Randomizing quantum states in Shatten $p$-norms

Kabgyun Jeong

$^1$ School of Computational Sciences, Korea Institute for Advanced Study, Hoegiro 87, Dongdaemun, Seoul 130-722, Korea

(Dated: July 23, 2014)

Abstract

In this paper, we formulate a method for randomizing quantum states with respect to the Shatten $p$-norm ($p \geq 1$). Our theorem includes the Lemma 2.2 of Hayden and Winter [Commun. Math. Phys. 284, 263–280 (2008)] for the norm case of $p > 1$. We exploit the methods of a net construction on the unit sphere and McDiard’s inequality in probability theory, and then we prove certain general cases (all $p$) of randomization tool for quantum states, which includes the operator norm and trace norm simultaneously in a single statement.

PACS numbers: 03.67.-a, 03.67.Hk

*Electronic address: kgjeong6@kias.re.kr
I. INTRODUCTION

Randomization of quantum states is a very useful tool in quantum information theory. For examples, the technique of randomization can be directly applied not only to higher entropic quantum encryption/decryption protocol such as quantum one-time pads or private quantum channels, but also to a proof of channel-additivity problems. The idea of an encoding/decoding scheme of quantum states was first proposed by Ambainis et al.\cite{1}, and its optimality has already been proven for any input quantum states by several groups\cite{1–3}. Beyond the quantum one-time pad, the randomizing methods in quantum information science has many applications in quantum communications such as superdense coding\cite{4}, quantum data hiding\cite{5}, entropic uncertainty principle\cite{6}, quantum state sharing protocol\cite{7}, and the proof of the additivity violation for the classical capacity on quantum channels\cite{8}.

As mentioned above, one of the most important application of randomizing quantum states is for the proof of an additivity problem on quantum channels. Mathematically quantum channel is a completely positive and trace-preserving (CPT) map. The existence proof of the counterexamples to the additivity conjecture of classical capacity originally makes use of the quantum channel defined to be $\varepsilon$-randomizing maps, where the study of Shatten $p$-norm from the operator norm to the trace norm sheds light on the proof of the additivity counterexample\cite{8, 9}. So, following the original work of Hayden, Leung, Shor, and Winter’s construction\cite{5} for the operator norm and Dickinson and Nayak’s\cite{10} for trace case, we try to give a special formula of the randomizing technique for quantum states in Shatten $p$-norms ($1 \leq p \leq \infty$). Note that the Hayden and Winter’s approach in which the $\varepsilon$-randomizing map doesn’t work at $p$ equal to one case (Lemma 2.2 in Reference\cite{9}). Strictly speaking, general $p$-norm case can be derived from the result of the operator norm case, but each norm has different meaning depending on which task or which property we analyze. In this reason our approach of the single formula for state randomization over Shatten $p$-norm makes sense. Also note that Aubrun’s research\cite{11, 12} on randomizing quantum states with respect to the operator norm improved the work of Reference\cite{3}, in which log-factor is removed, without changing the main point. For convenience, we take the log and exp functions to be always base 2, and an expectation and probability are denoted by $E$ and $P$, respectively.

This paper is organized as follows. First we describe basic materials in Section II.
tion III describes precise statement of the main theorem (Theorem I) and two formal lemmas within the general framework. The main theorem is proven in Section IV. Finally, we will summary our work in Section V.

II. USEFUL NOTIONS AND DEFINITIONS

We define and examine several intrinsic facts on Shatten $p$-norm required to prove main results. We suppose that $B(\mathbb{C}^d)$ is the space of (bounded) linear operators on the $d$-dimensional (complex) Hilbert space $\mathbb{C}^d$ and $U(d) \subset B(\mathbb{C}^d)$ the unitary group on the Hilbert space, and $1_d$ stands for the $d \times d$ identity matrix on the space. Let $\mathcal{P}(\mathbb{C}^d)$ be a set of all pure quantum states i.e., a set of unit vectors on the space $\mathbb{C}^d$. A density matrix of the pure state $|\psi\rangle \in \mathcal{P}(\mathbb{C}^d)$ will be written by $\psi \in B(\mathbb{C}^d)$.

For any matrix $A \in B(\mathbb{C}^d)$, suppose that $s_1, \ldots, s_d \in \mathbb{R}$ denote singular values of $A$, which are also defined by the square roots of the eigenvalues of $AA^\dagger$. Then, for all $1 \leq p \leq \infty$, the Shatten $p$-norm is defined \cite{13} by

$$\|A\|_p = \left(\sum_{i=1}^{d}|s_i|^p\right)^{1/p}. \quad (1)$$

For $p = 1$, the trace norm is defined by $\|A\|_1 = \text{tr} \sqrt{A^\dagger A}$, and hence, it is the sum of singular values of the matrix $A$. Similarly the Hilbert-Schmidt (or Frobenius) norm corresponds to the case $p = 2$, and it is defined by $\|A\|_2 = \text{tr} A^\dagger A = \sqrt{\sum_{i=1}^{d}s_i^2}$. Finally, for $p = \infty$ case, this definition of $p$-norm can be understood, $\|A\|_\infty = \max\{s_i\}$ for all $i$, and it is essentially equivalent to the usual operator norm. For this reason, the Shatten $p$-norm can be described in trace class as $\|A\|_p = \left(\text{tr}(A^\dagger A)^{p/2}\right)^{1/p}$.

By using the definition of Shatten $p$-norm \cite{11}, we review several facts on the relations between several orders of $p$ for the Shatten $p$-norms. For all matrix $A \in B(\mathbb{C}^d)$ and $1 \leq p \leq \infty$, Shatten $p$-norms always satisfy

$$\|A\|_\infty \leq \|A\|_p \leq \|A\|_1. \quad (2)$$

The bounds above are sometimes called interpolation inequalities. Also, for every $r > p \geq 1$, the following Hölder’s inequality (right side) holds

$$\|A\|_r \leq \|A\|_p \leq d^{(\frac{1}{p} - \frac{1}{r})}\|A\|_r. \quad (3)$$
Furthermore, for any matrices $A, B \in \mathcal{B}(\mathbb{C}^d)$, the reverse triangle inequality on $p$-norm holds as follows:

$$||A||_p - ||B||_p \leq ||A - B||_p.$$  \hfill (4)

Now, we define an $\varepsilon$-randomizing maps with respect to the Shatten $p$-norm.

**Definition 1.** For any quantum state $\rho \in \mathcal{B}(\mathbb{C}^d)$, suppose that a completely positive and trace-preserving map $\mathcal{R} : \mathcal{B}(\mathbb{C}^d) \to \mathcal{B}(\mathbb{C}^d)$ satisfies

$$\left\| \mathcal{R}(\rho) - \frac{1}{d} \right\|_p \leq \frac{\varepsilon}{\sqrt{d^{p-1}}}.$$  \hfill (5)

Then we say that the map $\mathcal{R}$ is $\varepsilon$-randomizing with respect to the Shatten $p$-norm $|| \cdot ||_p$.

The map $\mathcal{R}$ for any input state $\rho$ can be naturally constructed as follow:

$$\mathcal{R}(\varphi) = \frac{1}{m} \sum_{i=1}^{m} U_i \varphi U_i^\dagger,$$  \hfill (6)

where the unitary operators $U_i$ are chosen to be random from the unitary group $U(d)$, and $m$ generally depends on the number of unitary operators. As a special case, if $\varepsilon$ is equal to zero, we say that the map $\mathcal{R}$ is a complete randomizing map. The above definition of $\varepsilon$-randomizing map is well defined for some special cases $p$. For the map $\mathcal{R}$ with respect to the trace norm, the $\varepsilon$-randomizing map is defined by the condition $\left\| \mathcal{R}(\rho) - \frac{1}{d} \right\|_1 \leq \frac{\varepsilon}{\sqrt{d^{\nu-1}}}$.  \hfill [10]

Similarly, for $p = 2$ and $\infty$ cases, the condition naturally gives rise to $\left\| \mathcal{R}(\rho) - \frac{1}{d} \right\|_2 \leq \varepsilon/\sqrt{d}$ and $\left\| \mathcal{R}(\rho) - \frac{1}{d} \right\|_\infty \leq \varepsilon/d$, respectively. \hfill [3, 14]. Here, note that by the convexity of the Shatten $p$-norm, it suffices to consider the condition just for all pure input states.

Another definition of a probability measure is crucial in the proof of main theorem (Theorem [1]), it is an expectation value of given unitary operators.

**Definition 2.** Let $\mu$ be a probability measure $\mu$ on a unitary group $U(d)$. Suppose that $\rho \in \mathcal{B}(\mathbb{C}^d)$ is a density matrix (with unit trace). If

$$\int_{U(d)} U \rho U^\dagger d\mu(U) = \frac{1}{d},$$  \hfill (7)

then we say $\mu$ to be unitarily invariant or isotropic measure.

The above definitions will be used to prove Lemma [3] in Section [III]. From now on, we describe our main result, and compare the result to another well-known results such as in [2, 10, 11].
III. MAIN RESULTS

We are interested in an approximate (not complete) version of randomizing map $R$ in which the map has small cardinality $m$ of a unitary sequence in $U(d)$. Furthermore, we would like to reproduce the well-known two results of [5, 10] almost exactly. Our theorem is as follows.

**Theorem 1.** Let $\varphi \in \mathcal{P}(\mathbb{C}^d)$ be a pure state and $\mu$ the unitarily invariant measure on the unitary group $U(d)$. Suppose that all $\varepsilon > 0$ and the dimension $d$ is sufficiently large. If $R(\varphi) = \frac{1}{m} \sum_{i=1}^{m} U_i \varphi U_i^\dagger$ on $B(\mathbb{C}^d)$ is $\varepsilon$-randomizing map with respect to the Shatten $p$-norm (for all $p \geq 1$), then there exists a set of unitary operators $\{U_i\}_{i=1}^{m} \in U(d)$ with the cardinality $m \geq \frac{c_p d}{\varepsilon^2} \log \left( \frac{10d}{\varepsilon \sqrt{d}} \right)$, where $c_p$ is a constant.

Assume that $c_1$ and $c_\infty$ are absolute constants. If we restrict $p$ equal to 1, then the map $R$ is $\varepsilon$-randomizing with respect to the trace norm with an order of cardinality $m = \frac{c_1 d}{\varepsilon^2} \log \left( \frac{10d}{\varepsilon} \right)$. Suppose that $p = \infty$. Then, $m = \frac{c_\infty d}{\varepsilon^2} \log \left( \frac{10d}{\varepsilon} \right)$. The modification of [5] by Aubrun with $m = \mathcal{O}(d/\varepsilon^2)$ is given References [11, 12]. The condition of $d < m < d^2$ will be used several times under the assumption of dimension $d$ being sufficiently large. Note that, in the theorem, the probability of the map $R$ to be $\varepsilon$-randomizing is at least $1 - e^{-m}$.

We need some technical lemmas for the proof of our main theorem, so we postpone the proof of Theorem 1 to Section IV. First, let us precisely examine two non-trivial lemmas below.

**Lemma 2.** Suppose that $r > p \geq 1$ for all $r$ and $p$. Then, for any density matrix $A \in B(\mathbb{C}^d)$, we have

$$\left\| A - \frac{1}{d} \right\|_p^r \leq d^{\frac{r-p}{p}} \| A \|_r^r - d^{\frac{r-p}{p}}. \quad (8)$$

**Proof.** It is straightforward from the fact that $A$ is a density matrix and from the Hölder’s inequality Equation (3). \qed

**Lemma 3.** Let $\varphi \in \mathcal{P}(\mathbb{C}^d)$ be a fixed pure state. If we define a random variable $Y_{\varphi} = \|R(\varphi) - \frac{1}{d} \|_p$, then the following inequality holds (for all $r > p \geq 1$)

$$\mathbb{E}_{(U_i)} Y_{\varphi} \leq \left( \frac{\sqrt{d}}{mp} + \frac{r}{m^{p-1} \sqrt{d}} \right)^{1/r}. \quad (9)$$
Proof. (i) $p = 1$ and $r = 2$ case: We note that the expectation $\mathbb{E}$ is taken over the unitary operators $\{U_i\}$, and also recall that $\mathcal{R}(\varphi) = \frac{1}{m} \sum_{i=1}^{m} U_i \varphi U_i^\dagger$ and $Y_{[\varphi]} = \|\mathcal{R}(\varphi) - \frac{1}{d}\|_1$. (For convenience, we denote that $\mathbb{E}\{U_i\} := \mathbb{E}$ for simplicity.) Then,

$$
\mathbb{E}\|\mathcal{R}(\varphi)\|_2^2 = \frac{1}{m} + \frac{1}{m^2} \sum_{i \neq j} \mathbb{E}\text{tr}(U_i \varphi U_i^\dagger U_j \varphi U_j^\dagger)
$$

$$
\leq \frac{1}{m} + \text{tr}\left( \int_U U_i \varphi U_i^\dagger d\mu \cdot \int_U U_j \varphi U_j^\dagger d\mu \right)
$$

$$
= \frac{1}{m} + \text{tr}\frac{1}{d^2} = \frac{1}{m} + \frac{1}{d},
$$

where the inequality in Equation (10) results from the definition of the unitarily invariant measure $\int_U U \varphi U^\dagger d\mu(U) = \frac{1}{d^2}$ with independent unitary sets in the index $i, j$. By exploiting the Cauchy-Schwartz inequality, we have $Y_{[\varphi]}^2 \leq d\|\mathcal{R}(\varphi)\|_2^2 - 1$, and we can find $\mathbb{E}Y_{[\varphi]}^2 \leq d\mathbb{E}\|\mathcal{R}(\varphi)\|_2^2 - 1$ [10]. Therefore, for sufficiently large $d$,

$$
\mathbb{E}Y_{[\varphi]} \leq \sqrt{\mathbb{E}Y_{[\varphi]}^2} \leq \sqrt{d\mathbb{E}\|\mathcal{R}(\varphi)\|_2^2 - 1} = \sqrt{\frac{d}{m}},
$$

where the first inequality follows from the property of expectation values of square root for any random variables in probability theory.

(ii) $p = 2$ and $r = 3$ case: Consider that $Y_{[\varphi]} = \|\mathcal{R}(\varphi) - \frac{1}{d}\|_2$. As in the case (i), we can directly obtain the following inequality: $\mathbb{E}\|\mathcal{R}(\varphi)\|_3^2 \leq \frac{1}{m^2} + \frac{3}{md} + \frac{1}{d^2}$. Thus, from Hölder’s inequality on the Shatten $p$-norms,

$$
\mathbb{E}\left\|\mathcal{R}(\varphi) - \frac{1}{d}\right\|_2^3 \leq \sqrt{d}\mathbb{E}\|\mathcal{R}(\varphi)\|_3^3 - d^{-3/2} \leq \frac{\sqrt{d}}{m^2} + \frac{3}{md^{3/2}}.
$$

Finally, for all $r > p \geq 1$, $\|A\|_\infty \leq \|A\|_r \leq \|A\|_p \leq \|A\|_1$ is true. So the proof is completed. 

Before providing the full proof of the main theorem, we briefly review the previous key results on randomizing quantum states in certain norm classes.

**Theorem 4** (Hayden, Leung, Shor, and Winter [5]). Suppose that all $\varepsilon$ are positive and the dimension $d$ ($> 10/\varepsilon$) is sufficiently large. For any quantum state $\rho$, if a quantum channel $\mathcal{R}$ is $\varepsilon$-randomizing in the sense of the operator norm, then there exists a set of unitary operators $\{U_i\}_{i=1}^m$ with the cardinality $m = \frac{134d \log d}{\varepsilon^2}$.
Theorem 5 (Dickinson and Nayak [10]). Suppose that any \( \varepsilon > 0 \) and the dimension \( d \gg 1 \). Suppose that \( \mathcal{R} \) is \( \varepsilon \)-randomizing map with respect to the trace norm (and for any input state \( \rho \)), then there exists a random sequence of unitary operators \( \{U_i\}_{i=1}^m \subset U(d) \) with \( m = \frac{37d}{\varepsilon^2} \log(15/\varepsilon) \), and with a probability of at least \( 1 - \exp(-d/2) \).

Theorem 6 (Hayden and Winter, Lemma 2.2 in [9]). Suppose that \( \mathcal{R} \) is \( \varepsilon \)-randomizing map. Then, for all \( p > 1 \) and for any quantum state \( \rho \),

\[
\sup \|\mathcal{R}(\rho)\|_p \leq \left( \frac{1 + \varepsilon}{d} \right)^{1-1/p}.
\]

Theorem 7 (Aubrun [11]). For all \( \varepsilon > 0 \), suppose that a set \( \{U_i\}_{i=1}^m \) is independent random unitary matrices Haar-distributed on the unitary group \( U(d) \). Then there exists unitaries \( \{U_i\} \) with the cardinality \( m \geq \frac{Cd}{\varepsilon^2} \) for the \( \varepsilon \)-randomizing map \( \mathcal{R} \), where \( C \) is a universal constant.

Now we prove the main result, Theorem 1, by using two key lemmas (below) known as McDiarmid inequality and \( \eta \)-net bound, Lemma 8 and Lemma 9, respectively.

IV. PROOF OF THEOREM 1

The method of the proof is essentially equivalent to that in References [5, 10], but our tool is the Shatten \( p \)-norm (\( p \geq 1 \)). We need two key-lemmas known as McDiarmid inequality and the \( \eta \)-net argument. The former is a probability bound on estimating large deviation for certain random variables (with the unitarily invariant measure \( \mu \)), and the latter is a method for discretizing all pure quantum states to a finite set of states on the unit sphere. For convenience, we assume that all \( \varepsilon \) and \( \eta \) are small values, but not equal to zero. Once again, we note that \( d < m \leq d^2 \) and the dimension \( d \) goes to infinity.

Lemma 8 (McDiarmid inequality [15]). Let \( \{X_i\}_{i=1}^m \) be \( m \) independent random variables with \( X_i \) chosen at random from a set \( S \). Assume that the measurable function \( f : S^m \to \mathbb{R} \) satisfies \( |f(x) - f(\hat{x})| \leq c_i \), known as bounded difference, where the vectors \( x \) and \( \hat{x} \) differ only in the \( i \)-th position. Define \( Y = f(X_1, X_2, \ldots, X_m) \) to be the corresponding random variable. Then, for any \( t \geq 0 \), we have

\[
P[|Y - \mathbb{E}(Y)| \geq t] \leq 2e^{-2t^2/\sum_{i=1}^m c_i^2}.
\]

(12)
Lemma 9 ($\eta$-net [5]). Let $\eta > 0$ and the dimension $d$ be sufficiently large. Suppose that, for all pure states $|\varphi\rangle \in \mathbb{C}^d$, there exists $|\tilde{\varphi}\rangle \in N$ satisfying $\|\varphi - \tilde{\varphi}\|_1 \leq \eta$. Then there exists a set $N$ of pure states such that

$$|N| \leq \left(\frac{5}{\eta}\right)^{2d}.$$  \hspace{1cm} (13)

At first, we consider the bounded difference in Lemma 8. Suppose that a randomizing map $R$ is realized by a unitary sequence $(U_i)_{i=1}^m$, and another map $\hat{R}$ is constructed by $(U_1, \ldots, U_{i-1}, \hat{U}_i, U_{i+1}, \ldots, U_m)$, respectively. Then we have the bounded difference for the function $f$ as

$$\left\|R(\varphi) - \frac{1_d}{d}\right\|_p - \left\|\hat{R}(\varphi) - \frac{1_d}{d}\right\|_p \leq \left\|R(\varphi) - \hat{R}(\varphi)\right\|_p$$

$$= \frac{1}{m} \left\|U_i \varphi U_i^\dagger - \hat{U}_i \varphi \hat{U}_i^\dagger\right\|_p$$

$$\leq \frac{2^{1/p}}{m}.$$  

The McDiarmid inequality on positive part ($Y[\varphi] - \mathbb{E}Y[\varphi] > 0$) is given by

$$\mathbb{P}\left[Y[\varphi] \geq t + \left(\frac{\sqrt{d}}{m^p} + \frac{r}{m^{p-1} \cdot \sqrt{d}}\right)^{1/r}\right] \leq e^{-\frac{mt^2}{2(2-r)/r}},$$

and similarly for the negative part.

Proof of the theorem. Suppose that the sequence $(U_i)_{i\geq1}$ is i.i.d. $U(d)$-valued random variables, distributed according to the unitarily invariant measure. We will show that the corresponding map $R$ is $\varepsilon$-randomizing with high probability. The proof will be completed by the following bound on the probability by 1: For any pure state $\varphi \in \mathcal{B}(\mathbb{C}^d)$,

$$\mathbb{P}_\varphi \left[Y[\varphi] := \left\|\frac{1}{m} \sum_{i=1}^m U_i \varphi U_i^\dagger - \frac{1_d}{d}\right\|_p \geq \frac{\varepsilon}{\sqrt{d^{p-1}}}\right] < 1.$$  \hspace{1cm} (14)

Suppose that we fix the net $N$ and define $\tilde{\varphi}$ to be the net point on the sphere corresponding to $\varphi$, then, by unitary invariance, we have

$$\|R(\varphi) - R(\tilde{\varphi})\|_1 = \|\varphi - \tilde{\varphi}\|_1 \leq \frac{\varepsilon}{2\sqrt{d^{p-1}}}.$$  \hspace{1cm} (15)
Also, Lemma 9 provides a net with $|N| \leq \left( \frac{10d^{(p-1)/p}}{\varepsilon} \right)^{2d}$. Thus we can build up following inequalities:

$$
\mathbb{P}_{\varphi} \left[ \left\| R(\varphi) - \frac{1}{d} d \right\|_p \geq \frac{\varepsilon}{d^{(p-1)/p}} \right] \leq \mathbb{P}_{\varphi, \tilde{\varphi}} \left[ \left\| R(\varphi) - R(\tilde{\varphi}) \right\|_p + \left\| R(\tilde{\varphi}) - \frac{1}{d} d \right\|_p \geq \frac{\varepsilon}{d^{(p-1)/p}} \right]
$$

(16)

$$
\leq \mathbb{P}_{\varphi} \left[ \left\| R(\varphi) - \frac{1}{d} d \right\|_p \geq \frac{\varepsilon}{2d^{(p-1)/p}} \right].
$$

(17)

The first line makes use of the usual triangle inequality, and in the second line we exploit Equation (15). That is, $\|R(\varphi) - R(\tilde{\varphi})\|_p \leq \|R(\varphi) - R(\tilde{\varphi})\|_1 = \|\varphi - \tilde{\varphi}\|_1 \leq \frac{\varepsilon}{2d^{(p-1)/p}}$. The main point of the inequalities is that they change the bound from infinitely many pure states to a finite number of pure net points.

Now, if we use the union bound, the net construction (Lemma 9), and the McDiarmid inequality (Lemma 8), then we obtain

$$
\mathbb{P}_{\varphi} \left[ \left\| R(\varphi) - \frac{1}{d} d \right\|_p \geq \frac{\varepsilon}{d^{(p-1)/p}} \right] \leq |N| \cdot \mathbb{P}_{\tilde{\varphi}} \left[ \left\| R(\tilde{\varphi}) - \frac{1}{d} d \right\|_p \geq \frac{\varepsilon}{2d^{(p-1)/p}} \right]
$$

(18)

$$
\leq 2 \left( \frac{10d^{(p-1)/p}}{\varepsilon} \right)^{2d} \times \exp \left[ -\frac{m}{2^{2-2/p}} \left( \frac{\varepsilon}{2d^{(p-1)/p}} - \left( \frac{d^{1/p}}{m^{p}} + \frac{r}{m^{p-1}d^{1/p}} \right)^{1/r} \right)^2 \right].
$$

The existence of the $\varepsilon$-randomizing map with respect to the Shatten $p$-norm holds, if the probability is bounded above by 1. This situation is true, when $m \geq \frac{c_{p,d}\varepsilon}{\varepsilon^2} \log(\frac{10d^{(p-1)/p}}{\varepsilon})$ described below. This completes the proof.

□

Once again, we note that the inequality of Equation (18) follows from the union bound in probability theory, and the last inequality is direct consequence of the McDiarmid inequality. In the estimation of the cardinality $m$, we make use of the conditions $d < m < d^2$, $p < r$, and the following probability bound

$$
\left( \frac{10d^{p-1}}{\varepsilon} \right)^{2d} \times \exp \left[ -\frac{m}{2^{2-2/p}} \left( \frac{\varepsilon}{2d^{p-1}} - \left( \frac{d^{1/p}}{m^{p}} + \frac{r}{m^{p-1}d^{1/p}} \right)^{1/r} \right)^2 \right] < 1.
$$
For sufficiently larger $d$, above bound gives rise to \( \left( \frac{d^1/p}{m^p} + \frac{r}{m^{p-1}d^{1/p}} \right)^{1/r} \leq \left( \frac{2d^{1/p}}{m^p} \right)^{1/r} \). Suppose that we fix the dimension $d$ and select $m$ so that \( \left( \frac{\varepsilon}{2d^{p-1/p}} - \frac{2d^{1/r}d}{m^{p/r}} \right)^2 = o(\varepsilon^2) \). Then, up to a constant $c$, we obtain

\[
2d\log \left( \frac{10d^{p-1/p}}{\varepsilon} \right) < \frac{c_m \varepsilon^2}{2^{2-2/p}}.
\]

Thus we conclude that $m \geq \frac{c_p d}{\varepsilon^2} \log \frac{10d^{p-1/p}}{\varepsilon}$, where the constant $c_p$ is equivalent to $2^{4-2/p}/c$.

V. CONCLUSION

In conclusion, we have constructed a general formula for randomizing quantum states with respect to Shatten $p$-norms on $d$ dimensional Hilbert space. That is, there exists a random choice of a set of unitary operators \( \{U_i\}_{i=1}^m \) with $m = O(d\log(d^{p-1/p}/\varepsilon)/\varepsilon^2)$ in the unitary group $U(d)$ according to the unitarily invariant measure $\mu$, where the completely positive and trace-preserving map $R(\varphi)$ on $B(\mathbb{C}^d)$ is $\varepsilon$-randomizing with respect to the Shatten $p$-norm with high probability. As mentioned in Introduction, the work presented here suitably reproduces all the cases of Shatten $p$-norm of $p \geq 1$ for randomizing quantum states. Finally we hope that the construction can be used to quantum information science.

Acknowledgments

This work was supported by KIAS grant funded by the Korea government (MSIP) and partly supported by the IT R&D program of MOTIE/KEIT [10043464 (2013)]. The author especially would like to thank Dong Pyo Chi for providing valuable comments.

[1] A. Ambainis, M. Mosca, A. Tapp, and R. de Wolf, Private quantum channels, In IEEE Symposium on Foundations of Computer Sciences (FOCS), p. 547, (2000).
[2] D. Nagaj and I. Kerenidis, On the optimality of quantum encryption schemes, J. Math. Phys. 47, 092102 (2006).
[3] J. Bouda and M. Ziman, Optimality of private quantum channels, J. Phys. A: Math. Theor. 40, 5415–5426 (2007).
[4] A. Harrow, P. Hayden, and D. Leung, *Superdense coding of quantum states*, Phys. Rev. Lett. 92, 187901 (2004).

[5] P. Hayden, D. Leung, P. W. Shor, and A. Winter, *Randomizing quantum states: Constructions and applications*, Commun. Math. Phys. 250, 371–391 (2004).

[6] S. Wehner and A. Winter, *Entropic uncertainty relations—a survey*, New J. Phys. 12, 025009 (2010).

[7] D. P. Chi and K. Jeong, *Approximate Quantum State Sharings via Pair of Private Quantum Channels*, J. Quant. Info. Sci. 4, 64–70 (2014).

[8] M. B. Hastings, *Superadditivity of communication capacity using entangled inputs*, Nature Physics 5, 255–257 (2009).

[9] P. Hayden and A. Winter, *Counterexamples to the Maximal p-Norm Multiplicativity Conjecture for all p > 1*, Commun. Math. Phys. 284, 263–280 (2008).

[10] P. Dickinson and A. Nayak, *Approximate randomization of quantum states with fewer bits of key*, In AIP Conference Proceedings 864, 18–36 (2006).

[11] G. Aubrun, *On Almost Randomizing Channels with a Short Kraus Decomposition*, Commun. Math. Phys. 288, 1103–1116 (2009).

[12] G. Aubrun, *A REMARK ON THE PAPER “RANDOMIZING QUANTUM STATES: CONSTRUCTIONS AND APPLICATIONS”*, [http://arXiv.org/abs/0802.4193v1[quant-ph]], 2008.

[13] R. Bhatia, *Matrix analysis*, Graduate Texts in Mathematics 169. Berlin-Heidelberg-New York: Springer-Verlag, 1997.

[14] A. Ambainis and A. Smith, *Small Pseudo-random Families of Matrices: Derandomizing Approximate Quantum Encryption*, Proceedings of RANDOM’04, pp. 249–260 (2004).

[15] C. McDiarmid, *On the method of bounded differences*, Surveys in Combinatorics 141, 148–188 (1989).