IUTAM Symposium on 50 Years of Chaos : Applied and Theoretical
Kyoto, Japan, November 28 - December 2, 2011

Binary Sequences Using Chaotic Dynamics and Their Applications to Communications

Tohru Kohda[1], Kazuyuki Aihara[2]

[1]*Department of Informatics, Kyushu University, Motooka 744,Nisi-ku,Fukuoka, 819-0395, Japan,*
kohda@inf.kyushu-u.ac.jp

[2]*Institute of Industrial Science, The University of Tokyo, 4-6-1,Komaba Megro-ku, Tokyo, 153-8505, Japan,*
aihara@sat.t.u-tokyo.ac.jp

Shannon's communication system has three essential parts: (1) source or transmitter, (2) receiver or sink, and (3) channel or transmission network. Since the usual or real communication systems are of a *statistical* nature, the performance of the system can never be described in a *deterministic* sense; rather, it is always given in *statistical* terms. A source is a device that selects and transmits sequences of symbols from a given alphabet. The reason why we discuss several close relationships between information sources and chaos is that chaos is both of a *deterministic* and of a *probabilistic* nature. An information source is derived from a Markov chain producing a sequence of random variables $\cdots Z_{t-2}Z_{t-1}Z_tZ_{t+1}Z_{t+2}\cdots$. The simplest model of information sources is the one that produces a sequence of independent, identically distributed (or briefly, i.i.d) random variables. Such a sequence has found significant applications in modern digital communication systems such as in spread spectrum (SS) communication systems or cryptosystems as well as in computational applications requiring random numbers. Such a binary sequence can be generated in various ways. Nevertheless, linear feedback shift register (LFSR) sequences which have already been thoroughly investigated based on finite field theory are employed in nearly all the methods. Bernoulli shift and its associated binary function as *theoretic models of coin tossing* can produce a sequence of i.i.d. binary random variables (BRVs). Ulam and von Neumann [12] pointed out the logistic map, the most famous chaotic one stands as a good candidate for pseudo-random number generators (PRNGs). Furthermore, a particularly important finding in Kalman's early study [3] is that a *random* process can be generated by *deterministic* means of a nonlinear sampled-data system. This suggests an important role of "*chaotic dynamics.*"

Our review of statistical properties of sequences of BRVs generated by chaotic dynamics are twofold:

1. **generation method of sequences of i.i.d. BRVs**: Define a piecewise monotonic (PM) onto ergodic map $\tau(\omega) : J = [d, e] \to J$ that satisfies the following conditions:
   - **i)** there is a partition $d = d_0 < \cdots < d_{N_\tau} = e$ of J such that for each integer $i = 1, \cdots, N_\tau$, $(N_\tau \geq 2)$ the restriction of $\tau(\omega)$ to the interval $J_i = [d_{i-1}, d_i)$, denoted by $\tau_i(\omega)$, is a C^2 function; as well as
   - **ii)** $\tau(J_i) = (d, e)$;
   - **iii)** $\tau(\omega)$ has a unique absolutely continuous invariant (ACI) measure, denoted by $f^*(\omega)d\omega$.

   Several definitions are necessary for our discussion.

   Definition 1 *[10] The Perron-Frobenius operator P_τ acting on the function of bounded variation $H(\omega) \in L^\infty$ for $\tau(\omega)$ is defined as $P_\tau H(\omega) = \dfrac{d}{d\omega}\displaystyle\int_{\tau^{-1}([d,\omega])} H(y)dy = \sum_{i=1}^{N_\tau} |g_i'(\omega)| H(g_i(\omega))$, where $g_i(\omega) = \tau_i^{-1}(\omega)$ is the $i-$th preimage of ω.*

   Definition 2 *[8] The map $\tau(\omega)$ with its ACI measure $f^*(\omega)d\omega$ is said to satisfy equidistributivity property (EDP) if the relation $|g_i'(\omega)| f^*(g_i(\omega)) = \dfrac{f^*(\omega)}{N_\tau}$, $\omega \in J$, $1 \leq i \leq N_\tau$ holds.*

   Definition 3 *[8] If for a class of maps with EDP its associated function $F(\cdot)$ satisfies $\dfrac{1}{N_\tau}\displaystyle\sum_{i=1}^{N_\tau} F(g_i(\omega)) = \mathbf{E}[F]$, $\omega \in J$, then $F(\cdot)$ is said to satisfy the constant summation property (CSP), where $\mathbf{E}[F]$ is the ensemble average of $F(\omega)$, defined as $\mathbf{E}[F] = \int_I F(\omega) f^*(\omega)d\omega$.*

   Consider two sequences $\{G(\tau^n(\omega))\}_{n=0}^\infty$ and $\{H(\tau^n(\omega))\}_{n=0}^\infty$, where $G(\omega), H(\omega) \in L^\infty$. The second-order cross-covariance function between these sequences from a seed $\omega = \omega_0$ is defined by $\rho(\ell, G, H) = \int_I (G(\omega) - \mathbf{E}[G]) \cdot (H(\tau^\ell(\omega)) - \mathbf{E}[H]) f^*(\omega)d\omega$, where $\ell = 0, 1, 2, \cdots$. Then the $\tau(\omega)$ satisfying EDP can generate a sequence of i.i.d. BRVs if its associated binary function $F(\cdot)$ satisfies CSP[8, 5]. Fortunately, many well-known 1-dimensional maps satisfy EDP. The Bernoulli map, logistic map and Chebyshev polynomial are good examples. CSP is applicable to a sufficent condition for independence of the N-th power sequence $\{X_n^N\}_{n=0}^\infty$ of a real-valued trajectory generated by Chebyshev polynomial of degree

p, defined as $\omega_{n+1} = T_p(\omega_n) = \cos(p\cos^{-1}\omega_n), \omega_n \in [-1,1]$, *i.e.* $X_n = \omega_n$ too [8, 9]. Incidentally, CSP together with divisible property of Chebyshev polynomials with respect to the degree, defined as $P_{T_k}[T_n(\omega)f^*(\omega)] = T_{\frac{n}{k}}(\omega)f^*(\omega)$ for $k \mid n$, or 0 for $k \nmid n$ lead us to get a cryptanalysis [1] for a public-key encryption based on Chebyshev polynomials, proposed by Kocarev, Sterjev, and Makuraui [4]. Moreover, CSP is useful in discussing independence of 3-dimensional i.i.d. binary random vectors governed by Jacobian elliptic space curve dynamics, induced by Jacobian elliptic Chebyshev map, defined as $\omega_{n+1} = \mathrm{cn}(p\,\mathrm{cn}^{-1}(\omega_n, k), k)$, $\omega_n \in [-1,1]$, its derivative and second derivative, where $\mathrm{cn}(u,k)$ denotes the Jacobian elliptic function of modulus k. A mapping of the space curve with its coordinates, *e.g.* X, Y and Z, onto itself is introduced which defines 3 projective onto mappings, represented in the form of rational functions of $\{x_n, y_n, z_n\}_{n=0}^{\infty}$. Such mappings with their ACI measures as functions of elliptic integrals and their associated binary function can generate a 3-dimensional sequence of i.i.d. binary random vectors [6].

2. **designs of SS codes generated by a Markov chain**: Recently Mazzini, Rovatti, and Setti [11] have extensively discussed codes generated by piecewise-linear Markov maps as candidates of SS codes for chip-asynchronous DS/CDMA systems. In particular, their discussions on Markov versus i.i.d. codes in terms of bit error ratio (BER) temporarily astonished researchers in communication engineering and applied mathematics who believed previously that sequences of i.i.d. BRVs were best for BER. Based on the theory of Markov chains , we have given simple expressions for estimating two common performance measures of SS codes generated by a 2-state Markov chain with its nonunit eigenvalue λ to reduce the magnitude of (1) cross-interferences [7] and (2) self-ones [2] from other channels without the assumption of synchronization achievement. Such expressions lead the conclusion that SS codes generated by a Markov chain with negative λ look promising, *i.e.* Kalman's simple embedding of an N-state Markov chain with prescribed transition probabily matrix, defined as $P = \{p_{ij}\}_{i,j=1}^{N}$, $0 < p_{ij} < 1$, $1 < i,j < N$ into a picewise-linear map plays an important role in designing SS codes with negative eigenvalue of matrix P.

Acknowledgments

This research is supported by the Japan Society for the Promotion of Science (JSPS) through its "Funding Program for World-Leading Innovative R&D on Science and Technology (FIRST Program)".

References

[1] Hane,R. and Kohda, T., "Cryptanalysis of Chaos-based Elgamal Public-key Encryption," *International Journal of Bifurcation and Chaos*, **17**-10, pp.3619-3623, 2007.

[2] Jitsumatu,Y. and Kohda, T., "Bit error rate of incompletely synchronised correlator in asynchrnous DS/CDMA system using SS Markovian codes", *Electronics Letters,IEE*, **38**-9, 415-416, 2002.

[3] Kalman, R. E., "Nonlinear aspects of sampled-data control systems", *Proc. Symp. Nonlinear Circuit Analysis VI*, 273–313, 1956.

[4] Kocarev, L., Sterjev, M., and Makuraui, J., "Public-key Encryption based on Chebyshev polynomials," in *Proc.ISCAS'03, Int.Symp. Circuits and Systems,* **3**, 28-31, 2003.

[5] Kohda,T., "Information Sources using chaotic dynamics," *Proceedings of the IEEE*, **90**-5, 641-661, 2002.

[6] Kohda,T., "3-dimensional i.i.d. binary random vectors governed by Jacobian elliptic space curve dynamics," *Advanced Studies in Pure Mathematics*, **53**, Advances in Discrete Dynamical Systems, 95-112, 2009.

[7] Kohda,T. and Fujisaki,H., "Variances of multiple acess interference : code average against data average", *Electronics Letters, IEE*, **36**-20, 1717-1719, 2000.

[8] Kohda.T. and Tsuneda, A., "Statistics of Chaotic Binary Sequences," *IEEE Transactions on Information Theory*, **43**-1, 104-112, 1997.

[9] Kohda,T., Tsuneda, A., and Lawrance, A.L., "Correlational Properties of Chebyshev Chaotic Sequences," *Journal of Time Series Analysis*, **21**-2, 181-191, 2000.

[10] Lasota,A. and Mackey, M. C., *Chaos, Fractals, and Noise*, Springer-Verlag, 1994.

[11] Mazzini, G., Setti, G., and Rovatti, R., "Chaotic complex spreading sequences for asynchronous DS-CDMA part I : system modeling and results", *IEEE Trans. Circuit Syst.*, **CAS-44**, no.10, 937–947, 1997.

[12] Ulam, S.M. and Von Neumann, J., "On combination of stochastic and deterministic processes," *Bull.Amer.Math.Soc.*, **53**, 1120, 1947.