2004 International Symposium on Nonlinear
Theory and its Applications (NOLTA2004)
Fukuoka, Japan, Nov. 29 - Dec. 3, 2004

On Statistical Properties of Modulo-p Added p-Ary Sequences

Akio Tsuneda

Department of Electrical and Computer Engineering, Kumamoto University
2-39-1 Kurokami, Kumamoto 860-8555, Japan
Email: tsuneda@eecs.kumamoto-u.ac.jp

Abstract—Some statistical analyses of modulo-2 added binary sequences are generalized to modulo-p added p-ary sequences. First, we theoretically evaluate statistics of sequences obtained by modulo-p addition of two general p-ary random variables. Next, we consider statistics of modulo-p added chaotic p-ary sequences generated by a class of one-dimensional chaotic maps.

1. Introduction

Binary sequences are the most fundamental random numbers and have been extensively used in several applications such as spread-spectrum CDMA communications and cryptosystems. M-sequences, Kasami sequences, and Gold sequences, all of which can be generated by linear feedback shift registers (LFSRs), are well known as conventional binary sequences [1]. It is also well known that chaos phenomena can be used to generate random numbers and have been studied by many researchers, some of which are also engaged in binary sequences called *chaotic binary sequences* [2].

Since modulo-2 addition is one of fundamental operations for binary variables, we have studied statistical properties of modulo-2 added binary sequences [3]. We have shown that if one sequence is balanced and *i.i.d. (independent and identically distributed)*, then the modulo-2 added sequence is also balanced and i.i.d., which is independent of the other binary sequence. Furthermore, we have also given some conditions to generate two modulo-2 added sequences which are completely uncorrelated to each other from a single chaotic real-valued sequence.

In this paper, we discuss statistical properties of sequences obtained by modulo-p addition of two p-ary sequences, that is, we generalize some results for modulo-2 added binary sequences to the p-ary case. First, we theoretically evaluate statistics of sequences obtained by modulo-p addition of two general p-ary random variables. Under an assumption, we show that if one sequence is k-*distributed*, then the modulo-p added sequence is also k-distributed, which is independent of the other sequence.

Next, we consider statistics of modulo-p added chaotic p-ary sequences generated by one-dimensional chaotic maps. Our theoretical evaluation based on the theory of chaotic dynamical systems [2],[4] shows that if one sequence is balanced and i.i.d., then the modulo-p added sequence is also balanced and i.i.d., which is independent of the other chaotic p-ary sequence. Furthermore, some conditions for generating two modulo-p added sequences which are completely independent of each other from a single chaotic real-valued sequence are also given.

2. Synthesis of General p-ary Sequences by Modulo-p Addition

Let $\{X_n\}_{n=0}^{\infty}$ be a sequence of p-ary random variables, where $X_n \in \{0, 1, \cdots, p-1\}$ and p is a positive integer greater than 1. We denote a k-digit p-ary number by $\langle a_1 a_2 \cdots a_k \rangle$, where $a_i \in \{0, 1, \cdots, p-1\}$. A p-ary sequence $\{X_n\}_{n=0}^{\infty}$ is said to be *k-distributed* if

$$\Pr(\langle X_n X_{n+1} \cdots X_{n+k-1} \rangle = \langle q_1 q_2 \cdots q_k \rangle) = \frac{1}{p^k} \quad (1)$$

for all k-digit p-ary numbers $\langle q_1 q_2 \cdots q_k \rangle$ [5], where $\Pr(A)$ denotes the probability of an event A. When $k = 1$, the sequence is just said to be *balanced*. We consider a p-ary sequence $\{Z_n\}_{n=0}^{\infty} = \{X_n \oplus Y_n\}_{n=0}^{\infty}$, where

$$a \oplus b \equiv (a+b) \mod p, \quad a, b \in \{0, 1, \cdots, p-1\}. \quad (2)$$

Theorem 1: Let $\{X_n\}_{n=0}^{\infty}$ and $\{Y_n\}_{n=0}^{\infty}$ be two p-ary sequences which are statistically independent of each other. A p-ary sequence $\{Z_n\}_{n=0}^{\infty} = \{X_n \oplus Y_n\}_{n=0}^{\infty}$ is k-distributed if $\{X_n\}_{n=0}^{\infty}$ or $\{Y_n\}_{n=0}^{\infty}$ is k-distributed.
Proof: Denote X_n and Y_n by

$$X_n = \sum_{i=0}^{p-1} i S_i(X_n), \quad Y_n = \sum_{j=0}^{p-1} j S_j(Y_n), \quad (3)$$

where

$$S_i(x) = \begin{cases} 1 & (x = i) \\ 0 & (x \neq i). \end{cases} \quad (4)$$

Noting that

$$Z_n = \sum_{i=0}^{p-1} \sum_{j=0}^{p-1} (i \oplus j) S_i(X_n) S_j(Y_n), \quad (5)$$

we can write

$$\Pr(Z_n = q) = \sum_{i=0}^{p-1} \sum_{j=0}^{p-1} S_q(i \oplus j) E[S_i(X_n) S_j(Y_n)], \quad (6)$$

where $E[\cdot]$ denotes the expectation. Thus we can also write

$$\Pr(\langle Z_n Z_{n+1} \cdots Z_{n+k-1} \rangle = \langle q_1 q_2 \cdots q_k \rangle)$$

$$= E\left[\sum_{i_1=0}^{p-1}\sum_{j_1=0}^{p-1} S_{q_1}(i_1 \oplus j_1)S_{i_1}(X_n)S_{j_1}(Y_n)\right.$$
$$\sum_{i_2=0}^{p-1}\sum_{j_2=0}^{p-1} S_{q_2}(i_2 \oplus j_2)S_{i_2}(X_{n+1})S_{j_2}(Y_{n+1})$$
$$\left.\cdots \sum_{i_k=0}^{p-1}\sum_{j_k=0}^{p-1} S_{q_k}(i_k \oplus j_k)S_{i_k}(X_{n+k-1})S_{j_k}(Y_{n+k-1})\right]$$
$$= \sum_{j_1,j_2,\cdots,j_k} E[S_{j_1}(Y_n)S_{j_2}(Y_{n+1})\cdots S_{j_k}(Y_{n+k-1})]$$
$$\sum_{i_1,i_2,\cdots,i_k} S_{q_1}(i_1 \oplus j_1)S_{q_2}(i_2 \oplus j_2)\cdots S_{q_k}(i_k \oplus j_k)$$
$$E[S_{i_1}(X_n)S_{i_2}(X_{n+1})\cdots S_{i_k}(X_{n+k-1})]. \quad (7)$$

Assume that $\{X_n\}_{n=0}^{\infty}$ is k-distributed. Then we have

$$\Pr(\langle X_n X_{n+1}\cdots X_{n+k-1}\rangle = \langle i_1 i_2 \cdots i_k\rangle)$$
$$= E[S_{i_1}(X_n)S_{i_2}(X_{n+1})\cdots S_{i_k}(X_{n+k-1})] = \frac{1}{p^k}. \quad (8)$$

It is obvious that

$$\sum_{i=0}^{p-1} S_q(i \oplus j) = 1 \text{ for any } q \text{ and } j. \quad (9)$$

Furthermore, we also have

$$\sum_{j_1,j_2,\cdots,j_k} E[S_{j_1}(Y_n)S_{j_2}(Y_{n+1})\cdots S_{j_k}(Y_{n+k-1})] = 1 \quad (10)$$

because this means the total probability of all possible events $\langle Y_n Y_{n+1}\cdots Y_{n+k-1}\rangle = \langle j_1 j_2 \cdots j_k\rangle$ which are mutually exclusive. Using eqs.(7)–(10), we have

$$\Pr(\langle Z_n Z_{n+1}\cdots Z_{n+k-1}\rangle = \langle q_1 q_2 \cdots q_k\rangle) = \frac{1}{p^k} \quad (11)$$

for any $\langle q_1 q_2 \cdots q_k\rangle$, which is independent of the statistics of $\{Y_n\}_{n=0}^{\infty}$. This completes the proof.

3. Modulo-p Added Chaotic p-Ary Sequences

3.1. Preliminaries

The one-dimensional nonlinear difference equation defined by

$$x_{n+1} = \tau(x_n),\ x_n \in \Omega = [d, e],\ n = 0, 1, 2, \cdots, \quad (12)$$

can produce a *chaotic* real-valued orbit $\{x_n\}_{n=0}^{\infty}$. We also denote x_n by $\tau^n(x)$, where $x = x_0$ is called a *seed*. For an integrable function $G(x)$, the expectation of $\{G(x_n)\}_{n=0}^{\infty}$ is given by

$$E[G] = \int_{\Omega} G(x)f^*(x)dx \quad (13)$$

under the assumption that $\tau(\cdot)$ is mixing on Ω with respect to an absolutely continuous invariant measure, denoted by $f^*(x)dx$.

We now define the Perron-Frobenius operator P_τ of the map τ with an interval $I = [d, e]$ by

$$P_\tau G(x) = \frac{d}{dx}\int_{\tau^{-1}([d,x])} G(y)dy \quad (14)$$

which can be rewritten as

$$P_\tau G(x) = \sum_{r=1}^{N_\tau} |g_r'(x)| G(g_r(x)) \quad (15)$$

for piecewise monotonic onto maps with N_τ subintervals, where $g_r(x)$ is the r-th preimage of the map $\tau(\cdot)$ [4]. This operator is powerful in evaluating the statistical properties because it has the following important property:

$$\int_{\Omega} G(x)P_\tau\{H(x)\}dx = \int_{\Omega} G(\tau(x))H(x)dx. \quad (16)$$

Next, let us consider a chaotic p-ary sequence $\{B(x_n)\}_{n=0}^{\infty}$ obtained from a chaotic real-valued orbit $\{x_n\}_{n=0}^{\infty}$, where $B(\cdot) \in \{0, 1, \cdots, p-1\}$. Let $\{I_i\}_{i=0}^{p-1}$ be a set of p subintervals of a chaotic map satisfying

$$I_i \cap I_j = \phi\ \ (i \neq j), \quad \bigcup_{i=0}^{p-1} I_i = \Omega. \quad (17)$$

We define a p-ary function by

$$B(x) = \sum_{i=0}^{p-1} iQ_{I_i}(x), \quad (18)$$

where $Q_I(x)$ is the indicator function defined by

$$Q_I(x) = \begin{cases} 1 & (x \in I) \\ 0 & (x \notin I). \end{cases} \quad (19)$$

It should be noted that

$$\Pr(B(x_n) = i) = E[Q_{I_i}]. \quad (20)$$

A sufficient condition for such a p-ary sequence $\{B(x_n)\}_{n=0}^{\infty}$ to be i.i.d. is given by [2],[6]

$$P_\tau\{Q_{I_i}(x)f^*(x)\} = E[Q_{I_i}]f^*(x) \text{ for all } i \quad (21)$$

which, in conjunction with eq.(16), gives

$$\Pr(\langle B(x_n)B(x_{n+\ell_1})\cdots B(x_{n+\ell_{k-1}})\rangle = \langle i_1 i_2 \cdots i_k\rangle)$$
$$= E[Q_{I_{i_1}}(x)Q_{I_{i_2}}(\tau^{\ell_1}(x))\cdots Q_{I_{i_k}}(\tau^{\ell_{k-1}}(x))]$$
$$= E[Q_{I_{i_1}}]E[Q_{I_{i_2}}]\cdots E[Q_{I_{i_k}}], \quad (22)$$

where $k \geq 1$, $\ell_0 = 0$, and $1 \leq \ell_1 < \ell_2 < \cdots < \ell_{k-1}$. Furthermore, if $E[Q_{I_i}] = \frac{1}{p}$ for all i, we have

$$\Pr(\langle B(x_n)B(x_{n+\ell_1})\cdots B(x_{n+\ell_{k-1}})\rangle = \langle i_1 i_2 \cdots i_k\rangle)$$
$$= \frac{1}{p^k} \quad (23)$$

which implies that the sequence is k-distributed. It is easy to show that the 2nd-order auto-correlation function defined by

$$C(\ell; B) = E[(B(x_n) - E[B])(B(x_{n+\ell}) - E[B])] \quad (24)$$

is 0 for $\ell \geq 1$ if the sequence is i.i.d.

3.2. Auto-Correlation Property

Let $\{B(x_n)\}_{n=0}^{\infty}$ and $\{C(x_n)\}_{n=0}^{\infty}$ be two chaotic p-ary sequences generated from a common seed x, where $C(x)$ is defined by

$$C(x) = \sum_{j=0}^{p-1} jQ_{J_j}(x), \tag{25}$$

where $\{J_j\}_{j=0}^{p-1}$ also satisfies the condition given by eq.(17). Now consider a new p-ary sequence $\{D(x_n)\}_{n=0}^{\infty}$ obtained by modulo-p addition such that

$$\begin{aligned} D(x) &= B(x) \oplus C(\tau^m(x)) \quad (m \geq 1), \\ &= \sum_{i=0}^{p-1}\sum_{j=0}^{p-1}(i \oplus j)Q_{I_i}(x)Q_{J_j}(\tau^m(x)). \end{aligned} \tag{26}$$

Theorem 2: If $\{I_i\}_{i=0}^{p-1}$ satisfies eq.(21) and $E[Q_{I_i}] = \frac{1}{p}$ for all i, then $\{D(x_n)\}_{n=0}^{\infty}$ is balanced and i.i.d., that is, a k-distributed p-ary sequence as well as $\{B(x_n)\}_{n=0}^{\infty}$, which is independent of $C(\cdot)$ (*i.e.*, $\{J_j\}_{j=0}^{p-1}$).
Proof: First, we define

$$\widehat{Q}_q(x) = \sum_{i=0}^{p-1}\sum_{j=0}^{p-1} S_q(i \oplus j)Q_{I_i}(x)Q_{J_j}(\tau^m(x)). \tag{27}$$

Then we can rewrite $D(x)$ as

$$D(x) = \sum_{q=0}^{p-1} q\widehat{Q}_q(x). \tag{28}$$

Since $\widehat{Q}_q(x)$ corresponds to the indicator function $Q_I(x)$ for $B(x)$ or $C(x)$, the sufficient condition for $\{D(x_n)\}_{n=0}^{\infty}$ to be i.i.d. is given by

$$P_\tau\{\widehat{Q}_q(x)f^*(x)\} = E[\widehat{Q}_q]f^*(x) \ \text{ for all } q. \tag{29}$$

Thus we consider $P_\tau\{\widehat{Q}_q(x)f^*(x)\}$ as follows. From eq.(15), we can write

$$\begin{aligned} &P_\tau\{\widehat{Q}_q(x)f^*(x)\} \\ &= \sum_{i=0}^{p-1}\sum_{j=0}^{p-1} S_q(i \oplus j)\sum_{r=1}^{N_\tau}|g_r'(x)| \\ &\qquad Q_{I_i}(g_r(x))Q_{I_j}(\tau^m(g_r(x)))f^*(g_r(x)) \\ &= \sum_{j=0}^{p-1} Q_{I_j}(\tau^{m-1}(x))\sum_{i=0}^{p-1} S_q(i \oplus j) \\ &\qquad \sum_{r=1}^{N_\tau}|g_r'(x)|Q_{I_i}(g_r(x))f^*(g_r(x)). \end{aligned} \tag{30}$$

Note that

$$\begin{aligned} &\sum_{r=1}^{N_\tau}|g_r'(x)|Q_{I_i}(g_r(x))f^*(g_r(x)) \\ &= P_\tau\{Q_{I_i}(x)f^*(x)\} = \frac{1}{p}f^*(x), \end{aligned} \tag{31}$$

$$\sum_{j=0}^{p-1} Q_{I_j}(x) = 1. \tag{32}$$

Applying eqs.(9), (31), and (32) to eq.(30), we obtain

$$P_\tau\{\widehat{Q}_q(x)f^*(x)\} = \frac{1}{p}f^*(x) \ \text{ for all } q \tag{33}$$

which completes the proof.

3.3. Cross-Correlation Property

Consider two chaotic p-ary sequences $\{B(x_n)\}_{n=0}^{\infty}$ and $\{C(x_n)\}_{n=0}^{\infty}$ generated by a common seed x. If both of $\{I_i\}_{i=0}^{p-1}$ and $\{J_j\}_{j=0}^{p-1}$ satisfy eq.(21), we have

$$\begin{aligned} E[B(x)C(\tau^\ell(x))] &= E[C(x)B(\tau^\ell(x))] \\ &= E[B]E[C] \end{aligned} \tag{34}$$

for $\ell \geq 1$, which implies that the two sequences are uncorrelated for $\ell \geq 1$. Indeed, they are mutually independent for $\ell \geq 1$ because we have

$$\begin{aligned} &\Pr(B(x_n) = q_1, C(x_{n+\ell}) = q_2) \\ &\quad = E[Q_{I_{q_1}}(x)Q_{J_{q_2}}(\tau^\ell(x))] \\ &\quad = E[Q_{I_{q_1}}]E[Q_{J_{q_2}}]. \end{aligned} \tag{35}$$

However, they are not always independent nor uncorrelated for $\ell = 0$. As is well known, completely uncorrelated sequences are useful in several applications such as DS/CDMA communication systems. Such completely uncorrelated chaotic p-ary sequences can be obtained by designing an appropriate set of indicator functions [2],[6].

Now, we consider two chaotic p-ary sequences $\{B(x_n)\}_{n=0}^{\infty}$ and $\{C(x_n)\}_{n=0}^{\infty}$ obtained by

$$B(x) = B_1(x) \oplus B_2(\tau^{m_1}(x)) \quad (m_1 \geq 1) \tag{36}$$

$$C(x) = C_1(x) \oplus C_2(\tau^{m_2}(x)) \quad (m_2 \geq 1) \tag{37}$$

where

$$\left.\begin{aligned} B_1(x) &= \sum_{i=0}^{p-1} iQ_{I_i^{(1)}}(x),\ B_2(x) = \sum_{j=0}^{p-1} jQ_{J_j^{(1)}}(x), \\ C_1(x) &= \sum_{i=0}^{p-1} iQ_{I_i^{(2)}}(x),\ C_2(x) = \sum_{j=0}^{p-1} jQ_{J_j^{(2)}}(x). \end{aligned}\right\} \tag{38}$$

We assume that $\{I_i^{(1)}\}_{i=0}^{p-1}$ and $\{I_i^{(2)}\}_{i=0}^{p-1}$ satisfy

$$P_\tau\{Q_{I_i^{(1)}}(x)f^*(x)\} = P_\tau\{Q_{I_i^{(2)}}(x)f^*(x)\} = \frac{1}{p}f^*(x), \tag{39}$$

that is, $\{B(x_n)\}_{n=0}^{\infty}$ and $\{C(x_n)\}_{n=0}^{\infty}$ are balanced i.i.d. p-ary sequences, which also implies that they satisfy eqs.(34) and (35). Thus we consider the case $\ell = 0$, that is, $\Pr(B(x_n) = q_1, C(x_n) = q_2)$.

Lemma: Assume $B_1(x) = C_1(x)$ in eq.(38). Then

$$\Pr(B(x_n) = q_1, C(x_n) = q_2) = \frac{1}{p}\sum_{j_1=0}^{p-1}\sum_{j_2=0}^{p-1} E[Q_{J^{(1)}_{j_1}}(\tau^{m_1-1}(x))Q_{J^{(2)}_{j_2}}(\tau^{m_2-1}(x))]. \quad (40)$$

Proof: First we can write

$$\begin{aligned}&\Pr(B(x_n) = q_1, C(x_n) = q_2)\\ &= E\left[\sum_{i_1=0}^{p-1}\sum_{j_1=0}^{p-1} S_{q_1}(i_1 \oplus j_1)Q_{I^{(1)}_{i_1}}(x)Q_{J^{(1)}_{j_1}}(\tau^{m_1}(x)) \sum_{i_2=0}^{p-1}\sum_{j_2=0}^{p-1} S_{q_2}(i_2 \oplus j_2)Q_{I^{(2)}_{i_2}}(x)Q_{J^{(2)}_{j_2}}(\tau^{m_2}(x))\right]\\ &= E\left[\sum_{j_1,j_2} Q_{J^{(1)}_{j_1}}(\tau^{m_1}(x))Q_{J^{(2)}_{j_2}}(\tau^{m_2}(x)) \sum_{i_1,i_2} S_{q_1}(i_1 \oplus j_1)S_{q_2}(i_2 \oplus j_2)Q_{I^{(1)}_{i_1}}(x)Q_{I^{(2)}_{i_2}}(x)\right]. \quad (41)\end{aligned}$$

Note that $B_1(x) = C_1(x)$ (*i.e.*, $I^{(1)}_i = I^{(2)}_i$ for all i implies $Q_{I^{(1)}_{i_1}}(x)Q_{I^{(2)}_{i_2}}(x) = Q_{I^{(1)}_{i_1}}(x)$ which, in conjunction with eq.(9), gives

$$\begin{aligned}&\sum_{i_1,i_2} S_{q_1}(i_1 \oplus j_1)S_{q_2}(i_2 \oplus j_2)Q_{I^{(1)}_{i_1}}(x)Q_{I^{(2)}_{i_2}}(x)\\ &= \sum_{i_2} S_{q_2}(i_2 \oplus j_2)\sum_{i_1} S_{q_1}(i_1 \oplus j_1)Q_{I^{(1)}_{i_1}}(x)\\ &= \sum_{i} S_{q_1}(i \oplus j_1)Q_{I^{(1)}_{i}}(x). \quad (42)\end{aligned}$$

Substituting eq.(42) into eq.(41) and using eqs.(16) and (39), we obtain eq.(40), which completes the proof.

Theorem 3: In eqs.(36) and (37), assume that $B_1(x) = C_1(x)$ and either of the conditions such that

(i) $m_1 < m_2$ and $\{J^{(1)}_j\}_{j=0}^{p-1}$ satisfies eq.(21)

(ii) $m_1 > m_2$ and $\{J^{(2)}_j\}_{j=0}^{p-1}$ satisfies eq.(21)

is satisfied. Furthermore, assuming that $E[Q_{J^{(1)}_j}]$ or $E[Q_{J^{(2)}_j}]$ is equal to $\frac{1}{p}$ for all j, we have

$$\Pr(B(x_n) = q_1, C(x_n) = q_2) = \frac{1}{p^2} \quad (43)$$

which implies that $B(x_n)$ and $C(x_n)$ are independent, and hence, eqs.(34) and (35) hold for all $\ell \geq 0$.

Proof: For both cases of (i) and (ii) in Theorem 3, it is obvious from eq.(40) that

$$\Pr(B(x_n) = q_1, C(x_n) = q_2) = \frac{1}{p}\sum_{j_1=0}^{p-1}\sum_{j_2=0}^{p-1} E[Q_{J^{(1)}_{j_1}}]E[Q_{J^{(2)}_{j_1}}]. \quad (44)$$

Since

$$\sum_{j_1=0}^{p-1} E[Q_{J^{(1)}_{j_1}}] = \sum_{j_2=0}^{p-1} E[Q_{J^{(2)}_{j_1}}] = 1, \quad (45)$$

we have eq.(43) if $E[Q_{J^{(1)}_j}]$ or $E[Q_{J^{(2)}_j}]$ is equal to $\frac{1}{p}$. This completes the proof.

4. Conclusion

Statistical properties of modulo-p added p-ary sequences have been discussed. For general p-ary random variables, we have shown that if one sequence is k-distributed, then the modulo-p added sequence is also k-distributed regardless of the other sequence. For chaotic p-ary sequences generated by a class of 1-D maps, it has been shown that we can get balanced i.i.d. p-ary sequences by modulo-p addition of two chaotic p-ary sequences if one of the sequences is a balanced i.i.d. one. We have also given the conditions for generating two modulo-p added sequences which are completely independent of each other from a common chaotic real-valued sequence.

Acknowledgments

Part of this study was performed during the author's visit to the University of Birmingham in U.K. as a visiting professor, supported by the Ministry of Education, Culture, Sports, Science and Technology (Monbukagakusho) of Japan. Special thanks are given to Prof. Anthony J. Lawrance (presently a Professor of the University of Warwick) for his help and support during the stay. The author would also like to thank Dr. Hiroshi Fujisaki for encouraging him to study the problem discussed in this paper.

References

[1] D. V. Sarwate and M. B. Pursley, "Crosscorrelation Properties of Pseudorandom and Related Sequences," *Proc. IEEE*, vol.68, no.3, pp.593–619, 1980.

[2] T. Kohda and A. Tsuneda, "Statistics of Chaotic Binary Sequences", *IEEE Trans., Information Theory*, vol.43, no.1, pp.104–112, 1997.

[3] A. Tsuneda, T. Sugahara, and T. Inoue, "Statistical Properties of Modulo-2 Added Binary Sequences," *IEICE Trans. Fundamentals*, vol.E87-A, no.9, pp.2267–2273, 2004.

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

[5] D. Knuth, *The Art of Computer Programming*, vol.2, Seminumerical Algorithms, 2nd ed., Addison-Wesley, 1981.

[6] T. Kohda and A. Tsuneda, "Design of Sequences of I.I.D. p-Ary Random Variables", *Proc. of 1997 IEEE Int. Symp. Information Theory*, p.17, 1997.