NEW APPROXIMATIONS OF BIT ERROR RATE IN CHAOS SHIFT-KEYING SYSTEMS

GAN OHAMA[†] AND ANTHONY J LAWRANCE[‡]

Abstract. Though the calculation of exact bit error rate in some simple chaotic shift-keying based systems has been reported by the same authors recently, an efficient approximation of bit error rate is still in demand. It is due to the fact that the numerical calculation of exact bit error rate requires a lot of time and high computer performance. The paper explores several new approximations some of which can be calculated more easily, and shows the efficiency of new approximations. The comparison between a new and earlier approximations is also given.

1. Introduction

Chaos-based communication systems have been attracted a lot of interest since it can be the alternative of conventional modulation schemes in which trigonometric wave functions are used. Because of the periodicity of trigonometric wave functions the risk of interference in multiple user system is not low. Instead of trigonometric wave functions, chaotic sequences are used in chaotic modulation schemes and both improvement and problems of the use of chaotic sequences have been reported. Kennedy, Rovatti and Setti [3] is the first monograph in the area. The basic idea of chaotic modulation is as follows: A digital signal is carried by a *spreading sequence*, that is chaotic in our case, and goes through the *channel* where the sequence is corrupted by noise, generally assumed to be *additive white Gaussian noise* (AWGN). A receiver has to estimate the signal based on the corrupted sequence and therefore error occurs. A correlation decoder is widely used to decode the signal and has been proved to be the maximum likelihood estimator in coherent chaos shift-keying systems by Lawrance and Ohama [6]. The importance of considering maximum likelihood estimation has been suggested in Schmming and Hasler [9]. The performance of modulation schemes including the choice of a chaotic map is usually assessed by a *bit error rate* (*BER*), the error probability of estimation. Lawrance and Ohama [6] gives the calculation of an *exact* bit error rate while other earlier works, for example Abel *et al* [1], Kolumban [4], Lawrance and Balakrishna [5], Lipton and Dabke [7], Milanovic *et al* [8], Sushchik *et al* [10], and Tam *et al* [11], are based on either central limit theorem and give approximations of a bit error rate, or computational simulations. Though the difference in the performance of modulation schemes could be assessed by central limit theorem based approximations, the difference in the performance of chaotic maps could not be assessed because the difference of exact bit error rates is so small. We should not use the approximation based on simulation either unless sufficient statistical investigation is taken into account. Therefore an exact bit error rate is required to assess the performance. However, an exact bit error rate is not always calculated straightforwardly, especially when the *spreading factor* N is large, because numerical integration involves a too complicated function. For example, when a chaotic map is tent map on an interval $[0, 1]$ and $N = 20$, the numerical integration of a function with 2^{19} peaks

Key words and phrases. chaos, chaos communications, chaos-shift keying, exact bit error rate, Taylor expansion, Taylor approximation.

on $[0,1]$ is required to obtain the exact bit error rate. Such numerical integration is either poorly accurate or requires too much time to calculate, and thus an exact bit error rate is not the practical measurement of the performance when spreading factor is large. We therefore need a new approximation. What we require of a new approximation is

(C1) To be a function of a chaotic map τ, and preferably of a *signal to noise ratio* (*SNR*) and the spreading factor N.

(C2) As a function of a chaotic map, if τ_1 is mapped to a less value than the value τ_2 is mapped, an exact bit error rate with τ_1 is lower than one with τ_2, or at least there is a strong positive correlation between the mapped values and exact bit error rates.

(C3) To be calculated easily.

We will consider only coherent *chaos shift-keying* (CSK) systems , that is, all information of a spreading sequence $\{X_i\}$ is given to a receiver. It is because not only coherent systems are simple but also we might assume that a good chaotic map in coherent systems is also a good chaotic map in non-coherent systems. In section 2, we will give a brief explanation of CSK systems and the calculation of an exact bit error rate based on Lawrance and Ohama [6]. In section 3, we will give new approximations of a bit error rate based on Taylor expansion and see its efficiency. In section 4, we will modify the previous approximations so that it requires less time to calculate. Section 5 is dedicated to discussion.

2. Coherent chaos shift-keying systems and exact bit error rates

In coherent chaos shift-keying systems, digital bit signal b ($+1$ or -1) is sent to a receiver with being embedded in a spreading sequence $\{X_i\}$, which is generated by a chaotic map $\tau(z)$, $c \leq z \leq d$. The sequence is assumed to have been started with a random value from an invariant distribution of the map, thus the each element of the sequence has the common mean μ and the common variance ${\sigma_X}^2$. The embedded signal is of the form $\mu + b(X_i - \mu)$ and thus the bit is signed by either leaving the chaotic sequence unchanged as X_i ($b = 1$), or reflecting it about its mean μ as $2\mu - X_i$, a form of chaotic modulation. To avoid the reflected values being out of range, the invariant distribution is assumed to be symmetric and so $\mu = (d-c)/2$. Modulated signals go through the transmission channel and are corrupted by AWGN, $\{\varepsilon_i\}$, with variance σ^2. Thus the received signal is of the form $R_i = \mu + b(X_i - \mu) + \varepsilon_i$. A receiver is assumed to have all information of $\{X_i\}$ in coherent systems. If not, the systems are considered as non-coherent systems. We will treat only coherent systems in this paper. A receiver thus estimates b by $\{R_i\}$ and $\{X_i\}$. A widely known correlation decoder gives maximum likelihood estimation $\hat{b}$ in coherent CSK systems and it is of the form

$$\hat{b} = \begin{cases} 1 & \text{if} \quad \sum_{i=1}^{N}(X_i - \mu)(R_i - \mu) \geq 0 \\ -1 & \text{if} \quad \sum_{i=1}^{N}(X_i - \mu)(R_i - \mu) < 0. \end{cases}$$

Therefore a theoretical bit error rate of the case $b = 1$ is sent is

$$\Pr(\textstyle\sum_{i=1}^{N}(X_i - \mu)(R_i - \mu) < 0 \;\big|\; b = 1),$$

and one of the case $b = -1$ is sent is

$$\Pr(\textstyle\sum_{i=1}^{N}(X_i - \mu)(R_i - \mu) \geq 0 \;\big|\; b = -1).$$

It can be seen easily that the two probabilities are of the same, so we will consider only the case of $b = 1$ throughout this paper. In Lawrance and Ohama [6] it has been proved that

$$BER = E[\Phi(-\sqrt{\textstyle\sum_{i=1}^{N}(X_i - \mu)^2}/\sigma)],$$

where $\Phi(x)$ is the distribution function of a standard Gaussian random variable and expectation is taken over the spreading sequence. By the definition of the chaotic spreading sequence the expectation can be reduced to one argument expectation as

$$E[\Phi(-\sqrt{\textstyle\sum_{i=1}^{N}(\tau^{i-1}(X_1)-\mu)^2}/\sigma)].$$

A signal to noise ratio is usually standardized by multiplying the spreading factor N, that is, $N\sigma_x^2/\sigma^2$. It is called the *per bitsignal to noise ratio* (*pbSNR*). The reason for the standardization is to compensate for different spreading factors N and the use of the transmission channel. With this notation we have

$$\begin{aligned} BER &= E[\Phi(-\sqrt{pbSNR}\sqrt{N^{-1}\textstyle\sum_{i=1}^{N}(\tau^{i-1}(X_1)-\mu)^2/{\sigma_x}^2})] \\ &= 1-E[\Phi(\sqrt{pbSNR}\sqrt{N^{-1}\textstyle\sum_{i=1}^{N}(\tau^{i-1}(X_1)-\mu)^2/{\sigma_x}^2})]. \end{aligned}$$

As we have mentioned it takes enormous time to calculate the above expectation numerically when N is large, efficient approximation is thus of interest.

3. Taylor approximations of bit error rates.

Put $\delta=\sqrt{pbSNR}$ and $S_N(x)=N^{-1}\sum_{i=1}^{N}\left(\tau^{i-1}(x)-\mu\right)^2/\sigma_x^2$ for simplicity and δ is assumed to be a constant. We begin with approximating $\Phi(\delta\sqrt{S_N(X_1)})$ by using Taylor expansion. By the low of large number it might be assumed that $S_N(X_1)$ is close to 1 when N is large and so Taylor approximation of $\Phi(\delta\sqrt{S_N(X_1)})$ at δ might be a good approximation. Since $\Phi(x)$ is C^∞-*class*,

$$\begin{aligned} \Phi(\delta\sqrt{S_N(x)}) = &\sum_{k=0}^{K}\frac{1}{k!}\Phi^{(k)}(\delta)\{\delta(\sqrt{S_N(x)}-1)\}^k \\ &+\frac{\{\delta(\sqrt{S_N(x)}-1)\}^{K+1}}{(K+1)!}\Phi^{(K+1)}(\delta+\theta\delta(\sqrt{S_N(x)}-1)), \qquad (1) \end{aligned}$$

for some $\theta=\theta(x;K)$ in $(0,1)$, any x in $[c,d]$, and any K in $\mathbf{N}$. Define $R_{K+1}(x)=R_{K+1;N}(x)$ as the second term of the right-hand side of (1), we have

$$\begin{aligned} &E\big[\Phi(\delta\sqrt{S_N(X_1)})\big] \\ &=\int_c^d\Phi(\delta\sqrt{S_N(x)})f(x)dx \\ &=\int_c^d\big[\textstyle\sum_{k=0}^{K}\frac{1}{k!}\Phi^{(k)}(\delta)\big\{\delta(\sqrt{S_N(x)}-1)\big\}^k+R_{K+1}(x)\big]f(x)dx \\ &=\sum_{k=0}^{K}\frac{\delta^k}{k!}\Phi^{(k)}(\delta)\textstyle\int_c^d(\sqrt{S_N(x)}-1)^kf(x)dx+\int_c^dR_{K+1}(x)f(x)dx \\ &=\sum_{k=0}^{K}\frac{\delta^k}{k!}\Phi^{(k)}(\delta)E\big[(\sqrt{S_N(X_1)}-1)^k\big]+\textstyle\int_c^dR_{K+1}(x)f(x)dx. \qquad (2) \end{aligned}$$

Our purpose is approximating $E[\Phi(\delta\sqrt{S_N(X_1)})]$ by the first term of the right-hand side of (2), so the absolute value of the second term is of interest, especially in terms of K and N. Define $\phi(x)$ as the density function of a standard Gaussian random variable then we have

$$R_{K+1}(x)=\frac{\big\{\delta(\sqrt{S_N(x)}-1)\big\}^{K+1}}{(K+1)!}\phi^{(K)}\big(\delta+\theta\delta(\sqrt{S_N(x)}-1)\big). \qquad (3)$$

Note that if $\left|\int_c^d R_{K+1}(x)f(x)dx\right|$ converges to 0 as $K \to \infty$ or $N \to \infty$, the summation in (2) converges to $E[\Phi(\delta\sqrt{S_N(X_1)})]$. Put $y = x/\sqrt{2}$ and define $H_K(y)$ as Kth order Hermite polynomial then we have, for any x in $[c, d]$,

$$\begin{aligned}
\phi^{(K)}(x) &= \frac{d^K}{dx^K}\frac{1}{\sqrt{2\pi}}e^{-\frac{x^2}{2}} = \frac{1}{\sqrt{2\pi}}\left(\frac{dy}{dx}\right)^K \frac{d^K}{dy^K}e^{-y^2} \\
&= \frac{1}{\sqrt{2\pi}}\left(\frac{1}{\sqrt{2}}\right)^K H_K(y)(-1)^K e^{-y^2} = \frac{1}{\sqrt{2\pi}}\left(-\frac{1}{\sqrt{2}}\right)^K \tilde{h}_K(y)e^{-\frac{y^2}{2}} \\
&= \frac{1}{\sqrt{2\pi}}\left(-\frac{1}{\sqrt{2}}\right)^K \tilde{h}_K(\frac{x}{\sqrt{2}})e^{-\frac{x^2}{4}} = (-1)^K e^{-\frac{x^2}{4}}\sqrt{\frac{K!}{2\sqrt{\pi}}}\frac{\tilde{h}_K(\frac{x}{\sqrt{2}})}{\sqrt{2^K K!\sqrt{\pi}}} \\
&= (-1)^K e^{-\frac{x^2}{4}}\sqrt{K!/2\sqrt{\pi}}\, h_K(\frac{x}{\sqrt{2}}), \qquad (4)
\end{aligned}$$

where $\tilde{h}_K(y) = H_K(y)e^{-\frac{y^2}{2}}$ and $h_K(y) = \tilde{h}_K(y)/\sqrt{2^K K!\sqrt{\pi}}$. By Lemma 1.5.1 in Thangvelu [12]

$$\left|\phi^{(K)}(x)\right| = e^{-\frac{x^2}{4}}\sqrt{K!/2\sqrt{\pi}}\left|h_K(\frac{x}{\sqrt{2}})\right| \le C\sqrt{K!}, \qquad (5)$$

where C is some constant. So we have

$$\left|\int_c^d R_{K+1}(x)f(x)dx\right| \le C\delta^{K+1}\sqrt{K!}\int_c^d |\sqrt{S_N(x)} - 1|^{K+1} f(x)dx \;/\; (K+1)!. \qquad (6)$$

Since $c \le \tau(x) \le d$,

$$\begin{aligned}
S_N(x) &= N^{-1}\sum_{i=1}^N \left(\tau^{i-1}(x) - \mu\right)^2 / {\sigma_X}^2 \\
&= N^{-1}\sum_{i=1}^N \left(\tau^{i-1}(x) - \frac{c+d}{2}\right)^2 / {\sigma_X}^2 \le \left(\frac{d-c}{2\sigma_X}\right)^2, \qquad (7)
\end{aligned}$$

for any N and there thus exists the maximum M of $\left|\sqrt{S_N(x)} - 1\right|$. So we have

$$\begin{aligned}
\left|\int_c^d R_{K+1}(x)f(x)dx\right| &\le C\delta^{K+1}\sqrt{K!}\int_c^d M^{K+1} f(x)dx \;/\; (K+1)! \\
&\le C\delta^{K+1}M^{K+1}\sqrt{K!} \;/\; (K+1)! \\
&= \frac{C}{\sqrt{K+1}}\sqrt{\frac{(\delta M)^2}{K+1}\frac{(\delta M)^2}{K}\cdots\frac{(\delta M)^2}{2}\frac{(\delta M)^2}{1}} \xrightarrow{K\to\infty} 0, \qquad (8)
\end{aligned}$$

for any N. On the other hand, when K is fixed it can be proved that

$$\int_c^d |\sqrt{S_N(x)} - 1|^{K+1} f(x)dx \to 0 \quad \text{as} \quad N \to \infty, \qquad (9)$$

by Chebyshev inequality with the assumption that the variance of $S_N(X_1)$ converges as N increases. This assumption is not too strict when the sequence is chaotic. Therefore $|\int_c^d R_{K+1}(x)f(x)dx|$ converges to 0 as K or N increases and so we can approximate a bit error rate by Kth order Taylor approximation, $Approx(K)$ say,

$$Approx(K) = Approx(K; N, \delta, \tau) = 1 - \sum_{k=0}^K \frac{\delta^k}{k!}\Phi^{(k)}(\delta)E[(\sqrt{S_N(X_1)} - 1)^k]. \qquad (10)$$

with large K or N. Note that when $K = 0$ the approximation is lower bound $1 - \Phi(\sqrt{pbSNR})$ in Lawrance and Ohama [6]. It should also be noted that large $pbSNR$, that is, large δ^2 makes the right-hand side of (6) large and thus the rate of

convergence might be slower than when $pbSNR$ is small. Except $K = 0$, the approximations do not hold (C3) in Section 1 because of the term $E[(\sqrt{S_N(X_1)} - 1)^k]$. The required time for this numerical integration is not essentially different from the one for an exact bit error rate. However we will compare these approximations with rather small N in order to understand what is happening in the approximating. Chaotic maps employed are

(a) Tent map;

$$\tau(x) = \begin{cases} 2x & (0 \le x < 1/2) \\ 2(1-x) & (1/2 \le x \le 1). \end{cases}$$

(b) 3 branch shift map;

$$\tau(x) = \begin{cases} 3x & (0 \le x < 1/3) \\ 3x - 1/3 & (1/3 \le x < 2/3) \\ 3x - 2/3 & (2/3 \le x \le 1). \end{cases}$$

(c) (3,1)-tailed shift map;

$$\tau(x) = \begin{cases} 2x + 1/3 & (0 \le x < 1/3) \\ 2x - 1/3 & (1/3 \le x < 2/3) \\ x - 2/3 & (2/3 \le x \le 1). \end{cases}$$

(d) Skewed tent map;

$$\tau(x) = \begin{cases} 4x/3 & (0 \le x < 3/4) \\ 4(1-x) & (3/4 \le x \le 1). \end{cases}$$

(e) Order 2 Chebyshev map (usual Chebyshev map);

$$\tau(x) = \cos(2\arccos(x)) = 2x^2 - 1 \quad (-1 \le x \le 1).$$

(f) Order 3 Chebyshev map (cubic map);

$$\tau(x) = \cos(3\arccos(x)) = 4x^3 - 3x \quad (-1 \le x \le 1).$$

(g) A nonlinear map;

$$\tau(x) = \begin{cases} -\frac{1}{2}x + \frac{\sqrt{3}}{2}\sqrt{1-x^2} & (-1 \le x \le -1/2) \\ x^2 - \frac{1}{2} + x\sqrt{3(1-x^2)} & (-1/2 < x \le 1/2) \\ x^2 - \frac{1}{2} - x\sqrt{3(1-x^2)} & (1/2 < x \le 1) \end{cases}$$

(h) A nonlinear map;

$$\tau(x) = \begin{cases} \cos(4\arccos(x)) & (-1 \le x < -\sqrt{2}/2) \\ \cos(4\arccos(x)/3) & (-\sqrt{2}/2 \le x \le 1). \end{cases}$$

It is well known that maps (a) to (d) are piecewise linear maps on $[0, 1]$ with uniform invariant distribution and maps (e) and (f) are nonlinear maps on $[-1, 1]$ with $\beta(\frac{1}{2}, \frac{1}{2})$ invariant distribution. It will be seen in Appendix B that maps (g) and (h) are piecewise nonlinear maps on $[-1, 1]$ with the same invariant distribution as maps (e) and (f). See Geisel and Fairen [2] and Appendix B for further information of these maps. Figure 1 and the following similar figures are plots of exact bit error rates against theirs approximations with spreading maps (a) to (h) and several spreading factors. The spreading factor N employed are 2, 5 and 10, per bit signal to noise ratio $pbSNR$ employed are -5, 0, 5, 10, 15 and 20 (measured in decibel). Bit error rates with per bit signal to noise ratio $pbSNR = -5$ (star), $pbSNR = 0$ (triangle) and $pbSNR = 5$ (cross) are plotted against approximations $Approx(2)$, $Approx(3)$ and $Approx(4)$ in Figure 1, Figure 2 and Figure 3 respectively. Note that

there is no distinctive mark for different spreading maps and spreading factors. A line in each figure shows $y = x$ for comparison. The more points on this line, the better the approximation. These figures show that every approximation seems to be sufficiently good when $pbSNR$ is less than 5.

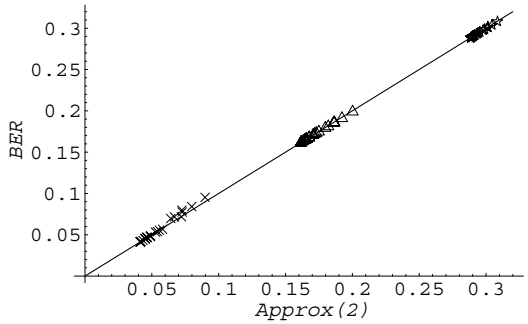

Figure 1. Bit error rates BER are plotted against approximations $Approx(2)$ with per bit signal to noise ratios $pbSNR = -5$ (star), $pbSNR = 0$ (triangle) and $pbSNR = 5$ (cross).

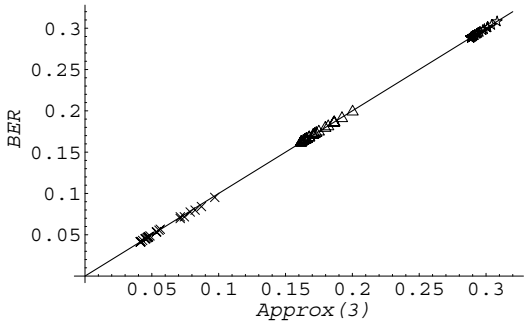

Figure 2. Bit error rates BER are plotted against approximations $Approx(3)$ with per bit signal to noise ratios $pbSNR = -5$ (star), $pbSNR = 0$ (triangle) and $pbSNR = 5$ (cross).

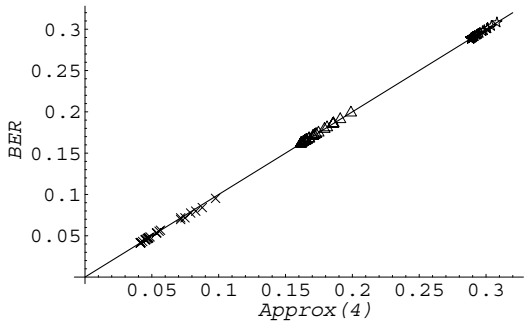

Figure 3. Bit error rates BER are plotted against approximations $Approx(4)$ with per bit signal to noise ratios $pbSNR = -5$ (star), $pbSNR = 0$ (triangle) and $pbSNR = 5$ (cross).

In Figure 4, exact bit error rates are plotted against approximation $Approx(k)$ with $k = 2$ (stars), $k = 3$ (triangles) and $k = 4$ (crosses). The common per bit signal to noise ratio 10 is employed here. This figure shows that when $pbSNR$ is 10,

$Approx(2)$ and $Approx(3)$ are not as good as the case $pbSNR$ is less than 5 while $Approx(4)$ is. It might be due to the fact that a large $pbSNR$ makes the rate of convergence slow as we have mentioned, so either an order of Taylor expansion or the spreading factor might not be large enough in these cases. However there seems to be a positive correlation between each order approximations $Approx(k)$ and bit error rates. Figure 5 is the same scatter plot as Figure 4 but plotted only against $Approx(4)$ and indicated different spreading factors by different shapes as triangles ($N = 2$), stars ($N = 5$) and crosses ($N = 10$). This figure suggests that even wiht 4th order approximation, spreading factor 2 is not large enough when $pbSNR = 10$. Figure 6 and Figure 7 are plots of bit error rates against $Approx(4)$ with per bit signal to noise ratio $pbSNR = 15$ and $pbSNR = 20$ respectively. These figures show that even $Approx(4)$ with spreading factor $N = 10$ is not a good approximation when $pbSNR$ is greater than 15. It might be suggested that either higher order Taylor approximation or larger spreading factor are required to approximate a bit error rate with large $pbSNR$ efficiently.

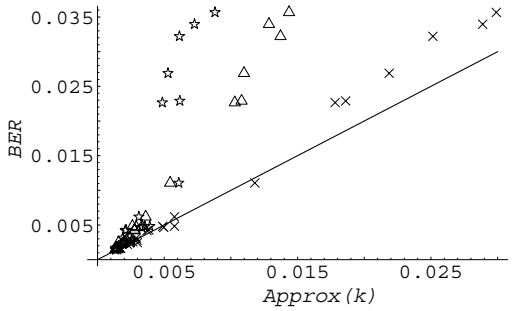

Figure 4. Bit error rates BER are plotted against approximation $Approx(k)$ with $k = 2$ (star), $k = 3$ (triangle) and $k = 4$ (cross). The common per bit signal to noise ratio $pbSNR = 10$ is employed.

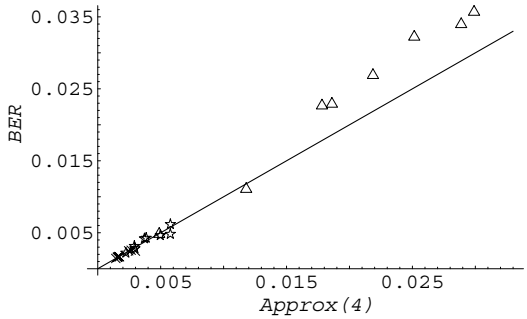

Figure 5. Bit error rates BER are plotted against approximation $Approx(4)$ with spreading factor $N = 2$ (triangle), $N = 5$ (star) and $N = 10$ (cross). The common per bit signal to noise ratio $pbSNR = 10$ is employed.

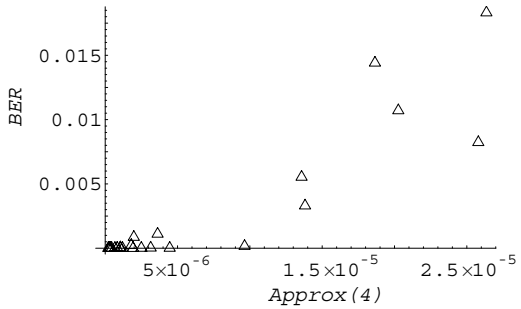

Figure 6. Bit error rates BER are plotted against approximations $Approx(4)$ with a per bit signal to noise ratio $pbSNR = 15$.

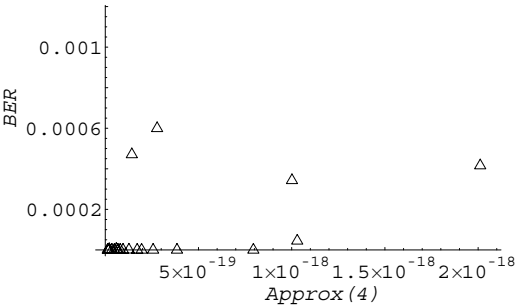

Figure 7. Bit error rates BER are plotted against approximations $Approx(4)$ with a per bit signal to noise ratio $pbSNR = 20$.

4. **Modification of Taylor approximation**

As we have mentioned in the previous section, Taylor approximation $Approx(k)$ does not hold (C3) in Section 1. We thus need to modify it so that a new approximation requires less time to be calculated. The cause of the long calculating time of $Approx(k)$ is the terms $E[(\sqrt{S_N(X_1)} - 1)^k]$, more explicitly $E[\sqrt{S_N(X_1)}]$ and $E[\sqrt{S_N(X_1)}^3]$ when $k = 4$. We again use Taylor approximation of these terms. Put $S_N = S_N(X_1)$ then we have

$$E[\sqrt{S_N}] \approx 1 + \frac{1}{2}E[(S_N - 1)] - \frac{1}{8}E[(S_N - 1)^2], \tag{11}$$

and

$$E[\sqrt{S_N}^3] \approx 1 + \frac{3}{2}E[(S_N - 1)] + \frac{3}{8}E[(S_N - 1)^2], \tag{12}$$

when S_N is close to 1, that is, N is large. Note that $E[(S_N - 1)] = 0$ so we have

$$\begin{aligned} E[\sqrt{S_N} - 1] &\approx -\frac{1}{8}E[(S_N - 1)^2], \\ E[(\sqrt{S_N} - 1)^2] &= 2(1 - E[\sqrt{S_N}]) \approx \frac{1}{4}E[(S_N - 1)^2], \\ E[(\sqrt{S_N} - 1)^3] &= E[\sqrt{S_N}^3] - 1 + 3(E[\sqrt{S_N}] - 1) \\ &\approx \frac{3}{8}E[(S_N - 1)^2] - \frac{3}{8}E[(S_N - 1)^2] = 0, \end{aligned} \tag{13}$$

and

$$\begin{aligned} E[(\sqrt{S_N}-1)^4] &= E[S_N^2] - 4E[\sqrt{S_N}^3] + 6E[S_N] - 4E[\sqrt{S_N}] + 1 \\ &= E[(S_N-1)^2] - 4(E[\sqrt{S_N}^3] - 1) + 4(1 - E[\sqrt{S_N}]) \\ &\approx (1 - \frac{12}{8} + \frac{4}{8})E[(S_N-1)^2] = 0. \end{aligned} \tag{14}$$

Therefore we have

$$\begin{aligned} & Approx(4)\ (\approx Approx(3) \approx Approx(2)) \\ &\approx 1 - \Phi(\delta) - \delta\Phi'(\delta)(-\frac{1}{8}E[(S_N-1)^2]) - \frac{\delta^2}{2}\Phi''(\delta)(\frac{1}{4}E[(S_N-1)^2]) \\ &= 1 - \Phi(\delta) + \delta(1+\delta^2)e^{-\frac{\delta}{2}}E[(S_N-1)^2] \ /\ (8\sqrt{2\pi}). \end{aligned} \tag{15}$$

Note that if we put $g(S_N) = \Phi(\delta\sqrt{S_N})$ and approximate it by second order Taylor approximation of $g(x)$ at $x = 1$, we have the same approximation as the above and this approximation is thus essentially second order. It might be because we approximate the terms $E[\sqrt{S_N}]$ and $E[\sqrt{S_N}^3]$ up to second order. If we approximate them up to third order we will have an approximation

$$1 - \Phi(\delta) - \frac{1}{2}g''(1)E[(S_N-1)^2] - \frac{1}{6}g'''(1)E[(S_N-1)^3]. \tag{16}$$

Therefore a new approximation might be

$$NewAp(K) \stackrel{\text{def}}{=} 1 - \sum_{k=0}^{K} g^{(k)}(1)E[(S_N-1)^k]/k!. \tag{17}$$

It should be noted that the required time to calculate $E[(S_N-1)^k]$ might possibly be less than the one for $E[(\sqrt{S_N}-1)^k]$ because *Perron-Frobenius* theorem can be applied, though it might not be so easy to calculate when k is greater than 2. Only $NewAp(2)$ has been calculated for the same maps and the same $pbSNR$ given in the previous section. In Figure 8, exact bit error rates are plotted against theirs new approximations $NewAp(2)$ with per bit signal to noise ratio $pbSNR = -5$ (stars), $pbSNR = 0$ (triangles) and $pbSNR = 5$ (crosses). There is no distinctive mark for different maps and spreading factors. Points are not quite on the $y = x$ line when $pbSNR = 5$ while they are so in Figure 1, Figure 2 and Figure 3.

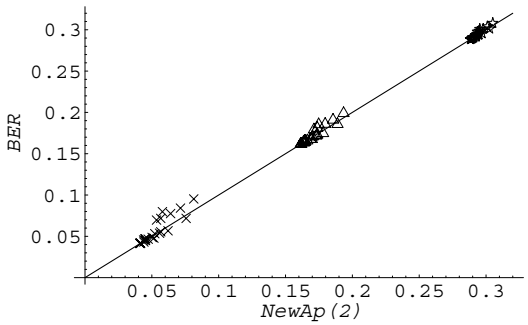

Figure 8. Bit error rates BER are plotted against new approximations $NewAp(2)$ with per bit singal to noise ratios $pbSNR = -5$ (star), $pbSNR = 0$ (triangle) and $pbSNR = 5$ (cross).

Figure 9 is the same scatter plot as Figure 8 but with a per bit singal to noise ratio $pbSNR = 10$. This figure suggests that higher order approximations will be required for large $pbSNR$ like the previous approximation $Approx(k)$. However, it

seems that there is a positive correlation between $NewAP(2)$ and exact bit error rates.

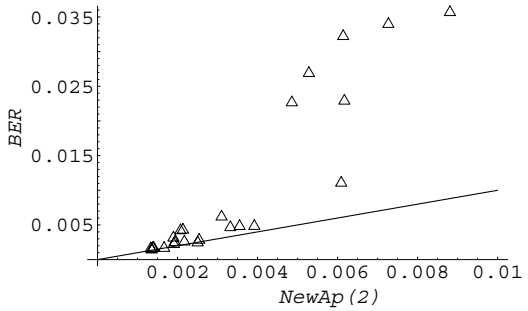

Figure 9. Bit error rates BER are plotted against new approximations $NewAp(2)$ with a per bit singal to noise ratio $pbSNR = 10$.

5. Discussion

It should be noted that $NewAp(2)$ is a linear function of $E[(S_N - 1)^2]$ when $pbSNR = \delta^2$ is fixed, therefore a chaotic map with small $E[(S_N - 1)^2]$ might lead a low bit error rate. Define ${\sigma_{(X-\mu)^2}}^2$ and $\rho_{(X-\mu)^2}(t)$ as variance and autocorrelation function of $(X_i - \mu)^2$ (mean-centered quadratic variance and autocorrelation function of X_i) respectively. Since

$$E[(S_N - 1)^2] = N^{-1} \frac{{\sigma_{(X-\mu)^2}}^2}{{\sigma_X}^4} \left\{ 1 + 2\sum_{t=1}^{N-1} (1 - \tfrac{t}{N}) \rho_{(X-\mu)^2}(t) \right\},$$

negative mean-centered quadratic autocorrelations might decrease a bit error rate to some extent as Lawrance and Balakrishna [5] has suggested, at least when $pbSNR$ is rather small. (This suggestion has been brought about by the approximation of a bit error rate based on the central limit theorem.) However the negativity is not enough to asses bit error rates' behaviour because $NewAp(2)$ is not a good approximation with large $pbSNR$. Furthermore, since any higher order dependency is not taken into account, it is impossible to distinguish different order Chebyshev maps by $E[(S_N - 1)^2]$, that is the same value among Chebyshev maps. Therefore it might be required to investigate higher order moments of $S_N - 1$ which will provide higher order approximations, and this investigation might lead us to the investigation of distribution of S_N, which is deeply concerned in outage probability. Outage probability is another idea of efficiency in communication systems. The further investigation of the relation between a bit error rate and outage probability will be reported by the same authors.

References

[1] A. Abel, W. Schwarz and M. Götz, "Noise performance of chaotic communication systems," *IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications*, 47,12, 1726-1732, 2000.

[2] T. Geisel and V. Fairen, "Statistical properties of chaos in Chebyshev maps" *Phisics Letters*, 105A, 6, 263-266, 1984.

[3] M.P. Kennedy, R. Rovati and G. Setti (eds), *Chaotic Electronics in Telecommunications*. CRC Press, London, 2000.

[4] G. Koloumban, "Theoretical noise performance of correlator-based chaotic communications systems," *IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications*, 47,12, 1692-1701, 2000.

[5] A.J. Lawrance and N. Balakrishna, "Statistical aspects of chaotic maps with negative dependency in a communications setting," *Journal of the Royal Statistical Society, Series B*, 63, 843-853, 2001.

[6] A.J. Lawrance and G. Ohama, "Exact calculation of bit error rates in chaos communication modelling," *submitted to IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications*, 2002.

[7] J.M. Lipton and K.P. Dabke, "Spread spectrum communications based on chaotic systems," *International Journal of Bifurcation and Chaos*, 12A, 2361-2374, 1996.

[8] V. Milanovic, K.M. Syed and M. Zaghloul, "Combationg noise and other channel distortions in chaotic communications," *International Journal of Bifurcation and Chaos*, 7, 215-225, 1997.

[9] T. Schimming and M. Hasler, "Optimal detection of differential chaos-shift keying," *IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications*, 47, 1712-1719, 2000.

[10] M. Sushchik, L.S. Tsimring and A.R. Volkovskii, "Performance analysis of correlation-based communication schemes utilizing chaos," *IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications*, 47, 1684-1691, 2000.

[11] W.M. Tam, F.C.M. Lau, C.K. Tse and M.M. Yip, "An approach to calculating the bit-error rate of a coherent choas-shift-keying digital communication system under a noisy multiuser enviroment," *IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications*, 49, 210-223, 2002.

[12] S. Thangavelu, *Lectures on Hermite and Laguerre Expansions.* Princeton University Press, Princeton, 1993.

APENDIX A.
Mean-centered quadratic autocorrelation function of (3,1)-tailed shift map

As we have already seen, a mean-centered quadratic autocorrelation function might play a important role in the assessment of chaotic maps. This function can be obtained by using Perron-Frobenius operator repeatedly, but this repetition tend to be in a mess when a chaotic map is not simple, like (3,1)-tailed shift map. In this appendix, the theoretical mean-centered autocorrelation function of (3,1)-tailed shift map will be given in recursive formulae. (3,1)-tailed shift map (Figure A1) is defined as follows.

$$\tau(x) = \begin{cases} 2x + 1/3 & (0 \le x < 1/3) \\ 2x - 1/3 & (1/3 \le x < 2/3) \\ x - 2/3 & (2/3 \le x \le 1). \end{cases}$$

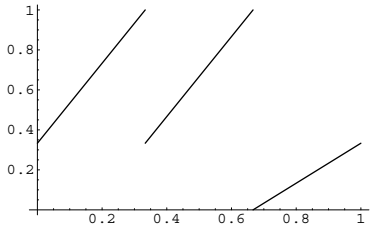

Figure A1. (3,1)-tailed shift map.

Put

$$\begin{aligned}
a_n &= E[I_{[0,1/3]}(X_t)\{(X_t-\mu)^2 - {\sigma_X}^2\}\{(X_{t+n}-\mu)^2 - {\sigma_X}^2\}], \\
A_n &= E[I_{[1/3,1]}(X_t)\{(X_t-\mu)^2 - {\sigma_X}^2\}\{(X_{t+n}-\mu)^2 - {\sigma_X}^2\}], \\
b_n &= E[I_{[0,1/3]}(X_t)(X_t-\mu)\{(X_{t+n}-\mu)^2 - {\sigma_X}^2\}], \\
B_n &= E[I_{[1/3,1]}(X_t)(X_t-\mu)\{(X_{t+n}-\mu)^2 - {\sigma_X}^2\}], \\
c_n &= E[I_{[0,1/3]}(X_t)\{(X_{t+n}-\mu)^2 - {\sigma_X}^2\}], \\
C_n &= E[I_{[1/3,1]}(X_t)\{(X_{t+n}-\mu)^2 - {\sigma_X}^2\}],
\end{aligned}$$

where $I_{[\alpha,\beta]}(x)$ is an indicator function on an interval $[\alpha, \beta]$, $X_{t+n} = \tau(X_{t+n-1}) = \tau^n(X_t)$, $\mu = 1/2$ and ${\sigma_X}^2 = 1/12$. Note that $a_n + A_n = Cov[(X_t-\mu)^2, (X_{t+n}-\mu)^2]$

and $c_n + C_n = 0$. From the definition of a_n we have

$$\begin{aligned} a_n &= \int_0^{1/3}\{(x-\tfrac{1}{2})^2 - \tfrac{1}{12}\}\{(\tau^n(x)-\tfrac{1}{2})^2 - \tfrac{1}{12}\}dx \\ &= \int_0^{1/3}\{(x-\tfrac{1}{2})^2 - \tfrac{1}{12}\}\{(\tau^{n-1}(\tau(x))-\tfrac{1}{2})^2 - \tfrac{1}{12}\}dx \\ &= \int_0^{1/3}\{(x-\tfrac{1}{2})^2 - \tfrac{1}{12}\}\{(\tau^{n-1}(2x+\tfrac{1}{3})-\tfrac{1}{2})^2 - \tfrac{1}{12}\}dx, \end{aligned}$$

put $y = 2x + \frac{1}{3}$ then

$$\begin{aligned} &= \frac{1}{2}\int_{1/3}^1\{(\tfrac{1}{2}(y-\tfrac{1}{3})-\tfrac{1}{2})^2 - \tfrac{1}{12}\}\{(\tau^{n-1}(y)-\tfrac{1}{2})^2 - \tfrac{1}{12}\}dy \\ &= \frac{1}{8}\int_{1/3}^1\{(y-\tfrac{1}{2})^2 - \tfrac{1}{12}\}\{(\tau^{n-1}(y)-\tfrac{1}{2})^2 - \tfrac{1}{12}\}dy \\ &\quad + \frac{5}{24}\int_{1/3}^1(y-\tfrac{1}{2})\{(\tau^{n-1}(y)-\tfrac{1}{2})^2 - \tfrac{1}{12}\}dy \\ &\quad + \frac{1}{18}\int_{1/3}^1\{(\tau^{n-1}(y)-\tfrac{1}{2})^2 - \tfrac{1}{12}\}dy \\ &= \frac{1}{8}A_{n-1} - \frac{5}{24}B_{n-1} + \frac{1}{18}C_{n-1}. \end{aligned}$$

By the similar calculation, we have the following recursive formulae.

$$\begin{aligned} a_n &= \frac{1}{8}A_{n-1} - \frac{5}{24}B_{n-1} + \frac{1}{18}C_{n-1}, \\ b_n &= \frac{1}{4}B_{n-1} - \frac{5}{24}C_{n-1}, \\ c_n &= \frac{1}{2}C_{n-1}, \\ A_n &= \frac{1}{8}A_{n-1} - \frac{1}{24}B_{n-1} - \frac{1}{36}C_{n-1} + a_{n-1} + \frac{4}{3}b_{n-1} + \frac{4}{9}c_{n-1}, \\ B_n &= \frac{1}{4}B_{n-1} - \frac{1}{24}C_{n-1} + b_{n-1} + \frac{2}{3}c_{n-1}, \\ C_n &= \frac{1}{2}C_{n-1} + c_{n-1}. \end{aligned}$$

From these formulae and initial values $a_0, b_0, c_0, A_0, B_0,$ *and* C_0, which can be calculated easily, any mean-centered quadratic autocorrelation $\rho(h)$ can be calculated as $\rho(h) = (a_h + A_h)/(a_0 + A_0)$. For example, exact $\rho(h)$ for $h = 0, 1, \ldots, 10$ are

$$\{1, -\frac{1}{3}, \frac{17}{324}, \frac{7}{96}, -\frac{475}{20736}, \frac{8717}{165888}, -\frac{11723}{1327104}, \frac{224413}{10616832}, -\frac{110011}{84934656}, \frac{5095213}{679477248}, \frac{2269525}{5435817984}\}.$$

It is not necessary to explain these formulae explicitly, but we can describe some of formulae as follows.

$$\begin{aligned} B_n &= 8^{-n}(170\sum_{t=0}^{[n/2]}\binom{n}{2t}17^t - 374\sum_{t=0}^{[(n+1)/2]}\binom{n}{2t-1}17^t - 119(-4)^n)/32848, \\ b_n &= \frac{1}{4}B_{n-1} - \frac{5}{972}(-2)^{-n}, \\ C_n &= -\frac{1}{81}(-2)^{-n}, \\ c_n &= \frac{1}{81}(-2)^{-n}, \end{aligned}$$

where $[r]$ denotes the greatest integer less than r. However, it seems impossible to explain A_n and a_n explicitly. It should be noted that recursive formulae for an

autocorrelation function of any (n,k)-tailed shift (also antishift, mixed shift) map can be obtained similarly by dividing interval $[0,1]$ into $[0,\frac{k}{n}]$ and $[\frac{k}{n},1]$.

APENDIX B
Nonlinear chaotic maps with $\beta(\frac{1}{2},\frac{1}{2})$ invariant distribution

It is well known that tent map on a interval $[0,1]$ and order 2 Chebyshev map are *homeomorphic* and the function $\arccos(x)/\pi$ is the one of *homeomorphism*, that is, when we define $\tau_1(x)$ and $\tau_2(x)$ as tent map and order 2 Chebyshev map respectively and put $F(x)=\arccos(x)/\pi$, the equation $\tau_2(x)=F^{-1}\circ\tau_1\circ F(x)$ holds for any $x\in[-1,1]$ (see Geisel and Fairen [2]). The invariant density function of Chebyshev map is $\beta(\frac{1}{2},\frac{1}{2})$ on $[-1,1]$ and its distribution function is $F(x)$. This fact can be shown easily as follows. Put $X_t=\tau_1(X_{t-1})$ and $Y_t=F^{-1}(X_t)$ then we have

$$Y_t=F^{-1}(X_t)=F^{-1}\circ\tau_1(X_{t-1})=\tau_2\circ F^{-1}(X_{t-1})=\tau_2(Y_{t-1}),$$

and thus the invariant distribution function of τ_2 is,

$$\Pr(\tau_2(Y_{t-1})\le y)=\Pr(Y_t\le y)=\Pr(F^{-1}(X_t)\le y)=\Pr(X_t\le F(y))=F(y)$$

since the invariant distribution of τ_1 is uniform on $[0,1]$. Furthermore, the invariant distribution of τ_2 does not change even if we replace τ_1 with another chaotic map as long as its invariant distribution is uniform on $[0,1]$. Therefore we can think of a set of nonlinear chaotic maps whose invariant density function is $\beta(\frac{1}{2},\frac{1}{2})$, a set of generalized Chebyshev maps, say, by replacing τ_1 with various piecewise linear map on $[0,1]$ with uniform invariant distribution like skewed tent map or (n,k)-tailed shift map. In this appendix, we will provide several nonlinear chaotic map with $\beta(\frac{1}{2},\frac{1}{2})$ invariant distribution that we used in the main part of this paper.

Skewed Chebyshev map. Skewed tent map with a peak at α (Figure B1) is given as follows.

$$\tau(x)=\begin{cases}\frac{x}{\alpha} & (0\le x<\alpha)\\ \frac{1-x}{1-\alpha} & (\alpha\le x\le 1).\end{cases}$$

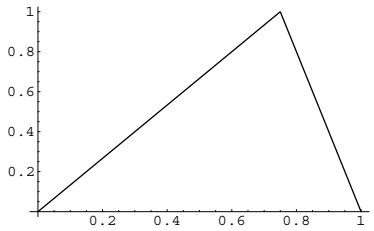

Figure B1.
Skewed tent map with a peak at 3/4.

It is usual tent map when $\alpha=\frac{1}{2}$. The nonlinear chaotic map induced by this map is as follows.

$$\tau_2(x)=F^{-1}\circ\tau_1\circ F(x)=F^{-1}\circ\tau_1(\arccos(x)/\pi).$$

Put $x_0=\cos(\alpha\pi)$. When $-1\le x<x_0$, that is, $\alpha<\arccos(x)/\pi\le 1$,

$$\tau_2(x)=F^{-1}((1-\frac{\arccos(x)}{\pi})/(1-\alpha))=\cos(\frac{\pi-\arccos(x)}{1-\alpha})$$
$$=\cos(\frac{\pi}{1-\alpha})\cos(\frac{\arccos(x)}{1-\alpha})+\sin(\frac{\pi}{1-\alpha})\sin(\frac{\arccos(x)}{1-\alpha}).$$

When $x_0\le x\le 1$, that is, $-1\le\arccos(x)/\pi\le\alpha$,

$$\tau_2(x)=F^{-1}(\arccos(x)/\alpha\pi)=\cos(\arccos(x)/\alpha).$$

Figure B2 shows its graph and this is the map we refered as (h) in Section 2.

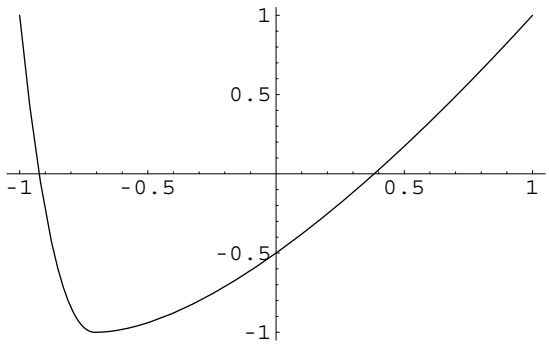

Figure B2. Skewed Chebyshev map induced by skewed tent map with a peak at 3/4. ($x_0 = -1/\sqrt{2}$)

(n,k)-tailed shift (antishift, mixed shift) Chebyshev map. We will see only one example here, $(3,1)$-tailed shift Chebyshev map, but we can produce other maps similarly. The definition of (3,1)-tailed shift map and its graph is given in the previous appendix. First of all, we need to know all undifferentiable points of an induced map, so we have to solve equations $\arccos(x)/\pi = k/n$ for $k = 1, \ldots, n-1$, in our case, $\arccos(x)/\pi = 1/3$ and $\arccos(x)/\pi = 2/3$. The solutions are $x_0 = 1/2$ and $x_1 = -1/2$ respectively. Therefore,

$$\begin{aligned}
\tau_2(x) &= F^{-1} \circ \tau_1(\arccos(x)/\pi) \\
&= F^{-1}(2\arccos(x)/\pi + 1/3) = \cos(2\arccos(x) + \pi/3) \\
&= \cos(\pi/3)\cos(2\arccos(x)) - \sin(\pi/3)\sin(2\arccos(x)) \\
&= \frac{1}{2}(2\cos(\arccos(x))^2 - 1) - \frac{\sqrt{3}}{2} 2\sin(\arccos(x))\cos(\arccos(x)) \\
&= x^2 - \frac{1}{2} - x\sqrt{3(1-x^2)}
\end{aligned}$$

for $x \in (1/2, 1]$,

$$\begin{aligned}
\tau_2(x) &= F^{-1} \circ \tau_1(\arccos(x)/\pi) \\
&= F^{-1}(2\arccos(x)/\pi - 1/3) = \cos(2\arccos(x) - \pi/3) \\
&= \cos(\pi/3)\cos(2\arccos(x)) + \sin(\pi/3)\sin(2\arccos(x)) \\
&= \frac{1}{2}(2\cos(\arccos(x))^2 - 1) + \frac{\sqrt{3}}{2} 2\sin(\arccos(x))\cos(\arccos(x)) \\
&= x^2 - \frac{1}{2} + x\sqrt{3(1-x^2)}
\end{aligned}$$

for $x \in (-1/2, 1/2]$,

$$\begin{aligned}
\tau_2(x) &= F^{-1} \circ \tau_1(\arccos(x)/\pi) \\
&= F^{-1}(\arccos(x)/\pi - 2/3) = \cos(\arccos(x) - 2\pi/3) \\
&= \cos(2\pi/3)\cos(\arccos(x)) + \sin(2\pi/3)\sin(\arccos(x)) \\
&= -\frac{1}{2}x + \frac{\sqrt{3}}{2}\sqrt{1-x^2}
\end{aligned}$$

for $x \in [-1, -1/2]$. Since $\arccos(x)$ is decreasing function on $[-1, 1]$, the induced map is left-continuous, not right-continuous. Figure B3 gives its graph and this is the map we refered as (g) in Section 2.

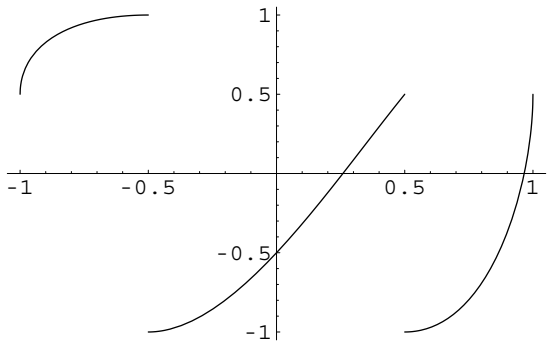

Figure B3. $(3, 1)$-tailed shift Chebyshev map

†The Fucluty of Economics, Shiga University, Hikone, Shiga 522-8522, Japan
E-mail address: ohama@biwako.shiga-u.ac.jp

‡The School of Mathematics and Statistics, University of Birmingham, Birmingham B15 2TT, UK
E-mail address: A.J.Lawrance@bham.ac.uk