \hat{P})^2)\right| &= \left|\text{tr}(\chi_2 \hat{P}x_2 \hat{P} - x_2 \hat{P}x_1 \hat{P} + \chi_2 \hat{P}x_1 \hat{P} - x_1 \hat{P}x_1 \hat{P})\right| \\
&= \left|\text{tr}[(x_2 + x_1)\hat{P}(x_2 - x_1)\hat{P}]\right| \\
&\leq \|\hat{P}(x_2 - x_1)\hat{P}\|_\infty \|x_2 + x_1\|_1 & \text{(by (23))} \\
&\leq \|\hat{P}\|_\infty^2 \|x_2 - x_1\|_\infty \left(\|x_1\|_1 + \|x_2\|_1\right) \\
&\leq 2N \|x_2 - x_1\|_\infty. 
\end{align*}
\]

Therefore, for each realization $\hat{P}$, the function $\varphi_2(\chi; \hat{P}) := \max_{\hat{P} \in \mathcal{P}} \text{tr}(\hat{P} - (\chi \hat{P})^2)$ is $2N$-Lipschitz on $C_2$.

We conclude that for any $\epsilon > 0$ there are (finite) $\epsilon$-nets $\Sigma_1^{(\epsilon)} \subseteq C_1$ and $\Sigma_2^{(\epsilon)} \subseteq C_2$ such that

\[
\begin{align*}
\mathbb{P} \left[\min_{\chi \in C_1} \max_{P \in \mathcal{P}} |\text{tr}(\chi P)| \leq c\sqrt{N + \log M}\right] \\
&\leq \mathbb{P} \left[\min_{\chi \in \Sigma_1^{(\epsilon)}} \max_{P \in \mathcal{P}} |\text{tr}(\chi P)| \leq c\sqrt{N + \log M} + c\sqrt{\frac{N}{2}}\right] \\
&\leq \sum_{\chi \in \Sigma_1^{(\epsilon)}} \mathbb{P} \left[\max_{P \in \mathcal{P}} |\text{tr}(\chi P)| \leq c\sqrt{N + \log M} + c\sqrt{\frac{N}{2}}\right], \quad (24)
\end{align*}
\]

and

\[
\begin{align*}
\mathbb{P} \left[\min_{\chi \in C_2} \max_{P \in \mathcal{P}} \text{tr}(P - (\chi P)^2) \leq c^2(N + \log M)\right] \\
&\leq \sum_{\chi \in \Sigma_2^{(\epsilon)}} \mathbb{P} \left[\max_{P \in \mathcal{P}} \text{tr}(P - (\chi P)^2) \leq c^2(N + \log M) + 2\epsilon N\right]. \quad (25)
\end{align*}
\]

We make two observations. First suppose $0 < \epsilon \leq 1$. According to the proof of Lemma 20, and since for every quantum coloring $\chi$, $\|\chi\|_2 = \sqrt{N}$,

\[
|\Sigma_1^{(\epsilon)}|, |\Sigma_2^{(\epsilon)}| \leq \left(\frac{2\sqrt{N} + \epsilon}{\epsilon}\right)^{N^2} \leq \left(\frac{3\sqrt{N}}{\epsilon}\right)^{N^2}. \quad (26)
\]
On the other hand, if $\Delta > 0$, then for any quantum coloring $\chi$

\[
\mathbb{P} \left[ \max_{P \in \mathcal{P}} |\text{tr}(\chi P)| \leq \Delta \right] = \mathbb{P} \left[ \bigcap_{P \in \mathcal{P}} \{ |\text{tr}(\chi P)| \leq \Delta \} \right] = \prod_{P \in \mathcal{P}} \mathbb{P} [ |\text{tr}(\chi P)| \leq \Delta ] \quad \text{(by independence)}
\]

\[
= (\mathbb{P} [ |\text{tr}(\chi P)| \leq \Delta ])^M, \quad (27)
\]

where $P$ is an arbitrary element of $\mathcal{P}$. The last equality holds because elements of $\mathcal{P}$ are identically distributed.

With the same argument, for any quantum coloring $\chi$

\[
\mathbb{P} \left[ \max_{P \in \mathcal{P}} \text{tr} (P - (\chi P)^2) \leq \Delta \right] = (\mathbb{P} [ \text{tr} (P - (\chi P)^2) \leq \Delta ])^M. \quad (28)
\]

Combining (24), (26), and (27) we get

\[
\mathbb{P} \left[ \min_{\chi \in \mathcal{C}_1} \max_{P \in \mathcal{P}} |\text{tr}(\chi P)| \leq c \sqrt{N + \log M} \right] \leq \left( \frac{3 \sqrt{N}}{\epsilon} \right)^{N^2} \left( \max_{\chi \in \Sigma_1^{(\epsilon)}} \mathbb{P} [ |\text{tr}(\chi P)| \leq c \sqrt{N + \log M + \epsilon \sqrt{N/2}} ] \right)^M. \quad (29)
\]

Similarly, (25), (26), and (28) lead to

\[
\mathbb{P} \left[ \min_{\chi \in \mathcal{C}_2} \max_{P \in \mathcal{P}} \text{tr} (P - (\chi P)^2) \leq c^2 (N + \log M) \right] \leq \left( \frac{3 \sqrt{N}}{\epsilon} \right)^{N^2} \left( \max_{\chi \in \Sigma_2^{(\epsilon)}} \mathbb{P} [ \text{tr} (P - (\chi P)^2) \leq c^2 (N + \log M + 2\epsilon N) ] \right)^M. \quad (30)
\]

It remains to provide upper bounds for $\max_{\chi \in \Sigma_1^{(\epsilon)}} \mathbb{P} [ |\text{tr}(\chi P)| \leq c \sqrt{N + \log M + \epsilon \sqrt{N/2}} ]$ and $\max_{\chi \in \Sigma_2^{(\epsilon)}} \mathbb{P} [ \text{tr} (P - (\chi P)^2) \leq c^2 (N + \log M) + 2\epsilon N ]$, and then to find proper values of $\epsilon, c > 0$. Calculation of these bounds will be done by the concentration inequality given in Proposition 18. First, we bound the expected values. Considering $\chi = VDV^*$ as a spectral decomposition of $\chi$, it holds that

\[
\text{tr}(\chi P) \stackrel{d}{=} \text{tr}(UDU^*\Pi), \quad \text{tr} (P - (\chi P)^2) \stackrel{d}{=} \text{tr} \left( \Pi - (UDU^*\Pi)^2 \right)
\]

for a random unitary $U$ with Haar distribution. Therefore, using the calculation done in the last subsection, we obtain that for $\chi \in C_1$

\[
|\mathbb{E} [\text{tr}(\chi P)]| = \left| \frac{1}{N} \text{tr}(\chi) \text{tr}(\Pi) \right| \geq 3 \sqrt{N \log N}, \quad (31)
\]
and for $\chi \in C_2$,
\[
\mathbb{E} \left[ \text{tr} \left( P - (\chi P)^2 \right) \right] = -\text{tr}^2(\chi) \left[ \frac{N}{2} \left( \frac{N}{N^2 - 1} \right) + N \left( \frac{N}{2} \right) \frac{N - \lfloor N/2 \rfloor}{N^2 - 1} \right] \\
\geq \left[ \frac{N}{2} \right] \frac{N - \lfloor N/2 \rfloor}{N^2 - 1} \left( -\log^2(N) + N \right)
\]
\[
\geq \frac{N}{6}.
\] (32)

Now, we calculate the upper bounds.
\[
\mathbb{P} \left[ \left| \text{tr}(\chi P) \right| \leq c\sqrt{N + \log M} + \sqrt{\frac{N}{2}} \right] \\
\leq \mathbb{P} \left[ \left| \text{tr}(\chi P) \right| \leq (c + \epsilon)\sqrt{N + \log M} \right] \\
\leq \mathbb{P} \left[ \left| \text{tr}(\chi P) - \mathbb{E}[\text{tr}(\chi P)] \right| \leq (c + \epsilon)\sqrt{1 + b\sqrt{N} - \frac{1}{3}\sqrt{N}\log N} \right] \\
\leq \mathbb{P} \left[ \left| \text{tr}(\chi P) - \mathbb{E}[\text{tr}(\chi P)] \right| \leq \frac{1}{4}\sqrt{N}\log N \right] \\
\leq 2 \exp \left[ -\frac{c}{16}N\log^2 N \right].
\] (33)

The inequality (33) is true by Proposition 18 for large enough $N$s and the constant $c_1$ introduced in the previous subsection.
\[
\mathbb{P} \left[ \text{tr}(P - (\chi P)^2) \leq c^2(N + \log M) + 2\epsilon N \right] \\
\leq \mathbb{P} \left[ \text{tr}(P - (\chi P)^2) - \mathbb{E}[\text{tr}(P - (\chi P)^2)] \leq c^2(N + \log M) + 2\epsilon N - \frac{N}{6} \right] \\
\leq \mathbb{P} \left[ \text{tr}(P - (\chi P)^2) - \mathbb{E}[\text{tr}(P - (\chi P)^2)] \leq (c^2(1 + b) + 2\epsilon - \frac{1}{6})N \right] \\
\leq \mathbb{P} \left[ \left| \text{tr}(P - (\chi P)^2) - \mathbb{E}[\text{tr}(P - (\chi P)^2)] \right| \geq \frac{1}{6} - c^2(1 + b) - 2\epsilon N \right].
\] (32), $N \geq 152$

The last inequality is valid if
\[
\frac{1}{6} - c^2(1 + b) - 2\epsilon > 0.
\] (34)

Assuming (34), we conclude from Proposition 18 that
\[
\mathbb{P} \left[ \text{tr}(P - (\chi P)^2) \leq c^2(N + \log M) + 2\epsilon N \right] \leq 2 \exp \left[ -c_2\left( \frac{1}{6} - c^2(1 + b) - 2\epsilon \right)^2N^2 \right],
\] (35)
where $c_2$ is the same as before and $N$ is large enough.

Substituting (33) in (29) gives

$$
P \left[ \min_{\chi \in C_1} \max_{P \in \mathcal{P}} |\text{tr}(\chi P)| \leq c\sqrt{N + \log M} \right] \leq \left( \frac{3\sqrt{N}}{\epsilon} \right)^{N^2} \left( 2 \exp \left[ -\frac{c_1}{16} N \log^2 N \right] \right)^M
$$

$$
= \exp \left[ N^2 \log \frac{3}{\epsilon} + \frac{N^2}{2} \log N + M \log 2 \right.
\left. \frac{-c_1}{16} NM \log^2 N \right]
$$

$$
\leq \exp \left[ N^2 \log N - \frac{c_1}{17} NM \log^2 N \right] \text{ (for large } N)$$

$$
\leq \exp \left[ N^2 \log N - \frac{c_1}{17} aN^2 \log^2 N \right] \text{ (by (20))}
$$

$$
\to 0. \quad \text{(as } N \to \infty)$$

Hence, $P \left[ \min_{\chi \in C_1} \max_{P \in \mathcal{P}} |\text{tr}(\chi P)| \leq c\sqrt{N + \log M} \right]$ is less than $1/2$ for large enough values of $N$.

Similarly, (35) and (30) give us that provided (34),

$$
P \left[ \min_{\chi \in C_2} \max_{P \in \mathcal{P}} \text{tr}(P - (\chi P)^2) \leq c^2(N + \log M) \right]
$$

$$
\leq \exp \left[ N^2 \log N - \frac{c_2}{2} \left( \frac{1}{6} - c^2(1 + b) - 2c \right) N^2 M \right] \text{ (for large } N)$$

$$
\leq \exp \left[ N^2 \log N - \frac{c_2}{2} \left( \frac{1}{6} - c^2(1 + b) - 2c \right) aN^3 \right] \text{ (by (20))}
$$

$$
\to 0. \quad \text{(as } N \to \infty)$$

Hence, $P \left[ \min_{\chi \in C_2} \max_{P \in \mathcal{P}} \text{tr}(P - (\chi P)^2) \leq c^2(N + \log M) \right]$ will, ultimately, be less than $1/2$.

Note that up to this point, no restriction has been imposed on $M$, and $N$ has been restricted finitely many times. Thus, to finish the proof it is enough to show that for any $a, b > 0$, (34) is satisfied by appropriate values of $\epsilon, c = c(b) > 0$ which are independent of $M, N$. This is true since we can put $\epsilon = 1/24$ and $c = 1/(4\sqrt{1 + b})$. \hfill \square

**Remark** 23. The range of tightness which is given in Theorem 4, includes projection systems with a size that can vary from linear to exponential with respect to the dimension of the ground space. Comparing with the combinatorial case, the quantum random coloring upper bound is tight in a wider range. The reason seems to be hidden in the strength of the concentration properties of random unitary matrices, e.g. what explained in Proposition 18.
4 Quantum Discrepancy of Set Systems

4.1 Proof of Theorem 5

Proof of Theorem 5 is based on the formulation given in Corollary 13, i.e.

\[ \text{QDisc}(P) = \min_{\chi} \max_{P \in P} \left[ \text{tr}^2(\chi P) + \frac{1}{2} ||[\chi, P]||_2^2 \right]^{1/2}. \]

Proof of Theorem 5. Since \( 0 \leq \text{QDisc}(P_S) \leq \text{Disc}(S) \), if \( \text{Disc}(S) = 0 \), then we have \( \text{QDisc}(P_S) = 0 \). Now, suppose that \( \text{QDisc}(P_S) = 0 \). By the above formula, there exists a quantum coloring \( \chi \) such that for each \( P \in P_S \), \( ||[\chi, P]||_2 = 0 \). This means that each element of \( P_S \) commutes with \( \chi \). Thus \( \chi \) and \( P_S \) are simultaneously unitarily diagonalizable. Assume that \( U \) is a unitary matrix such that

\[ \tilde{\chi} = U\chi U^*, \quad \tilde{P} = UPU^* \quad \text{for} \quad P \in P_S, \]

are diagonal. Hence, \( \tilde{P} := \{ \tilde{P} : P \in P_S \} \) is associated to a (unique) set system \( \tilde{S} \). By the cyclic property of the trace function, \( \text{QDisc}(\tilde{P}) = \text{QDisc}(P_S) = 0 \), and since \( \tilde{\chi} \) is diagonal, \( \text{Disc}(\tilde{S}) = 0 \). Now, it is enough to prove that \( \text{Disc}(\tilde{S}) = \text{Disc}(S) \). In order to establish this equality, we show that there exists a permutation \( \sigma \) on \([N]\) such that \( \tilde{S} = \{ \sigma(S) : S \in S \} \). Then \( \text{diag}(\tilde{\chi}) \circ \sigma \) will be a coloring of \([N]\) that produces zero discrepancy in \( S \).

We define an equivalence relation on \([N]\) as

\[ m \sim n \iff \forall S \in S[m \in S \iff n \in S]. \]

Suppose that \( C_1, \ldots, C_k \) are the equivalence classes of this relation. Since

\[ P_{C_i} = \prod_{S \in S \cap C_i \neq \emptyset} P_S \prod_{S \in S \cap C_i = \emptyset} (I - P_S), \]

\( U P_{C_i} U^* \) is a diagonal projection for each \( i = 1, 2, \ldots, k \). Let \( D_i \subseteq [N] \) be the corresponding set of this projection. The map \( P \mapsto UPU^* \) is rank-preserving, so \( |D_i| = |C_i| \). For each \( i = 1, 2, \ldots, k \) we fix a bijection \( \sigma_i : C_i \rightarrow D_i \). Now, \( \sigma : [N] \rightarrow [N] \) is uniquely determined by the set of relations \( \sigma \mid_{C_i} = \sigma_i \). The map \( \sigma \) is a permutation since the \( C_i \)'s are equivalence classes. It follows from the definition of \( \tilde{P} \) that \( \tilde{S} \in \tilde{S} \) exactly when there is a set \( S \in S \) such that \( \tilde{S} \) is the set associated to the projection \( U P_S U^* \). Consider a pair of \( S \in S \) and \( \tilde{S} \in \tilde{S} \) with this relation. We have

\[ \tilde{S} = \bigcup_{i : C_i \cap S \neq \emptyset} C_i, \quad P_S = \sum_{i : C_i \cap S \neq \emptyset} P_{C_i}. \quad (36) \]

Since \( P_{\tilde{S}} = U P_S U^* \), it holds that

\[ P_{\tilde{S}} = \sum_{i : C_i \cap S \neq \emptyset} U P_{C_i} U^* \quad \text{(by (36))}. \]
$$= \sum_{i : C_i \cap S \neq \emptyset} P_{D_i}$$
$$= \sum_{i : C_i \cap S \neq \emptyset} P_{\sigma(C_i)}$$
$$= P_{\left[ U_{C_i \cap S \neq \emptyset} \sigma(C_i) \right]} \quad (\sigma(C_i)s are disjoint)$$

and therefore,

$$\tilde{S} = \bigcup_{i : C_i \cap S \neq \emptyset} \sigma(C_i) = \sigma\left( \bigcup_{i : C_i \cap S \neq \emptyset} C_i \right) = \sigma(S). \quad \Box$$

### 4.2 Proof of Theorem 6

Suppose $S$ is a set system on $[N]$ and $P_S$ is its corresponding projection system. We know form Lemma 10 that

$$QDisc(P_S) = \min_{X : \det. \text{proj. process}} \max_{S \in S} \left[ \mathbb{E} \left[ (2X(S) - |S|)^2 \right] \right]^{1/2}.$$

The idea of the proof of Theorem 6 is that if there is a determinantal projection process $\mathbf{x}$ for which $\max_{S \in S} \left[ \mathbb{E} \left[ (2\mathbf{x}(S) - |S|)^2 \right] \right]^{1/2}$ is very small, then by means of the concentration of $\mathbf{x}(S)$ around its mean for every $S \in S$, we can find a deterministic coloring $\chi$ which makes $\max_{S \in S} |\chi(S)|$ and so $\text{Disc}(S)$ small. The following propositions provide a representation of $\mathbf{x}(S)$ for each $S \subseteq [N]$, and a concentration inequality applicable to such representations, respectively.

**Proposition 24.** Suppose $\mathbf{x}$ is a determinantal process on $[N]$ and $K$ is its Hermitian kernel. Then,

i. For each $S \subseteq [N]$, $\mathbf{x} \cap S$ is a determinantal process on $S$ that its kernel is equal to $K$ restricted to the set of rows and columns in $S$, i.e. the matrix $(K_{ij})_{i,j \in S}$.

ii. If $\{\lambda_1, \ldots, \lambda_N\}$ is the set of eigenvalues of $K$, then $\mathbf{x}([N])$ has the same distribution as $\sum_{i=1}^{N} X_i$, where $X_i$s are independent and $X_i \sim \text{Bernoulli}(\lambda_i)$, $i=1,\ldots,N$. In particular, if $\mathbf{x}$ is a projection determinantal process, i.e. if $K$ is an orthogonal projection, all realizations of $\mathbf{x}$ are of the same size which is $\text{tr}(K)$.

**Proposition 25** (Bernstein’s Inequality). Consider the set of independent random variables $\{X_i : i \geq 1\}$ with $\mathbb{E}[X_i] = 0$, and a number $K$ with $|X_i| \leq K$ for each $i$. For any $t > 0$ we have

$$\mathbb{P}\left[ \left| \sum_{i \geq 1} X_i \right| \geq t \right] \leq 2 \exp \left[ -\min \left( \frac{t^2}{4 \sum_{i \geq 1} \mathbb{E}[X_i^2]}, \frac{t}{2K} \right) \right].$$

See Remark 4.2.5 and Theorem 4.5.3 from [8] for Proposition 24, and Lemma 2.7.1 in [14] for Proposition 25.
Proof of Theorem 6. For writing the proof more conveniently, we put
\[ A = \max \left[ \frac{\sqrt{\log(2M)}}{\log(2M)} : \frac{\log(2M)}{\text{QDisc}(P_S)} \right] \]
\[ \max_{S \in \mathcal{S}} \left[ \mathbb{E} \left[ (2\mathcal{X}(S) - |S|)^2 \right] \right]^{1/2} \] is a continuous function of the kernel of \( \mathcal{X} \) and set of orthogonal projections is compact in \( \mathbb{R}^{N^2} \). Hence, there exists a determinantal projection process \( \mathcal{Y} \) for which
\[ \text{QDisc}(P_S) = \max_{S \in \mathcal{S}} \left[ \mathbb{E} \left[ (2\mathcal{Y}(S) - |S|)^2 \right] \right]^{1/2}. \]
We prove that
\[ \mathbb{P} \left[ \max_{S \in \mathcal{S}} |2\mathcal{Y}(S) - |S|| \geq (2cA + 1) \text{QDisc}(P_S) \right] < 1. \] (37)
This results in the existence of some realization \( \tilde{\mathcal{Y}} \) for which
\[ \max_{S \in \mathcal{S}} |2\tilde{\mathcal{Y}}(S) - |S|| < (2cA + 1) \text{QDisc}(P_S). \]
This relation together with \( \max_{S \in \mathcal{S}} |2\tilde{\mathcal{Y}}(S) - |S|| \geq \text{Disc}(S) \) completes the proof.
In order to prove (37), it’s enough, by the union bound, to show that for each \( S \in \mathcal{S} \)
\[ \mathbb{P} \left[ |2\mathcal{Y}(S) - |S|| \geq (2cA + 1) \text{QDisc}(P_S) \right] < \frac{1}{M}. \]
Now, for each \( S \in \mathcal{S} \)
\[ \mathbb{P} \left[ |2\mathcal{Y}(S) - |S|| \geq (2cA + 1) \text{QDisc}(P_S) \right] \]
\[ = \mathbb{P} \left[ |2\mathcal{Y}(S) - |S|| - \max_{S \in \mathcal{S}} \left[ \mathbb{E} \left[ (2\mathcal{Y}(S) - |S|)^2 \right] \right]^{1/2} \geq 2cA.\text{QDisc}(P_S) \right] \]
\[ \leq \mathbb{P} \left[ |2\mathcal{Y}(S) - |S|| - \left[ \mathbb{E} \left[ (2\mathcal{Y}(S) - |S|)^2 \right] \right]^{1/2} \geq 2cA.\text{QDisc}(P_S) \right] \]
\[ \leq \mathbb{P} \left[ |2\mathcal{Y}(S) - |S|| - \mathbb{E} [2\mathcal{Y}(S) - |S|| \geq 2cA.\text{QDisc}(P_S) \right] \]
\[ \leq \mathbb{P} \left[ |2\mathcal{Y}(S) - |S|| - \mathbb{E} [2\mathcal{Y}(S) - |S|| \geq 2cA.\text{QDisc}(P_S) \right] \]
\[ \leq \mathbb{P} \left[ |\mathcal{Y}(S) - \mathbb{E} [\mathcal{Y}(S)| \geq cA.\text{QDisc}(P_S) \right]. \]
By Proposition 24, \( \mathcal{Y}(S) \) \( \overset{d}{=} \sum_{i=1}^{\|S\|} Y_i^{(S)} \) where the \( Y_i^{(S)} \) are independent Bernoulli random variables. Hence, conditions of Proposition 25 are satisfied for
\[ \left\{ Y_i^{(S)} - \mathbb{E} [Y_i^{(S)}] : 1 \leq i \leq \|S\| \right\} \]
with \( K = 1 \), and hence
\[ \mathbb{P} \left[ |2\mathcal{Y}(S) - |S|| \geq (2cA + 1) \text{QDisc}(P_S) \right] \]
\[
\leq 2 \exp \left[ - \min \left( \frac{c^2 A^2 \max_{S} \mathbb{E} \left[ (2\mathbf{Y}(S) - |S|)^2 \right]}{4 \sum_i \mathbb{E} \left[ (Y^{(S)}_i - \mathbb{E}[Y^{(S)}_i])^2 \right]}, \frac{c}{2} A.\text{QDisc}(\mathcal{P}_S) \right) \right].
\]

If \( y \geq z \), \( \min(x, y) \geq \min(x, z) \), for any \( x, y, z \in \mathbb{R} \). By this and the independence of the \( Y_i^{(S)} \)'s, we obtain

\[
\mathbb{P} \left[ |2\mathbf{Y}(S) - |S|| \geq (2cA + 1) \text{QDisc}(\mathcal{P}_S) \right] 
\leq 2 \exp \left[ - \min \left( \frac{c^2 A^2 \mathbb{E} \left[ (2\mathbf{Y}(S) - |S|)^2 \right]}{4 \sum_i \mathbb{E} \left[ (Y^{(S)}_i - \mathbb{E}[Y^{(S)}_i])^2 \right]}, \frac{c}{2} A.\text{QDisc}(\mathcal{P}_S) \right) \right].
\]

For a random variable \( X, \mathbb{E}[(X - a)^2] \) takes its minimum value at \( a = \mathbb{E}[X] \). Hence,

\[
\mathbb{P} \left[ |2\mathbf{Y}(S) - |S|| \geq (2cA + 1) \text{QDisc}(\mathcal{P}_S) \right] 
\leq 2 \exp \left[ - \min \left( \frac{c^2 A^2 \mathbb{E} \left[ (2\mathbf{Y}(S) - |S|)^2 \right]}{4 \mathbb{E} \left[ (\mathbf{Y}(S) - \mathbb{E}[\mathbf{Y}(S)])^2 \right]}, \frac{c}{2} A.\text{QDisc}(\mathcal{P}_S) \right) \right] < 2 \exp \left[ - \log(2M) \right] \quad \text{(for each } c > 2 \text{ since } M \geq 2) \\
= \frac{1}{M}.
\]

To justify the last inequality, note that depending on whether \( 0 < \text{QDisc}(\mathcal{P}_S) < \sqrt{\log(2M)} \) or \( \text{QDisc}(\mathcal{P}_S) \geq \sqrt{\log(2M)} \), we have \( A = \frac{\log(2M)}{\text{QDisc}(\mathcal{P}_S)} \) or \( A = \sqrt{\log(2M)} \). Therefore,

\[ A^2, A.\text{QDisc}(\mathcal{P}_S) \geq \log(2M) \]

for every non-zero value of \( \text{QDisc}(\mathcal{P}_S) \).

\[ \square \]

5 Concluding Remarks

Quantum discrepancy, as we defined in this paper, is not the first non-commutative version of discrepancy. In [16] Weaver points briefly to the “interest in noncommutative discrepancy”, and implicitly gives a formulation for the discrepancy of a set of Hermitian matrices as follows. For a set system \( \mathcal{S} \) on \([N]\) with elements indexed as \( S_1, S_2, \ldots, S_M \), it can be proved that \( \text{Disc}(\mathcal{S}) = \min_{\epsilon_1, \ldots, \epsilon_n \in \{\pm 1\}} \left\| \sum_{i=1}^N \epsilon_i v_i \right\|_\infty \), where for each \( i \in [N] \), \( v_i \in \{0, 1\}^M \), and \( v_i(j) = 1 \) exactly when \( i \in S_j \). If the \( v_i \)'s are permitted to be arbitrary elements of \( \mathbb{C}^M \) instead of being restricted to \( 0 - 1 \) vectors, then it makes sense to talk about the discrepancy of a set of vectors. Weaver suggests to generalize this new notion to \( M \times M \) Hermitian matrices \( A_1, \ldots, A_N \) as

\[
\min_{\epsilon_1, \ldots, \epsilon_n \in \{\pm 1\}} \left\| \sum_{i=1}^N \epsilon_i A_i \right\|_\infty.
\]
By giving a definition of quantum discrepancy, we have introduced a notion of discrepancy for projection systems. In the given formulation, Hermitian unitary matrices play the role of (quantum) colorings. The generalization of set systems and colorings to projection systems and quantum colorings, respectively, is compatible with the general principles of quantization procedure, and it justifies using the term “quantum” in the denominations. Similar to the area of the combinatorial discrepancy, bounding the quantum discrepancy for general projection systems or projection systems with additional structures constitutes an important class of problems. Moreover, since the set of quantum colorings is strictly larger than the set of combinatorial colorings, the quantum discrepancy of a set system is, in general, different from its combinatorial discrepancy.

Investigating the quantum analogues of famous problems and results in combinatorial discrepancy theory would be a potential direction for future studies. Also, computation of the quantum discrepancy for some special classes of set systems provides us with another set of interesting problems. Bounding combinatorial discrepancy would be a potential important application of quantum discrepancy. According to the probabilistic interpretation of the quantum discrepancy of set systems, this might lead to upper bounds obtained by probabilistic constructive proofs.

Acknowledgements

We would like to express our great appreciation to Professor Amir Daneshgar for his valuable and constructive suggestions. Special thanks are also given to the anonymous reviewer for her/his helpful comments.

References

[1] K. Alishahi and M. Zamani. The spherical ensemble and uniform distribution of points on the sphere. Electron. J. Probab., 20, 2015.
[2] G. Anderson, A. Guionnet, and O. Zeitouni. An introduction to random matrices. Cambridge University Press, 1st edition, 2010.
[3] E. Carlen. Trace inequalities and quantum entropy: an introductory course. In Entropy and the Quantum, volume 529 of Contemp. Math. American Mathematical Society, 2010.
[4] B. Chazelle. The discrepancy method: randomness and complexity. Cambridge University Press, 2001.
[5] W. Chen, A. Srivastav, and G. Travaglini. A panorama of discrepancy theory. Springer, 2014.
[6] F. Hiai. and D. Petz. The semicircle law, free random variables and entropy. American Mathematical Society, 2000.
[7] R. Horn and C. Johnson. Matrix analysis. Cambridge University Press, 2012.
[8] J. Hough, M. Krishnapur, Y. Peres, and B. Virág. Zeros of Gaussian analytic functions and determinantal point processes. American Mathematical Society, 2010.
[9] J. Matoušek. Geometric discrepancy: an illustrated guide. Springer, 2010.
[10] J. Matoušek and J. Spencer. Discrepancy in arithmetic progressions. *J. Amer. Math. Soc.*, 9(1):195–204, 1996.
[11] K. Roth. Remark concerning integer sequences. *Acta Arithmetica*, 3(9):257–260, 1964.
[12] T. Rothvoß. Constructive discrepancy minimization for convex sets. *SIAM J. Comput.*, 46(1):224–234, 2017.
[13] J. Spencer. Six standard deviations suffice. *Trans. Amer. Math. Soc.*, 289(2):679–706, 1985.
[14] M. Talagrand. The generic chaining: upper and lower bounds of stochastic processes. Springer, 2005.
[15] T. Tao. Topics in random matrix theory. American Mathematical Society, 2012.
[16] N. Weaver. The Kadison–Singer problem in discrepancy theory. *Discrete Math.*, 278(1–3):227–239, 2004.
[17] N. Weaver. Mathematical quantization. Chapman and Hall/CRC, 2001.