<table>
<thead>
<tr>
<th>Title</th>
<th>Contributed Talk 2: Binary Sequences Using Chaotic Dynamics and Their Applications to Communications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>Kohda, Tohru; Aihara, Kazuyuki</td>
</tr>
<tr>
<td>Citation</td>
<td>IUTAM Symposium on 50 Years of Chaos: Applied and Theoretical (2011): 28-29</td>
</tr>
<tr>
<td>Issue Date</td>
<td>2011-12</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://hdl.handle.net/2433/163146">http://hdl.handle.net/2433/163146</a></td>
</tr>
<tr>
<td>Type</td>
<td>Book</td>
</tr>
<tr>
<td>Textversion</td>
<td>publisher</td>
</tr>
</tbody>
</table>

Kyoto University
Binary Sequences Using Chaotic Dynamics and Their Applications to Communications

Tohru Kohda\textsuperscript{1}, Kazuyuki Aihara\textsuperscript{2}

\textsuperscript{1}Department of Informatics, Kyushu University, Motoooka, Fukuoka, 819-0395, Japan, kohda@inf.kyushu-u.ac.jp

\textsuperscript{2}Institute of Industrial Science, The University of Tokyo, 4-6-1, Komaba Meguro-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 (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\textsuperscript{12} pointed out the logistic map, the most famous chaotic one stands as a good candidate for nature, the performance of the system can never be described in a deterministic sense.

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 $d = d_0 < \cdots < d_{N_r} = e$ of $J$ such that for each integer $i = 1, \cdots, N_r$, $(N_r \geq 2)$ 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) $\tau_i(J_i) = (d, e)$;
   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 $P_r$ acting on the function of bounded variation $H(\omega) \in L^\infty$ for $\tau(\omega)$ is defined as

$P_rH(\omega) = \frac{d}{d\omega} \int_{\tau^{-1}(\{d,\omega\})} H(y)dy = \sum_{i=1}^{N_r} g_i(\omega)|H(g_i(\omega))|$, where $g_i(\omega) = \tau_i^{-1}(\omega)$ is the $i$-th preimage of $\omega$.

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 $|g_i(\omega)|f^*(g_i(\omega)) = \frac{f_i^*(\omega)}{N_r}$, $\omega \in J$, $1 \leq i \leq N_r$ holds.

Definition 3 [8] If for a class of maps with EDP its associated function $F(\cdot)$ satisfies

$\frac{1}{N_r} \sum_{i=1}^{N_r} F(g_i(\omega)) = E[F], \omega \in J$, then $F(\cdot)$ is said to satisfy the constant summation property (CSP), where $E[F]$ is the ensemble average of $F(\omega)$, defined as $E[F] = \int_{J} F(w)f^*(w)d\omega$.

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 $\rho(\ell, G, H) = \int_{J} (G(\omega) - E[G]) \cdot (H(\tau^\ell(\omega)) - E[H])f^*(\omega)d\omega$, 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\textsuperscript{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 sufficient 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
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)".

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


