EUROPEAN JOURNAL OF PURE AND APPLIED MATHEMATICS
Vol. 14, No. 1, 2021, 1-18
ISSN 1307-5543 – ejpam.com
Published by New York Business Global

A hybrid inversive congruential pseudorandom number generator with high period

Constanza Riera[1], Tapabrata Roy[2], Santanu Sarkar[2], Pantelimon Stănică[3,*]

[1] *Department of Computer science, Electrical Engineering and Mathematical Sciences, Western Norway University of Applied Sciences, Bergen, Norway*
[2] *Department of Mathematics,Indian Institute of Technology Madras, Sardar Patel Road, Chennai TN 600036, INDIA*
[3] *Department of Applied Mathematics, Naval Postgraduate School, Monterey, CA 93943–5216, USA*

Abstract. Though generating a sequence of pseudorandom numbers by linear methods (Lehmer generator) displays acceptable behavior under some conditions of the parameters, it also has undesirable features, which makes the sequence unusable for various stochastic simulations. An extension which showed promise for such applications is a generator obtained by using a first-order recurrence based upon the inverse modulo a prime or a prime power, called inversive congruential generator (ICG). A lot of work has been dedicated to investigate the periods (under some conditions of the parameters), the lattice test passing, discrepancy and other statistical properties of such a generator. Here, we propose a new method, which we call hybrid inversive congruential generator (HICG), based upon a second order recurrence using the inverse modulo M, a power of 2. We investigate the period of this pseudorandom numbers generator (PRNG) and give necessary and sufficient conditions for our PRNG to have periods M (thereby doubling the period of the classical ICG) and $M/2$ (matching the one of the ICG). Moreover, we show that the lattice test complexity for a binary sequence associated to (a full period) HICG is precisely $M/2$.

2020 Mathematics Subject Classifications: 11B50, 11K36, 11K45
Key Words and Phrases: Pseudorandom numbers, congruences, period, lattice test.

1. Introduction

The linear congruential method is one of the standard methods of generating uniform pseudorandom numbers (PRNs) in the interval $I = [0, 1)$. In this method, for a (large) modulus M, a sequence $\{y_n\}$ of integers in $\mathbb{Z}_M = \{0, 1, \ldots, M-1\} = \mathbb{Z}/M\mathbb{Z}$ is generated by the linear recursion

$$y_{n+1} \equiv ay_n + b \mod M,\ n = 0, 1, \ldots;\ a, b \in \mathbb{Z}_M. \tag{1}$$

*Corresponding author.
DOI: https://doi.org/10.29020/nybg.ejpam.v14i1.3852

Email addresses: csr@hvl.no (C. Riera), tapabrata.roy.048@gmail.com (T. Roy), sarkar.santanu.bir1@gmail.com (S. Sarkar), pstanica@nps.edu (P. Stănică)

and then the PRNs are obtained by the normalization

$$x_n = y_n/M. \tag{2}$$

This linear method is popular and has been thoroughly analyzed [15]. However, it has been found that the linearity of the recursion leads to some drawbacks and as a result, recently, several nonlinear congruential generators [3–10, 12, 15, 19] have been proposed and also analyzed [11]. Amongst these, the inversive congruential method (ICG) [17–19], with modulus M (with M being either a prime or a large power of 2), is one of the most interesting ones. Here, we consider the case where $M = 2^\omega$, for some integer $\omega \geq 2$. Let $G_M = \{1, 3, \ldots, M-1\}$ be the set of all positive odd integers less than M. Clearly, for any $u \in G_M$, there is a unique $u^{-1} \in G_M$ such that $uu^{-1} \equiv 1 \pmod M$. The first sequence $\{y_n\} \subseteq G_M$ based upon the inverse modulo M is given by the recursion

$$y_{n+1} \equiv ay_n^{-1} + b \pmod M, n = 0, 1, \ldots. \tag{3}$$

Here $a, b \in \mathbb{Z}_M$ are chosen in such a way that $y_{n+1} \in G_M$ whenever $y_n \in G_M$. The following result is known (we use $per(\cdot)$ to denote the period of the argument sequence).

Theorem 1 ([19, p.188, Theorem 8.9])**.** *Let $M = 2^\omega, \omega \geq 3$. Then the Pseudorandom Number Generator (PRNG) $\{y_n\}$ corresponding to the inversive congruential generator with modulus M satisfies $per(y_n) = \frac{M}{2}$ if and only if $a \equiv 1 \pmod 4$ and $b \equiv 2 \pmod 4$.*

Later in [14], the authors modified (3) and proposed another nonlinear method, which we will describe below. For a modulus $M = 2^\omega$ and $y_0 \in G_M$, let

$$y_{n+1} \equiv ay_n^{-1} + b + cy_n \pmod M, n = 0, 1, \ldots, \tag{4}$$

where $a, b, c \in \mathbb{Z}_M$ are such that $y_{n+1} \in G_M$, whenever $y_n \in G_M$. The main result obtained in [14] is the following theorem.

Theorem 2 ([14])**.** *Let $M = 2^\omega, \omega \geq 3$. Then the PRNG $\{y_n\}$ derived from (4) is purely periodic with period $\frac{M}{2}$ if and only if $a + c \equiv 1 \pmod 4$ and $b \equiv 2 \pmod 4$.*

In this paper, we propose a new nonlinear method, which we will call *hybrid inversive congruential generator (HICG)*. For the modulus $M = 2^\omega$ and $y_0, y_1 \in G_M$, we let

$$y_{n+2} \equiv ay_{n+1}^{-1} + by_n + c \pmod M, n = 0, 1, \ldots, \tag{5}$$

where $a, b, c \in \mathbb{Z}_M$ are such that $y_{n+2} \in G_M$ whenever $y_n, y_{n+1} \in G_M$. Then, the PRNs $\{x_n\}$, defined by (2), belong to the set $H_M = \left\{\frac{1}{M}, \frac{3}{M}, \ldots, \frac{M-1}{M}\right\}$. Since some of the constants in our generator may be zero, equation (5) includes (1) and (3).

In our first result, we show that the period of the HICG sequence is at most M; further, we obtain explicit conditions on the involved parameters such that the sequence $\{y_n\}$ derived from (5) is purely periodic with period M; moreover, we give explicit conditions on the parameters to obtain an ultimate period of $M/2$. Furthermore, we look at the lattice test passing for a binary sequence obtained via HICG and show that it has a lattice test complexity (defined in Section 4) equal to $M/2$.

2. The maximum period of the HICG is M

Since two consecutive residues modulo $M = 2^\omega$ will determine the next residue (observe that our sequence has second order), the maximum period can be at most twice the number of pairs (residue repetitions allowed) of all odd integers modulo M, that is $\frac{M^2}{4}$. However, here, we will show that for any values of the parameters a, b, c and any odd initial conditions $y_0, y_1 \in G_M$, the (ultimate) period of $\{y_n\}$ can be at most M. Certainly, the sequence may not be purely periodic, rather ultimately periodic, but for simplicity, shifting the sequence to that first position of the period, we may assume in this section that the period starts from y_0. Throughout, we will use the notation $\because$ as a shorthand for "because/since".

Theorem 3. *Let $m = 2^\omega \geq 4$. The HICG sequence $\{y_n \pmod m\}$ has an ultimate period less than or equal to m.*

Proof. We will show our result by induction. We first note that for $m = 4$ (and $m = 8$), the period is at most m. We now assume that the result holds for m, that is, $\{y_n \pmod m\}$ has period $\ell \leq m$, and show that $\{y_n \pmod{2m}\}$ has period at most $2m$. The given sequence is $y_{n+2} \equiv a y_{n+1}^{-1} + b y_n + c \pmod{2m}$. Now, note that $(y_n + m)^{-1} \equiv y_n^{-1} + m \pmod{2m}$ for all n. Clearly, in order for the y_n to be odd, $a + b + c$ must be odd. And so, among a, b and c, either all of them are odd or one of them is odd and the others are even. So, we consider the following four cases.

Case 1. a, b **and** c **are all odd:** As $y_{n+2} \equiv a y_{n+1}^{-1} + b y_n + c \pmod m$ has period ℓ, then we can have the following four subcases:

(i) $y_\ell \equiv y_0 \pmod{2m}$ and $y_{\ell+1} \equiv y_1 \pmod{2m}$,

(ii) $y_\ell \equiv y_0 + m \pmod{2m}$ and $y_{\ell+1} \equiv y_1 + m \pmod{2m}$,

(iii) $y_\ell \equiv y_0 \pmod{2m}$ and $y_{\ell+1} \equiv y_1 + m \pmod{2m}$,

(iv) $y_\ell \equiv y_0 + m \pmod{2m}$ and $y_{\ell+1} \equiv y_1 \pmod{2m}$.

The first subcase follows immediately, and the period modulo $2m$ is also ℓ here. For the second subcase, we have,

$$\begin{aligned}
y_{\ell+2} &\equiv a(y_1^{-1} + m) + b(y_0 + m) + c \pmod{2m} \\
&\equiv y_2 + (a + b)m \pmod{2m} \\
&\equiv y_2 \pmod{2m} \ (\because a + b \text{ is even}), \\
y_{\ell+3} &\equiv a y_2^{-1} + b(y_1 + m) + c \pmod{2m} \\
&\equiv y_3 + bm \pmod{2m} \\
&\equiv y_3 + m \pmod{2m} \ (\because b \text{ is odd}), \\
y_{\ell+4} &\equiv a(y_3^{-1} + m) + b y_2 + c \pmod{2m} \\
&\equiv y_4 + am \pmod{2m}
\end{aligned}$$

$$\begin{aligned} &\equiv y_4 + m \pmod{2m} \ (\because a \text{ is odd}),\\ y_{\ell+5} &\equiv a(y_4^{-1} + m) + b(y_3 + m) + c \pmod{2m}\\ &\equiv y_5 + (a+b)m \pmod{2m}\\ &\equiv y_5 \pmod{2m} \ (\because (a+b) \text{ is even}). \end{aligned}$$

Proceeding similarly, we have, $y_{\ell+6} \equiv y_6 + m \pmod{2m}$, $y_{\ell+7} \equiv y_7 + m \pmod{2m}$, $y_{\ell+8} \equiv y_8 \pmod{2m}$, and so on. Now, computationally we can check that for $m = 16$, ℓ can be $1, 3, 6, 12$. Inductively, it follows that if $\{y_n \pmod m\}$ has period 1 then $\{y_n \pmod{2m}\}$ has period 3 and if $\{y_n \pmod m\}$ has a period that is a multiple of 3 then, $\{y_n \pmod{2m}\}$ can have at most a double period. Thus, in this case, $\{y_n \pmod{2m}\}$ can have the period at most $\frac{3m}{2} < 2m$.

The other two subcases follow similarly and it can be shown that even in these subcases $\{y_n \pmod{2m}\}$ can have period at most $\frac{3m}{2} < 2m$.

Note that, in this case, the proof implies that $\{y_n \pmod m\}$ can have period at most $\frac{3m}{4}$, for all $m \geq 16$.

Case 2. a **is odd and** b **and** c **are even:** Here we break the case into the same possible subcases as above. The first subcase is immediate. For, the second subcase, following exactly the same procedure as above, we obtain $y_{\ell+2} \equiv y_2 + m \pmod{2m}$, $y_{\ell+3} \equiv y_3 + m \pmod{2m}$, $y_{\ell+4} \equiv y_4 + m \pmod{2m}$, and so on. Now, it can be checked that for $m = 16$ the possible periods are $1, 2, 4$ and 8. So, inductively, it follows that, the period of $\{y_n \pmod{2m}\}$ can be at most m. The other cases can be similarly dealt with.

Note that, in this case, the proof implies that $\{y_n \pmod m\}$ can have period at most $\frac{m}{2}$, for all $m \geq 16$.

Case 3. b **is odd and** a **and** c **are even:** This case follows along the same lines as the previous case. In this case, one can computationally check that, for $m = 16$, the possible periods are $1, 2, 4, 8$ and 16. So, the period of $\{y_n \pmod{2m}\}$ can be at most $2m$. Therefore, in this case, the proof implies that $\{y_n \pmod m\}$ can have period at most m, for all $m \geq 16$.

Case 4. c **is odd and** a **and** b **are even:** Here we break the case into the same possible subcases as in Case 1. The first subcase follows immediately. For, the other subcases we can easily check that $y_{\ell+2} \equiv y_2 \pmod{2m}$, $y_{\ell+3} \equiv y_3 \pmod{2m}$, $y_{\ell+4} \equiv y_4 \pmod{2m}$, and so on. Now, in this case, one can observe that for $m = 16$ the period is (ultimately) 1. So, in this case, the (ultimate) period of $\{y_n \pmod{2m}\}$ is again $1 \leq 2m$. Note that, in this case, the proof implies that $\{y_n \pmod m\}$ has period 1, for all $m \geq 16$.

Example 1. *Consider the first case, i.e., a, b and c are all odd. Let $m = 16$, and let the period of the sequence be 6. Then $\{y_0, y_1, y_2, y_3, y_4, y_5\}$ is the core of the sequence modulo 16. Consider now the same sequence modulo 32. We show that the period can be at most 12 modulo 32. The first subcase would give a period of 6. For the second subcase, i.e., $y_6 \equiv y_0 + 16$ and $y_7 \equiv y_1 + 16$ (all congruences are modulo 32 in this example), we can*

easily calculate that $y_8 \equiv y_2, y_9 \equiv y_3 + 16, y_{10} \equiv y_4 + 16, y_{11} \equiv y_5, y_{12} \equiv y_6 + 16 \equiv y_0$ *and* $y_{13} \equiv y_7 + 16 \equiv y_1$. *And so,* $\{y_0, y_1, \ldots, y_{11}\}$ *is the core of the sequence and the period is* 12. *The other two subcases are similar.*

Remark 1. *Note that, from the proof, one can actually infer, for* $m \geq 16$, *that the HICG sequence* $\{y_n \pmod m\}$ *has an (ultimate) period less than or equal to* $\frac{3m}{4}$, *if* a, b *and* c *are odd; less than or equal to* $\frac{m}{2}$, *if* a *is odd and* b *and* c *are even; less than or equal to* m, *if* b *is odd and* a *and* c *are even; and, finally, the period is always* 1, *if* c *is odd and* a *and* b *are even.*

3. General periodicity analysis of the sequence

Let $M = 2^\omega$; $\omega \geq 3$, y_0 and y_1 are chosen at random from G_M.

3.1. Conditions when the period of the sequence is M

Theorem 4. *The PRNG* $\{y_n\}$ *derived from* (5) *(regardless of the odd initial conditions* y_0, y_1*) is purely periodic with period* M *and the set* $\{y_0, y_1, \ldots, y_{M-1}\}$ *gives the set* G_M, *uniformly distributed (that is, every element will occur exactly twice), if and only if*

$$a \equiv 0 \pmod 2, a + b \equiv 1 \pmod 4 \text{ and } c \equiv 2 \pmod 4.$$

Proof. We show this in two steps.

Necessity: Let us assume that for the sequence (5) and for any $y_0, y_1 \in G_M$, the period of y_n is M and $\{y_0, y_1, \ldots, y_{M-1}\}$ gives the set G_M with every element occurring exactly twice. We will prove that a is even, $a + b \equiv 1 \pmod 4$ and $c \equiv 2 \pmod 4$. Without loss of generality we may take $y_0 = y_1 = 1$. Now, it is easy to check that under the above assumption on the parameters a, b, c, if we reduce every element modulo 4 (respectively, 8), the period of $\{y_n \pmod 4\}$ (respectively, $\{y_n \pmod 8\}$) is 4 (respectively, 8) and $\{y_0, y_1, y_2, y_3\}$ (respectively, $\{y_0, y_1, \ldots, y_7\}$) gives the set $G_4 = \{1, 3\}$ (respectively, $G_8 = \{1, 3, 5, 7\}$) with every element occurring exactly twice.

Now, for our convenience, for the rest of the necessary part we consider every equality as a modulo 8 operation and hence (5) reduces to

$$y_{n+2} = ay_{n+1} + by_n + c,$$

since $t \equiv t^{-1} \pmod 8$, for every odd integer t. Also, we recall that we have $y_0 = y_1 = 1$.

By absurd, we now assume that $a + b$ is even. Then, $y_2 = a + b + c \equiv 3 \pmod 4$ implies that c is odd. So, let $a + b = 2d$ and $c = 1 + 2e$ for some integers d and e. We have, $y_2 = 1 + 2(d + e)$ where $d + e = 1 + 2f$, $f \in \mathbb{Z}$ is odd (since $y_2 \equiv 3 \pmod 4$). Then, from $y_3 \equiv 3a + b + c \equiv 3 \pmod 4$ we have $3 + 2a \equiv 3 \pmod 4$ and thus a is even. We let $a = 2g$, $g \in \mathbb{Z}$. Thus, $y_4 \equiv 3a + 3b + c \equiv 1 \pmod 4$ yields $3(2d) + 1 + 2e = 1 + 2(d + e) = 3 + 4f \equiv 3 \pmod 4$, which is a contradiction. Hence, $a + b$ is odd.

Suppose now that $a+b \equiv 3 \pmod 4$, and so $a+b = 3+4h, h \in \mathbb{Z}$. From $y_2 = a+b+c \equiv 3 \pmod 4$, we have, $c = 4l, l \in \mathbb{Z}$. Then, $y_3 = ay_2 + b + c = a(3 + 4(h + l)) + b + c = 3 + 2a + 4(h + l)(a + 1) \equiv 3 \pmod 4$ gives $a = 2r, r \in \mathbb{Z}$ and so, from $a + b = 3 + 4h$, b is odd. Thus, $y_3 = ay_2+b+c = 3+4(h+\ell+r)$. Thus, $y_4 = ay_3+by_2+c = 1+4(h+l)(b+1) \equiv 1 \pmod 8$ (as b is odd). However, the periodicity modulo 4 implies that $y_4 \equiv 1 \pmod 4$, and therefore, $y_4 \equiv 1$ or $5 \pmod 8$. But, 1 has already occurred twice. So, $y_4 \equiv 5 \pmod 8$, which contradicts $y_4 \equiv 1 \pmod 8$.

Hence, $a + b \equiv 1 \pmod 4$ which implies $c \equiv 2 \pmod 4$ and a is even (the parity of a can be deduced, for instance, from $y_2 \equiv a + b + c \equiv 3 \pmod 4$ and $y_3 \equiv 3a + b + c \equiv 3 \pmod 4$; then, $2a \equiv 0 \pmod 4$).

Sufficiency: Let now a be even, $a + b \equiv 1 \pmod 4$ and $c \equiv 2 \pmod 4$, and $y_0, y_1 \in G_M$. First, we will prove that $y_n \in G_M$ for all $n \geq 0$, that is, y_n is odd under these assumptions. Now, y_0 and y_1 are odd. Suppose that y_n is odd. Then,

$$y_{n+2} = ay_{n+1}^{-1} + by_n + c \equiv y_n \equiv 1 \pmod 2.$$

We will now prove that the period is M. We first rewrite the sequence (5) as

$$y_{n+2} \equiv (a + b)y_n + cy_{n+1} + \alpha_n \pmod M$$

where

$$\alpha_n = a(y_{n+1}^{-1} - y_n) + c(1 - y_{n+1}).$$

So,

$$\begin{pmatrix} y_n \\ y_{n+1} \end{pmatrix} \equiv A \begin{pmatrix} y_{n-1} \\ y_n \end{pmatrix} + \begin{pmatrix} 0 \\ \alpha_{n-1} \end{pmatrix} \pmod M \text{ where } A = \begin{pmatrix} 0 & 1 \\ a+b & c \end{pmatrix}.$$

Thus, we have,

$$\begin{pmatrix} y_n \\ y_{n+1} \end{pmatrix} \equiv A^n \begin{pmatrix} y_0 \\ y_1 \end{pmatrix} + R_n \pmod M \tag{6}$$

where

$$R_n = \sum_{i=0}^{n-1} A^i \begin{pmatrix} 0 \\ \alpha_{n-1-i} \end{pmatrix}.$$

Taking into account the fact that $a + b \equiv 1 \pmod 4$ and $c \equiv 2 \pmod 4$, from [16] or [19, p.188] we have for $m = 2^h, h \geq 2$,

$$A^m \equiv \begin{pmatrix} 2mp + m + 1 & 2mq + 3m \\ 2mq + 3m & 2mp + 3m + 1 \end{pmatrix} \pmod{4m} \tag{7}$$

for some integers p and q.

First, we will show that for $m = 2^h, 2 \leq h \leq \omega - 1$,

$$R_m \equiv \begin{pmatrix} m \\ m \end{pmatrix} \pmod{2m}. \tag{8}$$

It can be checked (tediously by hand, but computationally easily) that (8) holds for $m = 4$ (i.e., $h = 2$). Now, let us assume that it holds for $m = 2^h$. Then, from this hypothesis, (6) and (7), and using the fact that y_i's are odd, we have,

$$\begin{aligned} y_m &\equiv y_0 + 2m(py_0 + qy_1) + m(y_0 + 3y_1) + 4mT_0 + m + 2mS_0 \\ &= y_0 + m + 2mU_0 \pmod{M}, \\ y_{m+1} &\equiv y_1 + 2m(qy_0 + py_1) + 3m(y_0 + y_1) + 4mT_1 + m + 2mS_1 \\ &= y_1 + m + 2mU_1 \pmod{M}, \end{aligned}$$

for some integers T_0, T_1, S_0, S_1, U_0 and U_1. Now, it follows clearly from above that

$$y_m^{-1} \equiv y_0^{-1} + m + 2mV_0 \text{ and } y_{m+1}^{-1} = y_1^{-1} + m + 2mV_1 \pmod{M},$$

for some integers V_0 and V_1 (inverses are considered in $\mathbb{Z}_M$). Then, as a is even and $c \equiv 2 \pmod 4$, we get from above that

$$\begin{aligned} \alpha_m &= a(y_{m+1}^{-1} - y_m) + c(1 - y_{m+1}) \\ &\equiv a(y_1^{-1} + m + 2mV_1 - y_0 - m - 2mU_0) + c(1 - y_1 - m - 2mU_1) \\ &\equiv a(y_1^{-1} - y_0) + c(1 - y_1) + 2am(V_1 - U_0) - mc - 2mcU_1 \\ &\equiv \alpha_0 + 2m + 4mW_0 \pmod{M}, \end{aligned}$$

for some integer W_0. So, as $a + b \equiv 1 \pmod 4$ and $c \equiv 2 \pmod 4$ we have,

$$\begin{aligned} y_{m+2} &\equiv (a+b)y_m + cy_{m+1} + \alpha_m \\ &\equiv (a+b)y_0 + cy_1 + \alpha_0 + (a+b)(m + 2mU_0) \\ &\qquad + c(m + 2mU_1) + 2m + 4mW_0 \\ &\equiv y_2 + m + 2mU_2 \pmod{M}, \end{aligned}$$

for some integer U_2. Proceeding similarly as above, for all $0 \le k \le m-1$, we have

$$\begin{aligned} y_{m+k} &\equiv y_k + m + 2mU_k \pmod{M} \\ y_{m+k}^{-1} &\equiv y_k^{-1} + m + 2mV_k \pmod{M} \\ \alpha_{m+k} &\equiv \alpha_k + 2m + 4mW_k \pmod{M}, \end{aligned}$$

for integers U_k, V_k and W_k. Now, using the above analysis, we get (we let I be the identity matrix of the appropriate dimension),

$$\begin{aligned} R_{2m} &\equiv \sum_{i=0}^{2m-1} A^i \begin{pmatrix} 0 \\ \alpha_{2m-1-i} \end{pmatrix} \pmod{4m} \\ &\equiv \sum_{i=0}^{m-1} A^i \begin{pmatrix} 0 \\ \alpha_{2m-1-i} \end{pmatrix} + \sum_{i=m}^{2m-1} A^i \begin{pmatrix} 0 \\ \alpha_{2m-1-i} \end{pmatrix} \pmod{4m} \end{aligned}$$

$$\equiv \sum_{i=0}^{m-1}\left[A^i\begin{pmatrix}0\\ \alpha_{m-1-i}\end{pmatrix}+A^i\begin{pmatrix}0\\ 2m\end{pmatrix}\right]+A^m\sum_{i=0}^{m-1}A^i\begin{pmatrix}0\\ \alpha_{m-1-i}\end{pmatrix} \pmod{4m}$$

$$\equiv (I+A^m)R_m+2m\sum_{i=0}^{m-1}A^i\begin{pmatrix}0\\ 1\end{pmatrix} \pmod{4m}$$

$$\equiv (\frac{I+A^m}{2})2R_m+2m\sum_{i=0}^{m-1}A^i\begin{pmatrix}0\\ 1\end{pmatrix} \pmod{4m}$$

$$\equiv (\frac{I+A^m}{2})\begin{pmatrix}2m\\ 2m\end{pmatrix}+2m\sum_{i=0}^{m-1}A^i\begin{pmatrix}0\\ 1\end{pmatrix} \pmod{4m}$$

$$\equiv \begin{pmatrix}2m\\ 2m\end{pmatrix}+2m\sum_{i=0}^{m-1}A^i\begin{pmatrix}0\\ 1\end{pmatrix} \pmod{4m}$$

$$\equiv \begin{pmatrix}2m\\ 2m\end{pmatrix} \pmod{4m}$$

$$[\ \because \sum_{i=0}^{m-1}A^i\begin{pmatrix}0\\ 1\end{pmatrix}\equiv 0 \pmod 2,\ \text{i.e.,}\ \sum_{i=0}^{m-1}A^i\begin{pmatrix}0\\ 1\end{pmatrix}\ \text{is even}].$$

Therefore, (8) follows by induction. So, by the previous arguments, we conclude that for $m=2^h, h\geq 2$ and $0\leq k\leq m-1$,

$$\begin{array}{lll} y_{m+k} & \equiv y_k+m & \pmod{2m}\\ y_{m+k}^{-1} & \equiv y_k^{-1}+m & \pmod{2m}\\ \alpha_{m+k} & \equiv \alpha_k+2m & \pmod{4m}. \end{array}$$

Then in particular for $m=M$ we see that $y_{M+k}\equiv y_k \pmod M$, and for $m=\frac{M}{2}$ that $y_{\frac{M}{2}+k}\equiv y_k+\frac{M}{2} \pmod M$, so the period is M.

Now, for $M=8$ one can check that under the given conditions (i.e., a is even, $a+b\equiv 1 \pmod 4$ and $c\equiv 2 \pmod 4$), the period of $\{y_n\}$ is exactly eight and every element of $G_8=\{1,3,5,7\}$ occurs exactly twice in $\{y_0,y_1,\ldots,y_7\}$. Moreover, it is easy to verify that for any $m=2^h,\ h\geq 3$, if the period of $\{y_n \pmod m\}$ is exactly m and every element of G_m occurs exactly twice in $\{y_0,y_1,\ldots,y_{m-1}\}$ then the period of $\{y_n \pmod{2m}\}$ is exactly $2m$ and every element of G_{2m} occurs exactly twice in $\{y_0,y_1,\ldots,y_{2m-1}\}$. Hence, the period of y_n is M and $\{y_0,y_1,\ldots,y_{M-1}\}$ represents G_M, with every element occurring exactly twice.

Remark 2. *Computationally, and using the proof of Theorem* 3*, taking a random set of initial conditions, we obtain that these are the only conditions for* a,b,c *under which we obtain period* 16 *(modulo* 16*). From the proof of Theorem* 3*, this would imply that, regardless of frequency, we can only attain the maximal period* M *for any initial conditions if* $a\equiv 0 \pmod 2, a+b\equiv 1 \pmod 4$ *and* $c\equiv 2 \pmod 4$.

3.2. Conditions when the period of the sequence is $M/2$

Theorem 5. *The PRNG $\{y_n\}$ derived from (5) is purely periodic with period $M/2$, regardless of the odd initial conditions y_0, y_1, and the set $\{y_1, y_2, \ldots, y_{\frac{M}{2}}\} = G_M$ if and only if*

$$a \equiv 1 \pmod 4, b \equiv 0 \pmod{\tfrac{M}{2}} \text{ and } c \equiv 2 \pmod 4.$$

Proof. We show this in two parts.

Necessity: Let us assume that for the sequence (5) and for any $y_0, y_1 \in G_M$, the period of y_n is $\frac{M}{2}$ and $\{y_1, y_2, \ldots, y_{\frac{M}{2}}\} = G_M$. We will prove that $a \equiv 1 \pmod 4, b \equiv 0 \pmod{\frac{M}{2}}$ and $c \equiv 2 \pmod 4$. We consider $y_0 = y_1 = 1$ (there is no contradiction here with the inferred assumption that every residue occurs once only, since we consider the uniformity of the sequence starting with index 1; certainly, we could have taken $y_0 = 1$, $y_1 = 3$, but we preferred to start "at a zero time" and start counting the distribution of our sequence at index 1). Now, it is easy to check that under the above assumption if we reduce every element modulo 4 (respectively, 8), the period of $\{y_n \pmod 4\}$ (respectively, $\{y_n \pmod 8\}$) is 2 (respectively, 4) and $\{y_1, y_2\} = G_4 = \{1, 3\}$ (respectively, $\{y_1, y_2, y_3, y_4\} = G_8 = \{1, 3, 5, 7\}$). We have,

$$\begin{aligned} y_{n+2} &\equiv a y_{n+1} + b y_n + c \pmod 4, \text{ and} \\ y_{n+2} &\equiv a y_{n+1} + b y_n + c \pmod 8. \end{aligned}$$

As $y_0 = y_1 = 1$, we have, $y_2 \equiv 3 \pmod 4, y_3 \equiv 1 \pmod 4, y_4 \equiv 3 \pmod 4$ and $y_3 \equiv 5 \pmod 8, y_5 \equiv 1 \pmod 8$.

By absurd, we assume that a is even. Then, $y_2 \equiv a + b + c \equiv 3 \pmod 4$ gives $b + c$ is odd. So, let $a = 2d'$ and $b + c = 1 + 2e'$ for some integers d' and e'. We have, $y_2 = 1 + 2(d' + e')$ where $d' + e' = 1 + 2f'$, is odd for some $f' \in \mathbb{Z}$ (since $y_2 \equiv 3 \pmod 4$). Then, $y_3 \equiv 3a + b + c \equiv 3 + 2a \equiv 3 \pmod 4$. Which is a contradiction. So a is odd.

Now, let $a = 3 + 4g', g' \in \mathbb{Z}$ and from $y_2 \equiv a + b + c \equiv 3 \pmod 4$ we have $b + c = 4h', h' \in \mathbb{Z}$. Then, $y_3 \equiv a y_2 + b + c \equiv a(3 + 4(g' + h')) + b + c \equiv 3a + 4(g' + h') + b + c \equiv 1 \pmod 8$. Which contradicts $y_3 \equiv 5 \pmod 8$.

So, $a \equiv 1 \pmod 4$. Let $a = 1 + 4l'$, $l' \in \mathbb{Z}$. So, $b + c = 2 + 4r'$ for some integer r' ($\because y_2 \equiv a + b + c \equiv 3 \pmod 4$). Now, $y_4 \equiv a y_3 + b y_2 + c \equiv 5a + (3 + 4(l' + r'))b + c \equiv 7 + 2b + 4(l' + r') + 4b(l' + r') \pmod 8$. Hence, $y_4 \equiv 3 + 2b \pmod 4$ and so from $y_4 \equiv 3 \pmod 4$ we have, b is even.

Next, let $b = 2 + 4s'$. Then, from above, we have, $y_4 \equiv 3 + 4(l' + r') \pmod 8$. So, $y_5 \equiv a y_4 + b y_3 + c \equiv 3a + 4a(l' + r') + 5b + c \equiv 3a + b + c + 4(l' + r') \equiv 5 \pmod 8$ contradicting the fact $y_5 \equiv 1 \pmod 8$. Thus, $b \equiv 0 \pmod 4$ and hence, $c \equiv 2 \pmod 4$. We will next show that $b \equiv 0 \pmod{\frac{M}{2}}$. By our assumption, the period is $\frac{M}{2}$ and $\{y_1, y_2, \ldots, y_{\frac{M}{2}}\} = G_M$. Now, clearly every element in G_M has a unique inverse in G_M and so,

$$\sum_{i=1}^{\frac{M}{2}} y_i = \sum_{i=1}^{\frac{M}{2}} y_i^{-1} = \sum_{i=0}^{\frac{M}{2}-1} (2i + 1) = \frac{M^2}{4}.$$

Again, as $y_{\frac{M}{2}+1} \equiv y_1 \pmod M$, we have the sequence of equivalent congruences

$$\begin{aligned}
&\sum_{i=0}^{\frac{M}{2}-1} y_{i+2} \equiv \sum_{i=0}^{\frac{M}{2}-1} (a y_{i+1}^{-1} + b y_i + c) \pmod M,\\
&\sum_{i=1}^{\frac{M}{2}} y_i \equiv a \sum_{i=0}^{\frac{M}{2}-1} y_{i+1}^{-1} + b \sum_{i=0}^{\frac{M}{2}-1} y_i + c \sum_{i=0}^{\frac{M}{2}-1} 1 \pmod M,\\
&\sum_{i=1}^{\frac{M}{2}} y_i \equiv a \sum_{i=1}^{\frac{M}{2}} y_i^{-1} + b\,(y_0 + \sum_{i=1}^{\frac{M}{2}} y_i - y_{\frac{M}{2}}) + c\frac{M}{2} \pmod M,\\
&\frac{M^2}{4} \equiv a\frac{M^2}{4} + b\,(y_0 + \frac{M^2}{4} - y_{\frac{M}{2}}) + c\frac{M}{2} \pmod M,\\
&0 \equiv b\,(y_0 - y_{\frac{M}{2}}) \pmod M \ (\because c \text{ is } \text{ even } \text{ and } \omega \geq 3).
\end{aligned}$$

Now, in our case, we have, $y_0 = y_1 = 1$. And so, from above, we have,

$$b\,(y_1 - y_{\frac{M}{2}}) \equiv 0 \pmod M.$$

Next, note that, in our case $y_{\frac{M}{2}} - y_1 \equiv 2 \pmod 4$ and so, $b \equiv 0 \pmod{\frac{M}{2}}$.

Sufficiency: As $b \equiv 0 \pmod{\frac{M}{2}}$ so, $by_n \equiv b \pmod M$ and so (5) reduces to

$$y_{n+2} \equiv a y_{n+1}^{-1} + (b + c) \pmod M,$$

where $a \equiv 1 \pmod 4$ and $(b + c) \equiv 2 \pmod 4$. So, by (1), the period of $\{y_n\}$ is $\frac{M}{2}$ and $\{y_1, y_2, \ldots, y_{\frac{M}{2}}\} = G_M$.

Remark 3. *Note that, for some initial conditions, we can obtain period equal to* 8 (mod 16) *for other values of* a, b *and* c *where* a *is odd and* b *and* c *are even, or where* b *is odd and* a *and* c *are even. Thus, the conditions of Theorem* 5 *are only necessary if the period is* $\frac{M}{2}$*, regardless of initial conditions.*

4. Lattice testing for a binary sequence associated to HICG

Let $\{y_n\}$ be our HICG sequence with some initial conditions. In the spirit of the known Blum-Micali PRN [1], we define a pseudorandom binary sequence $\{z_n\}$ by $z_n = f(y_n)$, where $f : G_M \to \{0, 1\}$ is given by

$$f(x) = \begin{cases} 0 & \text{if } x < \frac{M}{2} \\ 1 & \text{if } x > \frac{M}{2}. \end{cases}$$

A Sagemath code with the parameters $\omega = 64$, $a = 1886906$, $b = 706715$, $c = 807782$, $y_0 = 430227$ and $y_1 = 1725239$ has been provided in the Appendix which will generate 10^8

PRNs. As for the linear and inversive congruential generator, one can define an s-dimensional lattice test for our hybrid sequence (of period, say T) for the characteristics 2 (hence of 2^ω modulus). For the binary sequence (defined above) $\{z_n\}$ passes the *L-dimensional lattice test* if the vectors

$$\{Z_n : Z_n = (z_n, z_{n+1}, \ldots, z_{n+L-1}), \text{ for } 0 \le n < T\},$$

span $\mathbb{F}_2^L$ (we will write below $span(\cdot)$ for the span of a set of vectors). We call the smallest dimension, with notation $\ell(z)$, such that $\{z_n\}$ passes the $\ell(z)$-dimensional lattice test, but not the $(\ell(z)+1)$-dimensional lattice test, the *lattice test complexity*. The lattice test complexity is known for the inversive congruential generator (see [6, 19], for more on this generator). It is known that for a prime characteristic p, the inversive congruential generator over $\mathbb{F}_p$ will pass the s-dimensional lattice test in $\mathbb{F}_p$ if and only if $s \le d$, where d is the degree of the polynomial g representing the sequence z_n modulo p, that is, $g(n) = z_n$ in $\mathbb{F}_p$ (see [2], for more on the connection between linear complexity and lattice tests).

To show our result, we shall be using below the following known result [13].

Proposition 1. *The rank of a circulant matrix C of order n is $n-d$, where d is the degree of the greatest common divisors of $1-x^n$ and the associated polynomial of C.*

Theorem 6. *Let $\{y_n\}$ be the HICG sequence modulo $M = 2^\omega$, $\omega \ge 2$, with some initial conditions, of full period M (see Theorem 4 for conditions on the parameters). The lattice test complexity of the associated binary sequence $\{z_n\}$ is $\ell(z) = \frac{M}{2}$.*

Proof. Let $Z_n = \left(z_n, z_{n+1}, \ldots, z_{n+\frac{M}{2}-1}\right)$. Computationally, one can check that for $M = 4$, the vectors $\{Z_n\}$ will not span $\mathbb{F}_2^L$ if $L = 3$, rather they will span $\mathbb{F}_2^L$ if $L = 2$. From the construction of the vectors Z_n, we see that if we can show that the vectors $\{Z_n\}$ for $L = \frac{M}{2}$ span $\mathbb{F}_2^L$, then the corresponding vectors will also span $\mathbb{F}_2^L$, for all $L \le \frac{M}{2}$. Therefore, it suffices to show that $\{Z_0, Z_1, \ldots, Z_{M-1}\}$ span $\mathbb{F}_2^{\frac{M}{2}}$. We know that, $y_{\frac{M}{2}+k} \equiv y_k + \frac{M}{2} \pmod M$ and so $z_{\frac{M}{2}+k} = \overline{z_k}$ where $\overline{0} = 1$ and $\overline{1} = 0$. To show our claim,

we need to prove that the matrix

$$Z=\begin{pmatrix} Z_0\\ Z_1\\ Z_2\\ \vdots\\ Z_{\frac{M}{2}-2}\\ Z_{\frac{M}{2}-1}\\ Z_{\frac{M}{2}}\\ Z_{\frac{M}{2}+1}\\ Z_{\frac{M}{2}+2}\\ \vdots\\ Z_{M-2}\\ Z_{M-1}\end{pmatrix}=\begin{pmatrix} z_0 & z_1 & z_2 & \dots & z_{\frac{M}{2}-2} & z_{\frac{M}{2}-1}\\ z_1 & z_2 & z_3 & \dots & z_{\frac{M}{2}-1} & \overline{z_0}\\ z_2 & z_3 & z_4 & \dots & \overline{z_0} & \overline{z_1}\\ & & & \vdots & & \\ z_{\frac{M}{2}-2} & z_{\frac{M}{2}-1} & \overline{z_0} & \dots & \overline{z_{\frac{M}{2}-4}} & \overline{z_{\frac{M}{2}-3}}\\ z_{\frac{M}{2}-1} & \overline{z_0} & \overline{z_1} & \dots & \overline{z_{\frac{M}{2}-3}} & \overline{z_{\frac{M}{2}-2}}\\ \overline{z_0} & \overline{z_1} & \overline{z_3} & \dots & \overline{z_{\frac{M}{2}-2}} & \overline{z_{\frac{m}{2}-1}}\\ \overline{z_1} & \overline{z_2} & \overline{z_3} & \dots & \overline{z_{\frac{M}{2}-1}} & z_0\\ \overline{z_2} & \overline{z_3} & \overline{z_4} & \dots & z_0 & z_1\\ & & & \vdots & & \\ \overline{z_{\frac{M}{2}-2}} & \overline{z_{\frac{M}{2}-1}} & z_0 & \dots & z_{\frac{M}{2}-4} & z_{\frac{M}{2}-3}\\ \overline{z_{\frac{M}{2}-1}} & z_0 & z_1 & \dots & z_{\frac{M}{2}-3} & z_{\frac{M}{2}-2}\end{pmatrix}$$

has rank at least $\frac{M}{2}$, which is equivalent to the fact that Z^T has rank at least $\frac{M}{2}$.

To achieve that goal, we define a circulant matrix C of order M, whose first $\frac{M}{2}$ rows form Z^T (we just add $\frac{M}{2}$ rows to Z^T accordingly to make it of order M). Now the associated polynomial of C is

$$\begin{aligned} g(x)&=\sum_{i=0}^{\frac{M}{2}-1} z_i x^i+\sum_{i=\frac{M}{2}}^{M-1}\overline{z_{i-\frac{M}{2}}}x^i\\ &=\sum_{i=0}^{\frac{M}{2}-1} z_i x^i+x^{\frac{M}{2}}\sum_{i=0}^{\frac{M}{2}-1}(z_i+1)x^i\\ &=\left(1+x^{\frac{M}{2}}\right)\sum_{i=0}^{\frac{M}{2}-1} z_i x^i+x^{\frac{M}{2}}\sum_{i=0}^{\frac{M}{2}-1}x^i\\ &=(1+x)^{\frac{M}{2}}\sum_{i=0}^{\frac{M}{2}-1} z_i x^i+x^{\frac{M}{2}}(1+x)^{\frac{M}{2}-1}\\ &=(1+x)^{\frac{M}{2}-1}((1+x)\sum_{i=0}^{\frac{M}{2}-1} z_i x^i+x^{\frac{M}{2}}) \end{aligned}$$

(all operations are considered modulo 2 here).

Thus, $\gcd\left(g(x),1-x^M\right)=\gcd\left(g(x),(1+x)^M\right)=(1+x)^{\frac{M}{2}-1}$. Hence, by Proposition 1, the rank of C is $M-\left(\frac{M}{2}-1\right)=\frac{M}{2}+1$. Now, it is easy to check that k-th and the $(\frac{M}{2}+k)$-th row of C add up to the row with all 1's; $k=1,2,\dots,\frac{M}{2}$. So, it is clear that

the rank of the $(\frac{M}{2}+1)\times M$ matrix, $\overline{C}$, formed by the first $\frac{M}{2}+1$ rows is of rank $\frac{M}{2}+1$. Again, Z^T is simply obtained by deleting the last row of $\overline{C}$, and so, it has rank at least $\frac{M}{2}$.

It is perhaps customary to define the lattice passing testing using the set $\{Z_0+Z_n\}$. We preferred for simplicity to use Z_n, but a similar result holds for this set, as well. We need the following lemma, which will certainly follow from general results (see [21]), but we provide here a simple proof for completeness.

Lemma 1. *Let $M=2^\omega$, $\omega\geq 2$ and C be an $M\times M$ binary circulant matrix. Then C is nonsingular if and only if there is an odd number of 1's in each row of C.*

Proof. First note that as C is circulant so every row has same number of 1's as any row is some permutation of the first row. So, it is enough to look at the first row of C, say $(a_0,a_1,\ldots,a_{M-1})$. Let $a(x)=\sum_{i=0}^{M-1}a_ix^i$ be the associated polynomial of C. Now, C is nonsingular if and only if the rank of C is M, if and only if $\gcd\left(a(x),(1+x)^M\right)=1$ (using Proposition 1 and the fact that M is a power of 2). Clearly, $\gcd\left(a(x),(1+x)^M\right)$ can either be 1 or some power of $(1+x)$. Again, $(1+x)\mid a(x)$, if and only if $a(1)=0$, if and only if there are an even number of a_i's that are 1. Or, in other words $\gcd\left(a(x),(1+x)^n\right)=1$ if and only if there are an odd number of a_i's that are 1, that is, each row contains an odd number of 1's.

Theorem 7. *Under the conditions of Theorem 6, the set $\{Z'_n=Z_n+Z_0; n=1,2,\ldots\}$ spans $\mathbb{F}_2^{\frac{M}{2}}$.*

Proof. Let $S=\text{span}\{Z'_n; n=1,2,\ldots\}$. Then, clearly, the vectors, $Z'_n+Z'_{n+1}=Z_n+Z_{n+1}\in S$ for all $n=1,2,\ldots,\frac{M}{2}$. Then, it is sufficient to show that the $\frac{M}{2}\times\frac{M}{2}$ matrix

$$Z'=\begin{pmatrix} Z'_1+Z'_2\\ Z'_2+Z'_3\\ Z'_3+Z'_4\\ \vdots\\ Z'_{\frac{M}{2}}+Z'_{\frac{M}{2}+1}\end{pmatrix}=\begin{pmatrix} Z_1+Z_2\\ Z_2+Z_3\\ Z_3+Z_4\\ \vdots\\ Z_{\frac{M}{2}}+Z_{\frac{M}{2}+1}\end{pmatrix}$$

has rank $\frac{M}{2}$.

Now, it is easy to check that Z' is a left circulant binary matrix of order $\frac{M}{2}\times\frac{M}{2}$. Again, $Z_1+Z_2=(z_1+z_2,z_2+z_3,z_3+z_4,\ldots,z_{\frac{M}{2}-1}+\overline{z_0},\overline{z_0}+\overline{z_1})=(z_1+z_2,z_2+z_3,z_3+z_4,\ldots,z_{\frac{M}{2}-1}+z_0+1,z_0+z_1)$. Every element among $z_0,z_1,\ldots,z_{\frac{M}{2}-1}$ occurs exactly twice in Z_1+Z_2 and an extra 1 occurs in the second of the last term. Therefore, there are odd number of 1's in each row of Z'. Hence, by Lemma 1, we infer that Z' has rank $\frac{M}{2}$.

5. Further comments and research problems

We wondered whether, besides the stochastic uses of HICG (and from our experiments, it seems that taking $M = 2^{64}$ performs very well), if one can also have some cryptographic applications of our sequence. Taking the least significant bit of every residues of $\{y_n\}$ and applying randomness tests on it, revealed too many patterns and the p-values were low. However, by taking the most significant bit (see the previous section) up to half the period (because for a HICG of period $2m$, $y_{m+k} \equiv y_k + m \pmod{2m}$), we were pleasantly surprised to see that for that bit sequence corresponding to half of a period and applying the NIST randomness suite tests (sts), our sequence passed all of the tests in multiple runs, and the p-values were above the 0.01 significance level (we do not go into details of the sts suite and the randomness requirements here). We visually display in Figure 1 below the outcome of such an experiment run with the parameters $\omega = 64$, $a = 1886906$, $b = 706715$, $c = 807782, y_0 = 430227$ and $y_1 = 1725239$ and 10^8 PRNs. Also with the same

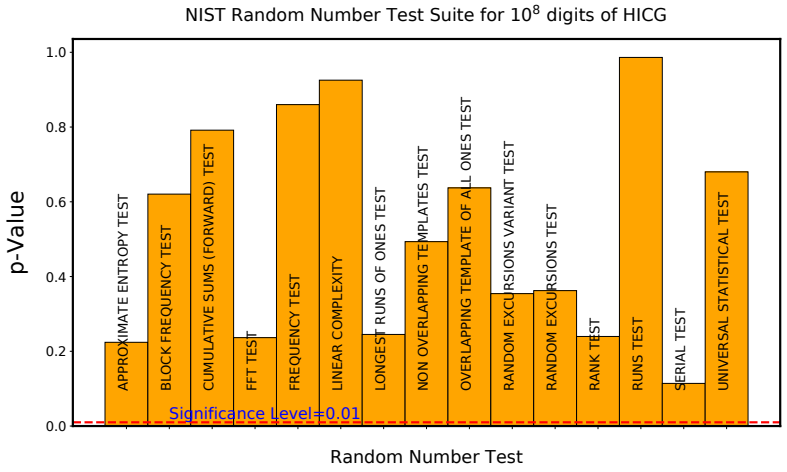

Figure 1: The NIST STS applied to HICG

parameters and 10^9 PRNs we ran the Dieharder Test which also showed promising results which are being visually displayed in Figure 2 (Here the 10^9 bits are partitioned into 31249999 32-bit numbers which are further converted to decimal numbers and then the Dieharder Test is run). We further computed the linear complexity profile of such a binary sequence for 10^5 bits and found an excellent profile. We display such an experiment in Figure 3.

While these observations were not initially the purpose of the paper, we just want to point them out as by-products. Further investigation is warranted.

There are several works (see [20] and the references therein) devoted to the computation of the discrepancy of the inversive congruential generator. Certainly, a similar inquiry can be addressed for our generator, and we leave the computation of the discrepancy (and its bounds) for our HICG for a subsequent project, or to the interested reader.

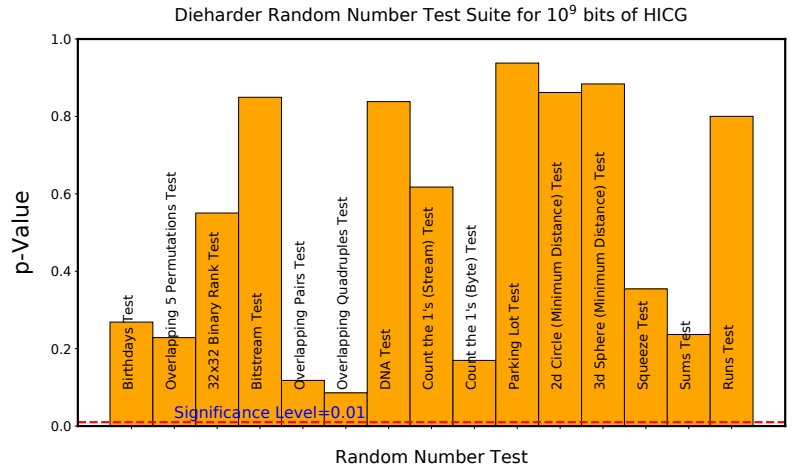

Figure 2: The Dieharder test applied to HICG

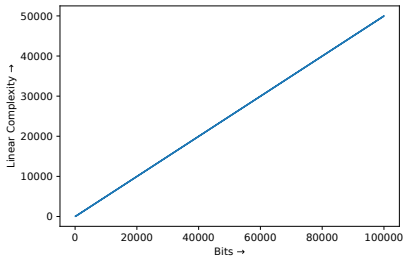

Figure 3: The linear complexity profile of HICG

In the spirit of our paper, for a modulus $M = 2^\omega$ and $y_0, y_1 \in G_M$, one can define

$$y_{n+2} \equiv a y_{n+1}^{-1} + b y_n^{-1} + c y_{n+1} + d y_n + e \pmod{M}, n = 0, 1, \ldots, \tag{9}$$

where $a, b, c, d, e \in \mathbb{Z}_M$ are such that $y_{n+2} \in G_M$, whenever $y_n, y_{n+1} \in G_M$. The study of such a generator (which includes as particular cases every other type of first-order linear and inversive congruential generator) is certainly an intriguing problem.

Finally, all of our considerations, results and inquiries can be investigated for an odd characteristic.

References

[1] Manuel Blum and Silvio Micali. How to generate cryptographically strong sequences of pseudorandom bits. *SIAM J. Comput.*, 13(4):850–864, 1984.

[2] Gerhard Dorfer and Arne Winterhof. Lattice structure and linear complexity profile of

nonlinear pseudorandom number generators. *Appl. Algebra Engrg. Comm. Comput.*, 13(6):499–508, 2003.

[3] Jürgen Eichenauer, Jürgen Lehn, and Alev Topuzoğlu. A nonlinear congruential pseudorandom number generator with power of two modulus. *Math. Comp.*, 51(184):757–759, 1988.

[4] J. Eichenauer-Herrmann, H. Grothe, H. Niederreiter, and A. Topuzoğlu. On the lattice structure of a nonlinear generator with modulus 2^α. *J. Comput. Appl. Math.*, 31(1):81–85, 1990. Random numbers and simulation (Lambrecht, 1988).

[5] Jürgen Eichenauer-Herrmann. Inversive congruential pseudorandom numbers avoid the planes. *Math. Comp.*, 56(193):297–301, 1991.

[6] Jürgen Eichenauer-Herrmann. Inversive congruential pseudorandom numbers: a tutorial. *International Statistical Review*, 560:2(193):167–176, 1992.

[7] Jürgen Eichenauer-Herrmann. Statistical independence of a new class of inversive congruential pseudorandom numbers. *Math. Comp.*, 60(201):375–384, 1993.

[8] Jürgen Eichenauer-Herrmann. On generalized inversive congruential pseudorandom numbers. *Math. Comp.*, 63(207):293–299, 1994.

[9] Jürgen Eichenauer-Herrmann and Harald Niederreiter. Lower bounds for the discrepancy of inversive congruential pseudorandom numbers with power of two modulus. *Math. Comp.*, 58(198):775–779, 1992.

[10] Reza Rezaeian Farashahi and Igor E. Shparlinski. Pseudorandom bits from points on elliptic curves. *IEEE Trans. Inform. Theory*, 58(2):1242–1247, 2012.

[11] Domingo Gómez, Jaime Gutierrez, and Álvar Ibeas. Attacking the Pollard generator. *IEEE Trans. Inform. Theory*, 52(12):5518–5523, 2006.

[12] Honggang Hu, Lei Hu, and Dengguo Feng. On a class of pseudorandom sequences from elliptic curves over finite fields. *IEEE Trans. Inform. Theory*, 53(7):2598–2605, 2007.

[13] A. W. Ingleton. The rank of circulant matrices. *J. London Math. Soc.*, 31:632–635, 1956.

[14] Takashi Kato, Li-Ming Wu, and Niro Yanagihara. On a nonlinear congruential pseudorandom number generator. *Math. Comp.*, 65(213):227–233, 1996.

[15] Donald E. Knuth. *The Art of Computer Programming, Volume II: Seminumerical Algorithms, 2nd Edition.* Addison-Wesley, Reading, MA, 1981.

[16] J. Mc Laughlin. Combinatorial identities deriving from the nth power of a 2×2 matrix. *Integers*, 4:A19, 15, 2004.

[17] Harald Niederreiter. The serial test for congruential pseudorandom numbers generated by inversions. *Math. Comp.*, 52(185):135–144, 1989.

[18] Harald Niederreiter. Recent trends in random number and random vector generation. *Ann. Oper. Res.*, 31(1-4):323–345, 1991. Stochastic programming, Part II (Ann Arbor, MI, 1989).

[19] Harald Niederreiter. *Random number generation and quasi-Monte Carlo methods*, volume 63 of *CBMS-NSF Regional Conference Series in Applied Mathematics*. Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, 1992.

[20] Harald Niederreiter and Igor E. Shparlinski. Exponential sums and the distribution of inversive congruential pseudorandom numbers with prime-power modulus. *Acta Arith.*, 92(1):89–98, 2000.

[21] Oystein Ore. Some studies on cyclic determinants. *Duke Math. J.*, 18:343–354, 1951.

Appendix

Sage Code with the parameters $\omega = 64$, $a = 1886906$, $b = 706715$, $c = 807782, y_0 = 430227$ **and** $y_1 = 1725239$**:**

```
n=64
N=2^n

a =1886906
b =706715
c =807782
y0 =430227
y1 =1725239

y=y0
z=y1

print("0,0,", end=''), # as y0 and y1 are less than N/2,
                         initial two PRNs are set to be 0.

for i in range(2,100):
    w=a*z.inverse_mod(N)+b*y+c
    w=w%N
    if (w<N/2):
        print("0,",end='')
    else:
        print("1,",end='')
    y=z
```

z=w