Chaotic Modeling and Simulation (CMSIM) 1: 187-192, 2013

Newtonian and special-relativistic probability densities for a low-speed system

Shiuan-Ni Liang and Boon Leong Lan

School of Science, Monash University, 46150 Bandar Sunway, Selangor, Malaysia

Abstract. The Newtonian and special-relativistic predictions for the position and momentum probability densities of a model *low-speed* (i.e., much less than the speed light) dynamical system are compared. The Newtonian and special-relativistic probability densities, which are initially the same Gaussian, are calculated using an ensemble of trajectories. Contrary to expectation, we show that the predictions of the two theories can rapidly disagree completely. This surprising result raises an important fundamental question: which prediction is empirically correct?

INTRODUCTION

It is conventionally believed [1-3] that the predictions of special-relativistic mechanics for the motion of a dynamical system are well approximated by the predictions of Newtonian mechanics for the same parameters and initial conditions if the speed of the system v is *low* compared to the speed of light c ($v << c$). However, contrary to expectation, it was shown in recent numerical studies [4-8] that the Newtonian prediction for the trajectory of a low-speed dynamical system can rapidly disagree completely with the special-relativistic prediction.

In this paper, we extend the studies in [4-8] from the comparison of single-trajectory predictions to the comparison of the probability-density predictions calculated from an ensemble of trajectories. The model system we study here is the periodically delta-kicked system previously studied in [4]. Details of the model system and the probability-density calculations are presented next, followed by the results and concluding remarks.

Model System

The periodically delta-kicked system [4] is a one-dimensional Hamiltonian system where a particle is subjected to a sinusoidal potential that is periodically turned on for an instant. The Newtonian equations of motion for this system are easily integrated exactly [9,10] to yield the well-known standard map, which

Received: 19 September 2012 / Accepted: 18 January 2013

ISSN 2241-0503

maps the dimensionless scaled position X and dimensionless scaled momentum P from just before the nth kick to just before the (n+1)th kick:

$$P_n = P_{n-1} - \frac{K}{2\pi}\sin(2\pi X_{n-1}) \tag{1}$$

$$X_n = (X_{n-1} + P_n) \bmod 1 \tag{2}$$

where n = 1,2,…, and K is a dimensionless positive parameter.

The special-relativistic equations of motion are also easily integrated exactly, producing a mapping known as the relativistic standard map [11,12] for the dimensionless scaled position X and dimensionless scaled momentum P from just before the nth kick to just before the (n+1)th kick:

$$P_n = P_{n-1} - \frac{K}{2\pi}\sin(2\pi X_{n-1}) \tag{3}$$

$$X_n = \left(X_{n-1} + \frac{P_n}{\sqrt{1+\beta^2 P_n^2}} \right) \bmod 1 \tag{4}$$

where n = 1,2, …, and β, like K, is a dimensionless positive parameter.

The initial probability density is a Gaussian for both position and momentum with means $<X_0>$ and $<P_0>$, and standard deviations σ_{X0} and σ_{P0}:

$$\frac{1}{2\pi\sigma_{X0}\sigma_{P0}}\exp\left[-\frac{(X_0 - <X_0>)^2}{2\sigma_{X0}^2} - \frac{(P_0 - <P_0>)^2}{2\sigma_{P0}^2} \right].$$

In each theory, the probability density is calculated using an ensemble of trajectories, where each trajectory is time-evolved using the map. The probability density is first calculated using 10^6 trajectories, where the accuracy of the double-precision calculation is determined by comparison with the quadruple-precision calculation. The probability density is then recalculated using 10^7 trajectories with the same accuracy determination. Finally, the accuracy of the probability density is determined by comparing the 10^6-trajectories calculation with the 10^7-trajectories calculation.

Results

In the example presented here, the means and standard deviations of the initially Gaussian probability density are $<X_0>$ = 0.5, $<P_0>$ = 99.9 and $\sigma_{X0} = \sigma_{P0} = 10^{-10}$. The parameters of the maps are K = 0.9 and $\beta = 10^{-7}$.

Figures 1, 2 and 3 show that the Newtonian and special-relativistic position and momentum probability densities evolve approximately as Gaussians with increasing widths up to at least kick 114.

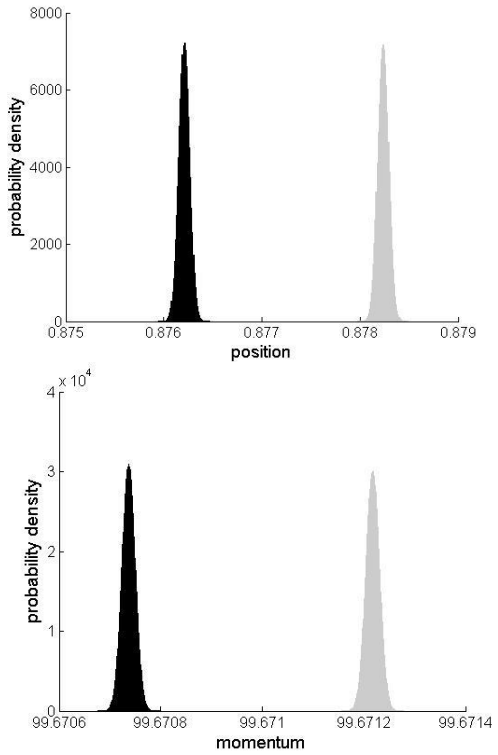

Figure 1. Comparison of Newtonian (grey) and special relativistic (black) position (top plot) and momentum (bottom plot) probability density for kick 80.

Figure 1 shows that, for both position and momentum, the Newtonian and special-relativistic probability densities are still close to one another on the whole at kick 80. The centers of the Newtonian and special-relativistic probability densities are displaced from each other in the figure because of the very small scale required for the horizontal axis to see the very narrow densities.

By kick 89, Figure 2 shows that, for both position and momentum, although the centers of the Newtonian and special-relativistic probability densities are still close, the Newtonian probability density is significantly wider and shorter than the special-relativistic probability density.

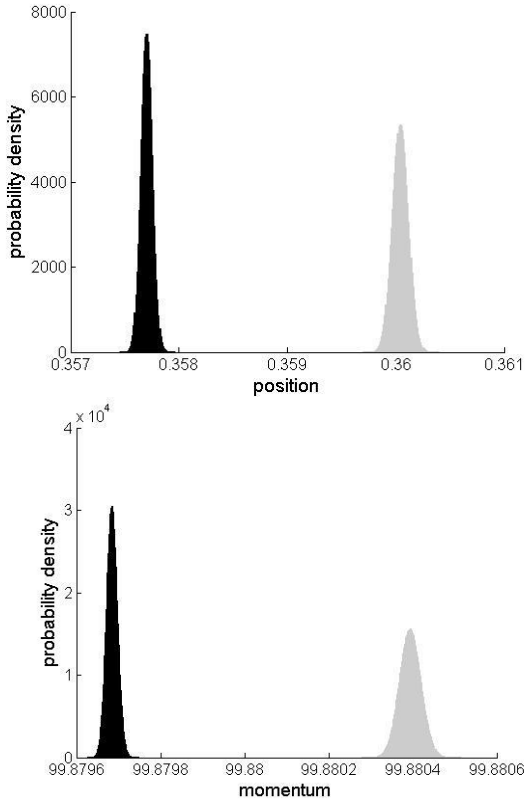

Figure 2. Comparison of Newtonian (grey) and special relativistic (black) position (top plot) and momentum (bottom plot) probability density for kick 89.

At kick 114, Figure 3 shows that not only are the widths and heights of the Newtonian and special-relativistic probability densities completely different for both position and momentum, the centers of the position probability densities are also completely different.

In summary, the three figures show that, although the mean speed of the system remains low, only 0.001% the speed of light, the Newtonian position and momentum probability densities disagree completely with the corresponding special-relativistic probability densities from kick 89 onwards.

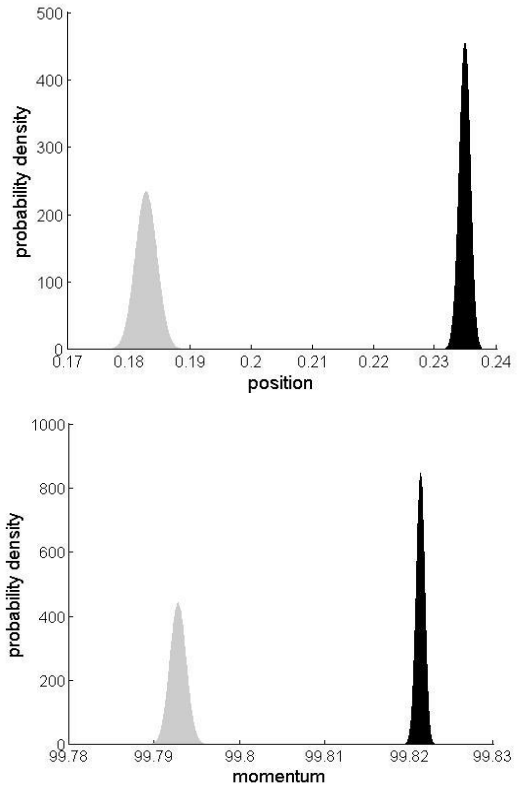

Figure 3. Comparison of Newtonian (grey) and special relativistic (black) position (top plot) and momentum (bottom plot) probability density for kick 114.

Concluding remarks

We have shown that, contrary to expectation, the Newtonian and special-relativistic probability-density predictions for a low-speed dynamical system can rapidly disagree completely.

Our result raises an important fundamental question: When Newtonian and special-relativistic mechanics predict completely different probability densities for a *low-speed* dynamical system, which of the two predictions is empirically correct? Since special relativity has survived many experimental tests in the high speed regime, it would be very strange indeed if the theory is invalid for low speed motion. If special relativity is also empirically correct at low speed as we expect, then it must be used, instead of the standard practice of using Newtonian theory, to correctly calculate the probability density for a low-speed dynamical system.

Acknowledgment

This study was supported by a Fundamental Research Grant Scheme, FRGS/2/2010/ST/MUSM/02/1.

References

1. A. P. French, *Special Relativity* (Thomas Nelson & Sons, 1968), p. 167.
2. W. D. McComb, *Dynamics and Relativity* (Oxford University Press, 1999), preface.
3. J. B. Hartle, *Gravity: An Introduction to Einstein's General Relativity* (Addison-Wesley, 2003), p. 88.
4. B. L. Lan, Chaos **16**, 033107 (2006).
5. B. L. Lan, in *Topics on Chaotic Systems*, edited by C. H. Skiadas, I. Dimotikalis, and C. Skiadas (World Scientific, 2009), pp. 199-203.
6. B. L. Lan and H. Y. Cheng, Commun. Nonlinear Sci. Numer. Simulat. **15**, 2497 (2009).
7. B. L. Lan and F. Borondo, Phys. Rev. E **83**, 036201 (2011).
8. B. L. Lan, Chaos, Solitons and Fractals **42**, 534 (2009).
9. B. V. Chirikov, *Phys. Rep*. **52**, 263 (1979).
10. G. Casati, B. V. Chirikov, F. M. Izrailev, and J. Ford, in *Stochastic Behavior in Classical and Quantum Hamiltonian Systems*, edited by G. Casati and J. Ford (Springer, 1979), pp. 334–351.
11. A. A. Chernikov, T. Tél, G. Vattay, and G. M. Zaslavsky, *Phys. Rev. A* **40**, 4072 (1989).
12. Y. Nomura, Y. H. Ichikawa, and W. Horton, *Phys. Rev. A* **45**, 1103 (1992).

Chaotic Modeling and Simulation (CMSIM) 1: 193-198, 2013

The Effects of Diffusion of Individuals between Two Single-Species Populations

Dumitru D. Deleanu

Maritime University of Constanta, Romania
E-mail: dumitrudeleanu@yahoo.com

Abstract: In the paper we focused on a general model for the growth of a single-species population with non-overlapping generations. The data we have used correspond to Nicholson's blow-flies population and lie in the chaotic regime. The population was divided in two groups. If these groups evolve in distinct locations, their behavior is chaotic and, after a few generations, the initial small difference in number of individuals becomes big enough and behaves randomly. The question I want to answer in the paper is: What happens with the two populations if the individuals can migrate in both directions within the time intervals between their reproduction and death? The effect of coupling the two groups consisted in a rich dynamic behavior depending on the coupling strength. It was found that there is a consistent region where the coupling brings out the full synchronization of the two chaotic systems, two transition regions where an intermittent behavior was observed and two peripheral regions where control of chaos is shown to coexist with quasi-periodic and chaotic regimes.
Keywords: Single-species populations, Synchronization, Intermittent chaos, Control of chaos.

1. Introduction

According to May [1], models for population growth in a limited environment are based on two fundamental premises: a) the populations have the potential to increase exponentially; b) there is a density-dependent feedback that progressively reduces the actual rate of increase. By using a variety of data from field and laboratory populations, some researchers have proposed continuous or discrete models of population growth. The most known of these models is the logistic equation (Verhulst, 1838). Other simple models were introduced by May (1974), Li & Yorke (1975), May & Oster (1976), and Hassel et al (1976). Their models, which refer to single-species population with discrete, non-overlapping generation, predict that most of the populations show monotonic damping back to an equilibrium following a disturbance, with some exceptions of oscillatory damping or some sort of low-order limit cycles. They concluded that high-order limit cycles and chaos appear to be relatively rare phenomena in naturally occurring single-species populations. Guckenheimer et al (1987) have found that more realistic models of population growth, such as these that include overlapping generations, are more likely to exhibit complex behaviors. If data from laboratory population are used, even for these simple models, it was found that some populations will not exhibit stable equilibrium points but stable cycles or chaotic behavior [2]. That is because the laboratory situation (homogeneous environment, constant food supply, no competitors, no predators) make possible an exaggerated non-linear behavior. In this paper we focused on a general model

Received: 28 March 2012 / Accepted: 5 August 2012

ISSN 2241-0503

for growth of a single-species population with non-overlapping generations, namely

$$N_{t+1} = f(N_t) = \lambda N_t (1 + a N_t)^{-b} \quad (1)$$

where N_t and N_{t+1} are the populations in successive generations, λ is the finite rate of increase and *a*, *b* are constant defining the density-dependent feedback term. The values for parameters correspond to Nicholson's blowflies and lie in the chaotic regime [3].

The population of blowflies was divided in two groups. If these groups evolve in distinct locations their behavior is chaotic and, after a few generations, the initial small difference in number of individuals becomes big enough and behaves randomly. The question I want to answer in the paper is: *What happens with the two populations if the individuals can migrate in both directions within the time intervals between their reproduction and death?*

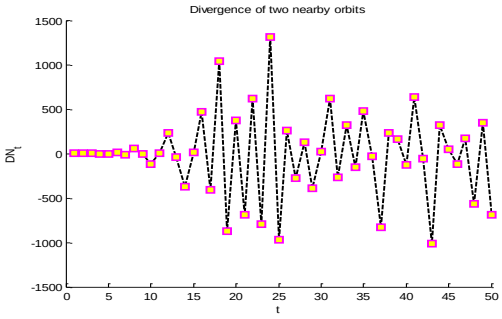

Fig. 1. Divergence of the two isolated populations versus time

2. The Model of Two-coupled Single-species Populations

To answer the above question let us hereafter turn our attention towards the following system of two-coupled single-species populations:

$$N_{t+1} = f(N_t) + c\left[f(M_t) - f(N_t)\right],\ M_{t+1} = f(M_t) + c\left[f(N_t) - f(M_t)\right] \quad (2)$$

where the coupling parameter *c* can be thought as the fraction of the two populations which migrate to the neighboring location. Throughout the paper I used the fixed parameter values $\lambda = 60, a = 0.003$ and $b = 6$. The total population $\overline{N}_t = 3950$ was divided in two unequal groups, $N_t = 1950$ and $M_t = 2000$. If no change between the groups was permitted, the initial small difference in number of individuals, $\Delta N_t = 50$, increased quickly and behaved chaotically (see Figure 1). The effect of coupling consisted in a rich dynamic behavior having the main features as follows.

2.1. Complete synchronization

If two or more chaotic systems are couple, it is possible that the attractive effect of a suitable coupling to counterbalance the trend of the trajectories to separate due to chaotic dynamics. Synchronization of chaotic systems can be explained by the suppression of expanding dynamics in the state space transversal to the synchronization manifold (here $M_t = N_t$). It is natural then to ask for which

values of coupling strength c the two systems will oscillate in a coherent and synchronized way.
Laureano et al [4] have demonstrated that, for this kind of coupling, the range of synchronization (in the linear approximation) is given by

$$0.5\left(1-\exp(-\lambda_u)\right) < c < 0.5\left(1\_\exp(-\lambda_u)\right) \quad (3)$$

where λ_u is the Lyapunov exponent for the uncoupled map *f*. For our data it was found that $\lambda_u \cong 0.35$, so $c \in (0.15\,;0.85) = S$ .As an example, let consider $c = 0.16$. The synchronization takes place after 200 generations (see figure 2).

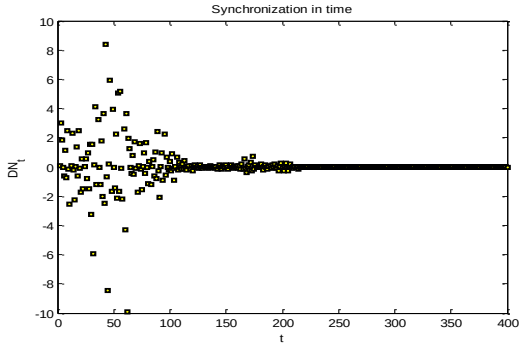

Fig. 2. Evolution to synchronous state for $c = 0.16$

Each of the systems shows chaos and their states are identical at each moment in time (full synchronization). To verify that the synchronous state is chaotic, a Lyapunov exponent versus coupling strength diagram was considered (see Figure 3.

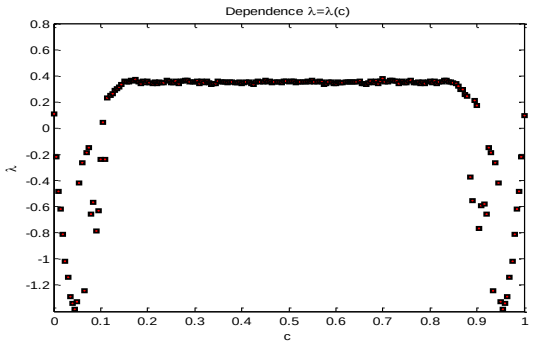

Fig. 3. Lyapunov exponent versus coupling strength

If *c* is chosen deep inside the interval S, the synchronous state is reached after only few steps (see Figure 4). Otherwise, if *c* is chosen near the borders of S the synchronization is hard to obtain, a lot of steps being necessary (e.g. 2000 steps for $c = 0.15$.

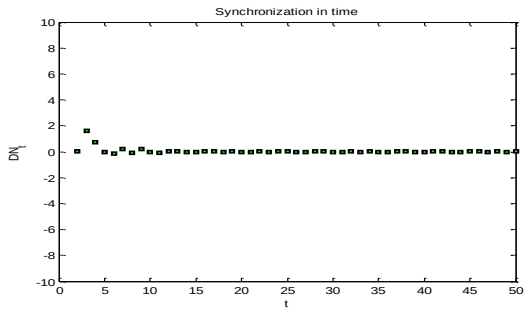

Fig. 4. Evolution to synchronous state for $c = 0.25$

2.2. Intermittent chaos

If the coupling strength c falls short of the critical value $c_{crit} = 0.15$ the synchronized state $M_t = N_t$ becomes unstable and an intermittent dynamics is observed. Figure 5 shows the time evolution of the transverse coordinate $DN_t = N_t - M_t$ for $c = 0.1467$. The time periods of synchronicity are interrupted by aperiodic chaotic bursts.

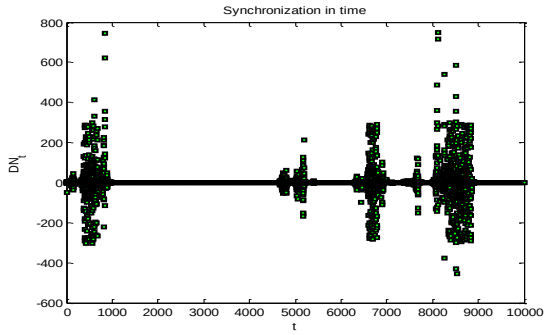

Fig. 5. Time periods of synchronicity interrupted by aperiodic chaotic bursts $(c = 0.1467)$

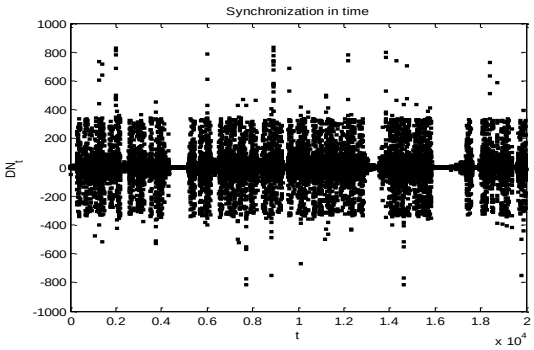

Fig. 6. A completely erratic state for $c = 0.14$

The basic intermittency mechanism comes from the competition between the trajectory instability of chaotic elements and the synchronization tendency due to the diffusion-type coupling [8]. For $c = 0.14$ the chaotic bursts were already merged so the synchronization started to dissolve into a completely erratic state (see Figure 6).

2.3. Stabilization to an ordered state

Outside the interval of synchronization the dynamics is quite complicated. For very small values of *c* (weak coupling) the system behaves chaotically, the N_t values being distributed over an entire interval. By increasing c the chaotic distribution of N_t comes undone in strips, thinner and thinner (see Figure 7).

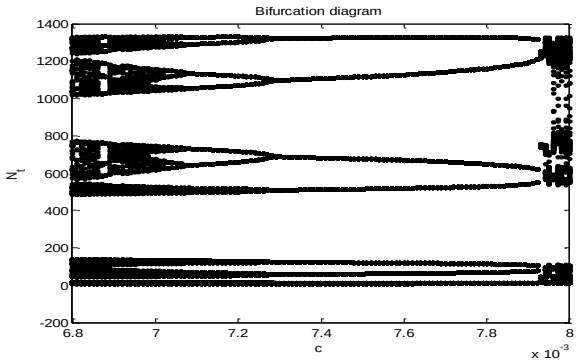

Fig. 7. A part of the bifurcation diagram $N_t = N_t(c)$

At $c \cong 0.007$ the system entered a periodic regime, and was subjected to a sequence of changes from a 2^n - period cycle to a 2^{n-1} - period cycle. A 8-period cycle was obtained for $c \in (0.0072; 0.0080)$ (see Figure 8).

Then, a quasi-periodic regime with two strips appeared (Figure 9) which, in its turn, was changed by a 2-period cycle for $c \in (0.013; 0.11)$. This periodic regime is interrupted by windows corresponding to a 4-period cycle or even to thin windows of chaotic regime.

Beginning with $c \cong 0.1$ the number of steps required for stabilization to the 2-period cycle became bigger and bigger so, finally, the chaotic regime was reached. An analogous discussion can be done for $c \in (0.85; 1)$.

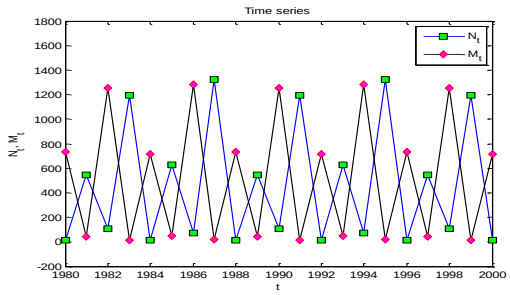

Fig. 8. Time evolution of N_t, M_t for $c = 0.0079$ (8-period cycle)

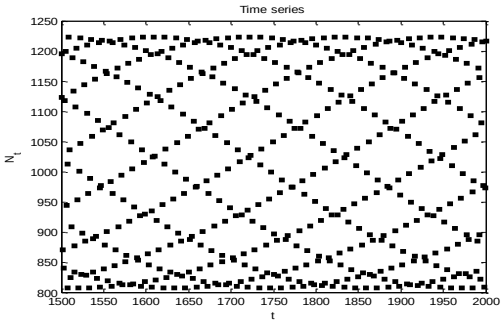

Fig. 9. Time evolution of N_t for $c = 0.99$ (quasi-period regime)

3. Conclusions

The dynamics for many biological populations, which breed seasonally and have non-overlapping generations, are described by a density-dependent relation of the form $N_{t+1} = f(N_t) = \lambda N_t (1 + a N_t)^{-b}$. If data from laboratory tests are used it was found that populations can exhibit even a chaotic behavior. Two almost identical populations, living in distinct locations, evolved so that the initial small difference in number of individuals became big enough and behaved randomly. If the individuals representing the two populations could migrate in both directions within the time intervals between their reproduction and death then a rich dynamic behavior depending on the coupling strength was observed. It was found that there is a consistent region where the coupling brings out the full synchronization of the two chaotic systems, two transition regions where an intermittent behavior was observed and two peripheral regions where control of chaos is shown to coexist with quasi-periodic and chaotic regimes.

References

1. M. Doebeli. Intermittent chaos in populations dynamics, *J. Theor. Biol.*, vol. 166, 325-330, 1994.
2. M. P. Hassell, J.H. Lawton and R.M.May. Patterns of Dynamical Behavior in single-species populations. *The Journal of Animal Ecology,* vol. 45, no. 2, 471–486, 1976.
3. M. P. Hassell. Density-dependence in single-species populations. *The Journal of Animal Ecology*, vol. 49, no.1, 283-295, 1975.
4. R. Laureano, D.A. Menales and M.A.M. Ferreira. Efficient synchronization of one-dimensional chaotic quadratic maps by different coupling terms. *Journal of Mathematics and Technology, 5*–12, 2010.
5. R. M. May. Bifurcation and dynamic complexity in simple ecological models. *The American naturalist,* vol. 110, no. 974, 573–599, 1976.
6. L. D. Mueller and H. J. Ayala. Dynamics of single-species population growth: stability or chaos? *Ecology*, vol. 62, no.5, 1148–1154, 1981.
7. L. M. Pecora and T.L. Carrol. Synchronization in chaotic systems. *Phs. Rev. Lett*., vol. 64, no. 8, 821-828, 1990.
8. H.G. Schuster and W. Just. Deterministic chaos: An introduction. *Wiley-VCH Verlag*. 2005.

Chaotic Modeling and Simulation (CMSIM) 1: 199-208, 2013

A Steganography Telecom System using a Chua Circuit Chaotic Noise Generator for data cryptography

Apostolos P. Leros (1,2) and Antonios S. Andreatos (2)

(1) Department of Automation, School of Technological Applications
Technological Educational Institute of Chalkis, 34400 Psachna, Evia, Greece
E-mail: lerosapostolos@gmail.com

(2) Div. of Computer Engineering & Information Science
Hellenic Air Force Academy, Dekeleia Air Force Base
Dekeleia, Attica, TGA-1010, Greece
E-mail: informatics.hafa@haf.gr, aandreatos@gmail.com

Abstract: This paper models an image steganography telecom system based on a Chua circuit chaotic noise generator. An unpredictable chaotic system based on a Master – Slave Chua circuit has been used as a random number generator. The whole system is modeled and simulated in Simulink. A continuous linear controller has been used to synchronize the two Chua circuits, with the same parameters at both the transmitter and the receiver. On the receiver side, usage of the same parameters with the Master circuit produce a similar chaotic signal via the Slave Chua circuit, synchronized to the Master by an analog controller, in order to produce the same noise (random sequence) as that of the Master circuit. After removing the noise from the received ciphertext, the original message is revealed. The proposed system presents advanced security features.
Keywords: Chua circuit, chaotic noise generator, image steganography, Master Chua circuit, Slave Chua circuit, LSB steganography, simulation, continuous linear controller.

1. Introduction

1.1 Random Number Generators

Traditionally, cryptography has been based on the generation of random numbers produced by hardware (true) random or pseudo-Random Number Generators (RNGs). Most pseudo-RNGs (PRNGs) are not suitable for cryptography for several reasons. First, while most pseudo-RNGs outputs appear random to assorted statistical tests, they do not resist determined reverse engineering. Specialized statistical tests that show the random numbers not to be truly random exist. Second, when the state of most PRNGs has been revealed, all past random numbers can be retrodicted, allowing an attacker to read not only future messages, but also, all past ones. This is not possible with a chaotic number generator; thus, Chua circuits resist this type of cryptanalysis. Furthermore, in our approach, even if the configuration circuit is revealed, it is still difficult to reproduce the crypto- signal since this also depends on the initial

Received: 11 March 2012 / Accepted: 8 October 2012

ISSN 2241-0503

conditions and the tolerance of the components. The role of the continuous linear controller is to compensate for the component tolerance.

1.2 Steganography

Steganography is a technique for concealing data within pure or often encrypted or even random/ chaotic data. The data to be concealed is first encrypted and then used to overwrite part of a much larger block of encrypted data or random data or different kinds of (usually redundant) data such as images [10, 15, 16].

2. System Overview

In the proposed steganography telecom application, the message to be transmitted is first encrypted using chaotic noise produced by a standard Chua circuit [2, 4]; then, the encrypted sequence is concealed in an image using the LSB's method (Figure 1).

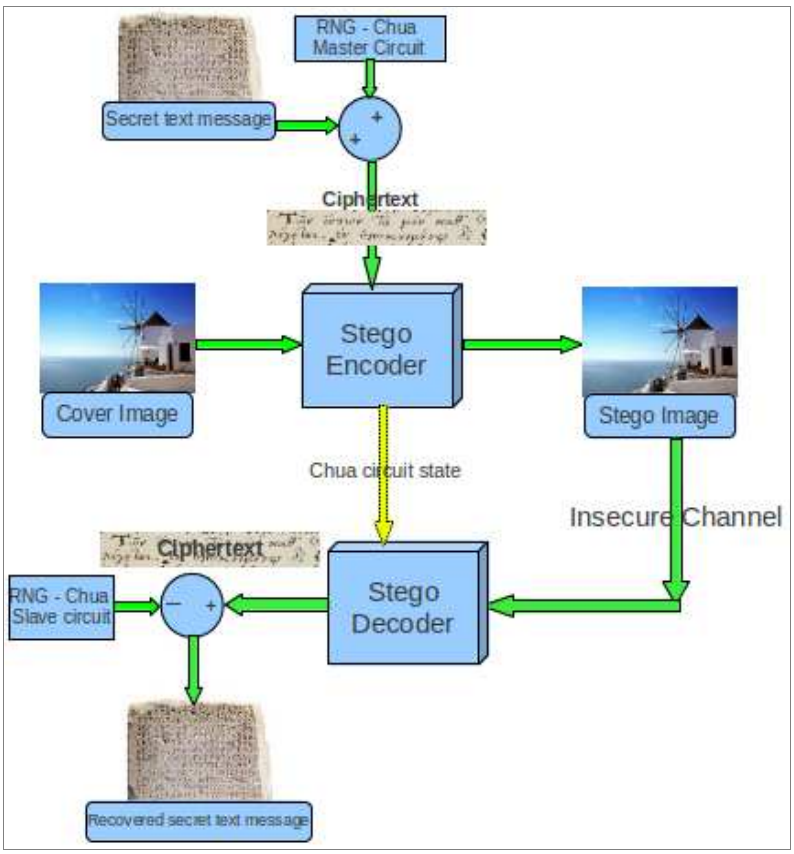

Fig. 1. Proposed steganography telecom application

The input message is in ASCII format; in order to be mixed with the chaotic

noise, it is successively converted from ASCII characters to a binary string. For the sake of simplicity, conversions are not shown in Fig. 1. In the receiver the reverse process takes place, in order to remove the secret text from the image.

3. The Chaotic True Random Number Generator

The Chaotic True Random Number Generator (CTRNG) used by our circuit is based on the Standard Chua's circuit; the latter was invented back in 1983 by Prof. Leon O. Chua in Japan, in his effort to demonstrate chaos in an actual physical model and to prove that the Lorenz double-scroll attractor is chaotic [2, 4]. The electronic circuit suits the study of chaos well because one can precisely control its parameters and observe the results on an oscilloscope. The circuit became popular because it is easy to construct, and many people have built the circuit using off-the-shelf electronic components. In fact, one can model the circuit using only resistors, capacitors, inductors, diodes and op-amps [6].

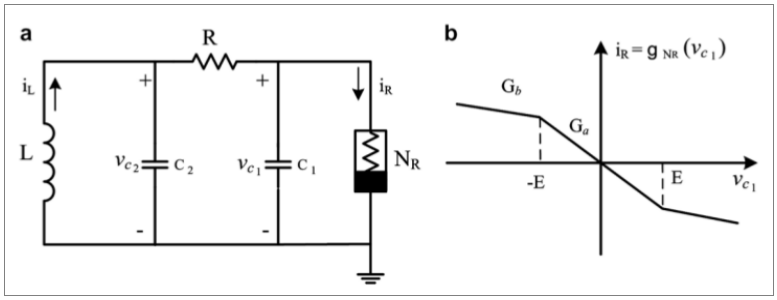

Fig. 2. (a) Standard Chua's circuit; (b) v–i characteristic of the nonlinear device
Source: [4].

In Figure 2 V_{C1} and V_{C2} denote the voltages across the capacitors C_1 and C_2, respectively, i_L is the current through the inductor L, and $gN_R(V_{C1})$ is the nonlinear function which defines the v–i characteristic of the nonlinear device, represented by the piecewise-linear function of Fig. 2b [3]. By solving the above circuit we get the following differential equations (1- 3):

$$C_1 \frac{dV_{C1}}{dt} = \frac{1}{R}(V_{C2} - V_{C1}) - g_{NR}(V_{C1}) \quad (1)$$

$$C_2 \frac{dV_{C2}}{dt} = \frac{1}{R}(V_{C1} - V_{C2}) + i_L \quad (2)$$

$$L \frac{di_L}{dt} = -V_{C2} - R_0 i_L \quad (3)$$

where:

$$g_{NR}(V_{C1}) = G_b V_{C1} + \frac{1}{2}(G_a - G_b)(|V_{C1} + E| - |V_{C1} - E|) \quad (4)$$

4. Simulink implementation

The whole telecom system was successfully implemented in Simulink [8]. In the following an overview of the system will be given; in addition, we shall present the implementation of some critical blocks.

4.1 Simulink implementation of the whole telecom system

The Simulink implementation of the cryptosystem was not as easy; several extra problems had to be solved starting from the input of the carrier image into Simulink; however, all problems were solved and finally the simulation works. The system overview is shown in Figure 3. Next the most important blocks will be briefly presented.

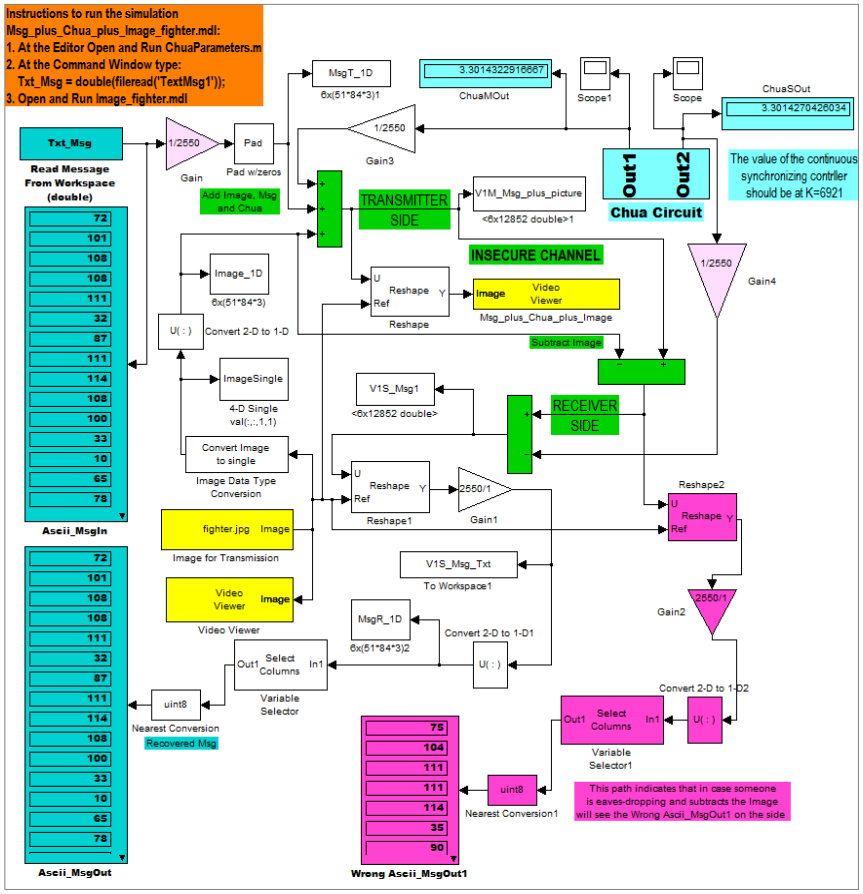

Fig. 3. Stego System overview in Simulink

The message to be encrypted appears on the left side (blue box with the indication Txt_Msg). The cover image for Transmission appears on the left side

in the middle (yellow box named "Image for Transmission"). The Transmitter occupies the top side of the diagram.
The summation element (in green) combines the image, the text message and the Chua chaotic noise, all properly formatted for compatibility. The image with the text message and the Chua chaotic value appears in the yellow box named **Msg_plus_Chua_plus_Image** below the Transmitter Side and it is also inserted into the channel.
The Chua circuits are on the top blue box with the indications Out1 and Out2 for the Master and Slave output values respectively. The value of the continuous linear controller which synchronized the two Chua circuits is **K=6921** as shown in the blue textbox (top right).
The receiver side occupies the bottom side of the diagram. In case an eavesdropper subtracts the image from the received information, he will see an invalid message (bottom right, in magenta).
Finally, at the bottom left side in the blue display with the indication **Ascii_MsgOut** the successfully recovered ASCII message appears.

4.2 Simulink implementation of Chua's circuits Figure 4 presents the Simulink implementation of Chua's circuit, based on the differential equations presented above. The Subsystem (bottom right) represents the nonlinear device.

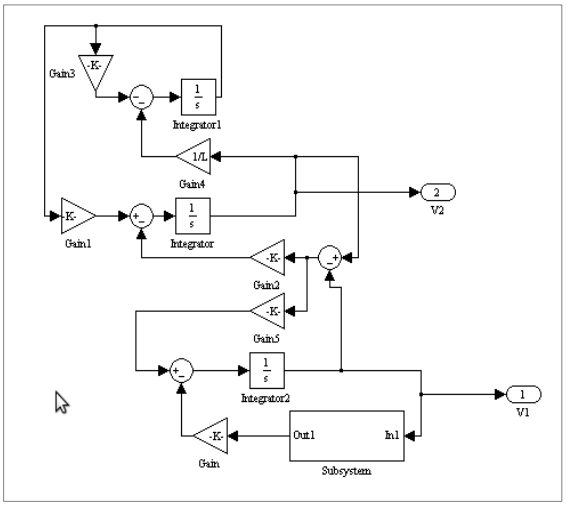

Fig. 4. Simulink implementation of Chua's circuit

4.3 Simulink implementation of the nonlinear device
Figure 5 presents the implementation of the nonlinear device with the v-i characteristic shown in Fig. 2b.

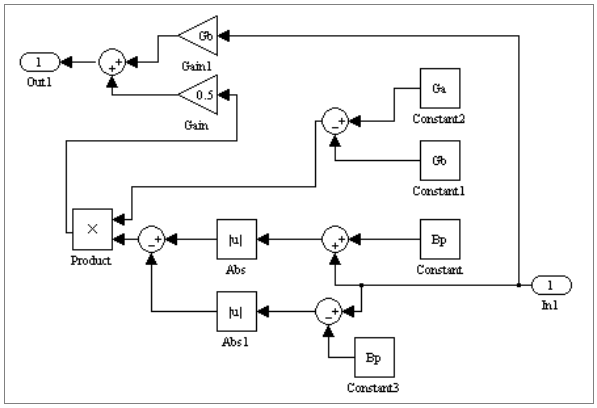

Fig. 5. Simulink implementation of the nonlinear device

5. Synchronization of the Master and Slave Chua circuits

5.1 The need for Master-Slave synchronization

Chaotic systems present an apparently infinite number of states. This characteristic, together with the dependence on the initial conditions as well as the tolerance of the Chua circuit components, make CTRNGs totally unpredictable and non-reproducible, hence ideal for cryptography. However, the receiver must be able to reproduce exactly the same chaotic noise in order to subtract it from the received signal (Figure 1). This becomes possible with synchronization between the two Chua circuits: through the use of specific controllers, we can guide the trajectory of chaotic systems to specific areas producing specific behavior. For this reason, the initial state of the Master Chua circuit [X0, Y0, Z0] has to be transmitted to the Slave Chua circuit via a secure channel (Fig. 6). In our implementation the initial conditions for the Master and Slave Chua circuits are: (Vc1=0, Vc2=1, I_L=0) and (Vc1=0, Vc2=1.1, I_L=0) respectively.

During the last two decades, the chaotic synchronization problem has received a tremendous interest [4]. This property is supposed to have interesting applications in different fields, especially in private and secure communication systems based on cryptography. The broadband and noise-like features of chaotic signals are seen as possibly highly secure media for communication. The cryptographic communication schemes usually consist of a chaotic system as transmitter along with an identical chaotic system as receiver; where the confidential information is embedded into the transmitted chaotic signal by direct modulation, masking, or another technique. At the receiver end, if chaotic synchronization can be achieved, then it is possible to extract the hidden information from the transmitted signal.

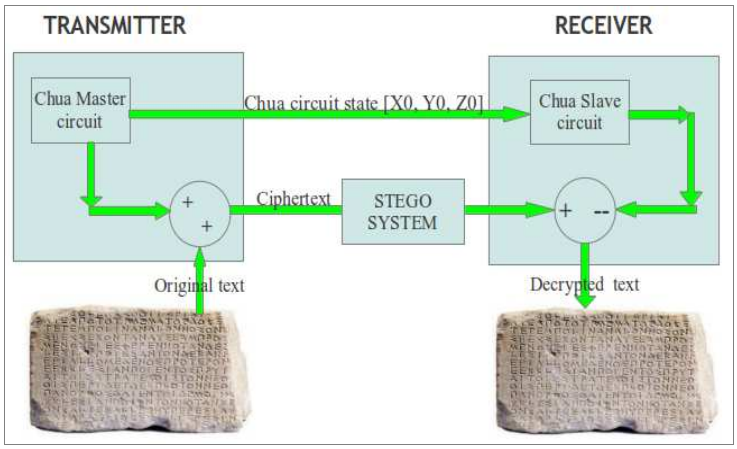

Fig. 6. Synchronization between Master and Slave Chua circuits

5.2 Master-Slave Synchronization circuit

For the synchronization between Master and Slave Chua circuits, Pyragas' continuous control method has been used [1, 3, 5, 7, 9, 11-14]. This method was chosen because it was relatively easy to implement. The synchronization circuit (simplified) is shown in Fig. 7.

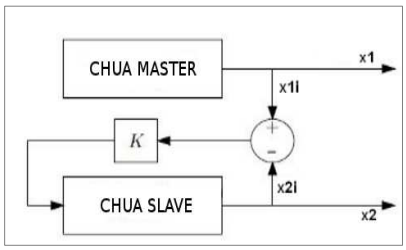

Fig. 7. Master-Slave Synchronization circuit

The Master and Slave Chua's circuits along with the Synchronization device are placed on the top-right side of Figure 4, in a block named Chua circuit. The interior of this block is shown in Figure 8 [6].

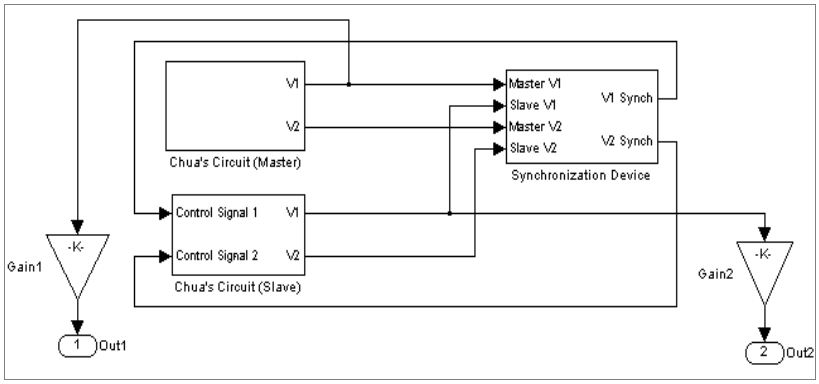

Fig. 8. Chua's circuits along with the synchronization device

6. Simulation results

Initial results show that the system works successfully. Using a small text message and the picture shown in Figure 9 as Cover image, the system produced the stego image of Figure 10.

Fig. 9. Cover image

Figure 10 contains the ciphertext, which is also shown (in ASCII) at the top left column of Figure 3. In this same Figure below we can see the decrypted message at the receiver. An eavesdropper with sufficient information about the image, even connected at a sensitive point of the receiver, won't be able to decode the message correctly, as shown at the bottom of Figure 3.

Fig. 10. Stego image

7. Security features of the proposed stegosystem

The security features of the proposed application are based on:

- ✓ the unknown Chua's circuit topology;
- ✓ the varying tolerance of components (which changes circuit behavior);
- ✓ the unknown initial conditions;
- ✓ the unknown type of the controller / compensator.

8. Conclusion

In this work we have proposed a Steganography Telecom System Based on a Chua Circuit Chaotic Noise Generator with advanced security features. In this system the text message is encrypted using a CTRNG and then the ciphertext is concealed in a cover image using the LSB insertion method. The system has been successfully simulated in Simulink and works with both grayscale and color images.

References

1. S. Boccaletti, C. Grebogi, Y.-C. Lai, H. Mancini, D. Maza, The Control of Chaos Theory and Applications. *Physics Reports*, Elsevier, 2000.
2. Leon O. Chua, Chua's circuit: ten years later. *IEICE Trans. Fundamentals*, vol. E77-A, no. 11, 1811-1822, Nov. 1994.
3. Alexander L. Fradkov and Robin J. Evans, Control of chaos: Methods and applications in engineering, *Annual Reviews in Control*, Elsevier B. V., 2005.
4. L. Gámez-Guzmán, C. Cruz-Hernández, R.M. López-Gutiérrez, E.E. García-Guerrero, Synchronization of Chua's circuits with multi-scroll attractors: Application to

communication, *Commun. Nonlinear Sci. Numer. Simulat.* 14, 2765–2775, 2009.

5. J. Gonzalez, Synchronization and Control of Chaos, *An Introduction for Scientists and Engineers*. Covent Garden, London: Imperial College Press, 2004.
6. Nicholaos N. Grigoropoulos, *Chaotic Systems, Analysis and applications of Chua's circuit*. Diploma Thesis. Supervisor: Prof. A. P. Leros, Technological Institute of Chalkis, School of Technological Applications, 34400 Psachna, Evia, Greece, 2009.
7. T. Kapitaniak, *Controlling Chaos Theoretical and Practical Methods in non-linear Dynamics*. Elsevier Ltd., 1996.
8. Steven T. Karris, *Introduction to Simulink with Engineering Applications*. Orchard Publications, 2006.
9. F. L. Lewis, *Chaos in Automated Control*. Boca Raton, FL: Taylor & Francis Group, 2006.
10. T. Morkel, J.H.P. Eloff and M.S. Olivier, An Overview of Image Steganography, in *Proceedings of the Fifth Annual Information Security South Africa Conference* (ISSA2005), Sandton, South Africa, June/July 2005.
11. Louis M. Pecora, Thomas L. Carroll, Gregg A. Johnson, and Douglas J. Mar, Fundamentals of synchronization in chaotic systems, concepts, and applications. *American Institute of Physics*, 1997.
12. A. Pikovsky, Synchronization, *A universal concept in nonlinear sciences*. New York: Cambridge University Press, 2001.
13. K. Pyragas, Continuous Control of Chaos by Self Controling Feedback. *Physics Letters A*, 1992.
14. E. Schöll, *Handbook of Chaos Control*, 2nd Ed. Weinheim: Verlag GmbH & Co., 2008.
15. Mohit Kr. Srivastava, Sharad Kr. Gupta, Sushil Kushwaha and Brishket S. Tripathi, *Steganalysis of LSB Insertion Method in Uncommpressed Images Using Matlab*. Available online from: http://www.tutorialspoint.com/white-papers/124.pdf
16. Dr Ekta Walia and Payal Jain, An Analysis of LSB & DCT based Steganography, *Global Journal of Computer Science and Technology*, Vol. 10 Issue 1, 4-8, 2010.

Chaotic Modeling and Simulation (CMSIM) 1: 209-214, 2013

Chaos in Compound Anti-Symmetric-Case Piecewise-Linear Delay Differential Equations

Phocharavidh Phuphatana and Banlue Srisuchinwong

Sirindhorn International Institute of Technology, Thammasat University, Pathum-Thani, Thailand 12000
E-mail: phocharavidh.pp@gmail.com, banlue@siit.tu.ac.th

Abstract: An existing anti-symmetric-case piecewise-linear delay differential equation (DDE) has exhibited chaos at a delay time $\tau = 3$ using an odd term $f_a = f_1$ for $a = 1$. Three new compound anti-symmetric-case piecewise-linear DDEs are presented. Each DDE exhibits chaos using $\tau < 3$. The first compound DDE is a combination of two odd terms f_1 and f_3 where $a = 1$ and 3, and $1.70 < \tau < 2.10$. The second compound DDE is a combination of two even terms f_2 and f_4 where $a = 2$ and 4, and $1.50 < \tau < 1.90$. Finally, the third compound DDE is a combination of two odd terms f_1 and f_3, and an even term f_2 where $a = 1$, 2, and 3, and $1.05 < \tau < 1.27$. Not only can the higher value of 'a' reduce the value of τ for chaos, but the more combination of terms f_a also can. The reduction in τ enables simple implementation of a LC network in the delay unit.
Keywords: chaos, delay differential equation; reduced-delay

1. Introduction

Since the discovery of the eminent Lorenz chaotic attractor in 1963 [1], studies of chaotic behavior in nonlinear systems have attracted great attention due to a variety of applications in science and technology, e.g. chaos-based secure communications [2], [3], [4]. Time-delay systems can exhibit chaos with a relatively simple model involving a value of the dynamical variable at one or more times in the past [5]. They have an infinite-dimensional state space with a large value of positive Lyapunov exponents and are good candidates for highly secure communications. In general, a first-order time-delay system is described by a delay differential equation (DDE) of the form.

$$\dot{x}(t) = f[x(t), x_\tau] \tag{1}$$

where the overdot denotes a time (t) derivative, $x_\tau = x(t-\tau)$ is the value of x at an earlier time ($t-\tau$), and τ is a delay time, i.e. $\tau \le t$.

One of the earliest and most widely studied DDE is the Mackey-Glass equation [6], as shown in (2), proposed to model the production of white blood cells. The equation exhibits chaos with parameters such as $a = 0.2$, $b = 0.1$, $c = 10$, and $\tau = 23$. Other examples of DDEs exhibiting chaos include Ikeda DDE [7] and sinusoidal DDE [5].

Received: 6 April 2012 / Accepted: 5 October 2012

ISSN 2241-0503

$$\dot{x} = \frac{ax_\tau}{1+x_\tau^c} + bx, \tag{2}$$

Recently, chaos in an anti-symmetric-case piecewise-linear DDE has been reported [5], as shown in (3).

$$\dot{x} = |x_\tau + 1| - |x_\tau - 1| - x_\tau \tag{3}$$

for $\tau = 3$. The largest Lyapunov exponent $\lambda = 0.0909$. Such a system is especially amenable to implementation with electronic circuits [8]. A delay unit may be implemented using an LC network [9]. As the size of the LC network is proportional to the value of the delay time τ, a reduction of τ in (3) is preferable.

In this paper, three new compound anti-symmetric-case piecewise-linear DDEs are presented. Each DDE exhibits chaos using delay time $\tau < 3$. Such a reduction of the delay time in the DDEs enables simple implementation of the LC network in the delay unit.

2. Compound Anti-Symmetric-Case Piecewise-Linear DDEs

For simplicity, the right hand side of (3) can be modified as a general function f_a as shown in (4)

$$f_a = |x_\tau + a| - |x_\tau - a| - x_\tau \tag{4}$$

where the parameter '*a*' is an integer. Equation (3) is therefore represented by an odd term f_1 as $a = 1$. Three new compound anti-symmetric-case piecewise-linear DDEs are proposed. The first compound DDE is a combination of two odd terms f_1 and f_3 where $a = 1$ and 3, as shown in (5). The second compound DDE is a combination of two even terms f_2 and f_4 where $a = 2$ and 4, as shown in (6). Finally, the third compound DDE is a combination of two odd terms f_1 and f_3, and an even term f_2 where $a = 1$, 2, and 3, as shown in (7).

$$\begin{aligned}\dot{x}_1 &= f_1 + f_3 \\ &= |x_\tau + 1| - |x_\tau - 1| + |x_\tau + 3| - |x_\tau - 3| - 2x_\tau\end{aligned} \tag{5}$$

$$\begin{aligned}\dot{x}_2 &= f_2 + f_4 \\ &= |x_\tau + 2| - |x_\tau - 2| + |x_\tau + 4| - |x_\tau - 4| - 2x_\tau\end{aligned} \tag{6}$$

$$\begin{aligned}\dot{x}_3 &= f_1 + f_2 + f_3 \\ &= |x_\tau + 1| - |x_\tau - 1| + |x_\tau + 2| - |x_\tau - 2| + |x_\tau + 3| - |x_\tau - 3| - 3x_\tau\end{aligned} \tag{7}$$

3. Numerical Results

For the first compound DDE shown in (5), Figures 1, 2 and 3 visualize numerical results of a chaotic waveform, a chaotic attractor, and a bifurcation diagram, respectively, using τ = 2.07. The largest Lyapunov exponent is λ = 0.3112.

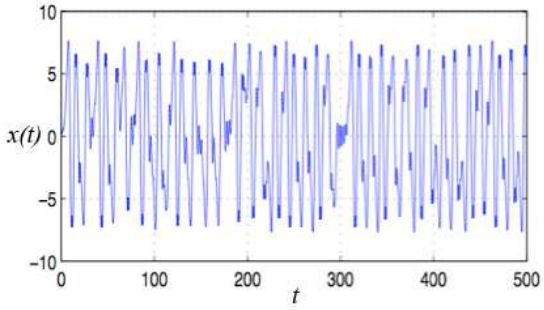

Fig. 1. A chaotic waveform of (5) with τ = 2.07.

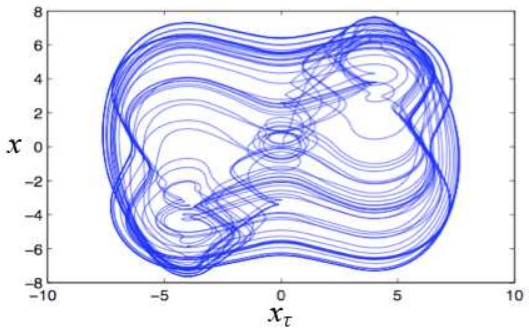

Fig. 2. A chaotic attractor of (5) with τ = 2.07.

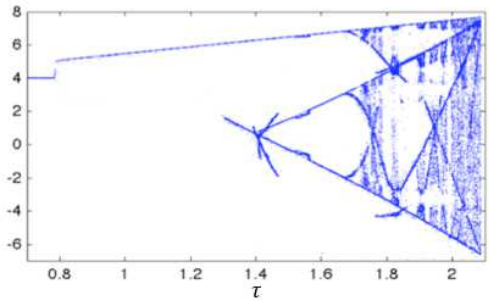

Fig. 3. A bifurcation diagram of (5).

For the second compound DDE shown in (6), Figures 4 and 5 illustrate numerical results of a chaotic attractor and a bifurcation diagram, respectively. (6), using $\tau = 1.75$. The largest Lyapunov exponent is $\lambda = 0.1174$.

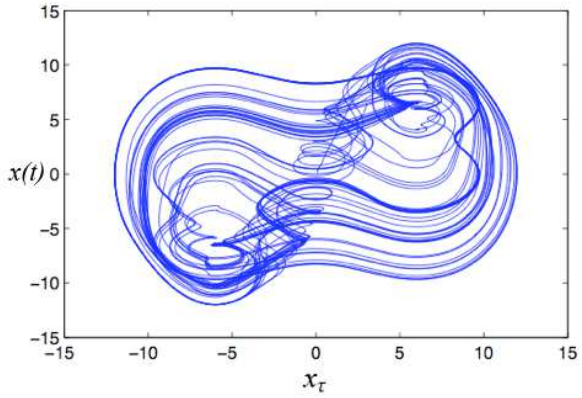

Fig. 4. A chaotic attractor of (6) with τ = 1.75.

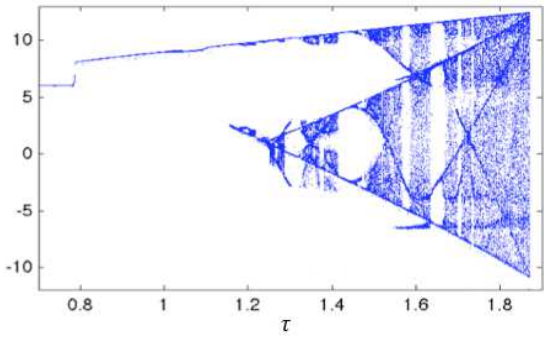

Fig. 5. A bifurcation diagram of (6).

For the third compound DDE shown in (7), Figures 6 and 7 depict numerical results of a chaotic attractor and a bifurcation diagram, respectively, using $\tau = 1.20$. The largest Lyapunov exponent is $\lambda = 0.2823$.

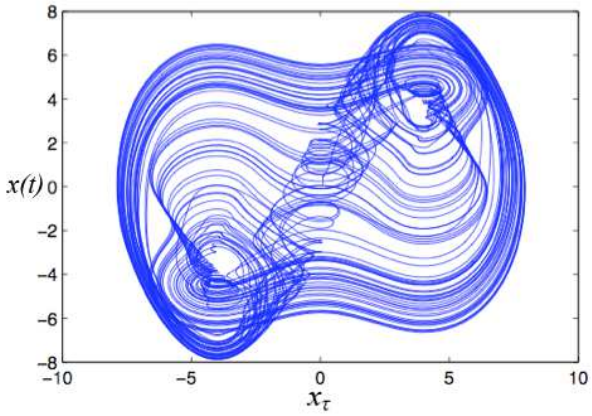

Fig. 6. A chaotic attractor of (7) with $\tau = 1.20$.

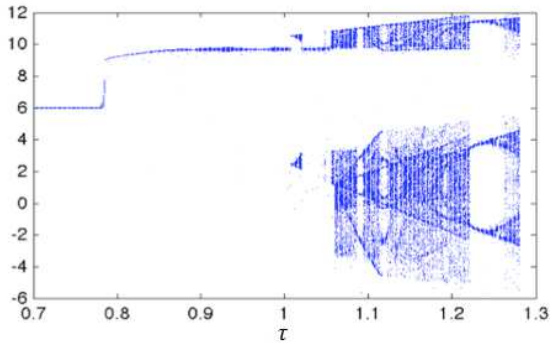

Fig. 7. A bifurcation diagram of (7).

Table 1 summarizes ranges of delay time τ of equations (5), (6), and (7), for which chaos occurs. There are various periodic windows immersed in chaos. It can be notice from Table 1 that not only can the higher value of the parameter 'a' of f_a reduce the value of the time delay τ for chaos, but the more combination of terms f_a also can.

Table 1: Summaries of Ranges of τ For Chaos

Equations	Ranges of τ
$\dot{x}_1 = f_1 + f_3$	$1.70 < \tau < 2.10$
$\dot{x}_2 = f_2 + f_4$	$1.50 < \tau < 1.90$
$\dot{x}_3 = f_1 + f_2 + f_3$	$1.05 < \tau < 1.27$

3. Conclusions

Three new compound anti-symmetric-case piecewise-linear DDEs have been presented. The first combines two odd terms f_1 and f_3 and chaos occurs for $1.70 \angle \tau \angle 2.10$. The second combines two even terms f_2 and f_4 and chaos occurs for $1.50 \angle \tau \angle 1.90$. Finally, the third combines three terms f_1, f_2 and f_3 and chaos occurs for $1.05 \angle \tau \angle 1.27$. Chaos occurs using less delay time τ than that of the existing approach. The reduction in delay time enables the reduction in size of the LC network of the delay unit.

Acknowledgments: This work was supported by telecommunications research and industrial development institute (TRIDI), NBTC, Thailand (grant TARG 2553/002), and the national research university project of Thailand, office of higher education commission.

References

1. E. N. Lorenz. Deterministic nonperiodic flow, *J. Atmos. Sci.*, vol. 20, 130-141, 1963.
2. K. M. Cuomo, A. V. Oppenheim and S. H. Strogatz. Synchronization of Lorenz-based chaotic circuits with applications to communications, *IEEE Trans. Cir. Sys.*, vol. 40, no. 10, 626-633, 1993.
3. L. Kocarev, K. S. Halle, K. Eckert and L. O. Chua. Experimental demonstration of secure communications via chaotic synchronization, *Int. J. Bifurcat Chaos*, vol. 2, no. 3, 709-713, 1992.
4. B. Srisuchinwong, B. Munmuangsaen. A highly chaotic attractor for a dual-channel single-attractor, private communication system. In: Christos H. Skiadas, Ioannis Dimotikalis, and Charilaos Skiadas *Chaos Theory: Modeling, Simulation and Applications*. World Scientific, pp 399–405, 2011.
5. J. C. Sprott. Time-Delay Systems. In: J. C. Sprott *Elegant Chaos*. World Scientific, pp 221–232, 2010.
6. M. Mackey and L. Glass. Oscillation and chaos in physiological control systems, *Science 197*, 287-289, 1977.
7. K. Ikeda. Multiple-valued stationary state and its instability of the transmitted light by a ring cavity system, *J. Opt. Commun. 30*, 257-261, 1979.
8. U. an der Heiden, and M. C. Mackey. The dynamics of production and destruction: Analytic insight into complex behavior, *J. Math. Biol. 16*, 75-101, 1982.
9. A. Namajūnas, K. Pyragas, and A. Tamaševičius. An electronic analog of the Mackey-Glass system, *Physics Letters A*, vol. 201, 42-46, 1995.

Chaotic Modeling and Simulation (CMSIM) 1: 215-221, 2013

Stability and Chaos in a Classical Yang – Mills - Higgs System

O. Ozgur Aybar[†•], Avadis S. Hacinliyan[†‡], Ilknur Kusbeyzi Aybar[*], Kamer Koseyan[‡], Berc Deruni[‡]

[†]Yeditepe University, Department of Information Systems and Technologies, Istanbul, Turkey
[‡]Yeditepe University, Department of Physics, Istanbul, Turkey
[*]Yeditepe University, Department of Computer Education and Instructional Technology, Istanbul, Turkey
[•]Gebze Institute of Technology, Department of Mathematics, Kocaeli, Turkey
E-mail: oaybar@yeditepe.edu.tr
E-mail: ahacinliyan@yeditepe.edu.tr
E-mail: ikusbeyzi@yeditepe.edu.tr
E-mail: kaderci.johannes@gmail.com
E-mail: berc_890@hotmail.com

Abstract: A motivation for looking at chaos in the classical realizations of the Yang-Mills or Yang Mills augmented by Higgs equations is the importance of this system in the initial (in)stability at big bang, since in the initial stages all interactions were of the same strength and were based on non abelian gauge theories, of which the SU(2) Yang Mills is a first example.
In this study we consider the following two particle effective Hamiltonian suggested by Biro, Matinyan and Müller:

$$H = \frac{p_x{}^2 + p_y{}^2}{2} + \frac{1}{2}x^2y^2 + \frac{1}{2}(a^2x^2 + b^2y^2) + \frac{1}{2}x^4 + \frac{1}{4}py^4$$

Keywords: Dynamical systems, Yang-Mills, Lyapunov exponents, Chaos.

1. Introduction

Global properties for mappings such as Poincare sections, Lyapunov exponents and other topological properties as introduced by Poincare and Birkhoff are important objects of study in nonlinear dynamical systems in addition to their local properties such as various bifurcations and invariant manifolds[1].
As Matinyan suggested, one of the ways to search for chaos is to investigate Poincare sections[4,5,6]. Since the system is described by a time independent Hamiltonian, the energy integral reduces the four dimensional system into a three dimensional system and a two dimensional Poincare map[1,2,3]. Unfortunately, the Hamiltonian involves the squares of the momentum. Taking the square root leads to missing information since the trajectory should cross into regions where the momentum can have either sign. There are two ways

Received: 30 May 2012 / Accepted: 25 September 2012

ISSN 2241-0503

known to solve this problem. One of the solutions to this problem is the symplectic numerical integration technique and the other one is to check the energy conservation numerically at every point. Results of these investigations lead to the same results obtained by KAM (Kolmogorov–Arnold–Moser) theory and hence this numerical study is proven to be an indicator for chaos.
If the system is integrable, the trajectory is closed. Hence a torus is obtained. If the system is not integrable, elliptic orbits are observed with a chaotic regime. According to KAM theory the invariant tori of an integrable system retain their topology under a perturbation that destroys the integrability of the Hamiltonian, however chaos is observed in some regions of the phase space of the system with random points on the surface of section.
In addition to the Poincare section study done by Matinyan et. al, a Lyapunov exponent study can reveal the parts of the parameter space in which chaos is observed. Preliminary results indicate that for the case in which the Higgs terms (x^4 and y^4) are absent, all regions for the parameters $a>0$ and $b>0$ give positive maximal Lyapunov exponents that indicate chaos For $a = b = 0$, the chaoticity is maximum. As a or b increase, the system is still chaotic, but the system loses its chaoticity gradually and tends to converge to a limit cycle. On the other hand, for the case the Higgs terms are present with $a=b=0$, the system still has a positive maximal Lyapunov exponent whose value is smaller than that in the Yang Mills case.

2. Chaos in Yang Mills Higgs system

Although there is no universally accepted definition of chaos, most experts think that chaos is the aperiodic, long – term behavior of a bounded, deterministic system that exhibits sensitive dependence on the on initial conditions. Lyapunov Exponents is the mathematical method for the determination of chaos in dynamical systems. It is the measure of the exponential separation of two trajectories with a very small initial separation. A system with positive values of Lyapunov Exponents is chaotic, and the value of these exponents the average rate at which predictability is lost.
In this section, we compute Lyapunov exponents with the aid of Fortran code that implement Wolf algorithm as we discussed before. In addition we also use Reduce code which calculates variational equations needed for the Wolf algorithm. Both programs are included in appendixes. We mostly emphasize on Yang Mills Higgs coupled system in order to demonstrate the corresponding chaotic behavior.
First of all we investigated how exponents are changing with respect to the scale parameter p, we found that system possesses chaotic motion in wide range of value of p. Especially we scan for the interval from $p=0.05$ to $p=4$. Here are some of graphs for the specific values of p.

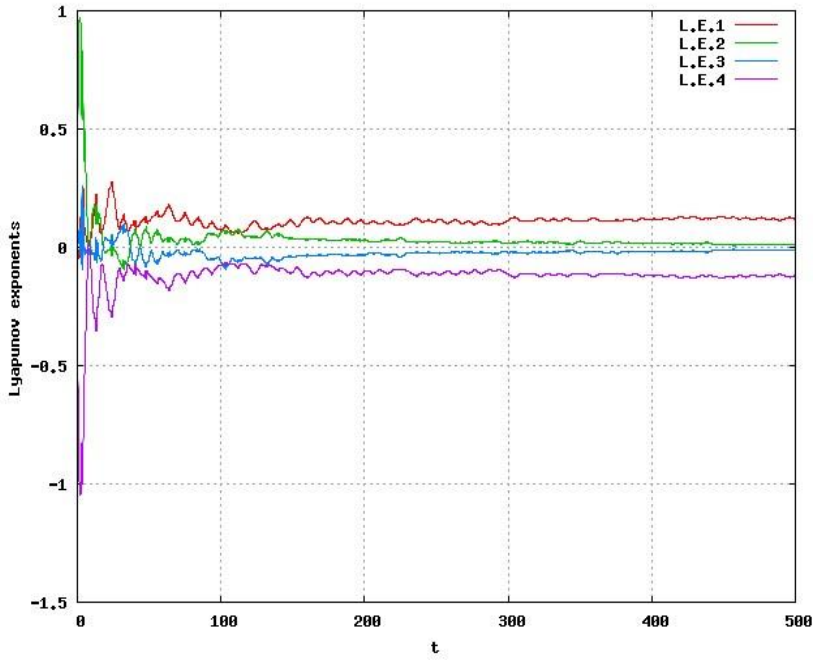

Fig. 1. Lyapunov exponents vs time for *p=0.2*

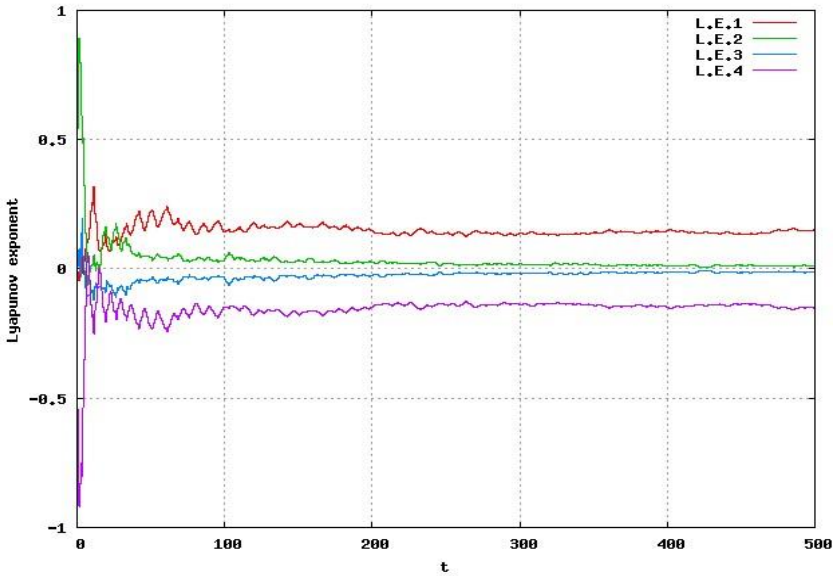

Fig. 2. Lyapunov exponents vs time for *p=0.5*

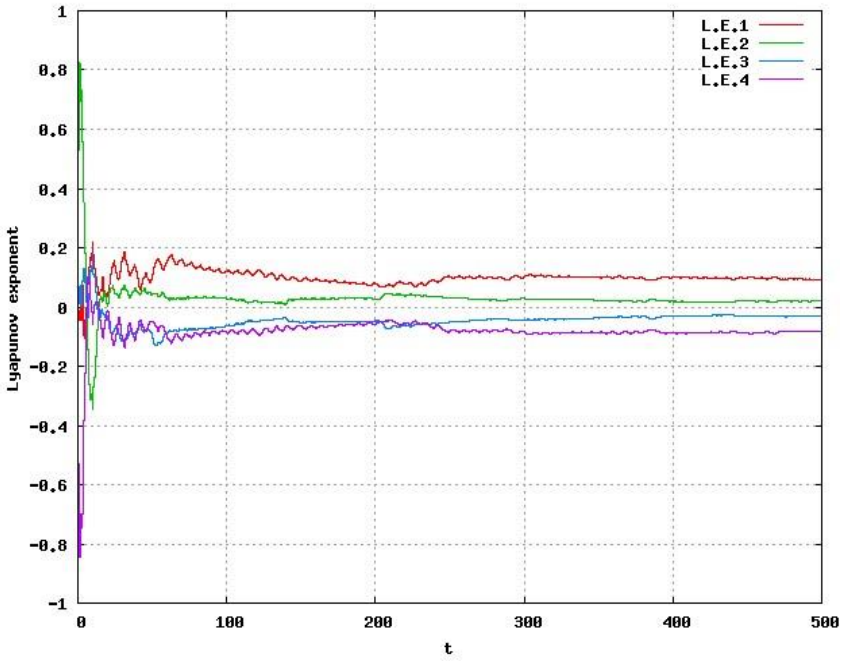

Fig. 3. Lyapunov exponents vs time for *p=0.8*

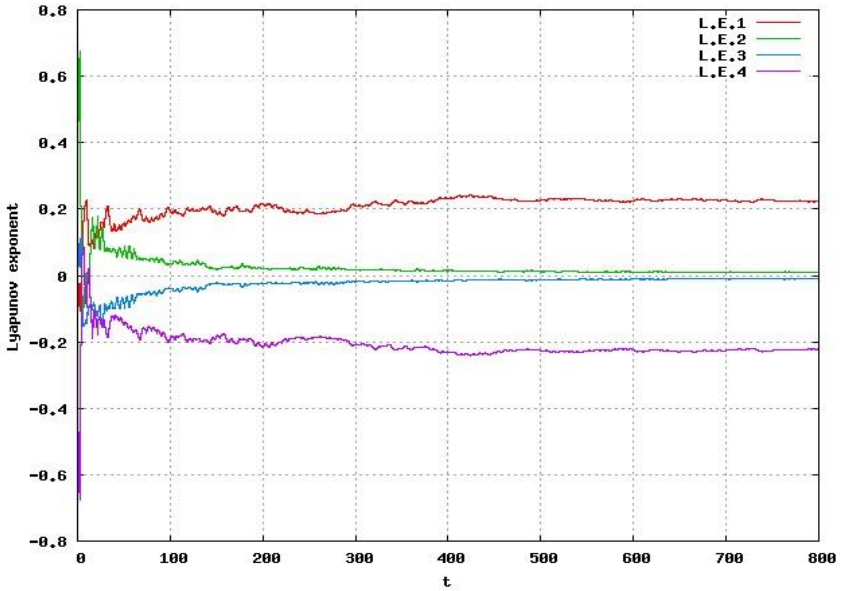

Fig. 4. Lyapunov exponent vs time for *p=2.2*

On the other hand we also analyze the results of adding oscillator term to dynamical system by giving a coefficient "a". We saw that all Lyapunov exponents tend to decrease for bigger value of "a" and there occurs a transition from chaotic motion to periodic or quasi periodic motion. We investigate this transition for the value of parameters where the Lyapunov exponents seem to be maximum. Some of the results are shown below

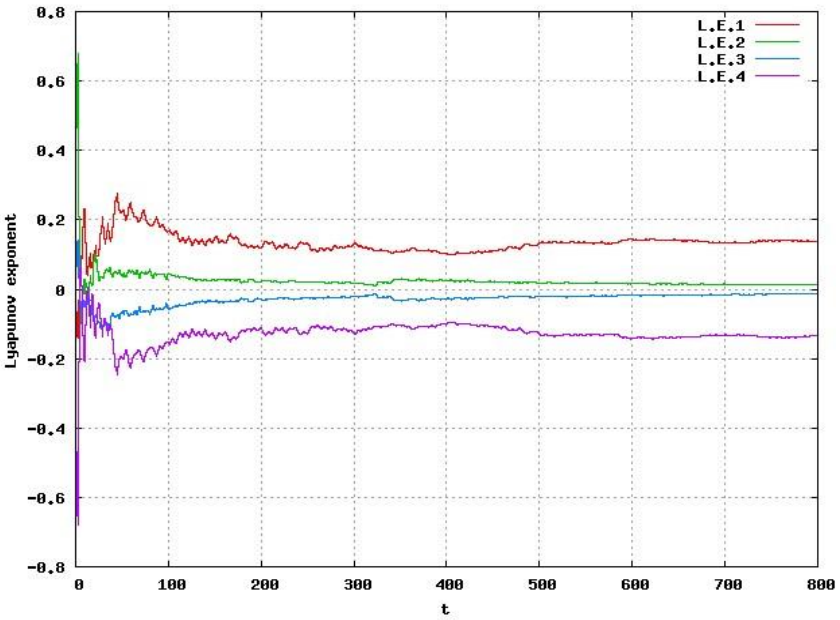

Fig. 6. Lyapunov exponents vs time for *a=0.1* and *p=2.2*

We can deduce from these graphs that, for small values of "*a*" the system persist for a chaotic behavior. But when "*a*" grows system start to possess periodic motion.On the other hand we can see that almost all Lyapunov spectrums are symmetrical which is the expected result since in Hamiltonian systems the sum of Lyapunov exponents must be zero as we stated before so when there is an expanding trajectory in phase space there must be also equally contracting trajectory to compensate for this.

We also investigate phase space trajectories for the corresponding system. Here are some of the trajectories for this system

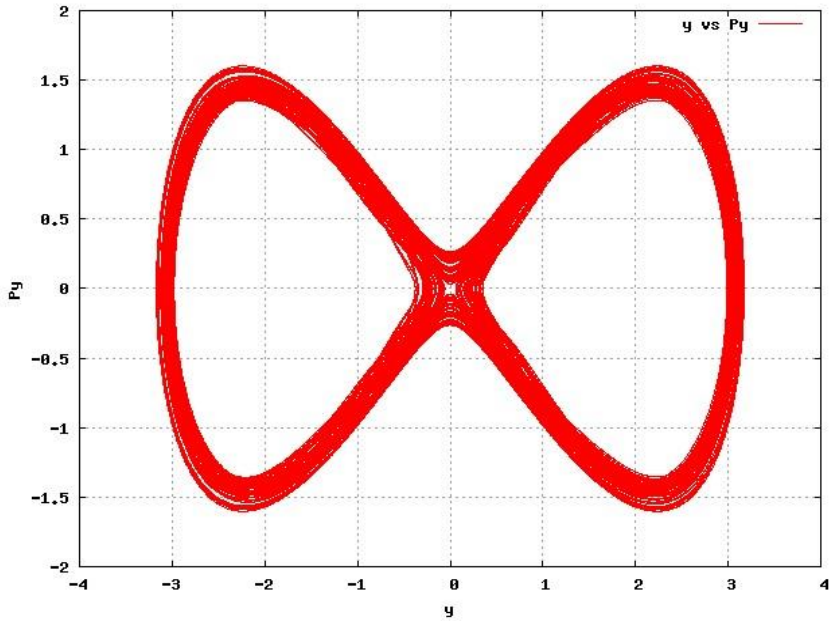

Fig. 7. Trajectory of y vs P_y

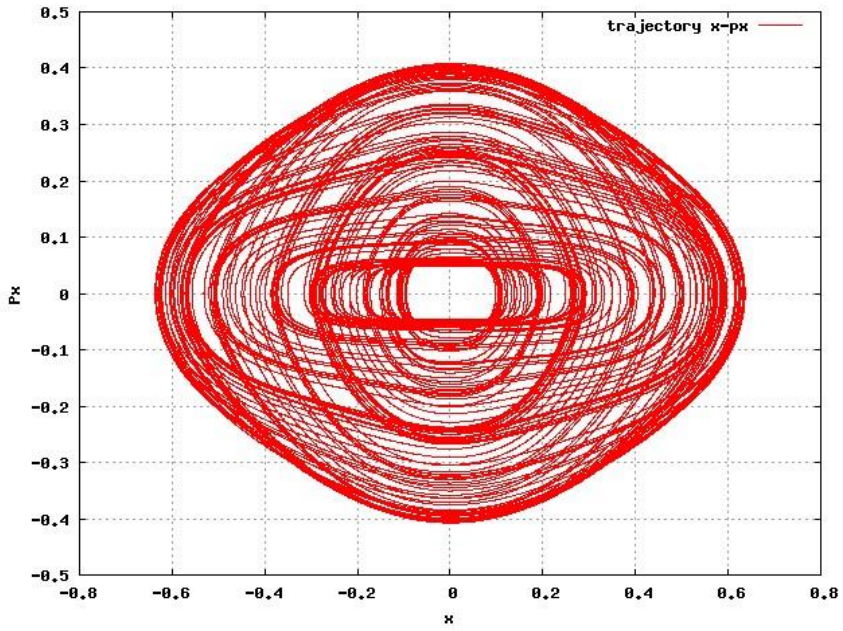

Fig. 8. Trajectory of x vs P_x

3. Conclusions

In this article we try to demonstrate chaotic behavior in the dynamically coupled Yang Mills Higgs system classically. We know that pure Yang Mills fields possess highly chaotic behavior. Although Yang Mills Higgs system also possess chaotic behavior for variety of range of scale parameter, in general the Higgs field is responsible for considerably regularizing motion in the dynamical system[4,6]. So we can say that Higgs mechanism has a stabilizing effect. On the other hand we also consider an additional oscillator term in the Yang Mills Higgs system and it is observed that for small coefficients of the oscillator term chaotic motion still persists. But when oscillator term gets larger chaos disappears and regular motion involving multi periodic motion takes place instead, since the oscillatory motion begins to dominate[5,6].

References

1. A. Wolf, J. B. Swift, H. L. Swinney and J. Vatsano. Determining Lyapunov Exponents From a Time Series. *Physica D,* 16: 285-317,1985.
2. C. H. Skiadas and C. Skiadas. *Chaotic Modeling and Simulation: Analysis of Chaotic Models, Attractors and Forms*, Taylor and Francis/CRC, London, 2009.
3. F. Verhulst. *Nonlinear Differential equations and dynamical systems*, Springer,Verlag, 1996.
4. S. G. Matinyan and B. Müller. *Chaos and Gauge Field Theory*, World Scientific, 1994.
5. S. G. Matinyan. *Chaos in Non-Abelian Gauge Fiels, Gravity and Cosmology*, NC, 1996.
6. S. G. Matinyan. *Dynamical Chaos of Non–Abelian Gauge Field*, Yerevan Physics Institute, 1983.

Chaotic Modeling and Simulation (CMSIM) 1: 223-230, 2013

Robustness and Bit Error Rate Performance of Qi Hyper Chaos Based Encryption

Guoyuan Qi
Department of Electrical Engineering
Tshwane University of Technology, Pretoria, South Africa
E-mail: qig@tut.ac.za

Dennis Luke Owuor
Department of Electrical Engineering
Tshwane University of Technology, Pretoria, South Africa
E-mail: dennisluke11@yahoo.com

André E. Botha
Department of Physics
University of South Africa, Pretoria, South Africa
E-mail: bothaae@unisa.ac.za

Abstract. Recently, in the field of telecommunication, chaotic encryption has drawn much attention because of its ease in design and implementation over conventional encryption methods. In this paper, chaos shift keying (CSK) models are designed based on Qi hyper-chaos. The efficiency and effectiveness of the developed models are evaluated using the bit error rate. By using power spectrum analysis and low pass filtering techniques, the robustness of CSK based on Qi hyper-chaos over CSK based on the Lorenz chaotic system is verified. The results show that the robustness and bit error rate performance of encryption based on Qi hyper-chaos is much better than that based on Lorenz chaos.
Keywords: Chaos, Encryption, Hyper-chaos, BER, CSK.

1. Introduction

Telecommunication as a field has tremendously grown in the last decade. Associated with this growth, is the requirement for efficient and effective secure communication methods [1]. One method of making data secure is through encryption and decryption. Over the past few years, methods of chaotic encryption have developed enormously, and several chaotic systems, such as the Lorenz, Chen and Rössler systems, have been proposed [2-5]. These systems have been employed for encryption and decryption of message signal, image and video during communication. In this context there are a number of different chaotic encryption methods that have been employed for encryption and decryption, for example, chaos synchronization, chaos shift keying and chaotic masking.

Traditional encryption schemes based on integer number theory have been studies for a long time and are considered to be reliable. In contrast, the security

Received: 30 March 2012 / Accepted: 23 September 2012

ISSN 2241-0503

of chaotic communication schemes often relies on a mixture of analytic methods and intuition. Encryption and cryptanalysis using chaotic dynamics is a relatively new field that has only been intensively researched on for less than a decade.

This paper aims to demonstrate the robustness and bit error rate performance of digital message signal encryption based on Qi hyper-chaos systems compared to message signal encryption based on Lorenz chaotic system.

2. Comparison between the Qi hyper-chaotic system and the Lorenz chaotic system

Many proposed chaos-based secure encryption have been totally or partially broken by different attacks [6, 7]. This section provides a detailed comparison between Qi hyper-chaos and the Lorenz chaotic system in terms of their randomness and disorder.
The nonlinear dynamic model representing Qi hyper-chaos is given by [8, 9]:

$$\begin{aligned} \dot{x}_1 &= a(x_2 - x_1) + x_2 x_3 \\ \dot{x}_2 &= b(x_1 + x_2) - x_1 x_3 \\ \dot{x}_3 &= -cx_2 - ex_4 + x_1 x_2 \\ \dot{x}_4 &= -dx_4 + fx_3 + x_1 x_2 \end{aligned} \tag{1}$$

Here $x_i \ (i = 1, 2, 3, 4)$ are the state variables and *a, b, c, d, e, f* are positive constant parameters. The well-known Lorenz system is given in Ref. [10].
The basic comparisons of the dynamic property between Qi hyper-chaos and Lorenz chaotic system are summarized in the next paragraph [8].

The attractor of Qi hyper-chaotic system exhibits a very irregular and disordered form unlike the butterfly shape produced by the Lorenz chaotic system. The Stochastic distribution of Qi hyper chaos is very similar to that of Gaussian white noise but that of Lorenz has three peaks at its trajectory is unlike Gaussian white noise. Qi hyper-chaotic signal is much more sensitive to initial condition than the Lorenz chaos and other hyper-chaos. With these rich advantages of Qi hyper chaos over Lorenz chaotic system, as demonstrated in [8], there is a need to explore the effects implementing the system for encryption of messages.

3. Qi-Hyper-Chaos-Shift Keying Encryption

3.1 Method 1: Non-Coherent Decryption Based on Bit-Energy Estimation

In this encryption scheme two hyper-chaotic signals are used to encrypt the message signal at the sending end and decryption is done at the receiving end based on energy bit estimation [11, 12].

Two chaos generators produce signals $c_1(t)$ and $c_2(t)$, respectively. During the bit duration, i.e. $[((l-1)T_b), lT_b]$, if a binary "+1" is about to be sent, $c_1(t)$ is transmitted, and if "−1" is about to be sent, $c_2(t)$ is transmitted.

The encrypted signal $r(t)$ is then sent through a channel of communication. Thus

$$r(t) = s(t) + \xi(t) \tag{2}$$

where $\xi(t)$ is the noise signal added to the sent signal during communication.

The decryption method used is called non-coherent demodulation based on an energy bit estimator. Decryption is done based on some distinguished characteristics of the signal transmitted. The property used in this paper is the bit energy, which is deliberately made different for different symbols in the encryption process.

A Qi hyper-chaos generator is used to produce two chaotic signals; the first chaotic system is assigned different value, i.e. $c_1(t) + M$, where M is the value assigned to separate with $c_2(t)$. At the receiving end the bit energy can be estimated by a square and integration process.

Let energy per bit be $y(lT_b)$. When the energy bit $y(lT_b) > T_h$ then binary "+1" was send, otherwise binary "−1" was send, where $T_h > 0$ is threshold value.

The simulation results of non-coherent demodulation based on bit-energy estimation are shown in Fig. 1, which demonstrates successful performance of encryption and decryption.

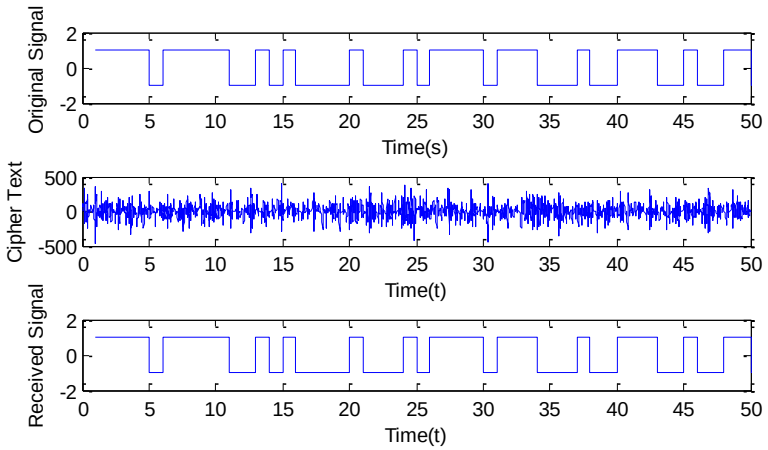

Fig. 1. Qi-Hyper-Chaos-Shift Keying Encryption and decryption

3.2 Method 2: Coherent Demodulation Based on Correlation

The process of correlation is where the "likeness" between two chaotic signals is evaluated. In this method two correlators are employed to evaluate the correlations between the received signal and the two recovered chaotic signals. The outputs of the correlators for the *l*th bit are given by

$$y_1(lT_b) = \int_{(l-1)T_b}^{lT_b} r(t)c_1'(t)\,dt \tag{3}$$

$$y_2(lT_b) = \int_{(l-1)T_b}^{lT_b} r(t)c_2'(t)\,dt \tag{4}$$

where $c_1'(t)$ and $c_2'(t)$ are synchronizations of $c_1(t)$ and $c_2(t)$, respectively. The following equation is used to determine the output to the threshold detector.

$$y_0(lT_b) = y_1(lT_b) - y_2(lT_b) \tag{5}$$

If the output $y_o(lT_b)$ is greater than T_h then +1 was sent, otherwise -1 was sent.

The process of encryption is the same as that of Method 1, but the decryption process takes place with the aid of synchronizations. The decryption proceed by evaluating the correlation of the transmitted signal and the regenerated chaotic carrier as in Eq. (3) and eq. (4), and followed by energy bit calculation then compared in Eq. (5). If the output is greater than the value specified at the threshold then "+1" is decoded otherwise "−1" is decoded.

The simulation results of correlation-type coherent decryption for CSK with two Qi hyper chaos generators are shown in Fig. 2.

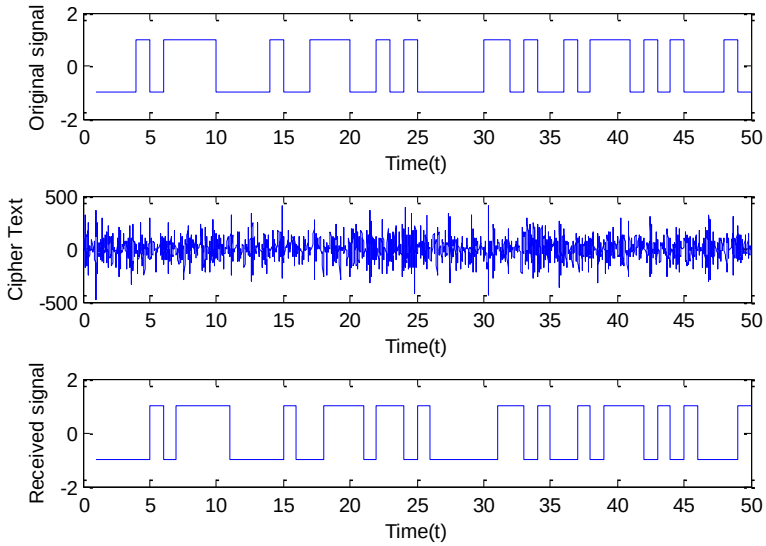

Fig. 2. Comparison between sent and received signal

4. BER Performance of CSK Based on Qi Hyper Chaos Compared to Lorenz Based CSK

Bit Error Rate (BER) is a performance measurement that specifies the number of bit corrupted or destroyed as they are transmitted from its source to its destination [13, 14].
BER measurements compare digital input and output signals to access what fractions of the bit are received incorrectly. It is defined as:

$$\mathrm{BER} = \frac{N_e}{N_t} \tag{6}$$

Where N_e is the number of error bits received over time t, and N_t is the total number of bits transmitted. Signal to Noise Ratio (SNR) is defined as the ratio of a signal power to noise power and it is normally expressed in decibel (dB). The mathematical expression of SNR is:

$$\mathrm{SNR} = 10\log_{10}\left(\frac{\mathrm{SignalPower}}{\mathrm{NoisePower}}\right)\mathrm{dB} \tag{7}$$

Relationship between the system's SNR and BER is that the higher the SNR, The lower would be the corresponding BER

$$\mathrm{BER} = \left(1/\mathrm{SNR}\right)^k \tag{8}$$

where k is a specific subcarrier index.
In this paper simulation of BER is done using Bertool tool in Matlab\Simulink.

Fig. 3 shows the comparison of the BER performance between chaos based CSK using energy bit estimation method for decryption (Simulation 0) and Qi hyper chaos CSK based using correlation method for decryption (Simulation 1).

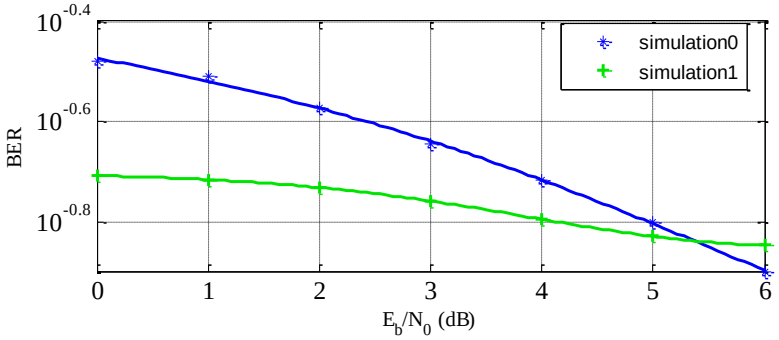

Fig 3: Comparing the BER performance between Qi hyper-chaos based CSK using energy bit estimation method for decryption and using correlation method for decryption.

The BER performance of the latter is seen to be much lower than the former; hence, the correlation method for decryption is more efficient compared the energy bit estimation method for decryption.

Qi hyper-chaos CSK based on correlation method has better performance because with the aid of synchronization the low frequency noise and high frequency noise can be easily eliminated.

5. Power Spectrum and Low Pass Filter Methods of Attacking Chaos Based Secure Communication

Security during communication is fundamental since it is one of the components that add up to effective and efficient communication. There are varieties of methods that have been proposed to attack chaos-based secure communication schemes. In different cases in literature [14] they have indicated successfully breaking of chaos encryption without knowing the secrete key or the parameters used during encryption. This kind of attack is only possible if the received message $m(t)$ is a periodic signal or if $m(t)$ consists of periodic frames within a given duration. The attack can be accomplished using two methods power spectrum analysis and low pass filter technique and return map analysis.

Power spectrum and low pass filter technique are very powerful schemes that can be used to break chaotic communication without knowing the parameters or the initial components used during encryption.These two methods are implemented in this paper to determine how robust CSK based on Qi hyper is.The message signal encrypted by Lorenz chaotic system hereby successfully extracted by the filter and decision circuit as shown Fig. 4

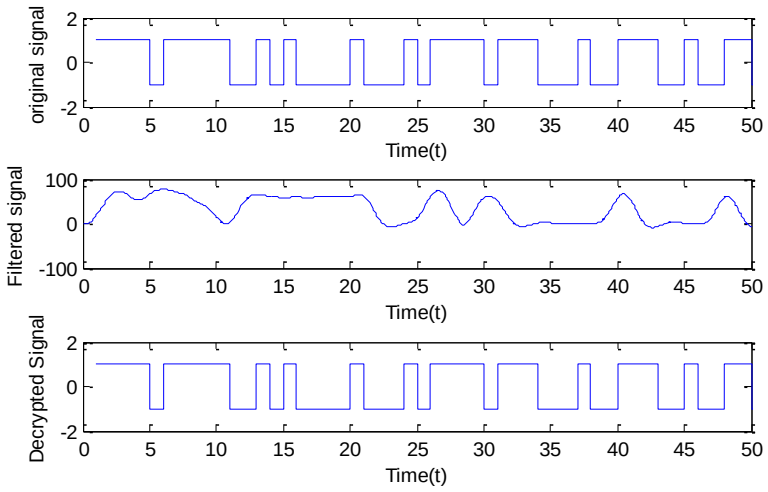

Fig. 4. Attacking Lorenz Chaos through power spectrum and low pass filter

The attempt to attack message signal encrypted based on Qi hyper-chaotic system was unsuccessfully as shown Fig. 5

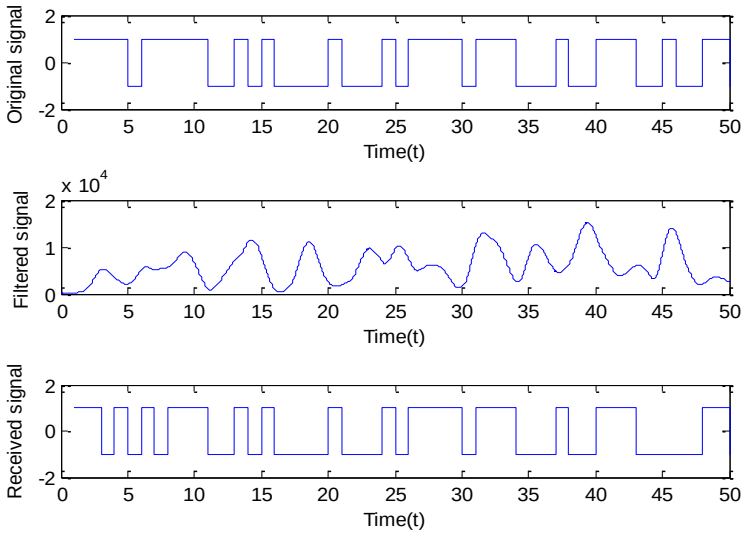

Fig. 5. Attacking Qi hyper-chaos through power spectrum and low pass filter, The simulation results in Fig. 5 indicates that it is not easy to attack digital message signal encryption based on Qi hyper-chaos. The difficulty in attacking message signal based on Qi hyper-chaos can be attributed to the rich properties of Qi hyper-chaos.

6. Conclusion

In this paper message signal based on Qi hyper-chaos has been implemented. The BER performance comparison between Qi hyper-chaos and Lorenz chaos shows that Qi hyper-chaos based CSK has better performance compared to Lorenz based CSK. The rich properties of Qi hyper chaos such us high frequency spectrum, high level of disorder, etc. have made it very cumbersome for low pass-filter and power spectrum analysis method to be successful in attacking and decrypting the encrypted message signal sent.

References

1. C. I. Rincu and A. Serbanescu. Chaos-Based Cryptography. A Possible Solution For Information Security, *Bulletin of the Transilvania University of Brasov*, vol. 2,51, 2009.
2. M. Baptista. Cryptography with chaos, *Physics Letters A*, vol. 240: 50-54, 1998.
3. L. M. Pecora and T. L. Carroll. Synchronization in chaotic systems, *Physical review letters*, vol 64: 821-824, 1990.
4. T. L. Carroll and L. M. Pecora. Synchronizing chaotic circuits, *Circuits and Systems, IEEE Transactions*, vol. 38: 453-456, 1991.
5. J. Lü and G. Chen. A new chaotic attractor coined, *Int. J. Bifurc. Chaos*, vol. 12: 659–661, 2002.
6. G. Álvarez, S. Li. Comput, *Commun*, vol. 27, 2004.

7. G. Hu, Z. Feng, R. Meng, *IEEE Trans. Circuits Syst.* 50-275, 2003.
8. G. Qi, et al. On a new hyperchaotic system, *Physics Letters A*, vol. 372:124-136, 2008.
9. G. Qi, et al. "A new hyperchaotic system and its circuit implementation, *Chaos, Solitons & Fractals*, vol. 40:2544-2549, 2009.
10. E. N. Lorenz. Deterministic nonperiodic flow, *J. Atmospheric Sc.*, vol. 20: 130-141, 1963.
11. C. Tse and F. Lau. Chaos-based digital communication systems, *Operating Principles, Analysis Methods and Performance Evaluation (Springer Verlag, Berlin)* 2004.
12. M. P. Kennedy and G. Kolumbán. *Digital communications using chaos*, *Signal processing*, vol. 80: 1307-1320, 2000.
13. W. M. Tam, et al. An approach to calculating the bit-error rate of a coherent chaos-shift-keying digital communication system under a noisy multiuser environment, Circuits and *Systems: Fundamental Theory and Applications*, *IEEE Transactions*, vol. 49:210-223, 2002.
14. M. Sushchik, et al. Performance analysis of correlation-based communication schemes utilizing chaos, Circuits *and Systems I: Fundamental Theory and Applications, IEEE Transactions*, vol. 47:1684-1691, 2000.

Chaotic Modeling and Simulation (CMSIM) 1: 231–238, 2013

Inversive congruential generator with a variable shift

P. D. Varbanets[1] and S. P. Varbanets[2]

[1] I.I. Mechnikov Odessa National University, str. Dvoryanskaya 2, 65026 Odessa, Ukraine
(E-mail: varb@sana.od.ua)
[2] I.I. Mechnikov Odessa National University, str. Dvoryanskaya 2, 65026 Odessa, Ukraine
(E-mail: varb@sana.od.ua)

Abstract. We give the description for elements of the sequence of inversive congruential pseudorandom numbers y_n as polynomials on number n and initial value y_0. We also estimate some exponential sums over y_n.
Keywords: inversive congruential numbers, exponential sum, discrepancy.

1 Introduction

Let p be a prime number, $m > 1$ be a positive integer. Consider the following recursion

$$y_{n+1} \equiv a\overline{y}_n + b(mod\ p^m), (a, b \in \mathbb{Z}), \tag{1}$$

where $\overline{y}_n$ is a multiplicative inversive $mod\ p^m$ for y_n if $(y_n, p) = 1$. The parameters a, b, y_0 we call the multiplier, shift and initial value, respectively.

In the works of Eichenauer, Lehn, Topuzoğlu, Niederreiter, Flahive, Shparlinski, Grothe, Emmerih ets were proved that the inversive congruential generator (1) produces the sequence $\{x_n\}$, $x_n = \frac{y_n}{p^m}$, $n = 0, 1, 2, \ldots$, which passes s-dimensional serial tests on equidistribution and statistical independence for $s = 1, 2, 3, 4$ if the defined conditions on relative parameters a, b, y_0 are accomplishable.

It was proved that this generator is extremely useful for Quasi-Monte Carlo type application (see, [3],[4]). The sequences of PRN's can be used for the cryptographic applications. Now the initial value y_0 and the constants a and b are assumed to be secret key, and then we use the output of the generator (1) as a stream cipher. By the works [1],[2] it follows that we must be careful in the time of using the generator (1).

In the current paper we give the generalization for the generator (1). We consider the following recursive relation

$$y_{n+1} \equiv a\overline{y}_n + b + cF(n+1)y_0(mod\ p^m) \tag{2}$$

Received: 4 April 2012 / Accepted: 12 October 2012

ISSN 2241-0503

under conditions

$$(a,p)=(y_0,p)=1,\ \ b\equiv c\equiv 0(mod\ p),\ \ F(u) \text{ is a polynomial over } \mathbb{Z}[u].$$

The generator (2) we call the generator with a variable shift $b+cF(n+1)y_0$. The computational complexity of generator (2) is the same as for the generator (1), but the reconstruction of parameters a, b, c, y_0, n and polynomial $F(n)$ is a tricky problem even if the several consecutive values $y_n, y_{n+1}, \dots, y_{n+N}$ will be revealed. Thus the generator (2) can be used in the cryptographical applications. Notice that the conditions $(a,p)=(y_0,p)=1$, $b\equiv c\equiv 0(mod\ p)$ guarantee that the recursion (2) produces the infinite sequence $\{y_n\}$.

Our purpose in this work is to show passing the test on equidistribution and statistical independence for the sequence $\{x_n\}$, $x_n=\frac{y_n}{p^m}$, and hence, the main point to be shown is the possibility for such sequences to be used in the problem of real processes modeling and in the cryptography.

Notations: For p being a prime number

$$\begin{aligned}
&R_m := \{0,1,\dots,p^m-1\},\\
&R_m^* := \{a\in R_m \mid (a,p)=1\},\\
&e_m(u) := e^{2\pi i\frac{u}{p^m}}, u\in\mathbb{R},\\
&exp(x) := e^x \text{ for } x\in\mathbb{R},\\
&\nu_p(A)=\alpha\in\mathbb{N}\cup\{0\} \text{ if } p^\alpha \parallel A,\ p^{\alpha+1}\not| A.
\end{aligned}$$

For $u\in\mathbb{Z}$, $(u,p)=1$ we write $\overline{u}$ if $u\cdot\overline{u}\equiv 1(mod\ p^m)$.

2 Auxiliary results

We need the following simple statements.

Let $f(x)$ be a periodic function with a period τ. For any $N\in\mathbb{N}$, $1\le N\le\tau$, we denote

$$S_N(f) := \sum_{x=1}^{N} e^{2\pi i f(x)}$$

Lemma 1. *The following estimate*

$$|S_N(f)|\le \max_{1\le n\le\tau}\left|\sum_{x=1}^{\tau} e^{2\pi i\left(f(x)+\frac{nx}{\tau}\right)}\right|\log\tau \tag{3}$$

holds.

Let $\mathfrak{I}(A,B;p)$ be a number of solutions of the congruence $A-Bu^2\equiv 0(mod\ p)$, $(u,p)=1$.

Lemma 2. *Let p be a prime number and let $f(x)$, $g(x)$ be the polynomials over* $\mathbb{Z}$

$$\begin{aligned}
f(x)&=A_1x+A_2x^2+p(A_3x^3+\cdots),\\
g(x)&=B_1x+p(B_2x^2+\cdots),
\end{aligned}$$

and, moreover, let $\nu_p(A_2)=\alpha>0$, $\nu_p(A_j)\geq\alpha$, $j=3,4,\ldots$. *Then we have the following estimates*

$$\left|\sum_{x\in R_m} e_m(f(x))\right|\leq\begin{cases}2p^{\frac{m+\alpha}{2}} & if\ \nu_p(A_1)\geq\alpha,\\ 0 & else;\end{cases} \tag{4}$$

$$\left|\sum_{x\in R_m^*} e_m(f(x)+g(\overline{x}))\right|\leq\begin{cases}(\mathfrak{I}(A_1,B_1;p)\cdot p)^{\frac{m}{2}} & if\ (B_1,p)=1,\\ 2p^{\frac{m+\alpha}{2}} & if\ \nu_p(A_1)\geq\alpha,\\ & \quad \nu_p(B_j)\geq\alpha,\\ & \quad j=1,2,\ldots,\\ 0 & if\ \nu_p(A_1)<\alpha\leq\nu_p(B_j),\\ & \quad j=1,2,3,\ldots.\end{cases} \tag{5}$$

3 Preparations

Consider the sequence $\{y_n\}$ produced by the recursion (2).
Let $n=2k$. We put

$$y_{2k}\equiv\frac{a_0^{(k)}+a_1^{(k)}y_0+\cdots}{b_0^{(k)}+b_1^{(k)}y_0+\cdots}:=\frac{A_k}{B_k}(mod\ p^m) \tag{6}$$

Twice using the recursion (2) we infer

$$\begin{aligned}y_{2(k+1)}=\frac{A_{k+1}}{B_{k+1}}&\equiv\frac{\left(aA^{(k)}+abB^{(k)}+b^2A^{(k)}\right)}{aB_k+bA_k+cA_kF(2k+1)y_0}+\\ &+\frac{\left(acB^{(k)}+bcA^{(k)}F(2k+2)+bcA^{(k)}F(2k+1)\right)y_0}{aB_k+bA_k+cA_kF(2k+1)y_0}\equiv\\ &\equiv\frac{(aA_k+abB_k+b^2A_k)}{aB_k+bA_k+cA_kF(2k+1)y_0}+\\ &+\frac{(acB_k+bcA_kF(2k+2)+bcA_kF(2k+1))\,y_0}{aB_k+bA_k+cA_kF(2k+1)y_0}+\\ &+\frac{c^2A_kF(2k+1)F(2k+2)y_0^2}{aB_k+bA_k+cA_kF(2k+1)y_0}\end{aligned} \tag{7}$$

Define the following matrices

$$\begin{aligned}&S_0=\begin{pmatrix}a+b^2 & ab\\ b & a\end{pmatrix},\ S_1=\begin{pmatrix}b & a\\ 0 & 0\end{pmatrix},\ S_2=\begin{pmatrix}1 & 0\\ 1 & 0\end{pmatrix},\ S_3=\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}\\ &T_k=S_0+cy_0F(2k+2)S_1+bcy_0F(2k+1)S_2+\\ &\quad+c^2y_0^2F(2k+1)F(2k+2)S_3\end{aligned} \tag{8}$$

Now from (6)-(7) we obtain the matrix equality

$$\begin{pmatrix}A_{k+1}\\ B_{k+1}\end{pmatrix}=T_kT_{k-1}\cdots T_1\begin{pmatrix}A_0\\ B_0\end{pmatrix},\ \begin{pmatrix}A_0\\ B_0\end{pmatrix}=\begin{pmatrix}y_0\\ 1\end{pmatrix} \tag{9}$$

Denote

$$Y_i = cy_0F(2i+2)S_1 + cby_0F(2i+1)S_2 + c^2y_0^2F(2i+1)F(2i+2)S_3$$

Then we have

$$T_1T_2\cdots T_k = S_0^k + \sum_{\ell=1}^{k-1} S_0^{k-\ell} \sum_{j=0}^{k} {\sum_{i_1,\dots,i_\ell}}' Y_{i_1}\cdots Y_{i_\ell}, \tag{10}$$

where the sum ${\sum_{i_1,\dots,i_\ell}}'$ takes over all collections $i_1,\dots,i_\ell$ for which $0 \le i_1,\dots,i_\ell \le k$, $i_t \ne i_s$ for $t \ne s$, and $i_t \ne j$, $t = 1,\dots,\ell$, $s = 1,\dots,\ell$.

We will suppose that $\nu = \nu_p(b) < \nu_p(c) = \mu$. Therefore $Y_i \equiv 0 (mod\ p^\mu)$, and hence, all summands of sum ${\sum_{i_1,\dots,i_\ell}}'$ are equal to zero modulo p^m if $\ell > k_0 := \left[\frac{m+1}{\mu}\right]$.

First we study S_0^k in detail.

We have

$$S_0 = aI + bZ,$$

where

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad Z = \begin{pmatrix} b & a \\ 1 & 0 \end{pmatrix}.$$

Hence, putting $\ell_0 = \min\left(\left[\frac{k+1}{2\nu}\right], \left[\frac{m+1}{2\nu}\right]\right)$ we can write

$$S_0^k = \sum_{j=0}^{k} \binom{k}{j} a^{k-j}b^jZ^j = \sum_{\substack{j=0 \\ \text{j is even}}}^{\ell_0} + \sum_{\substack{j=0 \\ \text{j is odd}}}^{\ell_0} := \sum\nolimits_1 + \sum\nolimits_2, \tag{11}$$

where modulo p^m

$$\begin{aligned} \sum\nolimits_1 &= \sum_{j=0}^{\ell_0} \binom{k}{2j} a^{k-2j}b^{2j}Z^{2j}, \\ \sum\nolimits_2 &= \sum_{j=0}^{\ell_0} \binom{k}{2j+1} a^{k-2j-1}b^{2j+1}Z^{2j+1}. \end{aligned} \tag{12}$$

Notice that

$$Z^2 = \begin{pmatrix} b & a \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} a+b^2 & ab \\ b & a \end{pmatrix} = aI + bZ.$$

Consequently, raising to square in series the matrix Z we derive for $j \le \ell_0$

$$Z^{2j} = F_0(j)I + F_1(j)Z \tag{13}$$

where

$$\begin{cases} F_0(j) = f_{0,j} + b^2f_{2,j} + \cdots + b^{2j-2}f_{2j-2,j}, \\ F_1 = bf_{1,j} + b^3f_{3,j} + \cdots + b^{2j-1}f_{2j-1,j}, \\ f_{0,j} = a^j, \ \ f_{1,j} = a^{j-1}j. \end{cases} \tag{14}$$

Moreover, it is easy to see that

$$\begin{cases} f_{2,j} = a^{j-1}(2j-3),\ f_{3,j} = \overline{2}a^{j-1}(3j^2-9j+8), \\ f_{2j-4,j} = a^2(2j-3),\ f_{2j-2,j} = a, \\ f_{2j-3,j} = a(f_{2j-3,j-1}+2j-3),\ f_{2j-1,j} = 1, \\ f_{2\ell,j} = a^{j-\ell}(f_{2\ell,j-1}+f_{2\ell-1,j-1}), \\ f_{2\ell+1,j} = a^{j-\ell}(f_{2\ell,j-1}+f_{2\ell+1,j-1}+f_{2\ell-1,j-1}), \\ \ell = 2,3,\ldots,j-2. \end{cases} \tag{15}$$

So, for $k \geq m$ the coefficients $f_{\ell,j}$ does not depend on k.
From (13)-(14) we derive

$$\begin{aligned} Z^{2j+1} &= (ja^jb + f_{3,j}a^{j-1}b^3 + \cdots + ab^{2j-1})I + \\ &+ (a^j + a^{j-1}b^2(f_{2,j}+j) + \cdots + ab^{2j-2}(2j-1) + b^{2j})Z = \\ &= G_0(j)I + G_1(j)Z. \end{aligned} \tag{16}$$

Thereby the relations (13)-(16) give

$$\begin{aligned} S_0^k = &\sum_{j=0}^{\ell_0} a^{k-2j-1}b^{2j}\left(\binom{k}{2j}aF_0(j) + \binom{k}{2j+1}bG_0(j)\right)I + \\ &+ \sum_{j=0}^{\ell_0} a^{k-2j-1}b^{2j}\left(\binom{k}{2j}aF_1(j) + \binom{k}{2j+1}bG_1(j)\right)Z. \end{aligned} \tag{17}$$

Now after the simple calculations we obtain

$$S_0^k = H_0(k)I + H_1(k)Z, \tag{18}$$

where modulo p^m

$$\begin{cases} H_0(k) = a^k + ka^{k-1}b(1+b^2h_{01}) + k^2a^{k-2}b^2(\overline{2}+b^2h_{02}) + \\ \qquad + k^3a^{k-2}b^3H_{03}(k), \\ H_1(k) = a^{k-1}bk(1+b^2h_{11}) + k^3b^3H_{13}(k), \\ H_{03}(k), H_{13}(k) \in \mathbb{Z}[k],\ \ h_{01}, h_{02}, h_{11} \in \mathbb{Z}. \end{cases} \tag{19}$$

Repeating the argument used in the proof of relations (18),(19) we easy deduce that

$$\sum_{\ell=1}^{k_0} S_0^{k-\ell} \sum_{j=0}^{k} {\sum_{i_1,\ldots,i_\ell}}' Y_{i_1}\cdots Y_{i_\ell} = \overline{H}_0(k)I + \overline{H}_1(k)Z, \tag{20}$$

where

$$\begin{cases} \overline{H}_0(k) = kca^k\left[(\overline{f}_{0,0} + \overline{H}_{01}b) + kb^2\overline{H}_{02}(k)\right], \\ \overline{H}_1(k) = kbca^k\overline{H}_{1,0}(k), \end{cases} \tag{21}$$

$\overline{H}_{01}(k), \overline{H}_{02}(k), \overline{H}_{10}(k)$ are the integer polynomials with coefficients depending only on $\overline{a}, (\overline{a})^2, \ldots, (\overline{a})^m$, $b_0, b_0^2, \ldots, b_0^{\left[\frac{m+1}{\nu}\right]}$, $c_0, c_0^2, \ldots, c_0^{\left[\frac{m+1}{\mu}\right]}$, $b_0 = \frac{b}{p^\nu}$, $c_0 = \frac{c}{p^\mu}$.

After all this preliminaries it is straightforward to establish two representations for y_n:

Lemma 3. *Let p be a prime number, $p \geq 5$, and let $m \in \mathbb{N}$, $m \geq 3$; $a, b, c \in \mathbb{Z}$, $GCD(a, p) = 1$, $b \equiv c \equiv 0 (mod\ p)$, $\nu = \nu_p(b)$, $\mu = \nu_p(c)$, $\nu < \mu$, also, let $\{y_k\}$ is the sequence from (2). Then for any $y_0 \in R_m^*$ and $k = 0, 1, 2, \dots$ we have*

$$\begin{aligned} y_{2k} &= (kb - 2^{-1}k(k^2-1)a^{-1}b^3 + G_0(k)) + \\ &+ (1 + k(k+1)a^{-1}c + G_1(k))y_0 + \\ &+ (-ka^{-1}b - (k^3c + k^2(k+1)a^{-1})bc + \\ &+ (2^{-1}3k^3 - 2k^2 + 2^{-1}k)a^{-2}b^3 + G_2(k))y_0^2 + \\ &+ (k^2a^{-2}b^2 - k^2a^{-1}c + G_3(k))y_0^3 + G_4(k, y_0)y_0^4; \\ y_{2k+1} &= ((k+1)b - k^2a^{-1}c + k(k-1)a^{-1}b^3 + H_0(k)) + \\ &+ ((2k+)c + H_1(k))y_0 + (a - k^2c - 2k^2b^2 + H_{-1}(k))y_0^{-1} + \\ &+ (-kab + 2^{-1}3k^2(k+1)b^3 + 4^{-1}k^2(k^2-1)a^{-1}b^3 + \\ &+ H_{-2}(k))y_0^{-2} + y_0^{-3}H_3(k, y_0^{-1}), \end{aligned}$$

where

$G_i(k) \in \mathbb{Z}[k]$, $G_i(0) = 0$, $G_i(k) \equiv 0 (mod\ p^{\min(2\nu+\mu, 4\nu)})$, $i = 0, 1, 2, 3$;
$H_i(k) \in \mathbb{Z}[k]$, $H_i(0) = 0$, $H_i(k) \equiv 0 (mod\ p^{\min(2\nu+\mu, 4\nu)})$, $i = -2, \pm 1, 0$;
$G_4(k, u)$, $H_3(k, u)$, *are the polynomials on* k, u,

moreover,

$$G_4(0, u) = H_3(0, u) = 0,\ G_4(k, u) \equiv H_3(k, u) (mod\ p^{\min(2\nu+\mu, 4\nu)}).$$

Lemma 4. *For $k = 0, 1, 2, \dots$ we have*

$$\begin{aligned} y_{2k} &= y_0 + k(b(1 - a^{-1}y_0^2) + 2a^{-1}b^3(a + y_0^2) + a^{-1}cy_0 + C_1(y_0)) + \\ &+ k^2(-a^{-1}b^2y_0 + a^{-1}cy_0(1 - y_0^2) + C_2(y_0)) + k^3C_3(k, y_0) \\ y_{2k+1} &= (b + cy_0 + ay_0^{-1}) + k(b(1 - ay_0^{-2}) + 2cy_0 + D_1(y_0, y_0^{-1})) + \\ &+ k^2(c(a^{-1} - y_0^{-1}) + D_2(y_0, y_0^{-1})) + k^3D_3(k, y_0, y_0^{-1}) \end{aligned}$$

where $C_1(y_0) \equiv C_2(y_0) \equiv C_3(k, y_0) \equiv 0 (mod\ p^{\min(\nu+\mu, 3\nu)})$,
$D_1(y_0, y_0^{-1}) \equiv D_2(y_0, y_0^{-1}) \equiv D_3(k, y_0, y_0^{-1}) \equiv 0 (mod\ p^{\min(\nu+\mu, 3\nu)})$
for every $y_0, y_0^{-1} \in R_m^*$, $k \in \mathbb{Z}$.

Corollary 1. *Let τ be a period length of the sequence $\{y_n\}$ generated by recursion (2), y_0 be an initial value, and let $\nu_p(b) = \nu$, $\nu_p(c) = \mu > \nu$.*

(A) If $a \not\equiv y_0{}^2 (mod\ p)$, then $\tau = 2p^{m-\nu}$.
(B) If $\nu_p(a - y_0^2) = \delta < \min(3\nu, \mu)$, then $\tau = 2p^{m-\nu-\delta}$.
(C) Otherwise: $\tau \leq 2p^{m-\nu-\min(3\nu,\mu)}$.

4 Main results

Let the sequence $\{y_n\}$ is produced by recursion (2) and let the least length of period for $\{y_n\}$ is equal to τ.

For any N, $1 \leq N \leq \tau$, and $h \in \mathbb{Z}$ we define the sum

$$S_N(h, y_0) = \sum_{n=0}^{N-1} e_m(hy_n)$$

Theorem 1. *Let $\{y_n\}$ is the sequence generated by the recursion (2) with the parameters a, b, c and the function $F(n)$, $F(0) = 0$, and let $0 \le \nu_p(a - y_0^2) < \nu = \nu_p(b)$, $2\nu < \mu = \nu_p(c)$, $\nu_p(h) = s$. Then we have*

$$|S_N(h, y_0)| \le \begin{cases} 2p^{\frac{m+\nu+s}{2}} \left(\frac{N}{\tau} + \frac{\log \tau}{p}\right) & if \quad \nu + s < m \\ N & else. \end{cases}$$

Theorem 2. *In the notations of Theorem 1 we have*

$$\overline{S}_N(h) = \frac{1}{\varphi(p^m)} \sum_{y_0 \in R_m^*} |S_N(h, y_0)| \le 3Np^{-\frac{m-s-\nu}{4}}$$

The proofs of these theorems are an analogue of the proofs for Theorem 7 and 8[5] and by the representations of y_n which have been obtained in Lemmas 3 and 4, and using Lemmas 1 and 2.

Now applying the Turan-Koksma inequality(see,[3]) for the discrepancy D_N we obtain

Theorem 3. *Let $p > 2$ be a prime number, $y_0, a, b, c, m \in \mathbb{Z}$, $m \ge 3$ and let a, y_0 are co-primes to p and let $b \equiv c \equiv 0 (mod\ p)$, $0 < \nu_p(b) < \nu_p(c)$, $a \not\equiv y_0^2 (mod\ p)$. Then for the sequence $\{x_k\}$, $x_k = \frac{y_k}{p^m}$, $k = 0, 1, \ldots$, where y_k determine by (2) we have*

$$D_N(x_0, x_1, \ldots, x_{N-1}) \le \frac{1}{p^m} + 2N^{-1}p^{\frac{m-\nu}{2}} \left(\frac{1}{p}\left(\frac{2}{\pi}\log p^m + \frac{7}{5}\right)^2 + 1\right),$$

where $1 \le N \le \tau$, and τ is the least length of a period for $\{y_k\}$.

Next, we denote

$$X_n^{(s)} = (x_n, x_{n+1}, \ldots, x_{n+s-1}),\ s = 2, 3, 4.$$

Theorem 4. *The discrepancy $D_N^{(s)}(X_0^{(s)}, X_1^{(s)}, \ldots, X_{N-1}^{(s)})$ produced by the recursion (2) with the period $\tau = 2p^{m-\nu}$ satisfies the inequality*

$$D_\tau^{(s)} \le \frac{\sqrt{p}}{\sqrt{p} - 1} p^{-\frac{m}{2}+\nu} \left(\frac{1}{\pi}\log p^{m-\nu} + \frac{3}{5}\right)^s + 2p^{-m+\nu}.$$

From the Theorems 3 and 4 it follows that the sequence $\{x_n\}$, $x - n = \frac{y_n}{p^m}$ passes the s-serial tests, $s = 2, 3, 4$ on equidistribution and statistical independence.

Thus, by the complexity of reconstruction for the parameters a, b, c, y_0, $F(u)$ under recursion (2) the sequence of PRN's $\{y_n\}$ can be used in cryptographical applications.

References

1. S.R. Blackburn, D. Gomez-Peres, I. Gutierrez and I. Shparlinski. Predicting nonlinear pseudorandom number generators. *Math. Comp.*, 74(251):1471–1494, 2004.

2. S.R. Blackburn, D. Gomez-Peres, I. Gutierrez and I. Shparlinski. Reconstructing noisy polynomial evaluation in residue rings. *J. of Algorithm*, 61(2):47–59, 2006.
3. H. Niederreiter. Random number generation and Quasi-Monte Carlo methods. *SIAM, Philadelphia*, 1992.
4. H. Niederreiter and I. Shparlinski. Recent advances in the theory of nonlinear pseudorandom number generators. *Proc. Conf. on Monte Carlo and Quasi-Monte Carlo Methods, 2000, Springer-Verlag, Berlin*, 86–102, 2002.
5. P. Varbanets, S. Varbanets. Exponential sums over the sequences of inversive congruential pseudorandom numbers with prime-power modulus. *VoronoÏ's impact on modern science*, Book 4(1):112–130, 2008.

Chaotic Modeling and Simulation (CMSIM) 1: 239–245, 2013

New vortex invariants in magneto-hydrodynamics and a related helicity theorem

Anatoliy K. Prykarpatsky[1] and Denis Blackmore[2]

[1] AGH University of Science and Technology, Krakow, Poland and
The Ivan Franko State Pedagogical University, Drohobych, Lviv region, Ukraine
(E-mail: pryk.anat@ua.fm)
[2] The NJIT, University Heights, Newark, 07102, NJ USA
(E-mail: deblac@m.njit.edu)

Long ago it was stated [7,5] that quantum vortices in superfluid helium can be studied either as open lines with their ends terminating on free surfaces of walls of the container or as closed curves. Nowadays the closed vortices are treated as topological objects equivalent to circles. The existence of structures such as knotted and linked vertex lines in the turbulent phase is almost obvious [12] and has forced researchers to develop new mathematical tools for their detailed investigation. In this proposed direction Z. Peradzyński [8] proved a new version of the Helicity theorem, based on differential-geometric methods applied to the description of the collective motion in the incompressible superfluid. The Peradzyński helicity theorem describes in a unique way, both the superfluid equations and the related helicity invariants, which are, in the conservative case, very important for studying the topological structure of vortices.

By reanalyzing the Peradzyński helicity theorem within the modern symplectic theory of differential-geometric structures on manifolds, we propose a new unified proof and give a magneto-hydrodynamic generalization of this theorem for the case of an incompressible superfluid flow. As a by-product, in the conservative case we construct a sequence of nontrivial helicity type conservation laws, which play a crucial role in studying the stability problem of a superfluid under suitable boundary conditions.

1 Symplectic and symmetry analysis

We consider a quasi-neutral superfluid contained in a domain $M \subset \mathbf{R}^3$ and interacting with a "frozen" magnetic field $B : M \longrightarrow \mathbf{E}^3$, where $\mathbf{E}^3 := (\mathbf{R}^3, < .,. >)$ is the standard three-dimensional Euclidean vector space with the scalar $< .,. >$ and vector "$\times$" products. The magnetic field is considered to be source-less and to satisfy the condition $B = \nabla \times A$, where $A : M \longrightarrow \mathbf{E}^3$ is

Received: 2 May 2012 / Accepted: 5 October 2012

ISSN 2241-0503

some magnetic field potential. The corresponding electric field $E : M \longrightarrow \mathbf{E}^3$, related with the magnetic potential, satisfies the necessary superconductivity conditions

$$E + u \times B = 0, \qquad \partial E/\partial t = \nabla \times B, \tag{1}$$

where $u : M \longrightarrow T(M)$ is the superfluid velocity.

Let ∂M denote the boundary of the domain M. The boundary conditions $\langle n, u\rangle|_{\partial M} = 0$ and $\langle n, B\rangle|_{\partial M} = 0$ are imposed on the superfluid flow, where $n \in T^*(M)$ is the vector normal to the boundary ∂M, considered to be almost everywhere smooth.

Then adiabatic magneto-hydrodynamics (MHD) quasi-neutral superfluid motion can be described, using (1), by the following system of evolution equations:

$$\begin{gathered} \partial u/\partial t = -\langle u, \nabla\rangle u - \rho^{-1}\nabla P + \rho^{-1}(\nabla \times B) \times B, \\ \partial\rho/\partial t = -\langle \nabla, \rho u\rangle, \qquad \partial\eta/\partial t = -\langle u, \nabla\eta\rangle, \qquad \partial B/\partial t = \nabla \times (u \times B), \end{gathered} \tag{2}$$

where $\rho : M \longrightarrow \mathbf{R}_+$ is the superfluid density, $P : M \longrightarrow \mathbf{E}^3$ is the internal pressure and $\eta : M \longrightarrow \mathbf{R}$ is the specific superfluid entropy. The latter is related to the internal MHD superfluid specific energy function $e = e(\rho, \eta)$ owing to the first law of thermodynamics:

$$T\, d\eta = de(\rho, \eta) - P\rho^{-2} d\rho, \tag{3}$$

where $T = T(\rho, \eta)$ is the internal absolute temperature in the superfluid. The system of evolution equations (2) conserves the total energy

$$H := \int_M \left[\frac{1}{2\rho}|\mu|^2 + \rho e(\rho, \eta) + \frac{1}{2}|B|^2\right] d^3x, \tag{4}$$

called the Hamiltonian, since the dynamical system (2) is a Hamiltonian system on the functional manifold $\mathcal{M} := C^\infty(M; T^*(M) \times \mathbf{R}^2 \times \mathbf{E}^3)$ with respect to the following [4] Poisson bracket:

$$\begin{aligned} \{f, g\} := \int_M \Big\{ & \langle \mu, [\tfrac{\delta f}{\delta \mu}, \tfrac{\delta g}{\delta \mu}]_c\rangle + \rho\left(\langle \tfrac{\delta g}{\delta \mu}, \nabla \tfrac{\delta f}{\delta \rho}\rangle - \langle \tfrac{\delta f}{\delta \mu}, \nabla \tfrac{\delta g}{\delta \rho}\rangle\right) \\ & + \eta\langle \nabla, (\tfrac{\delta g}{\delta \mu}\tfrac{\delta f}{\delta \eta} - \tfrac{\delta f}{\delta \mu}\tfrac{\delta g}{\delta \eta})\rangle + \langle B, [\tfrac{\delta g}{\delta \mu}, \tfrac{\delta f}{\delta B}]_c\rangle \\ & + \langle \tfrac{\delta f}{\delta B}, \langle B, \nabla\rangle \tfrac{\delta g}{\delta \mu}\rangle - \langle \tfrac{\delta g}{\delta B}, \langle B, \nabla\rangle \tfrac{\delta f}{\delta \mu}\rangle \Big\}\, dx, \end{aligned} \tag{5}$$

where we denoted by $\mu := \rho u \in T^*(M)$ the specific momentum of the superfluid motion and by $[.,.]_c$ the canonical Lie bracket of variational gradient vector fields:

$$[\frac{\delta f}{\delta \mu}, \frac{\delta g}{\delta \mu}]_c := \langle \frac{\delta f}{\delta \mu}, \nabla\rangle \frac{\delta g}{\delta \mu} - \langle \frac{\delta g}{\delta \mu}, \nabla\rangle \frac{\delta f}{\delta \mu} \tag{6}$$

for any smooth functionals $f, g \in \mathcal{D}(M)$ on the functional space $\mathcal{M}$. Moreover, as was shown in [4], the Poisson bracket (5) is, in reality, the canonical Lie–Poisson bracket on the dual space to the Lie algebra $\mathcal{G}$ of the semidirect product

of vector fields on M and the direct sum of functions, densities and differential one-forms on M. Namely, the specific momentum $\mu = \rho u \in T^*(M)$ is dual to vector fields, ρ is dual to functions, η is dual to densities and B is dual to the space of two-forms on M. Thus, the set of evolution equations (2) can be equivalently recast as follows:

$$\begin{aligned} \partial u/\partial t &= \{H, u\}, \qquad \partial \rho/\partial t = \{H, \rho\}, \\ \partial \eta/\partial t &= \{H, \eta\}, \qquad \partial B/\partial t = \{H, B\}. \end{aligned} \tag{7}$$

The Poisson bracket (5) can be rewritten for any $f, g \in \mathcal{D}(M)$ as

$$\{f, g\} = (Df, \vartheta\, Dg), \tag{8}$$

with $Df := \left(\frac{\delta f}{\delta \mu}, \frac{\delta f}{\delta \rho}, \frac{\delta f}{\delta \eta}, \frac{\delta f}{\delta B}\right) \in T^*(\mathcal{M})$ and $\vartheta : T^*(\mathcal{M}) \longrightarrow T(\mathcal{M})$, being the corresponding (modulo the Casimir functionals of bracket (5)) invertible [3] co-symplectic operator, satisfying the standard [10,2] properties

$$\vartheta^* = -\vartheta, \qquad \delta(\delta w, \wedge\, \vartheta^{-1} \delta w) = 0, \tag{9}$$

where the differential variation complex condition $\delta^2 = 0$ is assumed, the differential variation vector $\delta w := (\delta\mu, \delta\rho, \delta\eta, \delta B) \in T^*(\mathcal{M})$ and the symbol "$*$" denotes the conjugate mapping with respect to the standard bilinear convolution $(.,.)$ of the spaces $T^*(\mathcal{M})$ and $T(\mathcal{M})$. Note here that the second condition of (9) is equivalent [2,10] to the fact that the Poisson bracket (5) satisfies the Jacobi commutation condition. Thus, one can define the closed generalized variational differential two-form on $\mathcal{M}$

$$\omega^{(2)} := (\delta w, \wedge \vartheta^{-1}\, \delta w), \tag{10}$$

which provides the symplectic structure on the functional factor manifold $\mathcal{M}$ (modulo the Casimir functionals of bracket (5)). Owing now to the commutation property

$$[\partial/\partial t + L_u, L_v] = 0, \tag{11}$$

equivalent to the subgroup $\mathcal{D}_t$ and $\mathcal{D}_\tau$ commuting for any suitable $t, \tau \in \mathbf{R}$, from the invariance condition

$$\partial \rho/\partial \tau = 0, \tag{12}$$

we deduce that the quantities

$$\gamma_n := L_v^n \gamma \tag{13}$$

for all $n \in \mathbf{Z}_+$ are invariants of the MHD superfluid flow (2) if the density $\gamma \in \Lambda^3(M)$ is also an invariant on M.

We construct the following new functionals on the functional manifold $\mathcal{M}$

$$\tilde{H}_n := \int_M \tilde{\gamma}_n\, d^3x = \int_M \rho L_v^n (\rho^{-1} \langle B, A \rangle)\, d^3x \tag{14}$$

for all $n \in \mathbf{Z}_+$, which are invariants of our MHD superfluid dynamical system (2). In particular, when $n = 0$ we obtain the well-known [4] magnetic helicity invariant

$$\tilde{H}_0 = \int_M \langle A, \nabla \times A \rangle \, d^3x, \tag{15}$$

which exists independently of boundary conditions, imposed on the MHD superfluid flow equations (2).

The result obtained above can be formulated as the following theorem.

Theorem 1. *The functionals (14), where the Lie derivative L_v is taken along the magnetic vector field $v = \rho^{-1}B$, are global invariants of the system of compressible MHD superfluid and superconductive equations (2).*

Below we proceed to a symmetry analysis of the incompressible superfluid dynamical system and construct the related local and global new helicity invariants. The case of superfluid hydrodynamical flows [9] is of great interest for many applications owing to the very nontrivial dynamical properties of so-called vorticity structures appearing in the motion.

2 The incompressible superfluid: symmetry analysis and conservation laws

The helicity theorem result of [8], where the kinematic helicity invariant

$$H_0 := \int_M \langle u, \nabla \times u \rangle \, d^3x \tag{16}$$

was derived, employed differential-geometric tools in Minkowski space in the case of an incompressible superfluid in the absence of a magnetic field ($B = 0$). We shall now describe its general dynamical symmetry nature. The governing equations are

$$\partial u/\partial t = -\langle u, \nabla \rangle u + \rho^{-1} \nabla P, \qquad \partial \rho/\partial t + \langle u, \nabla \rho \rangle = 0, \qquad \langle \nabla, u \rangle = 0, \tag{17}$$

where the density conservation properties

$$(\partial/\partial t + L_u)\rho = 0, \qquad (\partial/\partial t + L_u) d^3x = 0 \tag{18}$$

hold for all suitable $t \in \mathbf{R}$. Define now the vorticity vector $\xi := \nabla \times u$ and find from (17) that it satisfies the vorticity flow equation

$$\partial \xi/\partial t = \nabla \times (u \times \xi). \tag{19}$$

Actually, the first equation of (17) can be rewritten as

$$\partial u/\partial t = u \times (\nabla \times u) - \rho^{-1} \nabla P - \frac{1}{2} \nabla |u|^2. \tag{20}$$

Then, applying the operation "$\nabla \times \cdot$" to (20), one easily obtains the vorticity equation (19). Moreover, equation (19) can be recast in the equivalent form

$$\partial \xi/\partial t + \langle u, \nabla \rangle \xi = \langle \xi, \nabla \rangle u, \tag{21}$$

which allows a new dynamical symmetry interpretation. Now, define $\beta^{(1)} \in \Lambda^1(M)$ as the one–form

$$\beta^{(1)} := \langle u, dx \rangle \tag{22}$$

and readily conclude that

$$(\partial/\partial t + L_u)\beta^{(1)} = -\rho^{-1} dP + \frac{1}{2} d|u|^2 = d(\rho^{-1} P + \frac{1}{2}|u|^2). \tag{23}$$

We have shown that the following generalized functionals

$$H_n := \int_M \rho L_v^n (u \times \xi)\, d^3x \tag{24}$$

for all $n \in \mathbf{Z}_+$are new helicity invariants for (17). Notice here that all of the constraints imposed above on the vorticity vector $\xi = \nabla \times u$ are automatically satisfied if the condition $supp\ \xi \cap \partial M = \emptyset$ holds. The result obtained can be summarized as follows.

Theorem 2. *Assume that an incompressible superfluid, governed by the set of equations (17) in a domain $M \subset \mathbf{E}^3$, possesses the vorticity vector $\xi = \nabla \times u$, which satisfies the boundary constraints $L^n_{\rho^{-1}\xi}\xi|_{\partial M}$ for all $n \in \mathbf{Z}_+$. Then all of the functionals (24) are generalized helicity invariants of (17).*

The results obtained above allow some interesting modifications. To present them in detail, observe that equality (23) can be rewritten as

$$(\partial/\partial t + L_u)\beta^{(1)} - dh = (\partial/\partial t + L_u)\tilde{\beta}^{(1)} = 0, \tag{25}$$

where, by definition,

$$h := \rho^{-1} P + \frac{1}{2}|u|^2, \qquad \tilde{\beta}^{(1)} := \langle u - \nabla\varphi, dx \rangle, \tag{26}$$

and the scalar function $\varphi : M \longrightarrow \mathbf{R}$ is chosen in such a way that

$$(\partial/\partial t + L_u)\varphi = \nabla h. \tag{27}$$

Then, obviously, one obtains the additional equation

$$(\partial/\partial t + L_u) d\tilde{\beta}^{(1)} = 0, \tag{28}$$

following from the commutation property $[d, \partial/\partial t + L_u] = 0$. Then, we see that the density $\tilde{\lambda} := \tilde{\beta}^{(1)} \wedge d\tilde{\beta}^{(1)} \in \Lambda^3(M)$ satisfies the condition

$$(\partial/\partial t + L_u)\tilde{\mu} = 0, \tag{29}$$

for all $t \in \mathbf{R}$. A similar result holds for densities $\tilde{\lambda}_n := L_v^n \tilde{\lambda} \in \Lambda^3(M)$, $n \in \mathbf{Z}_+$; namely,

$$(\partial/\partial t + L_u)\tilde{\lambda}_n = 0, \tag{30}$$

owing to the commutation property (11). Therefore, the following functionals on the corresponding functional manifold $\mathcal{M}$ are invariants of the superfluid flow (2):

$$\Upsilon_n := \int_M \tilde{\lambda}_n = \int_{D_t} \rho L^n_{\rho^{-1}\xi} \langle (u - \nabla\varphi), \xi \rangle \, d^3x \tag{31}$$

for all $n \in \mathbf{Z}_+$ and an arbitrary domain $D_t \subset M$, independent of boundary conditions, imposed on the vorticity vector $\xi = \nabla \times u$ on ∂M. Notice here that only the invariants (31) strongly depend on the function $\varphi : M \longrightarrow \mathbf{R}$, implicitly depending on the velocity vector $u \in T(M)$. It should be mentioned here that the practical importance of the constructed invariants (31) remains to be fully clarified.

3 Conclusions

The symplectic and symmetry analysis of compressible MHD super-fluids developed above, appears to be an effective approach for constructing the related helicity type conservation laws, which are generally important for practical applications. In particular, these conserved quantities play a decisive role [4,1] when studying the stability of MHD superfluid flows under special boundary conditions. Some of the results in this direction can also be obtained making use of group-theoretical and topological tools developed in [1,13,11], where the importance of the basic group of diffeomorphisms $Diff(M)$ of a manifold $M \subset \mathbf{R}^3$ and its differential-geometric characteristics were shown in considerable detail.

Acknowledgments

One of authors (A.P.) is cordially thankful to Prof. J. Slawianowski (IPPT of Warsaw, Poland) and Prof. Z. Peradzyński (Warsaw University, Poland) for their invitation to present the results of this work for their Seminar, their hospitality, and the fruitful discussions and the many useful comments they made.

References

1. Arnold V.I. and Khesin B.A. Topological methods in hydrodynamics. Springer, NY, 1998.
2. Abraham R. and Marsden J. Foundations of mechanics. Cummings Publ., NY, 1978.
3. Holm D. and Kupershmidt B. Poisson structures of superfluids. Phys. Lett., 91A (1982), pp. 425–430.
4. Holm D., Marsden J., Ratiu T. and Weinstein A. Nonlinear stability of fluid and plasma equilibria. Physics Reports, 123/(1 and 2) (1985), pp. 1–116.
5. Moffat H.K. The degree of knottedness of tangled vortex lines. Journal of Fluid Mechanics, 35/1 (1969), pp. 117–129.
6. Owczarek R. Topological defects in superfluid Helium. Int. J. Theor. Phys., 30/12 (1991), pp. 1605–1612.

7.Owczarek R. Frames and fermionic excitations of vortices in superfluid Helium. J. Phys: Condens. Matter, 5 (1993), pp. 8793–8798.
8.Peradzyński Z. Helicity theorem and vertex lines in superfluid ^{4}He. Int. J. Theor. Phys., 29/11 (1990), pp. 1277–1284.
9.Putterman S.J. Superfluid Hydrodynamics, North Holland, Amsterdam, 1974.
10.Prykarpatsky A. and Mykytiuk I. Algebraic integrability of nonlinear dynamical systems on manifolds: classical and quantum aspects. Kluwer Academic Publishers, the Netherlands, 1998.
11.Prykarpatsky A. and Zagrodziński J. Dynamical aspects of Josephson type media, Ann. of Inst. H. Poincaré, Phys. Theorique, 70/5 (1999), pp. 497–524.
12.Schwarz K.W. Physical Rev. B, 38 (1988), pp. 2398–2417.
13.Troshkin O.V. Nontraditional methods in mathematical hydrodynamics. Transl. Math. Monogr., AMS, Providence, v.114, 1995.