Available online at www.sciencedirect.com
ScienceDirect
Physics Letters A 367 (2007) 173–176
PHYSICS LETTERS A
www.elsevier.com/locate/pla

On the Poisson approximation to photon distribution for faint lasers

Yucheng Hu [a,*], Xiang Peng [b], Tiejun Li [a], Hong Guo [b,1]

[a] *LMAM and School of Mathematical Sciences, Peking University, Beijing 100871, PR China*
[b] *Key Laboratory for Quantum Information and Measurements of Ministry of Education, School of Electronics Engineering and Computer Science, Peking University, Beijing 100871, PR China*

Received 25 September 2006; received in revised form 21 December 2006; accepted 5 March 2007

Available online 12 March 2007

Communicated by R. Wu

Abstract

The photon number statistics for attenuated faint laser pulses is quantitatively studied. It confirms that, even for a non-Poissonian laser source, after being attenuated into faint laser with ultra-low mean photon number, the photon number distribution would approximately be a Poisson distribution. The error of such an approximation is estimated, and numerical tests verify our theoretical analysis. This work lays a sound mathematical foundation for the well-known intuitive idea which has been widely used in quantum cryptography.

1. Introduction

The security of Quantum Key Distribution (QKD) is based on the non-cloning principle of an unknown quantum state [1]. In the implement of QKD based on BB84 protocol [2], one expects that each pulse contains only one photon. If not, the eavesdropper can acquire information using beamsplitter attack [3] without exposing its existence. However, since an ideal single photon state is difficult to prepare, practically, faint laser pulse with ultra-low mean photon number is used as a convenient realization of pseudo-single photon source [4].

By letting a laser source pass through a strong attenuator we get faint laser pulse. For security concern the mean photon number in each faint laser pulse is kept very small (about 0.1). In the literature, the photon number in faint laser is treated as Poissonian distributed. More precisely, the probability of finding n photons in each faint laser pulse is $e^{-\langle n\rangle}\langle n\rangle^n/n!$, where $\langle n\rangle$ is the mean photon number in each pulse. It is all right if the input laser before attenuation is Poisson. However, practically we may have input laser whose photon number statistics is not Poisson [5]. In this case, the attenuated laser may not be Poisson either. But there is a common belief that no matter what distribution the input laser is, if we attenuate it into a faint laser with sufficient small mean photon number, then Poisson distribution would be a good approximation of photon number distribution in the faint laser pulse. So far, however, this claim has not been mathematical rigorously proved, which is the motivation of this work.

We investigated the quantitative relation between photon number distributions before and after the attenuation. We find that, even if the input laser source is not Poissonian, after strong attenuation, the photon number distribution in the faint laser can still approximately be a Poisson distribution. The errors of this approximation is estimated and numerical examples are carried out. The numerical result coincide with theoretical estimation.

2. Preliminary

Consider N independent particles (photons in laser pulses) passing through an attenuator. The attenuating coefficient is η ($0 \leqslant \eta \leqslant 1$), which means each particle has a probability of η to penetrate the attenuator. We define X to be the number of particles before decay (Input), and X_η to be the number of particles after decay (Output). X and X_η are random variables taking val-

* Corresponding author.
E-mail addresses: huyc@pku.edu.cn (Y. Hu), tieli@pku.edu.cn (T. Li), hongguo@pku.edu.cn (H. Guo).
[1] Tel.: +86 10 6275 7035; fax: +86 10 6275 3208.

0375-9601/$ – see front matter
doi:10.1016/j.physleta.2007.03.004

ues in the natural number system $\mathbb{N}$, and their probability mass functions (PMF) are $P(N)$ and $P_\eta(n)$, respectively.

$P(N)$ and $P_\eta(n)$ is connected by the *binomial decay transformation* [6]

$$P_\eta(n) = \sum_{N=n}^{\infty} \binom{N}{n} \eta^n (1-\eta)^{N-n} P(N), \tag{1}$$

where the parameter η is the attenuating coefficient we mentioned above. It is easy to check that $P_\eta(n) \geqslant 0$, $\forall n \in \mathbb{N}$, and $\sum_{n=0}^{\infty} P_\eta(n) = \sum_{N=0}^{\infty} P(N) = 1$, which indicates P_η is indeed a PMF. So the binomial decay transformation is a map from PMFs to PMFs. Here we present some properties of it.

Lemma 1. *For any positive integer l, we have*

$$E\left[\prod_{i=0}^{l-1}(X_\eta - i)\right] = \eta^l E\left[\prod_{i=0}^{l-1}(X - i)\right].$$

Proof. By the definition of expectation and Eq. (1),

$$\begin{aligned}
&E\left[\prod_{i=0}^{l-1}(X_\eta - i)\right] \\
&= \sum_{n=l}^{\infty}\left[\prod_{i=0}^{l-1}(n-i)\right]\sum_{N=n}^{\infty}\binom{N}{n}\eta^n(1-\eta)^{N-n}P(N) \\
&= \sum_{N=l}^{\infty} P(N)\sum_{n=l}^{N}\left[\prod_{i=0}^{l-1}(n-i)\right]\binom{N}{n}\eta^n(1-\eta)^{N-n} \\
&= \eta^l \sum_{N=l}^{\infty}\left[\prod_{i=0}^{l-1}(N-i)\right]P(N) \\
&= \eta^l E\left[\prod_{i=0}^{l-1}(X-i)\right]. \qquad \square
\end{aligned}$$

For $l = 1$, the result reduces to $E(X_\eta) = \eta E(X)$, which says the expectation of attenuated distribution is exactly η times the expectation of the input distribution.

Define $P^\lambda(n)$ the Poisson PMF with parameter λ, i.e., $P^\lambda(n) = e^{-\lambda}\lambda^n/n!$, $n \in \mathbb{N}$. It is a well-known fact that the binomial decay transformation preserves the Poisson character, which is formulated in Lemma 2.

Lemma 2. *If $P(N) = P^\lambda(N)$, then $P_\eta(n) = P^{\eta\lambda}(n)$.*

Proof. From Eq. (1),

$$\begin{aligned}
P_\eta(n) &= \sum_{N=n}^{\infty}\binom{N}{n}\eta^n(1-\eta)^{N-n}P^\lambda(N) \\
&= \frac{(\eta\lambda)^n}{n!}\sum_{N=n}^{\infty}\frac{e^{-\lambda}}{(N-n)!}\big[\lambda(1-\eta)\big]^{N-n} \\
&= \frac{(\eta\lambda)^n}{n!}e^{-\eta\lambda} \\
&= P^{\eta\lambda}(n). \qquad \square
\end{aligned}$$

3. Poisson approximation

From Lemma 2 we know that if $P(N)$, the photon number distribution in the laser pulse before attenuation, is Poisson, then $P_\eta(n)$, the decayed distribution, is also Poisson. However, practically $P(N)$ may not be a Poisson distribution [5]. If so, then $P_\eta(n)$ is not a Poisson distribution, either. Nevertheless, It is believed that faint laser with ultra-low mean photon number can be, at least approximately, treated as Poisson distributed. Now we shall verify this assertion.

Proposition. *Suppose that X is a random variable whose PMF is $P(N)$. $E(X)$ and $Var(X)$ are the mean and variance of X, respectively. For small positive value λ, choose the attenuating coefficient $\eta = \lambda/E(X)$. Then after a binomial decay transformation with parameter η,* (i) *the expectation of the decayed random variable X_η is λ, and* (ii) *its PMF P_η satisfies*

$$P_\eta(0) = 1 - \lambda + \frac{\lambda^2}{2} + C(X)\lambda^2 + \mathrm{O}\big(\lambda^3\big), \tag{2a}$$

$$P_\eta(1) = \lambda - \lambda^2 - 2C(X)\lambda^2 + \mathrm{O}\big(\lambda^3\big), \tag{2b}$$

$$P_\eta(2) = \frac{\lambda^2}{2} + C(X)\lambda^2 + \mathrm{O}\big(\lambda^3\big), \tag{2c}$$

$$\sum_{n=3}^{\infty} P_\eta(n) = \mathrm{O}\big(\lambda^3\big), \tag{2d}$$

where $C(X) \equiv \frac{Var(X)-E(X)}{2E(X)^2}$.

Proof.

(i) From Lemma 1, we have

$$E_\eta(X) = \eta E(X) = \frac{\lambda}{E(X)}E(X) = \lambda.$$

So the expectation of X_η is λ.

(ii) The generating function of X is

$$G(z) = \sum_{N=0}^{\infty} P(N) z^N, \quad z \in \mathbb{R}.$$

Taking the nth order derivatives of $G(z)$ with respect to z yields,

$$G^{(n)}(z) = \sum_{N=n}^{\infty} N(N-1)\cdots(N-n+1)P(N)z^{N-n}.$$

From Eq. (1), it follows,

$$\begin{aligned}
P_\eta(n) &= \sum_{N=n}^{\infty}\binom{N}{n}\eta^n(1-\eta)^{N-n}P(N) \\
&= \frac{\eta^n}{n!}\sum_{N=n}^{\infty} N(N-1)\cdots(N-n+1)P(N)(1-\eta)^{N-n} \\
&= \frac{\eta^n}{n!}G^{(n)}(1-\eta).
\end{aligned}$$

Expanding $G^{(n)}(1-\eta)$ into Taylor serials, in the case of $n = 0$, one has

$$P_\eta(0) = G(1) - \eta G'(1) + \frac{\eta^2}{2}G''(1) + \mathrm{O}\big(\eta^3\big).$$

By noticing

$$G(1) = 1,$$
$$G'(1) = E(X),$$
$$G''(1) = Var(X) + \big[E(X)\big]^2 - E(X),$$

we have

$$P_\eta(0) = 1 - \eta E(X) + \frac{\eta^2}{2}\big[Var(X) + \big[E(X)\big]^2 - E(X)\big] + \mathrm{O}\big(\eta^3\big).$$

Replace η with $\lambda/E(X)$, and note that $\mathrm{O}(\lambda^3) \sim \mathrm{O}(\eta^3)$ because $E(X)$ is a constant once X is given, it follows

$$P_\eta(0) = 1 - \lambda + \frac{\lambda^2}{2} + \lambda^2\frac{Var(X) - E(X)}{2[E(X)]^2} + \mathrm{O}\big(\lambda^3\big) = 1 - \lambda + \frac{\lambda^2}{2} + C(X)\lambda^2 + \mathrm{O}\big(\lambda^3\big).$$

Analogously, Eqs. (2b), (2c) can be derived. Finally,

$$\sum_{n=3}^{\infty} P_\eta(n) = 1 - \big[P_\eta(0) + P_\eta(1) + P_\eta(2)\big] = \mathrm{O}\big(\lambda^3\big),$$

which yields Eq. (2d). □

If we expand the Poisson distribution with expectation λ into Taylor series, then we have

$$P^\lambda(0) = 1 - \lambda + \frac{\lambda^2}{2} + \mathrm{O}\big(\lambda^3\big), \tag{3a}$$
$$P^\lambda(1) = \lambda - \lambda^2 + \mathrm{O}\big(\lambda^3\big), \tag{3b}$$
$$P^\lambda(2) = \frac{\lambda^2}{2} + \mathrm{O}\big(\lambda^3\big), \tag{3c}$$
$$\sum_{n=3}^{\infty} P^\lambda(n) = \mathrm{O}\big(\lambda^3\big). \tag{3d}$$

By comparing Eqs. (3a)–(3d) with Eqs. (2a)–(2d), we see that $P_\eta(n)$ asymptotically approaches the Poisson distribution $P^\lambda(n)$ for $\lambda \ll 1$. The error $\Delta(n) = P_\eta(n) - P^\lambda(n)$ is

$$\Delta(0) = \lambda^2 C(X) + \mathrm{O}\big(\lambda^3\big), \tag{4a}$$
$$\Delta(1) = -2\lambda^2 C(X) + \mathrm{O}\big(\lambda^3\big), \tag{4b}$$
$$\Delta(2) = \lambda^2 C(X) + \mathrm{O}\big(\lambda^3\big), \tag{4c}$$
$$\Delta(n) = \mathrm{O}\big(\lambda^3\big), \quad n \geqslant 3. \tag{4d}$$

Note that $C(X) = [G_2(X) - 1]/2$, where $G_2(X) = E[X(X-1)]/[E(X)]^2$ is the normalized second-order correlation coefficient [7]. With Lemma 1 it is easy to show that $G_2(X)$ is invariant under binomial decay transformation, i.e., for any $0 < \eta \leqslant 1$, $G_2(X_\eta) = G_2(X)$, which also means $C(X_\eta) = C(X)$.

$C(X)$ is crucial for estimating the error of a Poisson approximation. From Eqs. (4a)–(4c) we see that, when $Var(X) = E(X)$, for example if X is a Poisson distribution, then $C(X) = 0$ and the approximation error reduce to $\mathrm{O}(\lambda^3)$. For some singular $P(N)$, however, $C(X)$ may become so big that $P_\eta(n)$ can no longer be well approximated by Poisson. Fortunately, in practice the common photon number distributions, such as super(sub)-Poisson distribution, Bose–Einstein distribution and Gauss distribution, $C(X)$ is small and $\lambda^2 C(X)$ can be neglected for $\lambda \ll 1$. This explains why we can treat photon number distribution in faint laser pulse as Poisson distribution.

$C(X)$ also has close connection to the security of QKD. When we use faint laser to simulate a single photon source in QKD, it is important to estimate $P_\eta(n > 1|n > 0)$, the probability that a non-empty pulse contains more than one photon [4]. According to our estimation,

$$P_\eta(n > 1|n > 0) = \frac{1 - P_\eta(0) - P_\eta(1)}{1 - P_\eta(0)} \approx \frac{\frac{\lambda^2}{2} + C(X)\lambda^2}{\lambda - \frac{\lambda^2}{2} - C(X)\lambda^2}.$$

Here we have neglected the λ^3 and higher order terms. We further simplify it by removing the λ^2 terms in the denominator, which gives

$$P_\eta(n > 1|n > 0) \approx \left[\frac{1}{2} + C(X)\right]\lambda. \tag{5}$$

Since in QKD we want $P_\eta(n > 1|n > 0)$ as small as possible, Eq. (5) implies that the smaller $C(X)$ is, the better for the security concern. If the input distribution is Poisson, then $C(X) = 0$. After we attenuate it to faint laser that contains an average of 0.1 photon in each pulse, which means $\lambda = 0.1$, we would have $P_\eta(n > 1|n > 0) = 0.05$. Each non-empty faint laser pulse has about 5% chance to contain more than one photon. If the input laser X follows the Bose–Einstein distribution, then the PMF is

$$P(N) = \frac{E(X)^N}{[1 + E(X)]^{N+1}}, \tag{6}$$

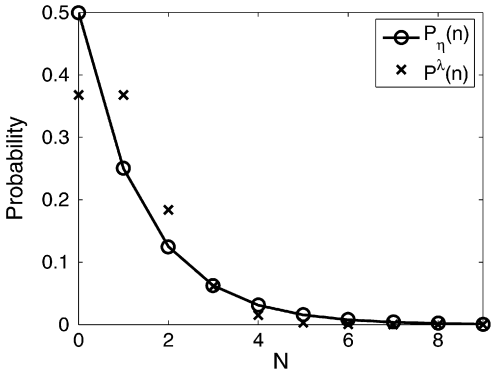
where $E(X)$ is the mean photon number in the input laser pulse. In this case, $C(X) = 0.5$ so $P_\eta(n > 1|n > 0) \approx \lambda$. Again for $\lambda = 0.1$ the probability for each non-empty faint laser pulse to contain more than one photon is about 10%.

One might think if we use sub-Poisson laser ($Var(X) < E(X)$) as input, then $C(X) < 0$ and $P_\eta(n > 1|n > 0)$ would become smaller. However, even if $Var(X) = 0$, we got $C(X) = -[2E(X)]^{-1}$, which is only slightly below zero because $E(X)$ is very big for practical laser pulse. So for strongly attenuated faint laser, a Poisson distribution is almost the best distribution one can expects in the sense that there hardly has any room to reduce $P_\eta(n > 1|n > 0)$ by attenuating some sub-Poisson laser.

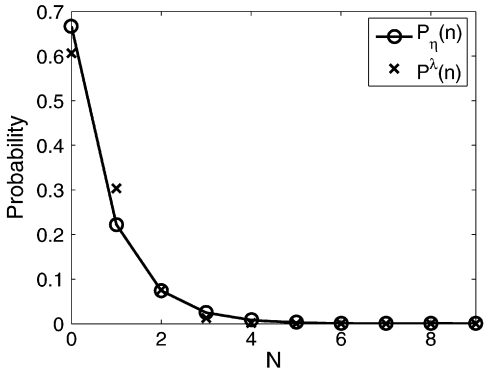
4. Numerical examples

Here we give two numerical examples. The results verify theoretical estimates in the last section quite well.

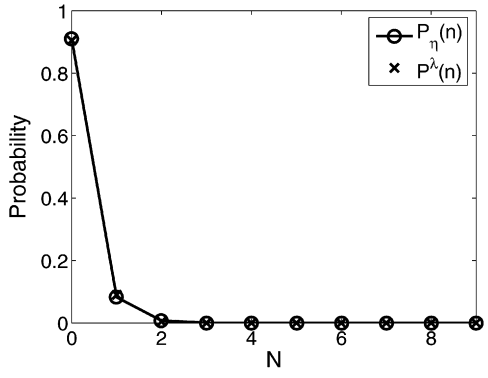
The first example illustrates $P_\eta(n)$ approaching $P^\lambda(n)$ asymptotically as $\lambda \to 0$. We choose X to obey the Bose–Einstein distribution (see Eq. (6)). The expectation of X is set as $E(X) = 100$. For different λ, we computed the attenuated distributions



(a) $\lambda = 1$



(b) $\lambda = 0.5$



(c) $\lambda = 0.1$

Fig. 1. Comparison between $P_\eta(n)$ and $P^\lambda(n)$. $P_\eta(n)$ is computed by Eq. (1) with a given $P(N)$, which is a Bose–Einstein distribution with expectation being 100. We choose η to be $\lambda/100$ for (a) $\lambda = 1$; (b) $\lambda = 0.5$ and (c) $\lambda = 0.1$, respectively. $P^\lambda(n)$ is the corresponding Poisson distribution with parameter λ. $P_\eta(n)$ (represent as '$\circ$'s) and $P^\lambda(n)$ (represent as '$\times$'s) are plotted for $n = 0, 1, \ldots, 9$ (since $P_\eta(n)$ and $P^\lambda(n)$ are neglecting small for big n). We can see for $\lambda = 1$ and 0.5 the difference between $P_\eta(n)$ and $P^\lambda(n)$ is evident. However, for $\lambda = 0.1$, the Poisson distribution $P^\lambda(n)$ makes a very good approximation to $P_\eta(n)$.

$P_\eta(n)$ ($\lambda = \eta E(X)$). In Fig. 1, the attenuated distributions $P_\eta(n)$ (represented in '$\circ$'s) are compared with Poisson distributions $P^\lambda(n)$ (represented as '$\times$'s) for $\lambda = 1$, 0.5 and 0.1. As we can see, the condition that $\lambda \ll 1$ is important for Poisson approximation. If λ is large, this approximation may be broken.

Table 1
Approximation errors between $P_\eta(n)$s and $P^\lambda(n)$s. For a given Poisson distribution with parameter $\lambda_0 = 100$, we randomly perturb it to get a PMF $P(N)$. $P_\eta(n)$ is then computed from $P(N)$ by Eq. (1). We choose a proper η to let the expectation of $P_\eta(n)$ always be 0.1. $\Delta(n) = P_\eta(n) - P^\lambda(n)$ ($\lambda = 0.1$) is the Poisson approximation error of $P_\eta(n)$. Each row corresponds to an independently perturbed $P(N)$, and the value of $\lambda^2 C(X)$ and $\Delta(n)$ for $n = 0, 1, 2, 3, 4$ are given in the table. It appears that generally $\Delta(1) \approx 2\Delta(0) \approx 2\Delta(2)$. And $\Delta(0)$, $\Delta(1)$, $\Delta(2)$ are bounded by Eqs. (4a)–(4c)

$\lambda^2 C(X)$	$\Delta(0)$	$\Delta(1)$	$\Delta(2)$	$\Delta(3)$	$\Delta(4)$
0.0044	0.0010	−0.0019	0.0007	0.0001	0.0000
0.0037	0.0010	−0.0019	0.0007	0.0001	0.0000
0.0020	0.0007	−0.0012	0.0005	0.0001	0.0000
0.0016	0.0006	−0.0011	0.0005	0.0001	0.0000
0.0007	0.0003	−0.0006	0.0002	0.0000	0.0000

In the second example, we quantitatively study the approximation errors $\Delta(n) = P_\eta(n) - P^\lambda(n)$. The input distribution $P(N)$ is generated as follows: (i) Set $P(N)$ initially as a Poisson distribution with parameter $\lambda_0 = 100$; (ii) Randomly perturb the value of $P(N)$ for some N; (iii) Make sure $P(N) \geqslant 0$ and renormalize it so that $P(N)$ is still a PMF. After this we get a distribution $P(N)$ perturbed from a Poisson distribution. The random perturbation process helps to study the behavior of the error and also has some physical meaning since practical laser source is perturbed by random noise constantly. We want the expectation of the attenuated distribution to be 0.1, which can be achieved by choosing a proper attenuating coefficient η. Then the attenuated distribution $P_\eta(n)$ is computed with $P(N)$ by Eq. (1). Subtracting $P_\eta(n)$ with the Poisson PMF which has the same expectation as $P_\eta(n)$, we get the approximation error $\Delta(n) = P_\eta(n) - P^\lambda(n)$. Table 1 lists the values of $\lambda^2 C(X)$ and $\Delta(n)$ for $n = 0, 1, 2, 3, 4$. Each row corresponds to an independent trial. We can see that generally $\Delta(1) \approx 2\Delta(0) \approx 2\Delta(2)$ and $\Delta(0)$, $\Delta(1)$, $\Delta(2)$ are all bounded by the theoretical estimates Eqs. (4a)–(4c).

Acknowledgement

This work is partially supported by National Science Foundation of China (Grant Nos. 10474004 and 10401004), National Basic Research Program (Grant 2005CB321704) and DAAD exchange program: D/05/06972 Projektbezogener Personenaustausch mit China (Germany/China Joint Research Program).

References

[1] W.K. Wootters, W.H. Zurek, Nature 299 (1982) 802.
[2] C.H. Bennett, G. Brassard, in: Proc. of IEEE Int. Conf. on Computers, Systems, and Signal Processing, Bangalore, India, IEEE, New York, 1984, p. 175.
[3] N. Lütkenhaus, Phys. Rev. A 61 (2000) 052304.
[4] N. Gisin, G. Riordy, W. Tittel, H. Zbinden, Rev. Mod. Phys. 74 (2002) 145.
[5] B.E.A. Saleh, Phys. Rev. Lett. 58 (1987) 2656.
[6] M.O. Scully, W.E. Lamb, Phys. Rev. 179 (1969) 368.
[7] H. Cao, Y. Ling, J.Y. Xu, C.Q. Cao, Phys. Rev. Lett. 86 (2001) 4524.