Scientific Research Publishing

Journal of Quantum Information Science, 2021, 11, 1-12
https://www.scirp.org/journal/jqis
ISSN Online: 2162-576X
ISSN Print: 2162-5751

Approximate Private Quantum Channels on Fermionic Gaussian Systems

Kabgyun Jeong

Research Institute of Mathematics, Seoul National University, Seoul, Korea
Email: kgjeong6@snu.ac.kr

How to cite this paper: Jeong, K. (2021) Approximate Private Quantum Channels on Fermionic Gaussian Systems. *Journal of Quantum Information Science*, **11**, 1-12.
https://doi.org/10.4236/jqis.2021.111001

Received: December 14, 2020
Accepted: February 2, 2021
Published: February 5, 2021

Abstract

The private quantum channel (PQC) maps any quantum state to the maximally mixed state for the discrete as well as the bosonic Gaussian quantum systems, and it has fundamental meaning on the quantum cryptographic tasks and the quantum channel capacity problems. In this paper, we primally introduce a notion of *approximate* private quantum channel (ε-PQC) on *fermionic* Gaussian systems (*i.e.*, ε-FPQC), and construct its explicit form of the fermionic (Gaussian) private quantum channel. First of all, we suggest a general structure for ε-FPQC on the fermionic Gaussian systems with respect to the Schatten p-norm class, and then we give an explicit proof of the statement in the trace norm case. In addition, we study that the cardinality of a set of fermionic unitary operators agrees on the ε-FPQC condition in the trace norm case. This result may give birth to intuition on the construction of emerging fermionic Gaussian quantum communication or computing systems.

Keywords

Fermionic Private Quantum Channel, Approximate FPQC, Isotropic Measure, ε-Net Analysis, McDiarmid's Inequality

1. Introduction

In general, we can classify two intrinsic physical systems known as a bosonic system and a fermionic system. Each physical system undergoes a certain unitary transformation known as a state evolution or a quantum channel, which is mathematically completely positive and trace-preserving (CPT) map in quantum information theory, from a quantum state to another one [1] [2] [3]. Besides, the bosonic quantum states and (bosonic) channels are familiar in quantum information theory [4], the fermionic systems and its informational properties are

relatively unknown [5] [6]. In this reason, we try to investigate a fermionic quantum channel in the Gaussian regime, and then construct a (Gaussian) fermionic private quantum channel (FPQC) in the sense of quantum information theory (QIT) [7] [8] [9]. The notion of private quantum channel is very useful in the quantum cryptographic protocols as well as the channel capacity problems in quantum information theory. For example, two conjugate pairs of private quantum channels give rise to an additivity violation of the classical capacity for quantum channels [10] [11], so we naturally expect that FPQC also has the non-additive property in quantum channel capacity problems.

The private quantum channel (PQC), first introduced by Ambainis *et al.* [12], is a quantum communication primitive for secure transmission of a quantum information, and already has been proved not only the informational-security including its optimality [13] [14] but also reported several asymptotic secure transmission rates [15] [16] [17]. After applying the PQC on any quantum state, the output of the channel is always equivalent to the maximally mixed state, which has the highest entropy for a given dimension of the state, thus any wire-tappings are fundamentally impossible. Owing to cryptographic importance of PQC, it has several names such as quantum one-time pad, random unitary channel, ε-randomizing map and so on, here we call the map as ε-private quantum channel (ε-PQC) in the approximate consideration. While the conventional PQC is required exactly d^2 unitary operations to encrypt a d-dimension quantum state to the perfect maximally mixed state, ε-PQC (*i.e.*, approximate PQC) is only sufficient to use the number of unitary operations being less than $O(d\log d)$ [18], even $O(d)$ [19].

Here, let us formally define the ε-PQC in the general-setting through the Schatten p-norm class [20] [21]: For every quantum state $\varrho\in\mathcal{B}(\mathbb{C}^d)$ and any $\varepsilon>0$, if a quantum channel $\Lambda:\mathcal{B}(\mathbb{C}^d)\to\mathcal{B}(\mathbb{C}^d)$ satisfies the following inequality of

$$\left\|\Lambda(\varrho)-\frac{\mathbb{1}}{d}\right\|_p \le \frac{\varepsilon}{\sqrt[p]{d^{p-1}}}, \tag{1}$$

then we *call* the map Λ as *ε-private quantum channel* with respect to the Schatten p-norm (for all $p\ge 1$) [22] [23]. Notice that $\mathcal{B}(\mathbb{C}^d)$ denotes the bounded linear operator on the d-dimensional Hilbert space $\mathbb{C}^d$, and the Schatten p-norm is defined as follows: For any matrix $A\in\mathcal{B}(\mathbb{C}^d)$ and for all $1\le p\le\infty$, it has in the form of trace class as

$$\|A\|_p=\left[\mathrm{Tr}\left(A^\dagger A\right)^{p/2}\right]^{1/p}.$$

For convenience, we only consider $p=1$ case below, *i.e.*, the trace norm given by $\|A\|_1=\mathrm{Tr}\sqrt{A^\dagger A}$, however, we formulate the fermionic ε-PQC for arbitrary $p\ge 1$ (see Proposition 1). The operator norm and the Hilbert-Schmidt norm are given similar ways [18] [22]. Thus the ε-PQC in this trace class is taken in the form of $\left\|\Lambda(\rho)-\frac{\mathbb{1}}{d}\right\|_1\le\varepsilon$. Also, there are several variants of the PQC in

continuous-variable regimes [24] [25] [26] [27] and the multi-qubit protocol [28] [29].

We also remark on the possibility of certain relations between the approximate fermionic private quantum channel (ε-FPQC) and other information-theoretic settings. For examples, Clifford group C_n for n-qubit states is a subgroup of the unitary group $\mathcal{U}(d)$ for a qudit (that is, d-dimensional quantum state). Thus, we can easily observe that the above construction (*i.e.*, ε-FPQC) has very similar structure to the n-qubit secure protocol for quantum sequential transmission [29], magic-state construction [30], and an operator system in mathematics for the error correction schemes in qubit levels [31].

Now it is natural to ask how we can characterize the PQC in fermionic Gaussian systems and their impact on quantum information sciences such as the channel-capacity problem. At first, we briefly review the basic concepts of fermionic Gaussian systems and the channels.

This paper is organized as follows. In Sections 2.1 and 2.2, we review the basic of fermionic Gaussian systems and its representation of private quantum channels, respectively. In Section 3, we describe our main result on approximate private quantum channels on the fermionic system with explicit construction and proof over the trace norm. Finally we conclude our result in Section 4.

2. Preliminary

2.1. Fermionic Gaussian States

Generally, M-mode fermionic systems are associated with a tensor product of Hilbert space $\mathcal{H}^{\otimes M} = \bigotimes_{j=1}^{M} \mathcal{H}_j$, where M pairs of fermionic annihilation and creation operators $\left\{\hat{f}_j, \hat{f}_j^\dagger\right\}_{j=1}^{M}$ correspond to each mode of the total Hilbert space. The operators in the form of $\hat{\boldsymbol{f}}^{\mathrm{T}} := \left(\hat{f}_1, \cdots, \hat{f}_M, \hat{f}_1^\dagger, \cdots, \hat{f}_M^\dagger\right)$ satisfy the canonical anti-commutation relation (CAR) such that $\left\{\hat{f}_k, \hat{f}_\ell^\dagger\right\} = \hat{f}_k \hat{f}_\ell^\dagger + \hat{f}_\ell^\dagger \hat{f}_k = \delta_{k\ell} \mathbb{1}$. It was known that CAR algebra of M-mode fermionic system can be described by a set of the M-mode Majorana operators $\{\hat{c}_1, \cdots, \hat{c}_{2M}\}$ such that $\left\{\hat{c}_k, \hat{c}_\ell\right\} = 2\delta_{k\ell} \mathbb{1}$ as well as $\hat{c}_k = \hat{c}_k^\dagger$, and those operators in the Clifford algebra have the explicit forms of

$$\begin{cases} \hat{c}_{2k-1} = \sigma_1^z \otimes \cdots \otimes \sigma_{k-1}^z \otimes \sigma_k^x \otimes \mathbb{1}_2 \otimes \cdots \otimes \mathbb{1}_2 \\ \hat{c}_{2k} = \sigma_1^z \otimes \cdots \otimes \sigma_{k-1}^z \otimes \sigma_k^y \otimes \mathbb{1}_2 \otimes \cdots \otimes \mathbb{1}_2, \end{cases} \tag{2}$$

where $\mathbb{1}_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \sigma_k^x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_k^y = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}$, and $\sigma_k^z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ are Pauli matrices on the k-th qubit. We notice that, for each k-mode, $\hat{f}_k \hat{f}_k^\dagger = |0\rangle\langle 0|_k = \frac{1}{2}\left(1 - i\hat{c}_{2k-1}\hat{c}_{2k}\right)$, $\hat{f}_k^\dagger \hat{f}_k = |1\rangle\langle 1|_k = \frac{1}{2}\left(1 + i\hat{c}_{2k-1}\hat{c}_{2k}\right)$, and $\hat{\boldsymbol{c}}^{\mathrm{T}} := \left(\hat{c}_1, \cdots, \hat{c}_{2M}\right)$.

By exploiting the ingredients, let us define a fermionic Gaussian state as follows.

Definition 1 (Fermionic Gaussian state). *A fermionic state* ρ_F *is Gaussian*,

if it can be defined by

$$\rho_F = \lim_{\beta\to\pm\infty} \frac{\mathrm{e}^{\beta\hat{H}}}{Z(\beta)}, \tag{3}$$

where β is the inverse temperature, $Z(\beta)=\mathrm{Tr}\left(\mathrm{e}^{\beta\hat{H}}\right)$ the normalization factor, and the second order Hamiltonian $\hat{H}$ is given by

$$\hat{H} = \frac{i}{2}\hat{\boldsymbol{c}}^{\mathrm{T}}\Gamma\hat{\boldsymbol{c}} + \hat{\boldsymbol{c}}^{\mathrm{T}}\boldsymbol{x}. \tag{4}$$

Here, $\Gamma=-\Gamma^{\mathrm{T}}\in\mathcal{M}_{2M}(\mathbb{R})$ is a real skew-symmetric matrix and $\boldsymbol{x}\in\mathbb{R}^{2M}$. For convenience, we will set the temperature parameter as $\beta=1$.

Now, we only consider the quadratic term of the Hamiltonian $\hat{H}'=\frac{i}{2}\hat{\boldsymbol{c}}^{\mathrm{T}}\Gamma\hat{\boldsymbol{c}}$, *i.e.*, fermionic "even" Gaussian states. For *M*-mode fermionic cases, a Gaussian unitary is naturally given by $\mathrm{e}^{i\hat{H}}\in\mathcal{U}(2M)$, which can be decomposed in the form of $\mathrm{e}^{i\left(\hat{H}_1+\hat{H}_2\right)}$ through the Lie theory. Then it was known that there *exist* a fermionic Gaussian unitary and $2M\times 2M$ orthogonal matrix $\mathrm{e}^{\Gamma}\in\mathrm{SO}(2M)$ satisfying

$$\mathrm{e}^{i\hat{H}}\hat{\boldsymbol{c}}\mathrm{e}^{-i\hat{H}} = \mathrm{e}^{\Gamma}\hat{\boldsymbol{c}}. \tag{5}$$

For any (*M*-mode fermionic) *even* Gaussian states ρ_F, note that there exists a Gaussian unitary operator $\mathrm{e}^{i\hat{H}'}$ and an orthogonal matrix $O_\Gamma\in\mathrm{SO}(2M)$ such that

$$\begin{aligned}\rho_F &= \frac{1}{Z}\mathrm{e}^{\hat{H}'} = \mathrm{e}^{i\hat{H}'}\cdot\frac{1}{Z}\mathrm{e}^{\frac{i}{2}\hat{\boldsymbol{c}}^{\mathrm{T}}O_\Gamma A O_\Gamma^{\mathrm{T}}\hat{\boldsymbol{c}}}\cdot\mathrm{e}^{-i\hat{H}'}\\ &= \bigotimes_{k=1}^{M}\left(\frac{1+\lambda_k}{2}|0\rangle\langle 0|_k + \frac{1-\lambda_k}{2}|1\rangle\langle 1|_k\right) \equiv \bigotimes_{k=1}^{M}\rho_{F,k},\end{aligned} \tag{6}$$

where $A=\bigoplus_{k=1}^{M}\begin{pmatrix}0 & \lambda_j\\ -\lambda_j & 0\end{pmatrix}$ with its spectrum $\lambda_k\in[0,1]$. Furthermore, for any *k*, if $\lambda_k=1$, then $\rho_F\in\mathcal{H}\left(\mathbb{C}^{2M}\right)$ is said to be a pure state, *i.e.*, pure fermionic Gaussian state is given by $\rho_F=|0\rangle\langle 0|_1\otimes\cdots\otimes|1\rangle\langle 1|_M$. In those cases, the entropy of the *M*-mode fermionic Gaussian state is defined by

$$S(\rho_F) = \sum_{k=1}^{M} S(\rho_{F,k}), \tag{7}$$

where $S(\rho_{F,k}) := -\frac{1+\lambda_k}{2}\log\frac{1+\lambda_k}{2} - \frac{1-\lambda_k}{2}\log\frac{1-\lambda_k}{2}$ is the von Neumann entropy of the fermionic system.

As mentioned above, it is useful to study a private quantum channel in quantum information science, because the output of PQC gives birth to a maximally mixed state (MMS) at the end of the channel. This output state of the channel directly corresponds to a maximally entangled state (MES) as in Ref. [32] [33] via a quantum purification method [34]. However, an explicit concept of "approximate" fermionic private quantum channel does not exist, so for. In this reason, our main purpose of this work is to introduce such a notion (*i.e.*, ε-FPQC) at first.

2.2. Representation of Fermionic Gaussian Quantum Channels: The Fermionic Private Quantum Channel

In 2005, Bravyi first introduced the notion of fermionic Gaussian quantum channels as follows [5]: For any completely positive and trace-preserving map, the fermionic Gaussian channel Λ_F is given by

$$\Lambda_F\left(\hat{c}_k\right)=\xi_k\hat{c}_k,\ \forall k=1,\cdots,2M \text{ and } \Lambda_F\left(\hat{\boldsymbol{c}}\left(\vec{b}\right)\right)=\prod_{k;b_k=1}\xi_k\hat{\boldsymbol{c}}\left(\vec{b}\right), \tag{8}$$

where $\hat{\boldsymbol{c}}\left(\vec{b}\right)=\hat{c}_1^{b_1}\hat{c}_2^{b_2}\cdots\hat{c}_{2M}^{b_{2M}}$ with a binary string $\vec{b}=\left(b_1,\cdots,b_{2M}\right)$. Here we note that $0\le\xi_1,\cdots,\xi_{2M}\le 1$ are real parameters characterizing the fermionic quantum channels and it is called the *attenuation* coefficient. Now, we are ready to define the fermionic private quantum channel in the form of Kraus representation. For any fermionic Gaussian state ρ_F, the fermionic Gaussian channel Λ_F is described by

$$\Lambda_F\left(\rho_F\right)=\frac{1}{|\mathcal{U}|}\sum_{\ell=1}^{|\mathcal{U}|}U_\ell\rho_F U_\ell^\dagger, \tag{9}$$

where $U_\ell=i\pi\hat{c}_\ell$ such that $U_\ell\hat{c}_m=\left(-1\right)^{\delta_{\ell m}}\hat{c}_m U_\ell$ with $\pi=\left(-1\right)^M\hat{c}_1\cdots\hat{c}_{2m},\forall m=1,\cdots,2M$. Note that $|\mathcal{U}|$ denotes the cardinality of the unitaries on the unitary group $\mathcal{U}(2M)$. In the optimal case, the cardinality of U is given by $|\mathcal{U}|=(2M)^2$ (See Figure 1).

Definition 2 (Fermionic ε-private quantum channel). *For any fermionic* (*Gaussian*) *state* ρ_F *and any* $\varepsilon>0$, *if a fermionic Gaussian quantum channel* $\Lambda_F:\mathcal{H}^{\otimes M}\to\mathcal{H}^{\otimes M}$ *satisfies*

$$\left\|\Lambda_F\left(\rho_F\right)-\frac{\mathbb{1}}{2M}\right\|_p\le\frac{\varepsilon}{\sqrt[p]{d^{p-1}}}, \tag{10}$$

then the channel $\Lambda_F(\cdot)$ is said to be *approximate fermionic private quantum channel* (or ε-FPQC) with respect to the Schatten p-norm (for all $p\ge1$).

For the case of $p=1$, ε-FPQCs are taken in the form of $\left\|\Lambda_F\left(\rho_F\right)-\frac{\mathbb{1}}{2M}\right\|_1\le\varepsilon$.

Here, we shortly introduce an isotropic measure, which preserves a symmetry of a set of quantum states. To intuitively obtain the relationship between FPQCs and symmetries, we need to take the notion of an isotropic measure (or Haar measure) on the unitary group $\mathcal{U}(2M)$. The isotropic measure for any quantum states is formally defined as follows [19].

Figure 1. Schematic diagram for M-mode fermionic private quantum channel Λ_F. For any fermionic Gaussian state ρ_F, if an output of the channel is $\frac{\mathbb{1}}{2M}$, then we call the channel as *perfact* fermionic PQC. Otherwise, *i.e.*, the channel's output is almost close to $\frac{\mathbb{1}}{2M}$, then the channel is called as approximate FPQC or ε-FPQC.

Definition 3. *For any fermionic quantum state* $\rho_F \in \mathcal{H}\left(\mathbb{C}^{2M}\right)$, *a probability measure* μ *on the unitary group* $\mathcal{U}(2M)$ *is said to be isotropic, if it satisfies that*

$$\int_{\mathcal{U}(2M)} U\rho_F U^\dagger \mathrm{d}\mu = \frac{\mathbb{1}}{2M}. \tag{11}$$

Moreover, a random vector v generated by $U \in \mathcal{U}(2M)$ is known to be isotropic if its law is isotropic. Conceptually, this implies that the integration over all random vectors (generated by U) equals to zero (that is, it forms a maximally mixed state).

Then, we are ready to state our main result of the approximate fermionic private quantum channel for randomizing fermionic Gaussian quantum states.

3. Main Results

We have briefly reviewed the concrete notions on fermionic Gaussian systems and the definition of the approximate private quantum channels on fermionic systems, so now we will introduce our main results. While the proposed results are simple, the proofs are subtle complicated. However, the statements have a fundamental meaning in quantum communication theory on whether the fermionic Gaussian systems are tractable in quantum channel capacity problems or not. If we find an explicit form of the fermionic PQC similar to the bosonic PQCs, e.g., in Refs. [24] [25], we can further argue on the topic of the quantum channel capacity problems as well as its non-additive properties.

According to the Hayden *et al.*'s [18], Dickinson and Nayak's [23], and also our previous result [20] [21], we suggest a following proposition.

Proposition 1 (Approximate fermionic PQC). *Let* ρ_F *be an M-mode fermionic Gaussian state, and* $\Lambda_F\left(\rho_F\right) = \frac{1}{|\mathcal{U}|}\sum_{\ell=1}^{|\mathcal{U}|} U_\ell \rho_F U_\ell^\dagger$ *be an ε-FPQC satisfying the isotropic measure with respect to the Schatten p-norm. Then, for any* $\varepsilon > 0$ *and for sufficiently large M, there exists a set of fermionic unitary operators* $\left\{U_\ell = i\pi\hat{c}_\ell\right\}_{\ell=1}^{|\mathcal{U}|}$ *in* $\mathcal{U}(2M)$ *with the cardinality at least*

$$|\mathcal{U}| \geq 2\kappa M \log \frac{10(2M)^{(p-1)/p}}{\varepsilon}, \tag{12}$$

where κ is an absolute constant.

Here, we present a proof only on the case of $p = 1$ as mentioned in Introduction. In this case, we can fix the logarithmic factor as $\log\frac{10}{\varepsilon}$, and from the independence of the mode *M*, it can be omitted. Also, notice that the cardinality could be reduced by $4M^2$ to $O(2M\log 2M)$ by the proposition 1.

Proposition 2 (*ε*-FPQC for $p = 1$ case). *Let* $\Lambda_F\left(\rho_F\right) = \frac{1}{|\mathcal{U}|}\sum_{\ell=1}^{|\mathcal{U}|} \pi\hat{c}_\ell \rho_F \left(\pi\hat{c}_\ell\right)^\dagger$ *be an ε-FPQC satisfying the isotropic measure with respect to the trace norm. Then, for any* $\varepsilon > 0$ *and* $M \gg 1$, *there exists a set of Majorana operators* $\left\{i\pi\hat{c}_\ell\right\}_{\ell=1}^{|\mathcal{U}|}$ *in* $\mathcal{U}(2M)$ *with the cardinality of*

$$\left|\mathcal{U}\right| \geq 2\kappa M, \tag{13}$$

where κ is also an absolute constant as in Proposition 1.

For the proof we are required two technical lemmas. Below Lemma 1 states that pure quantum states on Bloch sphere on any dimension can be discretized into net points forming a regularized polyhedron in the given dimension, and Lemma 2, which is a variant of the famous Lévy' theorem [35], endows us to estimate an exponentially decaying of the tale probability distribution on a random variable. Those lemmas are universal not only in the bosonic Gaussian system but also in the fermionic Gaussian one.

Lemma 1 (ε-net [18]). *Let* $\varepsilon > 0$ *and the Majorana mode* $M \gg 1$. *For any fermionic pure Gaussian states* $\left|\varphi_F\right\rangle \in \mathcal{H}^M$, *we can choose a net point* $\left|\tilde{\varphi}_F\right\rangle \in N$ *such that* $\left\|\varphi_F - \tilde{\varphi}_F\right\|_1 \leq \varepsilon$. *Then there exists a net N of pure fermionic states satisfying*

$$\left\|N\right\| \leq \left(5/\varepsilon\right)^{4M}. \tag{14}$$

Lemma 2 (McDiarmid inequality [36]). *Let* $\left\{X_k\right\}_{k=1}^m \subset S$ *be independent random variables chosen uniformly at random. Let a measurable function* $F: S^m \to \mathbb{R}$ *satisfy* $\left|F\left(x\right) - F\left(\hat{x}\right)\right| \leq c_k$, *called the bounded difference, where the vectors x and* $\hat{x}$ *differ only in the k-th position. If we define a random variable* $Y = F\left(X_1, \cdots, X_m\right)$, *then* ($\forall t \geq 0$)

$$\Pr\left[\left|Y - \mathbf{E}\left(Y\right)\right| \geq t\right] \leq 2\mathrm{e}^{-2t^2/\sum_{k=1}^m c_k^2}, \tag{15}$$

where $\mathbf{E}\left(Y\right)$ denotes the expectation value for the random variable *Y*.

In the fermionic Gaussian regime, suppose that the fermionic PQC Λ_F is realized by a sequence of the Majorana operators $\left(i\pi\hat{c}_k\right)_{k=1}^{\left|\mathcal{U}\right|}$, and the other map Λ_F' is given by $\left(i\pi\hat{c}_1, \cdots, i\pi\hat{c}_k', \cdots, i\pi\hat{c}_{\left|\mathcal{U}\right|}\right)$, respectively. Then we have the *bounded* difference as

$$\begin{aligned}
&\left|\left\|\Lambda_F\left(\varphi_F\right) - \frac{\mathbb{1}}{2M}\right\|_1 - \left\|\Lambda_F'\left(\varphi_F\right) - \frac{\mathbb{1}}{2M}\right\|_1\right| \\
&\leq \left\|\Lambda_F\left(\varphi_F\right) - \Lambda_F\left(\varphi_F\right)'\right\|_1 \\
&= \frac{1}{\left|\mathcal{U}\right|}\left\|\pi\hat{c}_k\varphi_F\left(\pi\hat{c}_k\right)^\dagger - \pi\hat{c}_k'\varphi_F\left(\pi\hat{c}_k'\right)^\dagger\right\|_1 \\
&\leq \frac{2}{\left|\mathcal{U}\right|},
\end{aligned}$$

where we make use of the norm convexity and the fact of $\left\|\phi - \phi'\right\|_1 \leq 2$ for any quantum states. From the McDiarmid inequality (on the positive part), we estimate that

$$\Pr\left[Y_{\varphi_F} \geq t + \left(\frac{2M}{\left|\mathcal{U}\right|} + \frac{1}{2M}\right)\right] \leq \mathrm{e}^{-\left|\mathcal{U}\right|t^2/2}, \tag{16}$$

where $Y_{\varphi_F} := \left\|\Lambda_F\left(\varphi_F\right) - \frac{\mathbb{1}}{2M}\right\|_1$.

Now, we are ready to prove the Proposition 2. That is, ε-FPQC can be fulfilled when we take the fermionic unitary operators as in the order of the cardinality $|\mathcal{U}|$.

Proof. Let the set of Majorana operators $\{i\pi\hat{c}_k\}_{k=1}^{|\mathcal{U}|}$ be an i.i.d. random variable distributed according to the Haar measure. We can prove that the fernionic map Λ_F is the ε-FPQC in high probability.

If we fix the net $\mathcal{N}$ in Lemma 1, and define $\tilde{\varphi}_F$ to be a net point on the fermionic pure Gaussian states φ_F. Then, by the unitary invariance, we can conclude that

$$\left\|\Lambda_F(\varphi_F)-\Lambda_F(\tilde{\varphi}_F)\right\|_1=\left\|\varphi_F-\tilde{\varphi}_F\right\|_1\le\frac{\varepsilon}{2}. \tag{17}$$

Thus, from the ε-net lemma, we can obtain the net with the cardinality $|N|\le(20M/\varepsilon)^{4M}$. This implies that

$$\begin{aligned}&\mathrm{Pr}_{\forall\varphi_F}\left[\left\|\Lambda_F(\varphi_F)-\frac{\mathbb{1}}{2M}\right\|_1\ge\varepsilon\right]\\&\le\mathrm{Pr}_{\forall\varphi_F,\tilde{\varphi}_F}\left[\left\|\Lambda_F(\varphi_F)-\Lambda_F(\tilde{\varphi}_F)\right\|_1+\left\|\Lambda_F(\tilde{\varphi}_F)-\frac{\mathbb{1}}{2M}\right\|_1\ge\varepsilon\right]\\&\le\mathrm{Pr}_{\forall\tilde{\varphi}_F}\left[\left\|\Lambda_F(\tilde{\varphi}_F)-\frac{\mathbb{1}}{2M}\right\|_1\ge\frac{\varepsilon}{2}\right],\quad(*)\end{aligned} \tag{18}$$

where we have used the triangle inequality and Equation (17).

Finally, by using the union bound and the net construction above, we can derive following inequalities:

$$\begin{aligned}(*)&\le|N|\cdot Pr_{\forall\tilde{\varphi}_F^{(1)}}\left[\left\|\Lambda_F(\tilde{\varphi}_F^{(1)})-\frac{\mathbb{1}}{2M}\right\|_1\ge\frac{\varepsilon}{2}\right]\\&\le2\left(\frac{20M}{\varepsilon}\right)^{4M}\exp\left[-|\mathcal{U}|\left(\frac{\varepsilon}{4M}-\frac{(2M)^{1/2M}}{|\mathcal{U}|}-\frac{1}{2M}\right)^2\right].\end{aligned} \tag{19}$$

This completes the proof if the probability is bounded by 1 (see Lemma 3 below), and $|\mathcal{U}|\ge2\kappa M$ with $\kappa:=\frac{1}{c\varepsilon^2}\log\left(\frac{10}{\varepsilon}\right)$ for a constant c.

Lemma 3. *For sufficiently large M, if we take the cardinality as in the form of*

$$|\mathcal{U}|\ge2M\frac{1}{c\varepsilon^2}\log\left(\frac{10}{\varepsilon}\right), \tag{20}$$

then the probability we required in Equation (*19*) *is upper bounded by 1.*

Proof. For sufficiently large $|\mathcal{U}|$ satisfying $2M<|\mathcal{U}|<(2M)^2$, we can take the bound as

$$2\left(\frac{20M}{\varepsilon}\right)^{4M}\exp\left[-|\mathcal{U}|\left(\frac{\varepsilon}{4M}-\frac{(2M)^{1/2M}}{|\mathcal{U}|}-\frac{1}{2M}\right)^2\right]<1. \tag{21}$$

By the straightforward calculation, this bound gives rise to $|\mathcal{U}|\le4M^2$ we

expected. Here, if we fix the mode M and choose $2M$ so that $\left(\frac{\varepsilon}{2}-\frac{2(2M)^{1/2M}}{|\mathcal{U}|}\right)^2 = o(\varepsilon^2)$, then we have

$$2M\log\left(\frac{10}{\varepsilon}\right) < c|\mathcal{U}|\varepsilon^2.$$

This construction shown to be that it is possible to construct an approximate fermionic private quantum channel using the fermionic unitaries only within cardinality $|\mathcal{U}| \geq 2\kappa M$, beside $O(M^2)$ in the optimal case. If we take a quantum purification, which describes that any mixed state can be transformed into a higher dimensional pure state, then we can always create a pure entangled state on fermionic Gaussian systems, for example in Ref. [37].

4. Conclusions

In this paper, we have firstly proposed an approximate private quantum channel for the fermionic Gaussian systems namely, ε-FPQC, and we make a useful formula to construct the quantum channel explicitly including its cardinality of needing unitary operations. While the fermionic PQC is needed exactly $4M^2$ fermionic unitary operations to encrypt an M-mode fermionic Gaussian state, our ε-FPQC is only sufficient to consume the number of unitary operations about $O(M\log M)$ in Proposition 2.

Beyond the bosonic Gaussian quantum channels, we expect that this kind of a research on fermionic channels will be meaningful for deep understanding of the quantum channel capacity problems *i.e.*, the additivity violations for general capacities in broad Gaussian regimes. That is if we know the exact form of a quantum purified state, which has a fermionic maximal entanglement, a research on the channel capacity problems could be also useful.

A few interesting questions remain for the fermionic private quantum channel itself or beyond. The first one is that how those channels can be applied on fermionic Gaussian systems such as a quantum communication or computing involving a certain condition of security issues. The second one is a question of that the approximate FPQCs can connect to a geometric shape, as in the case of the discrete PQCs relating regular polyhedra. Finally, this work is expected to contribute to establishing contact with physicists who are well acquainted on the fermionic theory with the quantum information soiciety.

Acknowledgements

This work was supported by the National Research Foundation of Korea through a grant funded by the Ministry of Science and ICT (NRF-2020M3E4A1077861) and the Ministry of Education (NRF-2018R1D1A1B07047512).

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Hayashi, M. (2016) Quantum Information Theory: Mathematical Foundation. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-49725-8

[2] Wilde, M.M. (2017) Quantum Information Theory. Cambridge University Press, Cambridge. https://doi.org/10.1017/9781316809976

[3] Watrous, J. (2018) The Theory of Quantum Information. Cambridge University Press, Cambridge.

[4] Weedbrook, C., Pirandola, S., García-Patrón, R., Cerf, N.J., Ralph, T.C., Shapiro, J.H., and Lloyd, S. (2012) Gaussian Quantum Information. *Reviews of Modern Physics*, **84**, 621. https://doi.org/10.1103/RevModPhys.84.621

[5] Bravyi, S. (2005) Classical Capacity of Fermionic Product Channels. https://arxiv.org/abs/quant-ph/0507282

[6] Spee, C., Schwaiger, K., Giedke, G. and Kraus, B. (2018) Mode Entanglement of Gaussian Fermionic States. *Physical Review A*, **97**, Article ID: 042325. https://doi.org/10.1103/PhysRevA.97.042325

[7] Friss, N., Lee, A.R. and Bruschi, D.E. (2013) Fermionic-Mode Entanglement in Quantum Information. *Physical Review A*, **87**, Article ID: 022338. https://doi.org/10.1103/PhysRevA.87.022338

[8] Gluza, M., Kliesch, M., Eisert, J. and Aolita, L. (2018) Fidelity Witnesses for Fermionic Quantum Simulations. *Physical Review Letters*, **120**, Article ID: 190501. https://doi.org/10.1103/PhysRevLett.120.190501

[9] Lugli, M., Perinotti, P. and Tosini, A. (2020) Fermionic State Discrimination by Local Operations and Classical Communication. *Physical Review Letters*, **125**, Article ID: 110403. https://doi.org/10.1103/PhysRevLett.125.110403

[10] Hastings, M.B. (2009) Superadditivity of Communication Capacity Using Entangled Inputs. *Nature Physics*, **5**, 255-257. https://doi.org/10.1038/nphys1224

[11] Hayden, P. and Winter, A. (2008) Counterexamples to the Maximal p-Norm Multiplicativity Conjecture for All p >1. *Communications in Mathematical Physics*, **284**, 263-280. https://doi.org/10.1007/s00220-008-0624-0

[12] Ambainis, A., Mosca, M., Tapp, A. and de Wolf, R. (2000) Private Quantum Channels. *Proceedings* 41*st Annual Symposium on Foundations of Computer Science*, Redondo Beach, 12-14 November 2000, 547-553.

[13] Nagaj, D. and Kerenidis, I. (2006) On the Optimality of Quantum Encryption Schemes. *Journal of Mathematical Physics*, **47**, Article ID: 092102. https://doi.org/10.1063/1.2339014

[14] Bouda, J. and Ziman, M. (2007) Optimality of Private Quantum Channels. *Journal of Physics A*: *Mathematical and Theoretical*, **40**, 5415. https://doi.org/10.1088/1751-8113/40/20/011

[15] Cai, N., Winter, A. and Yeung, R.W. (2004) Quantum Privacy and Quantum Wiretap Channels. *Problems of Information Transmission*. **40**, 318-336. https://doi.org/10.1007/s11122-005-0002-x

[16] Devetak, I. (2005) The Private Classical Capacity and Quantum Capacity of a Quantum Channel. *IEEE Transactions on Information Theory*, **51**, 44-55. https://doi.org/10.1109/TIT.2004.839515

[17] Hayashi, M. (2015) Quantum Wiretap Channel With Non-Uniform Random Number and Its Exponent and Equivocation Rate of Leaked Information. *IEEE Transactions on Information Theory*, **61**, 559-5622.

https://doi.org/10.1109/TIT.2015.2464215

[18] Hayden, P., Leung, D., Shor, P.W. and Winter, A. (2004) Randomizing Quantum States: Constructions and Applications. *Communications in Mathematical Physics*, **250**, 371. https://doi.org/10.1007/s00220-004-1087-6

[19] Aubrun, G. (2009) On Almost Randomizing Channels with a Short Kraus Decomposition. *Communications in Mathematical Physics*, **288**, 1103-1116. https://doi.org/10.1007/s00220-008-0695-y

[20] Jeong, K. (2012) Randomizing Channels in Quantum Information Theory. PhD Thesis, Seoul National University, Seoul.

[21] Jeong, K. (2014) Randomizing Quantum States to Shatten *p*-Norm for All p ≥1. *AIP Conference Proceedings*, **1633**, 171. https://doi.org/10.1063/1.4903127

[22] Ambainis, A. and Smith, A. (2004) Small Pseudo-Random Families of Matrices: Derandomizing Approximate Quantum Encryption. *Proceedings of 7th International Workshop on Approximation Algorithms for Combinatorial Optimization Problems 8th International Workshop on Randomization and Computation*, Cambridge, 22-24 August 2004, 249-260. https://doi.org/10.1007/978-3-540-27821-4_23

[23] Dickinson, P.A. and Nayak, A. (2006) Approximate Randomization of Quantum States with Fewer Bits of Key. *AIP Conference Proceedings*, **864**, 18. https://doi.org/10.1063/1.2400876

[24] Brádler, K. (2005) Continuous-Variable Private Quantum Channel. *physical review A*, **72**, Article ID: 042313. https://doi.org/10.1103/PhysRevA.72.042313

[25] Jeong, K., Kim, J. and Lee, S.-Y. (2015) Gaussian Private Quantum Channel with Squeezed Coherent States. *Scientific Reports*, **5**, Article No. 13974. https://doi.org/10.1038/srep13974

[26] Wu, Y., Cai, R., He, G. and Zhang, J. (2014) Quantum Secret Sharing with Continuous Variable Graph State. *Quantum Information Processing*, **13**, 1085-1102. https://doi.org/10.1007/s11128-013-0713-7

[27] Bouda, J., Sedlák, M. and Ziman, M. (2020) Private Quantum Channels for Multi-Photon Pulses and Unitary *k*-Designs. arXiv: 2009.06067. https://arxiv.org/abs/2009.06067

[28] Chi, D.P. and Jeong, K. (2014) Approximate Quantum State Sharings via Pair of Private Quantum Channels. *Journal of Quantum Information Science*, **4**, 64-70. http://dx.doi.org/10.4236/jqis.2014.41006

[29] Jeong, K. and Kim, J. (2015) Secure Sequential Transmission of Quantum Information. *Quantum Information Processing*, **14**, 3523-3531. https://doi.org/10.1007/s11128-015-1054-5

[30] Hebenstreit, M., Jozsa, R., Kraus, B., Strelchuk, S. and Yoganathan, M. (2019) All Pure Fermionic Non-Gaussian States Are Magic States for Matchgate Computations. *Physical Review Letters*, **123**, Article ID: 080503. https://doi.org/10.1103/PhysRevLett.123.080503

[31] Li, C.-K., Nakahara, M., Poon, Y.-T., Sze, N.-S. and Tomita, H. (2011) Efficient Quantum Error Correction for Fully Correlated Noise. *Physics Letters A*, **375**, 3255-3258. https://doi.org/10.1016/j.physleta.2011.07.027

[32] Jeong, K. and Lim, Y. (2016) Purification of Gaussian Maximally Mixed States. *Physics Letters A*, **380**, 3607-3611. https://doi.org/10.1016/j.physleta.2016.09.001

[33] Lim, Y., Kim, J., Lee, S. and Jeong, K. (2019) Maximally Entangled States in Discrete and Gaussian Regimes. *Quantum Information Processing*, **18**, Article No. 43. https://doi.org/10.1007/s11128-018-2160-y

[34] Hughston, L.P., Jozsa, R. and Wootter, W.K. (1993) A Complete Classification of Quantum Ensembles Having a Given Density Matrix. *Physics Letters A*, **183**, 14-18. https://doi.org/10.1016/0375-9601(93)90880-9

[35] Levy, P. (1951) Problèmes Concrets d'Analyse Fonctionnelle. Gauthier-Villars, Paris.

[36] McDiarmid, C. (1989) On the Method of Bounded Differences. *Surveys in Combinatorics*, 1989, **141**, 148-188. https://doi.org/10.1017/CBO9781107359949.008

[37] Di Tullio, M., Rossignoli, R., Cerezo, M. and Gigena, N. (2019) Fermionic Entanglement in the Lipkin Model. *Physical Review A*, **100**, Article ID: 062104. https://doi.org/10.1103/PhysRevA.100.062104