IEICE TRANS. INF. & SYST., VOL.E86–D, NO.2 FEBRUARY 2003

PAPER *Special Issue on Selected Papers from LA Symposium*

On the Distribution of Fractional Linear Congruential Pseudorandom Numbers*

Yoshinori TAKEI[†], **Toshinori YOSHIKAWA**[†], *and* **Xi ZHANG**[†], ***Regular Members***

SUMMARY As pseudorandom number generators for Monte Carlo simulations, inversive linear congruential generators (ICG) have some advantages compared with traditional linear congruential generators. It has been shown that a sequence generated by an ICG has a low *discrepancy* even if the length of the sequence is far shorter than its period. In this paper, we formulate *fractional linear congruential generators* (FCG), a generalized concept of the inversive linear congruential generators. It is shown that the sequence generated by an FCG is a geometrical shift of a sequence from an ICG and satisfies the same upper bounds of discrepancy. As an application of the general formulation, we show that under certain condition, "Leap-Frog technique," a way of splitting a random number sequence to parallel sequences, can be applied to the ICG or FCG with no extra cost on discrepancy.

key words: *pseudorandom generators, fractional linear transforms, discrepancy, inversive linear congruent generators, leap-frog*

1. Introduction

1.1 Background

Fast generator of good pesudorandom numbers is crucial in Monte Carlo simulations. The linear congruential generator (LCG) [16] is most traditional and well-known, however, due to the inherent linearity, the distribution of a sequence from the LCG has a unwanted regularity, lattice structure [17][20, Chapter 8]. The inversive linear congruential pseudorandom generator (ICG) [8], which passes s-dimensional lattice test for all $s \leqslant (p+1)/2$ [20, Theorem 8.5], is an attractive alternative. Let p be a prime, $\mathbb{F}_p$ be the field with p elements, and $\mathbb{F}_p^\times$ be the multiplicative group of $\mathbb{F}_p$.

Definition 1.1 (ICG [8]). Let a and b be two elements of $\mathbb{F}_p^\times$. Then

$$\psi_{a,b}(u) := \begin{cases} a & u = 0; \\ a + bu^{-1} & \text{otherwise}, \end{cases} \qquad (u \in \mathbb{F}_p) \qquad (1)$$

defines a permutation over $\mathbb{F}_p$. Then for an element $u_0 \in \mathbb{F}_p$, the recurrence

$$u_{n+1} = \psi_{a,b}(u_n) \quad (n \geqslant 0) \qquad (2)$$

defines a purely periodic sequence $(u_n \in \mathbb{F}_p)_{n \geqslant 0}$. Put

$$y_n := ((u_n))/p \in [0,1), \qquad (3)$$

where $((u))$ means the least nonnegative representative integer of $u \mod p$ and the division is taken over the rational number field. We say that $(y_n \in [0,1))_{n \geqslant 0}$ is the sequence generated by the ICG $\psi_{a,b}$ with initial value u_0. □

Many modified or generalized versions of ICG have been presented. The reader is referred to the survey article [7]. Some of them are: the compound inversive generator [6], [14], [24] which utilizes a composite modulus, the explicit inversive generator (EICG) [5] which is based on the inversion of a linear form of the index counter. A branch of generalization is replacing the prime field $\mathbb{F}_p$ with an arbitrary finite field $\mathbb{F}_q$, where $q = p^k$.

Definition 1.2 (ICVG [19]). Fix a basis $(\xi_1, \ldots, \xi_k) \in \mathbb{F}_q^k$ for the extention $\mathbb{F}_q/\mathbb{F}_p$. Let a, b and u_0 be elements of ${\mathbb{F}_q}^\times$. Then a permutation $\psi_{a,b}$ over $\mathbb{F}_q$ is defined as in Eq. (1) and a purely periodic sequence $(u_n \in \mathbb{F}_q)_{n \geqslant 0}$ is defined as in Eq. (2). For each n, write

$$u_n = u_n^{(1)} \xi_1 + \cdots + u_n^{(k)} \xi_k \qquad (4)$$

with $(u_n^{(1)}, \ldots, u_n^{(k)}) \in \mathbb{F}_p^k$, then component-wise applications of Eq. (3) yield the vector

$$\mathbf{y}_n := (y_n^{(1)}, \ldots, y_n^{(k)}) \in [0,1)^k. \qquad (5)$$

We say that $(\mathbf{y}_n \in [0,1)^k)_{n \geqslant 0}$ is the vector sequence generated by the inversive linear congruential vector generator (ICVG) $\psi_{a,b}$ with initial value u_0. □

Definition 1.3 (Digital ICG [10]). Let p, k, q, a, b, $u_n = u_n^{(1)} \xi_1 + \cdots + u_n^{(k)} \xi_k$ and $(y_n^{(1)}, \ldots, y_n^{(k)}) \in [0,1)^k$ as in Definition 1.2. Then define $y'_n \in [0,1)$ as

$$y'_n := \sum_{i=1}^{k} ((y_n^{(i)}))p^{-i}. \qquad (6)$$

We say that $(y'_n \in [0,1))_{n \geqslant 0}$ is the sequence generated by the digital ICG $\psi_{a,b}$ with initial value u_0. □

Discrepancy is a quantitive measure of quality of pseudorandom numbers, which gives certain upper bound on the error term of a Monte Carlo integration.

Manuscript received March 22, 2002.
Manuscript revised August 7, 2002.

[†]The authors are with the Department of Electrical Engineering, Nagaoka University of Technology, Nagaoka-shi, 940–2188 Japan.

*The preliminary version of this paper was presented as "On the distribution of the fractional linear pseudorandom generator" at LA Symposium, February 4–6, 2002, Kyoto.

Definition 1.4 (discrepancy [20, Chapter 3]). Let S be a finite multiset of points in the s-dimensional half-opened cube $[0,1)^s$. Let $\mathcal{J}$ be the family of all subcubes $\{\prod_{i=1}^{s}[a_i,b_i) \subseteq [0,1)^s\}$. The *extreme discrepancy* of S is the real number

$$D^{(s)}(S) := \sup_{J\in\mathcal{J}} \left| \frac{\|J\cap S\|}{\|S\|} - \mathrm{vol}(J) \right|, \tag{7}$$

where $\mathrm{vol}(J)$ denotes the s-dimensional volume of J and $\|S\|$ is the number of elements of the multiset S counted with multiplicity. The *star discrepancy* $D^{*(s)}(S)$ is defined similarly by replacing $\mathcal{J}$ with $\mathcal{J}^* := \{\prod_{i=1}^{s}[0,b_i) \subseteq [0,1)^s\}$ in Eq. (7). Also, for an integer e, the *discrete discrepancy* $D^{(s),e}(S)$ is defined by replacing $\mathcal{J}$ with $\mathcal{J}_e := \{\prod_{i=1}^{s}[a_i,b_i) \subseteq [0,1)^s : ea_i, eb_i \in \mathbb{Z}\}$. □

In practice, only a small part of the period of pseudorandom numbers is used. So bounding the discrepancy in parts of the period is important. The following discrepancy bound for the ICG in parts of the period has been found. Note that the bound is nontrivial if the length N of the sequence is of order $p^{\frac{1}{2}+\epsilon}$ ($\epsilon > 0$).

Theorem 1.5 (s-dimensional discrepancy bound of ICG [13], see also [21] for $s = 1$)
Let $(y_0, y_1, \dots)$ be the number sequence in $[0,1)$ generated by an ICG, and let T be its fundamental period. Let $s \geqslant 1$ and put $\mathbf{t}_n := (y_n, \dots, y_{n+s-1})$ for each n. Then the s-dimensional discrepancy of the vector sequence $\{\mathbf{t}_0, \dots, \mathbf{t}_{N-1}\}$ is bounded as:

$$\begin{aligned} D^{(s)}(\{\mathbf{t}_0,\dots,\mathbf{t}_{N-1}\}) &\leqslant \left(4s+\sqrt{8/3}\right)^{\frac{1}{2}} N^{-\frac{1}{2}} p^{\frac{1}{4}} \left((4/\pi^2)\log p\right)^s \\ &\quad + O(N^{-\frac{1}{2}} p^{\frac{1}{4}} (\log p)^{s-1}) \\ &\quad (1 \leqslant N \leqslant T), \end{aligned} \tag{8}$$

where the implied constant depends only on s. □

The statiscal test that calculates or bounds $D^{(s)}(\{\mathbf{t}_0,\dots,\mathbf{t}_{N-1}\})$ is reffered to as overlapping serial test of the $(y_0, y_1, \dots, y_N)$ [20, Sect. 7.2]. The above bound shows a level of statistical independence of succesive s-tuples of pesudorandom numbers $(y_n, \dots, y_{n+s-1})$ from any fixed ICG, for all small s. See [15] for empirical serial tests of LCG, ICG and EICG. As a way to obtain a sequence of s-tuples of pseudorandom numbers, so-called *low-discrepancy sequences* attain better s-dimentional discrepancy, namely $O(N^{-1}\log^s N)$, than the over-wrapping s-tuples $\mathbf{t}_0, \dots, \mathbf{t}_{N-1}$ from an ICG. (For constructions of such low-discrepancy sequences, see [27, Sect 3.2], [28] and the literatures cited there). On the other hand, the over-wrapping s-tuples from an ICG can be used even when the prescribed value of dimension s is unknown [27, Sect 3.3].

The $\mathbb{F}_q$ counterparts of Theorem 1.5, namely, the upper bound of star discrepancy for the digital ICG and the upper bound of discrete discrepancy for the ICVG have been obtained also:

Theorem 1.6 (s-dimensional discrepancy bound of digital ICG [22]). Let $(y'_0, y'_1, \dots)$ be the number sequence generated by a digital ICG, whose fundamental period is T. Let $s \geqslant 1$ and put $\mathbf{t}'_n := (y'_n, \dots, y'_{n+s-1})$ for each n. Then the s-dimensional star discrepancy of the vector sequence $\{\mathbf{t'}_0, \dots, \mathbf{t'}_{N-1}\}$ satisfies

$$D^{*(s)}(\{\mathbf{t'}_0,\dots,\mathbf{t'}_{N-1}\}) = O(N^{-\frac{1}{2}} q^{\frac{1}{4}} (\log q)^s) \quad (1 \leqslant N \leqslant T). \tag{9}$$

□

Theorem 1.7 (ks-dimensional discrepancy bound of ICVG [22]). Let $(\mathbf{y}_0, \mathbf{y}_1, \dots)$ be the vector sequence generated by an ICVG, whose fundamental period is T. Let $s \geqslant 1$ and let τ_n be the vector $\tau_n := (\mathbf{y}_n, \dots, \mathbf{y}_{n+s-1})$ of dimension ks for each n. Then the ks-dimensional discrete discrepancy of the vector sequence $\{\tau_0, \dots, \tau_{N-1}\}$ satisfies

$$D^{(ks),p}(\{\tau_0,\dots,\tau_{N-1}\}) = O(N^{-\frac{1}{2}} q^{\frac{1}{4}} (\log p)^{ks}) \quad (1 \leqslant N \leqslant T). \tag{10}$$

□

We also note the corresponding bounds for the explicit digital inversive number and the explicit inversive vector generators over $\mathbb{F}_q$ have been obtained [23].

1.2 Contribution of the Paper

In this paper, we formulate *fractional linear congruential generators,* over a finite field $\mathbb{F}_q$ of odd characteristic p, a generalized version of the inversive linear congruential generators. It is shown that the sequence generated by a fractional linear congruential generator is in fact a geometrical shift (modulo one) of a sequence by an inversive linear congruential generator, and the same upper bounds as Theorems 1.5, 1.6 and 1.7 hold for these generalized generators. As an application of the general formulation, we show that fractional linear congruential generators are robust in discrepancy, under decimations of the output sequence. The robustness with respect to the decimations implies the applicability of so-called Leap-Frog technique, a way of splitting pseudo random numbers in distributed Monte Carlo simulations.

In Sect. 2, some basic terminologies and known facts are introduced from the theory of fractional linear transforms over finite fields. In Sect. 3 the fractional linear congruential generators are defined (Definition 1.1). It is proved that a fractional linear sequence is a geometrical shift (modulo one) of an inversive linear sequence (Proposition 3.3). Section 4 extends the discrepancy bounds for fractional linear generators (Theorems 4.1, 4.2 and 4.3). Section 5 shows the robustness

result on the the decimation or the Leap-Frog use (Theorem 5.1.) Section 6 concludes the paper.

Hereafter, p is a (large) odd prime.

2. Fractional Linear Transforms over Finite Fields

We introduce some basic concepts, terminologies and results of the theory of fractional linear transforms over a finite field $\mathbb{F}_q$, where q is a power p^k of odd prime, based on [25, Chapter 21]. Let $\mathbf{GL}_2(\mathbb{F}_q)$ be the group of 2×2 invertible matrices over $\mathbb{F}_q$. The projective line $\mathbb{P}^1(\mathbb{F}_q)$ is the set

$$\{[z_1 : z_2] : (z_1, z_2) \in \mathbb{F}_q \times \mathbb{F}_q \setminus \{(0,0)\}\},$$

where $[z_1 : z_2]$ is the equivalence class of (z_1, z_2) under the equivalence relation

$$[z_1 : z_2] = [z_1' : z_2'] \Leftrightarrow (z_1, z_2) = (az_1', az_2') \text{ for some } a \in \mathbb{F}_q^\times.$$

If we take the representative of each class as $(z_1 z_2^{-1}, 1)$ for $z_2 \in \mathbb{F}_q^\times$ and as $(1,0)$ for $z_2 = 0$ then $\mathbb{P}^1(\mathbb{F}_q)$ is identified with the set $\mathbb{F}_q \cup \{\infty\}$, where $z \in \mathbb{F}_q$ corresponds to $[z : 1]$ and the symbol ∞ is identified with $[1 : 0]$. Hereafter we always use this alias for $\mathbb{P}^1(\mathbb{F}_q)$.

For $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathbf{GL}_2(\mathbb{F}_q)$ and $z \in \mathbb{F}_q \cup \{\infty\}$, put

$$A\langle z\rangle := \begin{cases} ac^{-1} & \text{if } c \neq 0,\ z = \infty; \\ \infty & \text{if } c = 0,\ z = \infty; \\ \infty & \text{if } cz + d = 0,\ z \in \mathbb{F}_q; \\ (az+b)(cz+d)^{-1} & \text{otherwise,} \end{cases} \tag{11}$$

where the operations are taken over $\mathbb{F}_q$ in the first and fourth cases. Then it holds that

$$(AB^{-1})\langle z\rangle = A\langle B^{-1}\langle z\rangle\rangle \quad (A, B \in \mathbf{GL}_2(\mathbb{F}_q),\ z \in \mathbb{F}_q \cup \{\infty\}) \tag{12}$$

and the map $A\langle\cdot\rangle : z \mapsto A\langle z\rangle$ defines a permutation over the set $\mathbb{F}_q \cup \{\infty\}$. We call such a permutation $A\langle\cdot\rangle$ as a fractional linear transform over $\mathbb{F}_q$. By Eq. (12), $A \mapsto A\langle\cdot\rangle$ is a homomorphism from $\mathbf{GL}_2(\mathbb{F}_q)$ onto the group of fractional linear transforms over $\mathbb{F}_q$ and by Eq. (11) its kernel is the center, i.e. the normal subgroup $\mathcal{C} := \left\{\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right) : a \in \mathbb{F}_q^\times\right\}$ of scalar matrices:

$$A\langle\cdot\rangle = \mathrm{id}|_{\mathbb{F}_q \cup \{\infty\}} \ \Leftrightarrow\ A \in \mathcal{C}. \tag{13}$$

Thus the group of the fractional linear transforms is isomorphic to the quotient group $\mathbf{GL}_2(\mathbb{F}_q)/\mathcal{C}$, which is reffered to as $\mathbf{PGL}_2(\mathbb{F}_q)$. For notational convenience, we shall inspect $\mathbf{GL}_2(\mathbb{F}_q)$ rather than $\mathbf{PGL}_2(\mathbb{F}_q)$, noting the redundancy of Eq. (13).

2.1 Borel Subgroup

The subgroup

$$\mathcal{B} = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathbf{GL}_2(\mathbb{F}_q) \right\}$$

of $\mathbf{GL}_2(\mathbb{F}_q)$ is called *the Borel subgroup*. Since the fractional linear transform defined by an element of $\mathcal{B}$ has very special properties, we should treat it separately. Namely, from Eq. (11) we have

$$\mathcal{B} = \{A \in \mathbf{GL}_2(\mathbb{F}_q) : A\langle\infty\rangle = \infty\} \tag{14}$$

and

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\langle z\rangle = ad^{-1}z + bd^{-1} \quad (z \in \mathbb{F}_q).$$

Thus, a Borel element defines a linear transform over $\mathbb{F}_q$, rather than a proper fractional linear transform.

For elements outside the Borel subgroup $\mathcal{B}$, we note the following normalization by conjugacy. Let $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathbf{GL}_2(\mathbb{F}_q) \setminus \mathcal{B}$. Then it holds that

$$A = \begin{pmatrix} 1 & c^{-1}d \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} a+d & -c^{-1}(ad-bc) \\ c & 0 \end{pmatrix} \begin{pmatrix} 1 & c^{-1}d \\ 0 & 1 \end{pmatrix}. \tag{15}$$

2.2 Conjugacy Classes

Two elements $A, B \in \mathbf{GL}_2(\mathbb{F}_q)$ are said to be conjugate if there exists $P \in \mathbf{GL}_2(\mathbb{F}_q)$ such that $A = P^{-1}BP$. Obviously, it is an equivalent relation. Furthur, if A and B are conjugate with $A = P^{-1}BP$,

- $\Phi_A(X) = \Phi_B(X)$; where $\Phi_A(X) = X^2 - \mathrm{tr}(A)X + \det(A)$ is the characteristic polynomial of A; i.e. they share the eigenvalues.
- For all $z \in \mathbb{F}_q \cup \{\infty\}$, $A\langle z\rangle = z$ iff $B\langle P\langle z\rangle\rangle = P\langle z\rangle$; i.e. the numbers of fixed points are the same.

Now we excerpt a basic classification of conjugacy classes in $\mathbf{GL}_2(\mathbb{F}_q)$.

Fact 2.1 (Classification of conjugacy classes of $\mathbf{GL}_2(\mathbb{F}_q)$ [25, Chapter 21]). For any $A \in \mathbf{GL}_2(\mathbb{F}_q)$, there exists $P \in \mathbf{GL}_2(\mathbb{F}_q)$ such that one of the following cases (i)(ii)(iii)(iv) is true for some $r, s, t \in \mathbb{F}_q$. The case that (A, P) falls is uniquely determinated by the conjugacy class to which A belongs.

(i) $PAP^{-1} = \left(\begin{smallmatrix} r & 0 \\ 0 & r \end{smallmatrix}\right)(r \neq 0)$. In this case A is said to be *central*. Obviously $A = \left(\begin{smallmatrix} r & 0 \\ 0 & r \end{smallmatrix}\right)$. So A is *central* iff $A \in \mathcal{C}$. The number r is the double root of $\Phi_A(X) = 0$. Clearly $A\langle\cdot\rangle$ fixes any element of $\mathbb{F}_q \cup \{\infty\}$. There are $q-1$ different conjugacy classes of this type, each containing sole element. Union of these classes forms the subgroup $\mathcal{C}$.

(ii) $PAP^{-1} = \left(\begin{smallmatrix} r & 1 \\ 0 & r \end{smallmatrix}\right) (r \neq 0)$ In this case A is said to be *parabolic*. The number r is the double root of $\Phi_A(X) = 0$. The representative $\left(\begin{smallmatrix} r & 1 \\ 0 & r \end{smallmatrix}\right)$ fixes exactly one point ∞, thus A fixes exactly one point $P^{-1}\langle\infty\rangle$. The smallest positive integer ℓ such that $A^\ell \in \mathcal{C}$ is p. There are $q-1$ different conjugacy classes of this type, each containing q^2-1 elements.

(iii) $PAP^{-1} = \left(\begin{smallmatrix} r & 0 \\ 0 & s \end{smallmatrix}\right) ((r-s)rs \neq 0)$. In this case A is said to be *hyperbolic*. The numbers r and s are the two different roots of $\Phi_A(X) = 0$. The representative $\left(\begin{smallmatrix} r & 0 \\ 0 & s \end{smallmatrix}\right)$ fixes exactly two points ∞ and 0 and A fixes exactly two points $P^{-1}\langle\infty\rangle$ and $P^{-1}\langle 0\rangle$. The smallest positive integer ℓ such that $A^\ell \in \mathcal{C}$ is the order of rs^{-1} in the multiplicative group $\mathbb{F}_q^\times$. There are $(q-1)(q-2)/2$ classes of this type, each containing q^2+q elements.

(iv) $PAP^{-1} = \left(\begin{smallmatrix} r & st \\ s & r \end{smallmatrix}\right) (s \neq 0, t$:nonsquare $\in \mathbb{F}_q)$. In this case A is said to be *elliptic*. The characteristic equation $\Phi_A(X) = 0$ has two different roots $\lambda = r + s\sqrt{t}$ and $\bar{\lambda} = r - s\sqrt{t}$ in $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$. No element of $\mathbb{F}_q \cup \{\infty\}$ is fixed by the representative $\left(\begin{smallmatrix} r & st \\ s & r \end{smallmatrix}\right)$, thus by A. Also, there exists $Q \in \mathbf{GL}_2(\mathbb{F}_{q^2})$ such that $A = Q^{-1}\left(\begin{smallmatrix} \lambda & 0 \\ 0 & \bar{\lambda} \end{smallmatrix}\right)Q$. The smallest positive integer ℓ such that $A^\ell \in \mathcal{C}$ is $\mathrm{ord}(\bar{\lambda}/\lambda) = \mathrm{ord}(\lambda^{q-1})$ where $\mathrm{ord}(x)$ is the order of an element x in the multiplicative group $\mathbb{F}_{q^2}^\times$. There are $q(q-1)/2$ classes of this type, each containing q^2-q elements.

□

Proposition 2.2. Let ℓ be an integer and $A \in \mathbf{GL}_2(\mathbb{F}_q)$ and $z_0 \in \mathbb{F}_q \cup \{\infty\}$.

(a) If $A \notin \mathcal{B}$, then $A^\ell \in \mathcal{B} \Leftrightarrow A^\ell \in \mathcal{C}$.
(b) Suppose that $z_0, A^1\langle z_0\rangle$ and $A^2\langle z_0\rangle$ are three different points. Then $A^\ell\langle z_0\rangle = z_0$ implies $A^\ell \in \mathcal{C}$.
(c) If $A \notin \mathcal{B}$ and the period of the sequence $(z_0, A^1\langle z_0\rangle, A^2\langle z_0\rangle, \dots)$ is at least 3, then $A^\ell\langle z_0\rangle = z_0 \Leftrightarrow A^\ell \in \mathcal{B}$.

Proof. (a) ($\Rightarrow$) It is verified by direct calculations based on the classification of Fact 2.1. When A is elliptic, writing $A = Q^{-1}\left(\begin{smallmatrix} \lambda & 0 \\ 0 & \bar{\lambda} \end{smallmatrix}\right)Q$ with $Q = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathbf{GL}_2(\mathbb{F}_{q^2})$ and $A^\ell = \left(\begin{smallmatrix} a_\ell & b_\ell \\ c_\ell & d_\ell \end{smallmatrix}\right)$, we obtain

$$\begin{pmatrix} a_\ell & b_\ell \\ c_\ell & d_\ell \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}^{-1} \begin{pmatrix} \lambda^\ell & 0 \\ 0 & \bar{\lambda}_\ell \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \quad (16)$$

and

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} a_\ell & b_\ell \\ c_\ell & d_\ell \end{pmatrix} = \begin{pmatrix} \lambda^\ell & 0 \\ 0 & \bar{\lambda}^\ell \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}. \quad (17)$$

Suppose that $A^\ell \in \mathcal{B}$, i.e. $c_\ell = 0$. From the lower left of Eq. (17), we obtain $a_\ell\gamma = \bar{\lambda}^\ell\gamma$. If $\gamma = 0$ then $A \in \mathcal{B}$ by Eq. (16), which contradicts the assumption. Thus we have $a_\ell = \bar{\lambda}^\ell$. Taking the conjugation $\bar{\cdot}$ (that is, the unique nontrivial element of the Galois group of the quadratic extension $\mathbb{F}_{q^2}/\mathbb{F}_q$) we also have $a_\ell = \bar{a_\ell} = \lambda^\ell$. Taking the trace of Eq. (16), we obtain $a_\ell = \lambda^\ell = \bar{\lambda}^\ell = d_\ell$. Writing them back to Eq. (16) tells

$$\begin{pmatrix} a_\ell & b_\ell \\ 0 & a_\ell \end{pmatrix} = \begin{pmatrix} a_\ell & 0 \\ 0 & a_\ell \end{pmatrix} \quad (18)$$

and $A^\ell \in \mathcal{C}$. Hyperbolic and parabolic cases are verified similarly.

($\Leftarrow$): Clear.

(b) Observe that A^ℓ fixes the three different points. From the classification of Fact 2.1, A^ℓ should be central.

(c) Immediate from (a) and (b).

□

3. Fractional Linear Congruential Generators

3.1 The FCG

Utilizations of matrices or their characteristic polynomials already appeared in the contexts of the period analyses of ICG or ICVG [2], [7], [9]. Here, we use matrices, or fractional linear transforms induced by them, to define a generalized class of pseudorandom number generators based on the inversion.

Definition 3.1. We fix a basis $(\xi_1, \dots, \xi_k) \in \mathbb{F}_q^k$ for the extention $\mathbb{F}_q/\mathbb{F}_p$. Let A be an element of $\mathbf{GL}_2(\mathbb{F}_q)$. Then

$$\psi_A(u) := \begin{cases} A^2\langle u\rangle & \text{if } A\langle u\rangle = \infty; \\ A\langle u\rangle & \text{otherwise,} \end{cases} \quad (u \in \mathbb{F}_q) \quad (19)$$

defines a permutation over $\mathbb{F}_q$. We call the map ψ_A as a fractional linear congruential generator. If A is not an element of the Borel subgroup $\mathcal{B}$, then we say that ψ_A is nonlinear. For an element $u_0 \in \mathbb{F}_q$,

$$u_{n+1} = \psi_A(u_n) \quad (n \geqslant 0)$$

or equivalently

$$u_n = \psi_A^n(u_0) \quad (n \geqslant 0),$$

where ψ_A^n denotes n composition of ψ_A, defines a purely periodic sequence $(u_n \in \mathbb{F}_q)_{n\geqslant 0}$. We call $(u_n)_{n\geqslant 0}$ the sequence generated by the fractional linear generator (FCG) ψ_A with initial value u_0.

Further, we define maps;

(i) (defined only for $k = 1$)

$$\mathrm{GI} : \mathbb{F}_p \ni u \mapsto ((u))/p \in [0, 1).$$

(ii)

$$\mathrm{GI}' : \mathbb{F}_q \ni u \mapsto \sum_{i=1}^{k} ((u^{(i)}))p^{-i} \in [0, 1),$$

where $u^{(i)} \in \mathbb{F}_p$ is defined through $\sum_{i=1}^k u^{(i)}\xi_i = u$.

(iii)

$$\mathsf{GI} : \mathbb{F}_q \ni u \mapsto (((u^{(1)}))/p, \dots, ((u^{(k)}))/p) \in [0,1)^k,$$

where $u^{(i)} \in \mathbb{F}_p$ is defined as in (ii).

and we call them geometric interpretations.

We say that $(\mathrm{GI}(u_n) \in [0,1))_{n\geqslant 0}$ is the sequence generated by the fractional linear generator ψ_A and geometric interpretation GI, with initial value u_0. Same terminologies are defined for $(\mathrm{GI}'(u_n) \in [0,1))_{n\geqslant 0}$ and $(\mathsf{GI}(u_n) \in [0,1)^k)_{n\geqslant 0}$. □

Let ℓ be the smallest positive index that $A^\ell \in \mathcal{C}$ holds (See the classification Fact 2.1). By Proposition 2.2 (b), the period of the sequence by an FCG is $\ell - 1$ when the orbit $\{A^n\langle u_0\rangle : 0 \leqslant n < \ell\}$ contains ∞ and the first case of Eq. (19) occurs exactly once in the period. Otherwise, the orbit avoids ∞, the period is ℓ and it holds that $\psi_A^n(u_0) = \psi_{A^n}(u_0) = A^n\langle u_0\rangle$ for all n.

Especially, the period takes its maximum value q if A is elliptic and the ratio of two roots of $\Phi_A(X)$ in $\mathbb{F}_{q^2}$ has the order $q+1$. In this case, $\Phi_A(X)$ is said to be an inversive maximal period (IMP) [12],[3],[2]. Periods of ICG and ICVG have been extensively studied in literatures including the above three. We note that these results on periods of ICG and ICVG are directly translated for FCG, using Proposition 3.3 of the next subsection.

3.2 How General They Are

First, the following example shows that LCG and ICG are both FCG.

Example 3.2. (a) A LCG is defined by a matrix of the form $\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) \in \mathcal{B}$.

(b) An ICG is defined by a matrix of the form

$$\begin{pmatrix} a & b \\ 1 & 0 \end{pmatrix} (b \neq 0). \tag{20}$$

□

Next we consider how many FCG exist other than the above example. From Proposition 2.2 (b), it immediately follows that if two elements $A, B \in \mathbf{GL}_2(\mathbb{F}_q)$ generates the same sequence up to a shift of index and choices of initial values, i.e., if $\psi_A^\ell(u_0) = \psi_B^{\ell+\ell_0}(u'_0)$ for for some $\ell_0 \in \mathbb{Z}, u_0, u'_0 \in \mathbb{F}_q$ and for $\ell \geqslant 0$ holds, then A is a scalar multiple of B unless their periods are too short ($\leqslant 3$). So removing the redundancy by a scalar multiplication, an FCG of nonlinear type is exactly characterized by $\left(\begin{smallmatrix} a & b \\ 1 & d \end{smallmatrix}\right) \in \mathbf{GL}_2(\mathbb{F}_q)$. On the other hand, an ICG is characterized by two elements of $\mathbb{F}_q$. Thus there exist many FCG that are not covered by ICG.

In fact, this extra degree of freedom is completely explained by the choice of the geometric interpretation. Let $A := \left(\begin{smallmatrix} a & b \\ 1 & d \end{smallmatrix}\right)$ and $A_0 := \left(\begin{smallmatrix} a+d & -(ad-b) \\ 1 & 0 \end{smallmatrix}\right)$. Then ψ_{A_0} is an ICG. Recall from Eq. (15) that

$$A = \begin{pmatrix} 1 & d \\ 0 & 1 \end{pmatrix}^{-1} A_0 \begin{pmatrix} 1 & d \\ 0 & 1 \end{pmatrix}. \tag{21}$$

Noting that $\left(\begin{smallmatrix} 1 & d \\ 0 & 1 \end{smallmatrix}\right) \in \mathcal{B}$ fixes ∞, we have

$$\psi_A^\ell(u_0) = \psi_{A_0}^\ell(u_0 + d) - d$$

for all $\ell \geqslant 0$ and $u_0 \in \mathbb{F}_q$. If we redefine the geometric interpretations $\mathrm{GI}, \mathrm{GI}'$ and GI by

$$\mathrm{GI}_d(u) := \mathrm{GI}(u-d), \tag{22}$$

$$\mathrm{GI}'_d(u) := \mathrm{GI}'(u-d), \tag{23}$$

$$\mathsf{GI}_d(u) := \mathsf{GI}(u-d), \tag{24}$$

respectively, then it follows that

$$\mathrm{gi}_0(\psi_A^\ell(u_0)) = \mathrm{gi}_d(\psi_{A_0}^\ell(u_0+d)) \quad (\ell \geqslant 0),$$

where gi is either of $\mathrm{GI}, \mathrm{GI}'$ or GI. This asserts the following statement.

Proposition 3.3. Let $(\mathrm{GI}_0(u_n))_{n\geqslant 0}$ be the sequence generated by a nonlinear FCG and the geometric interpretation GI_0. Then there exists an ICG which generates the same sequence, by appropriate choice of the geometric interpretation GI_d and the initial value. Same hold for GI' and GI. □

Especially, for the cases GI and GI, the output sequence of an FCG is a geometrical shift (modulo one) of the sequence by an ICG. In this sense, FCGs do not provide random numbers of new type. However, the definition of FCG shall be meaningful, at least, to inspect properties with respect to compositions of ICGs. Observe that ψ_{A^ℓ} are not, in general, an ICG even if ψ_A is so (The form Eq. (20) is fragile under multiplications). Of course they remain to be FCG, and we shall explain some applications of this fact in Sect. 5.

4. Discrepancy Bounds of FCG in Parts of the Period

For the case $k = 1$, Theorem 1.5 is transparently extended to FCG of nonlinear type.

Theorem 4.1 Suppose that $k = 1$, i.e. $\mathbb{F}_q = \mathbb{F}_p$. Let ψ_A be an FCG of nonlinear type (i.e. $A \notin \mathcal{B}$). Let $(y_0, y_1, \dots)$ be the sequence after a geometric interpretation GI_d of the form Eq. (22) generated by ψ_A, and let T be its period. Let $s \geqslant 1$ and put $\mathbf{t}_n := (y_n, \dots, y_{n+s-1})$ for each n. Then the discrepancy bound Eq. (8) of Theorem 1.5 holds for this sequence.

Proof. By proposition 3.3, there exists an integer C such that $y_n = ((u_n + C))/p$ $(n \geqslant 0)$, where $(u_n \in \mathbb{F}_p)$ is the sequence from some ICG of the same period T. So it suffices to check that the robustness of bound Eq. (8)

with respect to the transform $u_n \mapsto u_n + C$ in $\mathbb{F}_p$. Since Definition 1.4 slightly depends on the boundary of the cube $[0,1)^s$, we look into the proofs of Theorem 1.5

In [13], the bound Eq. (8) is derived as follows. For any $\mathbf{v} = (v_n \in \mathbb{F}_p)_{n \geqslant 0}$ and $\mathbf{h} = (h_0, \dots, h_{s-1}) \in \mathbb{F}_p^s$, define the exponential sum

$$S_{\mathbf{h}}(\mathbf{v}; N) := \sum_{n=0}^{N-1} \exp\left(\frac{2\pi\sqrt{-1}\sum_{i=0}^{s-1} h_i v_{n+i}}{p}\right), \quad (25)$$

where we omit $((\cdot))$ around $\sum h_i v_{n+i}$ because the quantity depends only on the mod p class.

(i) Bound the exponential sums on the ICG.
It is shown that [13, Theorem 4]
If $\mathbf{u} = (u_0, u_1, \dots)$ is the sequence from an ICG of period T, then for all $\mathbf{h} = (h_0, \dots, h_{s-1}) \in (\mathbb{F}_p^\times)^s$ it follows that

$$|S_{\mathbf{h}}(\mathbf{u}; N)| \leqslant \left(4s + \sqrt{8/3}\right)^{\frac{1}{2}} N^{\frac{1}{2}} p^{\frac{1}{4}} + O(p^{\frac{1}{2}}) \quad (1 \leqslant N \leqslant T), \quad (26)$$

where the implied constant depends only on s. (The key to prove this bound is the bound [18] for certain exponential sum of rational functions, which in turn depends on the Weil-Bombieri bounds [1], [26].)

(ii) Apply the general discrepancy bound [20, Corollary 3.11]. This bound depends only on the upper bound B of $|S_{\mathbf{h}}(\mathbf{u}; N)|$ for all $\mathbf{h} \in (\mathbb{F}_p^\times)^s$; no special property of $\mathbf{u}$ is used. The bound is:

$$D^{(s)}(\{\mathbf{t}_0, \dots, \mathbf{t}_{N-1}\}) \leqslant 1 - (1 - p^{-1})^s + \frac{B}{N}\left((4/\pi^2)\log p\right)^s, \quad (27)$$

where $\mathbf{t}_n = (u_n, u_{n+1}, \dots, u_{n+s-1})$.

So only to check is (i). However, replacing v_{n+i} with $v_{n+i} + C$ in Eq. (25) changes $S_{\mathbf{h}}(\mathbf{v}; N)$ only by the constant factor

$$\exp\left(\frac{2\pi\sqrt{-1}\sum_{i=0}^{s-1} h_i C}{p}\right),$$

whose absolute value is obviously 1. Thus the inequality Eq. (26) is not affected by $u_n \mapsto u_n + C$. □

Also for arbitrary $k \geqslant 1$, Theorems 1.6 and 1.7 are transparently extended to FCG of nonlinear type, since these bounds are derived from the upper bound (in absolute value) of

$$\sum_{n=0}^{N-1} \chi\Big(\sum_{i=1}^{s} \mu_i u_{n+i-1}\Big)$$

where $\mu_i \in \mathbb{F}_q$ are constants and χ is a nontrivial character of $\mathbb{F}_q$, and the shift $u_n \mapsto u_n + C$ changes the quantity only by a complex constant of absolute value one.

Theorem 4.2. Let ψ_A be an FCG of nonlinear type (i.e. $A \notin \mathcal{B}$). Let $(y'_0, y'_1, \dots)$ be the sequence by ψ_A and a geometric interpretation GI'_d of the form Eq. (23), and let T be its period. Let $s \geqslant 1$ and put $\mathbf{t}'_n := (y'_n, \dots, y'_{n+s-1})$ for each n. Then the discrepancy bound Eq. (9) of Theorem 1.6 holds for this sequence.

Theorem 4.3. Let ψ_A be an FCG of nonlinear type (i.e. $A \notin \mathcal{B}$). Let $(\mathbf{y}_0, \mathbf{y}_1, \dots)$ be the sequence by ψ_A and a geometric interpretation GI_d of the form Eq. (24), and let T be its period. Let $s \geqslant 1$ and put $\tau_n := (\mathbf{y}_n, \dots, \mathbf{y}_{n+s-1})$ for each n. Then the discrepancy bound Eq. (10) of Theorem 1.7 holds for this sequence.

5. Robustness under Decimation

Here we explain an application of Definition 3.1 and Theorems 4.1, 4.2 and 4.3. Namely, using group theoretic properties, some robustness is shown in discrepancy and nonlinearity, under a decimation of the sequence.

By definition, $\mathbf{GL}_2(\mathbb{F}_q) \ni A \mapsto \psi_A$ is *almost* homomorphism. However, the first case of Eq. (19) prevents the correspondence to be homomorphic. In fact the sequence $(u_n)_{n=0}^{N-1} = (\psi_A^n(u_0))_{n=0}^{N-1}$ in a part of the period avoids the first case of Eq. (19), by appropriate choices of A and u_0. We write this partial homomorphic condition as:

$$C(A, u_0, N): \quad A^n\langle u_0\rangle \neq \infty \text{ for } 0 \leqslant n < N.$$

Obviously this is equivalent to:

$$A^n\langle u_0\rangle = \psi_A^n(u_0) = \psi_{A^n}(u_0) \text{ for } 0 \leqslant n < N.$$

For example, if A is elliptic and ψ_A has the maximum period q, the following choice of u_0 ensures the condition $C(A, u_0, N)$ $(N \leqslant q)$. Choose r arbitrarily with $1 \leqslant r \leqslant q - N$. Then put $u_0 := A^r\langle\infty\rangle$ (Here u_0 can be computed by squaring and multiplicating of A.)

5.1 Decimation of the Sequence

Theorem 5.1. Let A be an element of $\mathbf{GL}_2(\mathbb{F}_q) \setminus \mathcal{B}$ and u_0 an element of $\mathbb{F}_q$. Let $T \geqslant 3$ be the period of $(\psi_A^n(u_0))_{n \geqslant 0}$, and let m and N_1 be positive integer with $mN_1 \leqslant T$, then put $N := mN_1$ and $A_1 := A^m$ respectively. Suppose that the condition $C(A, u_0, N)$ is met. Then the followings hold:

(i) ψ_{A_1} is of nonlinear type.
(ii) The period T_j of the sequence $(\psi_{A_1}^n(A^j\langle u_0\rangle))_{n \geqslant 0}$ satisfies $T_j \geqslant T/m - 1$ $(0 \leqslant j < m)$.

(iii) $\psi^n_{A_1}(A^j\langle u_0\rangle) = \psi^{mn+j}_A(u_0)$ holds for all integers $0 \leqslant j < M$ and $0 \leqslant n < N_1$, i.e, each of sequences $(\psi^n_{A_1}(A^j\langle u_0\rangle))^{N_1-1}_{n=0}$ is a $(1:m)$ decimated version of $(\psi^n_A(u_0))^N_{n=0}$ starting with $\psi^j_A(u_0)$.

(iv) For each of the decimated sequences $(u_{n,j})^{N_1-1}_{n=0} := (\psi^n_{A_1}(A^j\langle u_0\rangle))^{N_1-1}_{n=0}$, put $y_{n,j} := \mathrm{GI}_0(u_{n,j})$ if $k = 1$, where GI_0 is defined as Eq. (22). Also put $y'_{n,j} := \mathrm{GI}'_0(u_{n,j})$ and $\mathbf{y}_{n,j} := \mathrm{GI}_0(u_{n,j})$ respectively. Define corresponding $\mathbf{t}_n, \mathbf{t'}_n$ and τ_n as in Theorems 4.1, 4.2 and 4.3 respectively. Then they satisfy corresponding discrepancy bounds Eqs. (8) (9), and (10) respectively, with substitution T by $T/m - 1$ in these expressions.

Proof. (i) From the assumption, we have $m < T$. On the other hand, by the assumption $T \geqslant 3$ and Proposition 2.2(c), $A^\ell \notin \mathcal{B}$ for $m < T'$, where T' is the smallest positive index that $A^{T'} \in \mathcal{C}$, and $T \leqslant T'$ is satisfied (in fact $T = T'$ or $T = T' - 1$.)

(ii) Let T' be as above and define T'' similarly for A_1. Then mT'' should be a multiple of T'. Then $0 \leqslant T' - T \leqslant 1$ and $0 \leqslant T'' - T_j \leqslant 1$ give the lower bound for T_j.

(iii) By the condition $C(A, u_0, N)$, we have

$$\begin{aligned}\psi^n_{A_1}(A^j\langle u_0\rangle) &= {A_1}^n A^j\langle u_0\rangle \\ &= A^{mn+j}\langle u_0\rangle \\ &= \psi^{mn+j}_A(u_0)\end{aligned}$$

for all integers $0 \leqslant j < M$ and $0 \leqslant n < N_1$.

(iv) By (i), (ii) and (iii) the decimated sequence $(u_{n,j})^{N_1-1}_{n=0}$ is a subsequence of $(\psi^n_{A_1}(A^j\langle u_0\rangle))_{n\geqslant 0}$, which is generated by the FCG ψ_{A_1} of nonlinear type, with the period $\geqslant T/m - 1$. Then by Theorems 4.1, 4.2 and 4.3, the corresponding bounds follow.

□

Thus, under the condition $C(A, u_0, N)$, each decimated sequence preserves nonlinearity and reasonable discrepancy bounds. Note that the discrepancy bound of the decimated sequence is weaker than that of the original sequence, due to the shrink of the length $N \to N_1$, however we paid nothing for any other overheads.

5.2 Leap-Frog Use

Consider the situation that m parties $\mathrm{P}_0, \ldots, \mathrm{P}_{m-1}$ perform a large-scale Monte Carlo simulation corporately and parallelly. Each P_j perform N_1 simulations using their own random numbers to obtain N_1 results (local data, for short). Total $mN_1 = N$ data are gathered from all the parties (global data, for short) for further analysis. Each party should choose pseudorandom numbers carefully so that the whole simulation is based on a low-discrepancy set of random number sequence. Also suppose that they wish to decide whether they gather all the simulation results for analysis based on the global data, depending on how successful (in the sense of that application) local data are. To make this decision, it is also required that each party choose their own pseudorandom numbers to keep a reasonable quality (in nonlinearity or discrepancy) in their local simulation result.

A solution for this problem is that

$$\mathrm{P}_j \quad \text{uses} \quad \psi^n_A(U_j) \quad (0 \leqslant n < N_1),$$

where the ICG ψ_A is common for all parties and $U_j = \psi^{jN_1}_A(u_0)$ (Compute these values by the repeated squaring of the matrix) with the common value $u_0 \in \mathbb{F}_q$. That is, a sequence of length mN_1 from A is divided into m contiguous blocks and they are assigned to each party (This technique is called as sequence splitting [4], [11]). The global and local data depend on a set of reliable (in nonlinearity and discrepancy) random numbers from A. However, until all of the parties finish their own N_1 simulations, the discrepancy of the global data is not guaranteed.

Another one is so-called *Leap-Frog* use [4], [11]:

$$\mathrm{P}_j \quad \text{uses} \quad \psi^n_{A_1}(A^j\langle u_0\rangle) \quad (0 \leqslant n < N_1),$$

where $A_1 = A^m$, ψ_{A_1} fractional linear of nonlinear type, as in the theorem. Then the quality of both local and global data are guaranteed by the theorem. An extra merit is that the global data have a low-discrepancy (depending on the length) even if the simulations are in progress. So prescribed value of N_1 is not needed. To save cost for generations, one may take A_1 (for which each party actually computes the recurrence) , rather than A, to be inversive linear.

6. Concluding Remarks

Fractional linear congruent generators, which include the linear and inversive linear congruent generators, have been formulated and analyzed in a group theoretic manner. The fractional linear generators of nonlinear type are in fact geometrically shifted version of the inversive linear generators. The upperbounds on discrepancy in parts of the period have been extended for these generalized generators. Then it has been verified that if certain condition is satisfied, the extended bounds are robust under a decimation of the sequence. The robustness enables so-called Leap-Frog use of FCG in the distributed Monte Carlo.

References

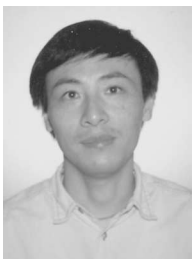
[1] E. Bombieri, "On exponential sums in finite fields," Amer. J. Math., vol.83, pp.71–105, 1966.

[2] W.-S. Chou, "The period lengths of inversive pseudorandom vector generations," Finite Fields Appl., vol.1, pp.126–132, 1995.

[3] W.-S. Chou, "On inversive maximal period polynomials over finite fields," Appl. Algebra Eng. Comm. Comput., vol.6, pp.245–250, 1995.
[4] P. Coddington, "Random number generators for parallel computers," NHSE Review, 2nd Issue, Northeast Parallel Architecture Center, 1996. Available at: http://nhse.cs.rice.edu/NHSEreview/RNG/
[5] J. Eichenauer-Herrmann, "Statistical independence of a new class of inversive congruential pseudorandom numbers," Math. Comp., vol.60, pp.375–384, 1993.
[6] J. Eichenauer-Herrmann, "Compound nonlinear congruential pseudorandom numbers," Monatsh. Math., vol.117, pp.213–222, 1994.
[7] J. Eichenauer-Herrmann, E. Herrmann, and S. Wegenkittl, "A survey of quadratic and inversive congruential pseudorandom numbers," Monte Carlo and Quasi-Monte Carlo Methods 1996, LNCS, vol.127, pp,66–97, 1998.
[8] J. Eichenauer and J. Lehn, "A non-linear congruential pseudo random number generator," Statist. Papers, vol.27, pp.315–326, 1986.
[9] J. Eichenauer, J. Lehn, and A. Topuzoglu, "A nonlinear congruential pseudorandom number generator with power of two modulus," Math. Comp., vol.51, pp.757–759, 1988.
[10] J. Eichenauer-Herrmann and H. Niederreiter, "Digital inversive pseudorandom numbers," ACM Trans. Model. Comput. Simul., vol.4, pp.339–349, 1994.
[11] K. Entacher, A. Uhl, and S. Wegenkittl, "Linear and inversive pseudorandom numbers for parallel and distributed simulation," Proc. 12th Workshop on Parallel and Distributed Simulation (PADS'98) , pp.90–97, IEEE Computer Society Press, 1998.
[12] M. Flahive and H. Niederreiter, "On inversive congruential generators for pseudorandom numbers," in Finite Fields, Coding Theory and Advances in Numbers, eds. G.L. Mullen, and P. J-S. Shuie, pp.75–80, Decker, New York, 1993.
[13] J. Guiterrez, H. Niederreiter, and I.E. Shparlinski, "On the multidimensional distribution of inversive congruential pseudorandom numbers in parts of the period," Monatsh. Math., vol.129, pp.31–36, 2000.
[14] K. Huber, "On the period length of generalized inversive pseudorandom number generators," Appl. Algebra Eng. Comm. Comput., vol.5, pp.255–260, 1994.
[15] H. Leeb and S. Wegenkittl, "Inversive and linear congruential pseudorandom gererators in empirical tests," ACM Trans. Model. Comput. Simul., vol.7, pp.272–286, 1997.
[16] D.H. Lehmer, "Mathematical methods in large-scale computing units," Proc. 2nd Symp. on Large-Scale digital calculating machinery, (Cambridge, MA, 1949) Harvard Univ. Press, Cambridge, MA., pp.141–146, 1951.
[17] G. Marsaglia, "The structure of linear congruential sequences," in Applications of Number Theory to Numerical Analysis, ed. S.K. Zaremba, Academic Press, New York, 1972.
[18] C.J. Moreno and O. Moreno, "Exponential sums and Goppa codes: I," Proc. Amer. Math. Soc. vol.111, pp.523–531, 1991.
[19] H. Niederreiter, "Finite fields and their applications," Contributions to General Algebra, vol.7, pp.251–264, Vienna 1990, Teubner, Stuttgart, Germany 1991.
[20] H. Niederreiter, Random number generation and quasi-Monte Carlo methods, CBMS-NSF Reginal conference series in applied mathematics, vol.63, SIAM, Philadelphia, 1992.
[21] H. Niederreiter and I.E. Shparlinski, "On the distribution of inversive congruential pseudorandom numbers in parts of the period," Math. Comp., vol.70, pp.1569–1574, 2000.
[22] H. Niederreiter and I.E. Shparlinski, "On the distribution of inversive congruential pseudorandom numbers and vectors generated by inversive methods," Appl. Algebra Eng. Comm. Comput., vol.10, pp.189–202, 2000.
[23] H. Niederreiter and A. Winterhof, "Incomplete exponential sums over finite fields and their applications to new inversive pseudorandom number generators," Acta. Arith., vol.93, pp.387–399, 2001.
[24] H. Niederreiter and A. Winterhof, "On the distribution of compound inversive congruential pseudorandom numbers," Monatsh. Math., vol.132, pp.35–48, 2001.
[25] A. Terras, Fourier Analysis on Finite Groups and Applications, London Mathematical Society Student Texts vol.43, Cambridge Univ. Press, New York, 1999.
[26] A. Weil, "On some exponential sums," Proc. Natl. Acad. Sci. USA vol.34, pp.204–207, 1948.
[27] P. L'Ecuyer and C. Lemieux, "Recent Advances in Randomized Quasi-Monte Carlo Methods," in Modeling Uncertainty: An Examination of Stochastic Theory, Methods, and Applications, eds. M. Dror, P. L'Ecuyer, and F. Szidarovszki, pp.419–474, Kluwer Academic Publishers, 2002.
[28] H. Faure, "Variations on $(0, s)$-Sequences," J. Complexity, vol.17, pp.741–753, 2001.

Yoshinori Takei was born in Tokyo, Japan in 1965. He received the B. Sc. and the M. Sc. degrees in mathematics in 1990, 1992, respectively from Tokyo Institute of Technology, Tokyo, Japan, and the D. Eng. degree in information processing in 2000, from Tokyo Institute of Technology, Yokohama, Japan. From 1992 to 1995 he was with Kawasaki Steel System R&D Inc. From 1999 to 2000, he was an Assistant Professor in the Department of Electrical and Electronic Engineering, Tokyo Institute of Technology. Since 2000, He has been with the Department of Electrical Engineering, Nagaoka University of Technology, Niigata, Japan, where he is currently an Assistant Professor. His current research interests include computational complexity theory, public-key cryptography, combinatorics and digital signal processing. Dr. Takei is a member of LA, SIAM, ACM, AMS and IEEE.

Toshinori Yoshikawa was born in Kagawa, Japan 1948. He received the B.E., M.E. and Doctor of Engineering degree from Tokyo Institute of Technology, Tokyo, Japan, in 1971, 1973 and 1976, respectively. From 1976 to 1983, he was with Saitama University engaging in research works on signal processing and its software development. Since 1983, he has been with Nagaoka University of Technology, Niigata, Japan, where he is currently a Professor. His main research area is digital signal processing. Dr. Yoshikawa is a member of the IEEE Computer Society.



Xi Zhang received the B.E. degree in electronics engineering from the Nanjing University of Aeronautics and Astronautics (NUAA), Nanjing, China, in 1984, and the M.E. and Ph.D. degrees in communication engineering from the University of Electro-Communications (UEC), Tokyo, Japan, in 1990 and 1993, respectively. He was with the Department of Electronics Engineering at NUAA from 1984 to 1987, and the Department of Communications and Systems at UEC from 1993 to 1996, all as an Assistant Professor. Currently, he is with the Department of Electrical Engineering, Nagaoka University of Technology, Niigata, Japan, as an Associate Professor. He was a visiting scientist of the Ministry of Education, Culture, Sports, Science and Technology (MEXT) of Japan at the Massachusetts Institute of Technology (MIT), Cambridge, MA, USA, from 2000 to 2001. He is serving as an Associate Editor for the IEEE Signal Processing Letters since 2002. His research interests are in the areas of digital signal processing, filter design theory, filter banks and wavelets, and its applications to image coding. Dr. Zhang is a senior member of the IEEE. He received the third prize of the Science and Technology Progress Award of China in 1987, and the challenge prize of 4th LSI IP Design Award of Japan in 2002.