ISIT'2013 1569718495

Second Order Asymptotics for Random Number Generation

Wataru Kumagai*† and Masahito Hayashi†‡,
*Graduate School of Information Sciences, Tohoku University, Japan
Email: kumagai@ims.is.tohoku.ac.jp
†Graduate School of Mathematics, Nagoya University, Japan
Email: masahito@math.nagoya-u.ac.jp
‡Centre for Quantum Technologies, National University of Singapore, Singapore

***Abstract*—We treat a random number generation from an i.i.d. probability distribution of P to that of Q. When Q or P is a uniform distribution, the problems have been well-known as the uniform random number generation and the resolvability problem respectively, and analyzed not only in the context of the first order asymptotic theory but also that in the second asymptotic theory. On the other hand, when both P and Q are not a uniform distribution, the second order asymptotics has not been treated. In this paper, we focus on the second order asymptotics of random number generation for arbitrary probability distributions P and Q on a finite set. In particular, we derive the optimal second order generation rate under an arbitrary permissible confidence coefficient.**

I. Introduction

Random number generation is one of the most basic problems in information theory. The purpose of random number generation is to approximate a sequence of target probability distributions Q_n by transforming another sequence of probability distributions P_n. When Q_n or P_n is a uniform distribution, each problem corresponds to the uniform random number generation problem or the resolvability problem respectively, and has been well studied. For example, when P_n and Q_n are the i.i.d. probability distributions P^n and U_2^{an} where U_2 is the uniform distribution with the support size 2, the optimal first order generation rate a from P^n is the entropy $H(P)$ under the condition that the error goes to 0. Those problems are analyzed not only in the context of the first order asymptotic theory but also that in the second asymptotic theory. In the most general case, it is known that the first and the second order optimal rates in those problems can be described by information spectrum methods [1], [3], [4]. In particular, for transformation between P^n and $U_2^{an+b\sqrt{n}}$, the results in information spectrum gives optimal rates a and b. On the other hand, when both P_n and Q_n are not a uniform, the problem has not been treated sufficiently. In this paper, we do not restrict both P_n and Q_n to a uniform distribution and focus on the second order asymptotics of a random number generation for arbitrary i.i.d. probability distributions on a finite set. In particular, we derive the optimal second order generation rate under an arbitrary permissible confident coefficient.

In this paper, we utilize the notion of the majorization. It is a pre-order between two probability distributions which can be defined on different finite sets. If a probability distribution P_n is transformed to $W_n(P_n)$ by a deterministic transformation W_n, the transformed probability distribution $W_n(P_n)$ "majorizes" the original probability distribution P_n. In other words, $W_n(P_n)$ is larger than P_n in the sense of the majorization relation. Therefore, when we want to approximate a target probability distribution Q_n from an original probability distribution P_n, for an arbitrary deterministic transformation W_n, there is a probability distribution P'_n which majorizes P_n and is close to Q_n than $W_n(P_n)$. Thus, the performance of the optimization under the majorization condition gives a bound of that under deterministic transformations. The majorization is used in a transformation theory of quantum entangled states and corresponds to a operation called LOCC in the quantum information theory [9], [6]. Our results can be extended to the quantum settings but we do not mention it in this paper.

The paper is organized as follows. In section II, we introduce a notion of majorization, and consider approximation problems under a majorization condition and by a deterministic transformation. In section III, although the purpose of the paper is to treat the case when both a source and a target distribution are non-uniform, we firstly treat the second order asymptotics of the approximation problem when a source or a target distribution is a uniform distribution. In analysis of the non-uniform cases, it is required to use the fact that the variance of logarithms of a source and a target distribution are not zero. On the other hand, in the uniform cases, since the variance of a logarithm of a uniform distribution is zero, a method used in the non-uniform cases can not be applied, and hence, we have to separately treat the uniform case. In section IV, we state about the main results in the paper, that is, the second order asymptotics of the approximation problem when both a source and a target distributions are not a uniform distribution. In section V, we prove one of propositions which is essential to derive our main theorem. In section VI, we state the conclusion of the paper.

II. One-Shot Formulation

In this section, we introduce some notation and definition, and formulate our problem. For a probability distribution P on finite set $\mathcal{X}$ and a map $W : \mathcal{X} \to \mathcal{Y}$, the probability distribution $W(P)$ on $\mathcal{Y}$ is defined by $W(P)(y) :=$

$\sum_{x\in W^{-1}(y)} P(x)$. We introduce a value F called the Bhattacharyya coefficient or the fidelity between probability distributions over the same discrete set $\mathcal{Y}$ as

$$F(Q,Q') := \sum_{y\in\mathcal{Y}} \sqrt{Q(y)Q'(y)}. \tag{1}$$

This value F represents how close two probability distributions are and relates to the Hellinger distance d_H as $d_H(\cdot,\cdot) = \sqrt{1-F(\cdot,\cdot)}$. Then our main purpose is to analyze the following value

$$L(P,Q|\nu) := \max\{L|F(W(P),Q^L) \geq \nu, W : \mathcal{X} \to \mathcal{Y}^L\}. \tag{2}$$

This means the maximal number L of Q^L which can be transformed from P under a confidence coefficient $0 < \nu < 1$. When we define the maximal fidelity F from P on $\mathcal{X}$ to Q on $\mathcal{Y}$ by

$$F(P \to Q) := \max\{F(W(P),Q)|W : \mathcal{X} \to \mathcal{Y}\}, \tag{3}$$

then L is rewritten as

$$L(P,Q|\nu) = \max\{L|F(P \to Q^L) \geq \nu\}. \tag{4}$$

Next, we will introduce the notion of the majorization to evaluate F. For a probability distribution P on a finite set, let $P^{\downarrow}$ be a sequence $\{P_i^{\downarrow}\}_{i=1}^{\infty}$ where $P_i^{\downarrow}$ is the element of $\{P(x)\}_{x\in\mathcal{X}}$ sorted in decreasing order for $1 \leq i \leq |\mathcal{X}|$ and $P_i^{\downarrow}$ is 0 for $|\mathcal{X}| < i$. When probability distributions P and Q satisfy $\sum_{i=1}^{l} P_i^{\downarrow} \leq \sum_{i=1}^{l} Q_i^{\downarrow}$ for any l, it is said that P is majorized by Q and written as $P \prec Q$. Here, note that the sets where P and Q are defined do not necessarily coincide with each other. The majorization relation is a pre-order on a set of probability distributions in which each distribution is defined on a finite set [2]. We introduce the maximal fidelity under the majorization condition as

$$F^M(P \to Q) := \max\{F(P',Q)|P \prec P' \ on \ \mathcal{Y}\} \tag{5}$$

where P and Q are probability distribution on $\mathcal{X}$ and $\mathcal{Y}$, respectively. Since $P \prec W(P)$ for a map $W : \mathcal{X} \to \mathcal{Y}$,

$$F^M(P \to Q) \geq F(P \to Q) \tag{6}$$

holds. In many case, $F^M(P \to Q)$ is easily treatable than $F(P \to Q)$. In particular, the value of F^M can be explicitly described in one-shot situation [8]. We proceed to the asymptotics of random number generation in the next section.

III. Second Order Asymptotics for Uniform Distribution

We focus on the approximation from P^n to $Q^{an+b\sqrt{n}}$. For a fixed confidence coefficient $0 < \nu < 1$, we derive the second order asymptotic expansion of $L_n(P,Q|\nu)$. Let U_2 be the uniform distribution with the support size 2 in the following.

At first, we consider the second order asymptotics for resolvability. For a fixed confidence coefficient $0 < \nu < 1$, the second order asymptotic expansion is represented as follows.

Theorem 1: Let Q be an arbitrary probability distribution on a finite set except for a uniform distribution. Then the second order asymptotic expansion is described as

$$\begin{aligned} &L_n(U_2,Q|\nu) \\ &= H(Q)^{-1}n - \sqrt{\frac{V(Q)}{H(Q)^3}}\Phi^{-1}(\nu^2)\sqrt{n} + o(\sqrt{n}), \end{aligned} \tag{7}$$

where Φ is the cumulative distribution function of the standard normal distribution, $H(P)$ is the entropy of P and

$$V(P) := \sum_{x\in\mathcal{X}} P(x)(-\log P(x) - H(P))^2. \tag{8}$$

We remark that Nomura and Han [3] treated the second order rate, which is the coefficient of $\sqrt{n}$ in the expansion, under a constraint for the variational distance. Since we consider a constraint for the fidelity as in (4), the formulations in [3] and ours are slightly different, and hence, Theorem 1 has not been obtained. The optimal second order rate in (7) is easily calculated by the following proposition.

Proposition 2: Let Q be an arbitrary probability distribution on a finite set except for a uniform distribution. Then

$$\begin{aligned} &\lim_{n\to\infty} F(U_2^n \to Q^{H(Q)^{-1}n+b\sqrt{n}}) \\ &= \lim_{n\to\infty} F^M(U_2^n \to Q^{H(Q)^{-1}n+b\sqrt{n}}) \\ &= \sqrt{\Phi\left(\frac{-H(Q)^{\frac{3}{2}}b}{\sqrt{V(Q)}}\right)}. \end{aligned} \tag{9}$$

Theorem 1 is easily obtained from Proposition 2 as follows. For a fixed real number $\nu \in (0,1)$, we set a real number as $b_\nu = -\sqrt{\frac{V(Q)}{H(Q)^3}}\Phi^{-1}(\nu^2)$. Proposition 2 guarantees that

$$F(U_2^n \to Q^{H(Q)^{-1}n+(b_\nu-\epsilon)\sqrt{n}}) > \nu \tag{10}$$

when the number n is sufficiently large for an arbitrary constant $0 < \epsilon$. Thus, $L_n(U_2,Q|\nu)$ is greater than the right side in (7). Moreover, Proposition 2 guarantees that

$$F(U_2^n \to Q^{H(Q)^{-1}n+(b_\nu+\epsilon)\sqrt{n}}) < \nu \tag{11}$$

when the number n is sufficiently large for an arbitrary constant $0 < \epsilon$. Thus, $L_n(U_2,Q|\nu)$ is less than the right side in (7). Taken together, Theorem 1 is obtained.

From Proposition 2, it turned out that the limit of the maximal fidelity depend on the second order rate b when $a = H(P)/H(Q)$. On the other hand, note that the limit value does not depend on the second order rate b when $a \neq H(P)/H(Q)$. We emphasize that the lower order term does not affect the limit value if $an + b\sqrt{n}$ has lower order term as $an + b\sqrt{n} + o(\sqrt{n})$ (e.g. $o(\sqrt{n}) = \log n$). Hence, when we want to analyze the maximum fidelity, we only have to treat the first and second order rate and do not need the third order asymptotics.

Next, we consider the second order asymptotics for intrinsic randomness. Similarly, for a fixed confidence coefficient $0 <$

$\nu < 1$, the second order asymptotic expansion is represented as follows.

Theorem 3: Let P be an arbitrary probability distribution on a finite set except for a uniform distribution. Then the second order asymptotic expansion is described as

$$\begin{aligned} &L_n(P, U_2|\nu) \\ &= H(P)n - \sqrt{V(P)}\Phi^{-1}(\nu^2)\sqrt{n} + o(\sqrt{n}). \end{aligned} \tag{12}$$

We remark that Hayashi [4] treated the second order rate under a constraint for the variational distance. Thus, the formulations in [4] and ours are slightly different, and hence, Theorem 3 has not been obtained. Theorem 3 is shown via an analogous proposition to Proposition 2, however, we omit the proof.

IV. Second Order Asymptotics for Non Uniform Distribution

In this section, we treat non-uniform distribution cases. We note that the results itself in this section do not contain that in the section III because we use the property that both $V(P)$ and $V(Q)$ are not 0, which is equivalent to that both P and Q are not uniform distributions. But we mention a relation between the sections III and IV in the end of this section. We define some notations for non-uniform probability distributions P, Q and a constant $b \in \mathbb{R}$. Theorems which appear later are represented by those symbols.

$$N_P := N(0, V(P)), \tag{13}$$

$$N_{P,Q,b} := N\left(H(Q)b, \frac{H(P)}{H(Q)}V(Q)\right), \tag{14}$$

$$\Phi_P(x) := \Phi\left(\frac{x}{\sqrt{V(P)}}\right), \tag{15}$$

$$\Phi_{P,Q,b}(x) := \Phi\left(\sqrt{\frac{H(Q)}{H(P)V(Q)}}(x - H(Q)b)\right), \tag{16}$$

$$\begin{aligned} I_{P,Q,b}(x) &:= \int_{-\infty}^{x} \sqrt{N_P(t)N_{P,Q,x}(t)}dt \\ &= \sqrt{\frac{2\sqrt{C_{P,Q}}}{1+C_{P,Q}}}e^{-\frac{(H(Q)b)^2}{4V(P)(1+C_{P,Q})}} \\ &\quad \times \Phi\left(\sqrt{\frac{1+C_{P,Q}}{2V(P)C_{P,Q}}}\left(x - \frac{H(Q)b}{1+C_{P,Q}}\right)\right), \end{aligned} \tag{17}$$

$$\begin{aligned} I_{P,Q,b}(\infty) &:= \int_{-\infty}^{\infty} \sqrt{N_P(t)N_{P,Q,x}(t)}dt \\ &= \sqrt{\frac{2\sqrt{C_{P,Q}}}{1+C_{P,Q}}}e^{-\frac{(H(Q)b)^2}{4V(P)(1+C_{P,Q})}} \end{aligned} \tag{18}$$

where $N(\mu, v)$ is the normal distribution with the mean μ and the variance v, and $C_{P,Q} := \frac{H(P)}{V(P)}\left(\frac{H(Q)}{V(Q)}\right)^{-1}$. Note that $\Phi_P, \Phi_{P,Q,b}$ means the cumulative distribution functions of $N_P, N_{P,Q,b}$.

We derive the second order asymptotic expansion for $L_n(P, Q|\nu)$. The expansion is divided into three cases according to the relation between $\frac{H(P)}{V(P)}$ and $\frac{H(Q)}{V(Q)}$. The following is the first case.

Theorem 4: When $\frac{H(P)}{V(P)} > \frac{H(Q)}{V(Q)}$,

$$\frac{N_P(x)}{N_{P,Q,b}(x)} = \frac{\Phi_P(x)}{\Phi_{P,Q,b}(x)} \tag{19}$$

has the unique solution $\alpha_b \in \mathbb{R}$ with respect to x. When a function $F_1 : \mathbb{R} \to [0, 1]$ is defined by

$$F_1(b) = \sqrt{\Phi_P(\alpha_b)\Phi_{P,Q,b}(\alpha_b)} + I_{P,Q,b}(\infty) - I_{P,Q,b}(\alpha_b), \tag{20}$$

the second order asymptotic expansion for a confidence coefficient $0 < \nu < 1$ is described as

$$L_n(P, Q|\nu) = (H(P)/H(Q))n + F_1^{-1}(\nu)\sqrt{n} + o(\sqrt{n}). \tag{21}$$

Theorem 4 is derived by using the following proposition in the same way as the proof of Theorem 1.

Proposition 5: When $\frac{H(P)}{V(P)} > \frac{H(Q)}{V(Q)}$, the following hold.

$$\begin{aligned} &\lim_{n\to\infty} F(P^n \to Q^{\frac{H(P)}{H(Q)}n + b\sqrt{n}}) \\ &= \lim_{n\to\infty} F^M(P^n \to Q^{\frac{H(P)}{H(Q)}n + b\sqrt{n}}) = F_1(b). \end{aligned} \tag{22}$$

We give the proof of Proposition 5 in Section V. For the continuous differentiable function

$$A(x) = \begin{cases} \frac{\Phi_P(\alpha_b)}{\Phi_{P,Q,b}(\alpha_b)}\Phi_{P,Q,b}(x) & \text{if } x \le \alpha_b \\ \Phi_P(x) & \text{if } \alpha_b \le x, \end{cases} \tag{23}$$

the following equation holds

$$F_1(b) = F\left(\frac{dA}{dx}, N_{P,Q,b}\right), \tag{24}$$

where the right side in (24) is the value defined as

$$F(p, q) := \int_{\mathbb{R}} \sqrt{p(x)q(x)}dx, \tag{25}$$

and is called the fidelity or the Bhattacharyya coefficient for continuous distributions. Therefore, Proposition 5 can be represented as

$$\begin{aligned} &\lim_{n\to\infty} F(P^n \to Q^{\frac{H(P)}{H(Q)}n + b\sqrt{n}}) \\ &= \lim_{n\to\infty} F^M(P^n \to Q^{\frac{H(P)}{H(Q)}n + b\sqrt{n}}) = F\left(\frac{dA}{dx}, N_{P,Q,b}\right). \end{aligned} \tag{26}$$

The functions A defined in (23), $G_{P,Q,b}$ and G_P are shown in Fig. 1. In the proof of Proposition 5, we show (26).

When $\frac{H(P)}{V(P)} < \frac{H(Q)}{V(Q)}$ and $\frac{H(P)}{V(P)} = \frac{H(Q)}{V(Q)}$, the second order asymptotic expansion of $L_n(P, Q|\nu)$ are represented as follows, however, we omit the proofs.

Theorem 6: When $\frac{H(P)}{V(P)} < \frac{H(Q)}{V(Q)}$,

$$\frac{N_P(x)}{N_{P,Q,b}(x)} = \frac{1 - \Phi_P(x)}{1 - \Phi_{P,Q,b}(x)} \tag{27}$$

has the unique solution $\beta_b \in \mathbb{R}$ with respect to x. When a function $F_2 : \mathbb{R} \to [0, 1]$ is defined by

$$F_2(b) = I_{P,Q,b}(\beta_b) + \sqrt{(1 - \Phi_P(\beta_b))(1 - \Phi_{P,Q,b}(\beta_b))}, \tag{28}$$

the second order asymptotic expansions for a confidence coefficient $0 < \nu < 1$ are described as

$$L_n(P, Q|\nu) = (H(P)/H(Q))n + F_2^{-1}(\nu)\sqrt{n} + o(\sqrt{n}). \tag{29}$$

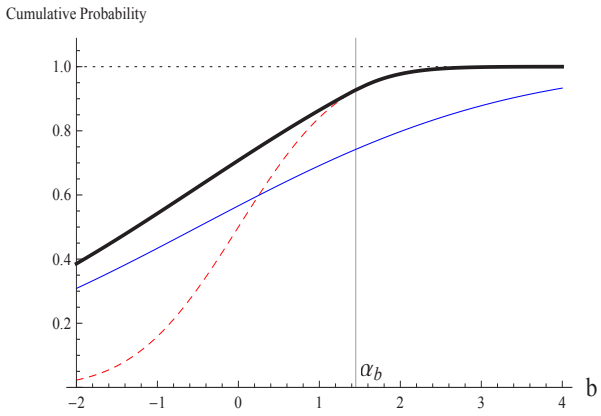

Fig. 1. The normal and the dashed lines show the cumulative distribution functions $\Phi_{P,Q,b}$ and Φ_P of N_P and $N_{P,Q,b}$, respectively. The thick shows the function A defined in (23). The intersection point of b-axes and the vertical line shows α_b defined in (19). When $H(P)/V(P) > H(Q)/V(Q)$, the limit of the maximal fidelity in Proposition 5 coincides with the fidelity between the continuous probability density functions of A and $G_{P,Q,b}$.

Theorem 7: When $\frac{H(P)}{V(P)} = \frac{H(Q)}{V(Q)}$, the second order asymptotic expansions for a confidence coefficient $0 < \nu < 1$ are described as

$$L_n(P,Q|\nu) = \frac{H(P)}{H(Q)}n + \sqrt{\frac{8V(P)\log\nu^{-1}}{H(Q)}}\sqrt{n} + o(\sqrt{n}) \quad (30)$$

We note that Proposition 5 coincides with Proposition 2 in the limit $Q \to U_2$ as

$$\lim_{Q\to\infty} F_{2,Q}(b) = \sqrt{\Phi\left(\frac{-H(Q)^{\frac{3}{2}}b}{\sqrt{V(Q)}}\right)}, \quad (31)$$

where we rewrote F_2 in (28) as $F_{2,Q}$ to show the dependency of F_2 for a probability distribution Q. In particular, Theorem 4 coincides with Theorem 1 in the limit $Q \to U_2$ since the second order rate in Theorems 4 convergences to that in Theorem 1. Similarly, Theorem 6 coincides with Theorem 3 in the limit $P \to U_2$.

V. Proof of Proposition 5

At first, we show that there is the unique solution of the equation (19) with respect to x. Here, the existence of the unique solution is equivalent to the existence of the unique zero point of the function $f(x) = (N_P(x)/N_{P,Q,b}(x))\Phi_{P,Q,b}(x) - \Phi_P(x)$. Since

$$\frac{df}{dx} = \frac{d}{dx}\left(\frac{N_P}{N_{P,Q,b}}\right)\Phi_{P,Q,b}, \quad (32)$$

the function f is strictly monotone increasing when $x < \mathrm{argmax}(N_P/N_{P,Q,b}) = \frac{-V(P)H(Q)^2b}{H(P)V(Q)-H(Q)V(P)}$ and is strictly monotone decreasing when $x > \frac{-V(P)H(Q)^2b}{H(P)V(Q)-H(Q)V(P)}$. Since

$$\lim_{x\to-\infty} f(x) = 0, \quad \lim_{x\to\infty} f(x) = -1, \quad (33)$$

the function f has the unique zero point $\alpha_b > \frac{-V(P)H(Q)^2b}{H(P)V(Q)-H(Q)V(P)}$ due to the intermediate value theorem.

(Direct) We prove the direct part of Proposition 4. The following lemma is essential for the proof of the direct part.

Lemma 8: Let P and Q be probability distributions on a finite set. When a function A on $\mathbb{R}$ is continuously differentiable, monotone increasing and $\Phi_P \le A \le 1$, the following holds.

$$\liminf_{n\to\infty} F\left(P^n \to Q^{\frac{H(P)}{H(Q)}n+b\sqrt{n}}\right) \ge F\left(\frac{dA}{dx}, N_{P,Q,b}\right). \quad (34)$$

We do not give the proof of the above lemma here. We set the funstion $A : \mathbb{R} \to [0,1]$ as

$$A(x) = \begin{cases} \frac{\Phi_P(\alpha_b)}{\Phi_{P,Q,b}(\alpha_b)}\Phi_{P,Q,b}(x) & if\ x \le \alpha_b \\ \Phi_P(x) & if\ \alpha_b \le x. \end{cases} \quad (35)$$

Since this function A is continuously differentiable, monotone increasing and satisfies $\Phi_P \le A \le 1$, the following holds by Lemma 8.

$$\sqrt{\Phi_P(\alpha_b)\Phi_{P,Q,b}(\alpha_b)} + \int_{\alpha_b}^{\infty}\sqrt{N_P(x)N_{P,Q,b}(x)}dx \le \liminf_{n\to\infty} F\left(P^n \to Q^{\frac{H(P)}{H(Q)}n+b\sqrt{n}}\right). \quad (36)$$

Moreover, by using (6), we obtain

$$\liminf_{n\to\infty} F\left(P^n \to Q^{\frac{H(P)}{H(Q)}n+b\sqrt{n}}\right) \le \limsup_{n\to\infty} F^M\left(P^n \to Q^{\frac{H(P)}{H(Q)}n+b\sqrt{n}}\right). \quad (37)$$

(Converse) We prove the converse part, that is,

$$\limsup_{n\to\infty} F^M\left(P^n \to Q^{\frac{H(P)}{H(Q)}n+b\sqrt{n}}\right) \le \sqrt{\Phi_P(\alpha_b)\Phi_{P,Q,b}(\alpha_b)} + \int_{\alpha_b}^{\infty}\sqrt{N_P(x)N_{P,Q,b}(x)}dx. \quad (38)$$

In the following, we abbreviate $Q^{\frac{H(P)}{H(Q)}n+b\sqrt{n}}$ as Q_n. Then, for an arbitrary $0 < \epsilon$ and an arbitrary sequence $\{P'_n\}_{n=1}^{\infty}$ of probability distributions such that $P'_n \succ P^n$, it is enough to show that

$$\limsup_{n\to\infty} F(P'_n, Q_n) \le \sqrt{\Phi_P(\alpha_b)\Phi_{P,Q,b}(\alpha_b)} + \int_{\alpha_b}^{\infty}\sqrt{N_P(x)N_{P,Q,b}(x)}dx + \epsilon. \quad (39)$$

We take a constant $c \in \mathbb{R}$ which satisfies $\alpha_b < c$ and

$$\sqrt{(1-\Phi_P(c))(1-\Phi_{P,Q,b}(c))} < \epsilon. \quad (40)$$

Then, we set a sequence $\{x_i^I\}_{i=-\infty}^{I}$ for a natural number I as $x_i^I := \alpha_b + \frac{c-\alpha_b}{I}i$. Let $S_n(x) := \{1, 2, ..., [e^{H(P)n+x\sqrt{n}}]\}$, and $S_n(x, x') := S_n(x') \setminus S_n(x)$. By the monotonicity of the

fidelity, the following holds.

$$\begin{aligned}
&F(P'_n, Q_n) \\
&\le \sqrt{P'_n(S_n(\alpha_b))Q_n(S_n(\alpha_b))} \\
&\quad + \sum_{i=1}^{I} \sqrt{P'_n(S_n(x_{i-1}^I, x_i^I))Q_n(S_n(x_{i-1}^I, x_i^I))} \qquad (41) \\
&\quad + \sqrt{P'_n(S_n(c,\infty))Q_n(S_n(c,\infty))}.
\end{aligned}$$

Since $P'_n \succ P^n$, we obtain

$$\limsup_{n\to\infty} P'_n(S_n(c,\infty)) \le \lim_{n\to\infty} P^n(S_n(c,\infty)) = 1 - \Phi_P(c). \qquad (42)$$

Moreover,

$$\lim_{n\to\infty} Q_n(S_n(c,\infty)) = 1 - \Phi_{P,Q,b}(c). \qquad (43)$$

Thus, the following inequality holds.

$$\begin{aligned}
&\limsup_{n\to\infty} F(P'_n, Q_n) \\
&\le \limsup_{n\to\infty} \Big(\sqrt{P'_n(S_n(\alpha_b))Q_n(S_n(\alpha_b))} \qquad (44) \\
&\quad + \sum_{i=1}^{I-1} \sqrt{P'_n(S_n(x_{i-1}^I, x_i^I))Q_n(S_n(x_{i-1}^I, x_i^I))} \Big) + \epsilon.
\end{aligned}$$

Then, there exists a subsequence $\{n_l\}_{l=1}^{\infty}$ such that the limits

$$\lim_{l\to\infty} P'_{n_l}(S_{n_l}(\alpha_b)), \qquad (45)$$

$$\lim_{l\to\infty} P'_{n_l}(S_{n_l}(x_{i-1}^I, x_i^I)) \qquad (46)$$

exist and we define a real number c_i^I by

$$c_0^I := \Phi_P(\alpha_b) - \lim P'_{n_l}(S_{n_l}(\alpha_b)), \qquad (47)$$

$$c_i^I := \Phi_P(x_i^I) - \Phi_P(x_{i-1}^I) - \lim P'_{n_l}(S_{n_l}(x_{i-1}^I, x_i^I)). \qquad (48)$$

Then the following hold:

$$\begin{aligned}
&\limsup_{n\to\infty} \Big(\sqrt{P'_n(S_n(\alpha_b))Q_n(S_n(\alpha_b))} \\
&\quad + \sum_{i=1}^{I-1} \sqrt{P'_n(S_n(x_{i-1}^I, x_i^I))Q_n(S_n(x_{i-1}^I, x_i^I))} \Big) \\
&= \sqrt{\lim_l P'_{n_l}(S_{n_l}(\alpha_b))} \sqrt{\Phi_{P,Q,b}(\alpha_b)} \qquad (49) \\
&+ \sum_{i=1}^{I-1} \sqrt{\lim_l P'_{n_l}(S_{n_l}(x_{i-1}^I, x_i^I))} \sqrt{\Phi_{P,Q,b}(x_i^I) - \Phi_{P,Q,b}(x_{i-1}^I)} \\
&= \sqrt{(\Phi_P(\alpha_b) - c_0^I)\Phi_{P,Q,b}(\alpha_b)} \qquad (50) \\
&\quad + \sum_{i=1}^{I-1} \sqrt{\Phi_P(x_i^I) - \Phi_P(x_{i-1}^I) - c_i^I} \\
&\quad \times \sqrt{\Phi_{P,Q,b}(x_i^I) - \Phi_{P,Q,b}(x_{i-1}^I)} \\
&\le \sqrt{\Phi_P(\alpha_b)\Phi_{P,Q,b}(\alpha_b)} \qquad (51) \\
&\quad + \sum_{i=1}^{I-1} \sqrt{\Phi_P(x_i^I) - \Phi_P(x_{i-1}^I)} \\
&\quad \times \sqrt{\Phi_{P,Q,b}(x_i^I) - \Phi_{P,Q,b}(x_{i-1}^I)}.
\end{aligned}$$

We used the following lemma in (51), however, omit the proof.

Lemma 9: Let a_j and b_j $(j = 0, 1, ..., I)$ be positive real numbers and satisfy $\frac{a_{i-1}}{b_{i-1}} > \frac{a_i}{b_i}$. When $u_j \in \mathbb{R}$ satisfies $c_j \le a_j$ $(j = 0, 1, ..., I)$ and $\sum_{j=0}^{I} c_j \le 0$, then

$$\sum_{j=0}^{I} \sqrt{(a_j - c_j)b_j} \le \sum_{j=0}^{I} \sqrt{a_j b_j}. \qquad (52)$$

Taking the limit with respect to I, we obtain the following.

$$\begin{aligned}
&\lim_{I\to\infty} \sum_{i=1}^{I-1} \sqrt{\Phi_P(x_i^I) - \Phi_P(x_{i-1}^I)} \sqrt{\Phi_{P,Q,b}(x_i^I) - \Phi_{P,Q,b}(x_{i-1}^I)} \\
&= \int_{\alpha_b}^{c} \sqrt{N_P(x) N_{P,Q,b}(x)}\, dx \qquad (53) \\
&\le \int_{\alpha_b}^{\infty} \sqrt{N_P(x) N_{P,Q,b}(x)}\, dx. \qquad (54)
\end{aligned}$$

Taken the above evaluations together, we obtain (39), and hence, Proposition 5 was verified.

VI. Conclusion

We treated the second order asymptotics of random number generation from an i.i.d. probability distribution of P to that of Q. In existing studies, P or Q has been assumed to be a uniform distribution, but in this paper, both probability distributions have not been restricted to a uniform distribution. In particular, we provided the second order asymptotic expansion for the maximal number L_n of Q which can be transformed from P^n under the fidelity constraint $F(P^n \to Q^{L_n}) \ge \nu$ in Theorems 4, 6 and 7. We remark that the majorization relation has an operational meaning as a transformation called LOCC for quantum entangled states in the quantum information theory, and our results can be extended to the quantum settings. A part of extensions of our results to quantum information theory is treated in [5], [6], [7].

Acknowledgment

WK acknowledges support from Grant-in-Aid for JSPS Fellows No. 233283. MH is partially supported by a MEXT Grant-in-Aid for Scientific Research (A) No. 23246071. The Center for Quantum Technologies is funded by the Singapore Ministry of Education and the National Research Foundation as part of the Research Centres of Excellence programme.

References

[1] T. S. Han, *Information-Spectrum Methods in Information Theory*. New York, Springer, 2003.
[2] A. W. Marshall and I. Olkin, *Inequalities: Theory of Majorization and Its Applications*. New York, Academic Press, 1979.
[3] R. Nomura and T. S. Han, IEEE Trans. Inf. Theory, vol. 59, pp. 1-16, Jan. 2013.
[4] M. Hayashi, IEEE Trans. Inf. Theory, vol. 54, pp. 4619-4637, Oct. 2008.
[5] M. Hayashi, IEEE Trans. Inf. Theory, vol. 52, pp. 1904-1921, May 2006.
[6] D. Jonathan and M. B. Plenio, Phys. Rev. Lett., vol. 83, pp. 1455-1458, 1999.
[7] C. H. Bennett *et al.*, Phys. Rev. A, vol. 53, pp. 2046-2052, 1996.
[8] G. Vidal *et al.*, Phys. Rev. A, vol. 62, 012304, 2000.
[9] M. A. Nielsen, Phys. Rev. Lett., vol. 83, pp. 436-439, 1999.