On the Lattice Structure of Inversive PRNG via the Additive Order

Domingo Gómez-Pérez and Ana Gómez

University of Cantabria
Avd. Los Castros, s/n, Santander, Spain
domingo.gomez@unican.es
http://personales.unican.es/gomezd

Abstract. One of the main contributions which Harald Niederreiter made to mathematics is related to pseudorandom sequences theory. In this article, we improve on a bound on one of the pseudorandom number generators (PRNGs) proposed by Harald Niederreiter and Arne Winterhof and study its lattice structure. We obtain that this generator passes general lattice tests for arbitrary lags for high dimensions.

Keywords. lattice tests, inversive methods, additive order.
Mathematics subject classification number: 11K45.

Dedicated to Harald Niederreiter on the occasion of his 70th birthday

1 Introduction

Pseudorandom numbers are used in many fields, like cryptography, financial mathematics, simulations, etc. The diversity among methods comes from the different nature of requirements, citing a famous sentence "what is appropiate for a video game is not appropiate for a nuclear reactor".

Linear methods are the most popular choice for generating pseudorandom sequences and are implemented in the API of the java language. Inversive methods are popular and competitive alternatives to the linear method for generating pseudorandom numbers, see [7] and the surveys [8, 9, 16, 17].

In this paper we analyze the lattice structure of *digital explicit inversive pseudorandom numbers* introduced in [10] and further analyzed in [6, 11, 12, 14]. To introduce this class of generators we need some notation.

Let $q = p^r$ be a prime power and $\mathbb{F}_q$ the finite field of order q. Let

$$\overline{\gamma} = \begin{cases} \gamma^{-1}, \text{ if } \gamma \in \mathbb{F}_q^*, \\ 0, \quad \text{if } \gamma = 0. \end{cases}$$

We order the elements of $\mathbb{F}_q = \{\xi_0, \xi_1, \ldots, \xi_{q-1}\}$ using an ordered basis $\{\gamma_1, \ldots, \gamma_r\}$ of $\mathbb{F}_q$ over $\mathbb{F}_p$ for $0 \leq n < q$,

$$\xi_n = n_1\gamma_1 + n_2\gamma_2 + \cdots + n_r\gamma_r,$$

if

$$n = n_1 + n_2 p + \cdots + n_r p^{r-1},\ 0 \leq n_i < p, \quad i = 1, \ldots, r.$$

For $n \geq 0$ we define $\xi_{n+q} = \xi_n$. Then the *digital explicit inversive pseudorandom number generator* of period q is defined by

$$\rho_n = \overline{\alpha\xi_n + \beta},\ n = 0, 1, \ldots$$

for some $\alpha, \beta \in \mathbb{F}_q$ with $\alpha \neq 0$. Digital explicit inversive pseudorandom number generators are used for generating low discrepancy sequences. If

$$\rho_n = c_{n,1}\gamma_1 + c_{n,2}\gamma_2 + \cdots + c_{n,r}\gamma_r$$

with all $c_{n,i} \in \mathbb{F}_p$, we derive *digital explicit inversive pseudorandom numbers of period* q in the interval $[0, 1)$ by defining

$$y_n = \sum_{j=1}^{r} c_{n,j} p^{-j}, \quad n = 0, 1, \ldots.$$

Bounds on the discrepancy of points generated from these sequences appear in [10] and in [1, 2]. Also, inversive methods were considered by Hu and Gong in [5] where it was proven a bound on the autocorrelation of this family of sequences.

Our goal in this paper is to study the behaviour of the digital explicit inversive pseudorandom number generator under a generalized test introduced in [13]. For the convenience of the reader, we give here a brief description of this test.

For given integers $L \geq 1$, $0 < d_1 < \cdots < d_{L-1} < T$ and (s_n) a sequence of elements in $\mathbb{F}_q$, (s_n) passes the $L-$dimensional N-*Lattice Test* with lags $d_1, \ldots, d_{L-1}$ if the vectors

$$\{\boldsymbol{s}_n - \boldsymbol{s}_0\ :\ \boldsymbol{s}_n = (s_n, s_{n+d_1}, \ldots, s_{n+d_{L-1}}), \quad \text{for } 0 \leq n < N\},$$

span $\mathbb{F}_q^L$. The greatest dimension L such that (s_n) passes the L-dimensional N-lattice test for all lags $d_1, \ldots, d_{L-1}$ is denoted by $\mathcal{T}((s_n), N)$.

The authors in [14] studied the lattice test for digital explicit inversive generators and they obtained bounds on $\mathcal{T}((\rho_n), N)$, even in parts of the sequence. We cite here part of their main result.

Lemma 1 (Theorem 1 and 2 in [14]). *Let (ρ_n) be a sequence arising from a digital explicit inverse pseudorandom number generator defined over $\mathbb{F}_q$ with $q = p^r$, then we have that,*

$$\mathcal{T}((\rho_n), N) \geq \frac{\log N - \log\log N - 1}{r - 1} - 1,$$

for $2 \leq N < q$ *if* $r > 1$. *For* $r = 1$ *the inequality*

$$\mathcal{T}((\rho_n), N) \geq \frac{N}{2} - 1,$$

holds for $2 \leq N < q$.

We want to stress the different nature of both results. For $r = 1$, the bound is linear in N whereas only a logarithmic lower bound is given for $r > 1$. Indeed, the bound for $r > 2$ can be obtained when $N = q$ for any sequence (s_n) of period q with sufficiently high linear complexity, see [4].

Here, we show that this bound can be improved using hyperplane arrangements.

2 Hyperplane Arrangements

Hyperplane arrangements is a concept well studied in the field of combinatorial geometry, see [3]. We only introduce enough theory to understand the proof of the main result and follow the nice introduction given in [15].

Let d be a positive integer and $\mathbb{R}$ the field of real numbers. We denote by

$$\boldsymbol{a} = (a_1, \ldots, a_d), \quad a_1, \ldots, a_d \in \mathbb{R}$$

elements of $\mathbb{R}^d$, where $\mathbb{R}^d$ is a vector space of dimension d over the field $\mathbb{R}$. We also consider matrices with the usual operations involving matrices, namely multiplication, addition and transposition. Also, it is needed the topological concept of dimension of a set of points in $\mathbb{R}^d$. Vectors in $\mathbb{R}^d$ are matrices with d rows and 1 column. The notation for the transposition of a matrix $\mathbf{A}$ is $\mathbf{A^T}$.

Definition 1. *Given* $\boldsymbol{a} \in \mathbb{R} - \{\mathbf{0}\}$ *and* $b \in \mathbb{R}$, *the set* $\{\boldsymbol{x} \in \mathbb{R}^d : \boldsymbol{a^T x} = b\}$ *is called a hyperplane.*

We also use $\boldsymbol{a} \cdot \boldsymbol{x}$ to denote $\boldsymbol{a^T x}$, which correspond to the standard dot product, and the matrix form $\mathbf{A}\boldsymbol{x} = \boldsymbol{b}$ to encode the finite set of hyperplanes $\mathcal{H} = \{\mathcal{H}_1, \ldots, \mathcal{H}_m\}$, where

$$\mathcal{H}_i = \{\boldsymbol{x} \in \mathbb{R}^d : \sum_{j=1}^{d} a_{i,j} x_j = b_i\}. \tag{1}$$

Definition 2. *A set of hyperplanes in* $\mathbb{R}^d$ *partitions the space into relatively open convex polyhedral regions, called faces, of all dimensions. This partition is called a hyperplane arrangement.*

We make a distinction between the two sides of a hyperplane. A point $\boldsymbol{p} \in \mathbb{R}^d$ is on the positive side of hyperplane $\mathcal{H}_i$, denoted by $\mathcal{H}_i^+$, if

$$\sum_{j=1}^{d} a_{i,j} p_j > b_i.$$

Similarly, we define $\boldsymbol{p} \in \mathbb{R}^d$ is on the negative side of hyperplane $\mathcal{H}_i$ and we denote it by $\mathcal{H}_i^-$.

For each point $\boldsymbol{p} \in \mathbb{R}^d$ we define a sign vector of length m consisting of $1, 0, -1$ signs as follows:

$$sv(\boldsymbol{p})_i = \begin{cases} 1 & \text{if } \boldsymbol{p} \in \mathcal{H}_i^+, \\ -1 & \text{if } \boldsymbol{p} \in \mathcal{H}_i^-, \\ 0 & \text{if } \boldsymbol{p} \in \mathcal{H}_i, \end{cases}$$

where $i = 1, \ldots, m$ and m is the number of hyperplanes.

Definition 3. *A face is a set of points with the same sign vector. It is called a i-face if its dimension is $i \leq d$ and a cell if the dimension is d.*

As a small comment, the dimension of a face is at least d minus the number of ceros in the sign vector of any of the points of the face. The number of faces of given dimension in a hyperplane arragement is given in the following result

Lemma 2 (Theorem 1.3 in [3]). *Given any set of hyperplanes $\mathcal{H} = \{H_1, \ldots, H_m\}$ in $\mathbb{R}^d$, then the number of i-faces in the correspondent hyperplane arrangement can be bounded by,*

$$\sum_{j=0}^{i} \binom{d-j}{i-j} \binom{m}{d-j}.$$

3 Main Result

Now, we have all the technical tools to prove the main result. The proof is a minor modification of the one in [14, Theorem 1] and the only difference is the estimate for the number of possible carries. Nevertheless, for the sakeness of completeness, we include it here without claiming any priority over it.

Theorem 1. *For the sequence of elements (ρ_n) defined by an inversive pseudo-random number generator of period $q = p^r$, we have*

$$6\mathcal{T}((\rho_n), N) \geq \left(\frac{N}{(r)^{r-1}}\right)^{1/r},$$

for $2 \leq N \leq q$.

Proof. The case $r = 1$ is stated in Lemma 1 so assume that $r \geq 2$ and the sequence (ρ_n) does not pass the L-dimensional N-lattice test for some lags $0 < d_1 < d_2 < \cdots < d_{L-1} < q$. Put

$$\boldsymbol{\rho}_n = (\rho_n, \rho_{n+d_1}, \ldots, \rho_{n+d_{L-1}}), \quad n \geq 0,$$

and let V be the subspace of $\mathbb{F}_q^L$ spanned by all $\boldsymbol{\rho}_n - \boldsymbol{\rho}_0$ for $0 \leq n < N$. Consider the orthogonal space of V, i. e. $\{\boldsymbol{u} \,:\, \boldsymbol{u} \cdot \boldsymbol{v} = 0,\ \forall \boldsymbol{v} \in V\}$, whose dimension is different from 0. So, there exits $\boldsymbol{\alpha} \neq \boldsymbol{0}$ such that,

$$\boldsymbol{\rho}_n \cdot \boldsymbol{\alpha} = \boldsymbol{\rho}_0 \cdot \boldsymbol{\alpha}, \quad \text{for } 0 \leq n < N.$$

Calling $\delta = \boldsymbol{\rho}_0 \cdot \boldsymbol{\alpha}$ and j the smallest index with $\alpha_j \neq 0$ we have [1]

$$\alpha_j \rho_{n+d_j} + \alpha_{j+1}\rho_{n+d_{j+1}} + \cdots + \alpha_{L-1}\rho_{n+d_{L-1}} = \delta, \quad \text{for } 0 \leq n < N. \tag{2}$$

For all $1 \leq i < L$ and $0 \leq d_i, n < q$, let

$$d_i = \sum_{j=1}^{r} d_{i,j} p^{j-1}, \quad 0 \leq d_{i,1}, \ldots, d_{i,r} < p,$$

and

$$n = \sum_{j=1}^{r} n_j p^{j-1}, \quad 0 \leq n_1, \ldots, n_r < p,$$

be the p-adic expansions of d_i and n, respectively. We now define the vectors of the carries that occur in the additions of $n + d_i$. Let $w_{i,1} = 0$ and define for $1 \leq h \leq r$ recursively

$$w_{i,h+1} = \begin{cases} 1, & \text{if } d_{i,h} + n_h + w_{i,h} \geq p, \\ 0, & \text{otherwise.} \end{cases}$$

Then we have

$$n + d_i = \sum_{j=1}^{r} z_{i,j} p^{j-1}, \quad 0 \leq z_{i,1}, \ldots, z_{i,r} < p,$$

with

$$z_{i,j} = d_{i,j} + n_j + w_{i,j} - w_{i,j+1} p, \ 1 \leq j \leq r,$$

and

$$\xi_{n+d_i} = \xi_n + \xi_{d_i} + w_i, \quad \text{where } w_i = \sum_{j=1}^{r} w_{i,j}\gamma_j.$$

Previously only trivial estimates were used to count the number of possible choices for $w_j, \ldots, w_{L-1}$. Now, we are going to use hyperplane arrangements to bound this number. Consider the following sets of hyperplanes in $\mathbb{R}^r$,

$$\{H^1_{i,j} : 1 \leq i \leq L, \ 1 \leq j \leq r\} \cup \{H^2_{i,j} : 1 \leq i \leq L, \ 1 \leq j \leq r\},$$

where

$$H^1_{i,j} = \{\boldsymbol{x} \in \mathbb{R}^r : x_j + d_{i,j} = p - 0.1\}, \quad H^2_{i,j} = \{\boldsymbol{x} \in \mathbb{R}^r : x_j + d_{i,j} = p - 1.1\}.$$

It is easy to encode the union of these two sets of hyperplanes by $\mathbf{A}\boldsymbol{x} = \boldsymbol{b}$ as in Equation (1). Matrix $\mathbf{A}$ is a matrix with $2Lr$ rows and r columns that

[1] if $j = 0$, we will denote $d_0 = 0$, although the lags are $d_1, \ldots, d_{L-1}$.

it is constructed by stacking $2L$ identity matrices of dimension r. The first L components of vector $\boldsymbol{b}$ are just joining the following L vectors,

$$(p-0.1,\ldots,p-0.1),(p-d_{1,1}-0.1,\ldots,p-d_{1,r}-0.1),\\ \ldots,(p-d_{L-1,1}-0.1,\ldots,p-d_{L-1,r}-0.1),$$

and the next L components are,

$$(p-1.1,\ldots,p-1.1),(p-d_{1,1}-1.1,\ldots,p-d_{1,r}-1.1),\\ \ldots,(p-d_{L-1,1}-1.1,\ldots,p-d_{L-1,r}-1.1).$$

Using the previous notation, it is trivial that if n, n' are two different integers satisfying

$$\xi_{n+d_i}=\xi_n+\xi_{d_i}+w_i,\quad \xi_{n'+d_i}=\xi_{n'}+\xi_{d_j}+w'_i,$$

with $w_i\neq w'_i$ for some $i\in 1,\ldots,r$, then the sign vectors of the points $(n_1,\ldots,n_r)$, $(n'_1,\ldots,n'_r)\in\mathbb{R}^r$ are different, where

$$n=\sum_{j=1}^{r}n_jp^{j-1},\quad n'=\sum_{j=1}^{r}n'_jp^{j-1},\quad 0\leq n_1,\ldots,n_k,n'_1,\ldots,n'_k<p.$$

The reason is the following, if $sv((n_1,\ldots,n_r))=sv((n'_1,\ldots,n'_r))$, then both points must be in the same side of the hyperplanes $H^1_{i,1},H^2_{i,1}$ for $i=1,\ldots,L$, which is equivalent to,

$$d_{i,1}+n_1>p-0.1\iff d_{i,1}+n'_1>p-0.1,\implies w_{i,2}=w'_{i,2}.$$

In general, $w_{i,h}=w'_{i,h}$ because

- $w_{i,h}=w'_{i,h}=1$ and the points lie in the same side of $H^2_{i+L,h+1}$.
- $w_{i,h}=w'_{i,h}=0$ and the points lie in the same side of $H^1_{i,h+1}$.

We are only interested in the faces of dimension greater or equal than $r-1$ [2] Using Lemma 2, we get that the number of $(r-1)$-faces plus the number of r-faces is less than

$$(r+1)\sum_{j=0}^{r-1}\binom{2rL}{r-j}\leq(6rL)^{r-1}.$$

So there exists a vector $(w_j,\ldots,w_{r-1})$ such that for at least

$$\frac{N}{(6rL)^{r-1}},$$

different n with $0\leq n<N$ we have $\xi_{n+d_i}=\xi_n+\xi_{d_i}+w_i$, $j\leq i<r$. We have $\rho_{n+d_i}=0$ for some value $1\leq i<r$ for at most $r-j$ different n. If $\rho_{n+d}\neq 0$ then we can write $\rho_{n+d}=\overline{\alpha\xi_{n+d}+\beta}$. By Equation (2), we have

$$\alpha_j\overline{\alpha\xi_n+\xi_{d_j}+w_j+\beta}+\ldots+\alpha_{L-1}\overline{\alpha\xi_n+\xi_{d_{L-1}}+w_{L-1}+\beta}=\delta,$$

[2] because we always consider $w_{i,1}=0$. It is also equivalent to discard x_1, i. e. working in $\mathbb{R}^{r-1}$.

for at least $N/(6rL)^{r-1} - L$ different elements ξ_n. Operating and using Lagrange theorem, the number of solutions of the previous equation is less than L, so $2L \geq N/(6rL)^{r-1}$ or, $6L \geq \left(\frac{N}{(r)^{r-1}}\right)^{1/r}$ and this finishes the proof.

Final Comments

No effort has been put in getting the best possible constant in the theorem. The reason is to avoid technical details as much as possible and focus on hyperplane arrangements. The new idea in this paper is using hyperplane arrangements, which seems to be new to study sequences via additive order. We think that this could lead to improvements to study distribution of sequences via additive order. However, new ideas are needed to be added. For example, hyperplane arrangements applied to the results in [2], give better constants in the results but not significant improvements. Also, the result in this paper applies only when p is sufficiently large. It would certainly be very interesting to see how to apply this technique for $p = 2$.

This work is supported in part by the Spanish Ministry of Science, project MTM2011-24678

References

1. Zhixiong Chen. Finite binary sequences constructed by explicit inversive methods. *Finite Fields and Their Applications*, 14(3):579–592, 2008.
2. Zhixiong Chen, Domingo Gomez, and Arne Winterhof. Distribution of digital explicit inversive pseudorandom numbers and their binary threshold sequence. In *Monte Carlo and Quasi-Monte Carlo Methods 2008*, pages 249–258. Springer, 2009.
3. Herbert Edelsbrunner. *Algorithms in combinatorial geometry*, volume 10. Springer, 1987.
4. Domingo Gomez-Perez and Jaime Gutierrez. On the linear complexity and lattice test of nonlinear pseudorandom number generators, 2013.
5. Honggang Hu and Guang Gong. A study on the pseudorandom properties of sequences generated via the additive order. In *Sequences and Their Applications-SETA 2008*, pages 51–59. Springer, 2008.
6. Wilfried Meidl and Arne Winterhof. On the linear complexity profile of explicit nonlinear pseudorandom numbers. *Information Processing Letters*, 85(1):13–18, 2003.
7. Harald Niederreiter. *Random number generation and quasi-Monte Carlo methods*, volume 63. SIAM, 1992.
8. Harald Niederreiter and Igor E Shparlinski. Recent advances in the theory of nonlinear pseudorandom number generators. In *Monte Carlo and Quasi-Monte Carlo Methods 2000*, pages 86–102. Springer, 2002.
9. Harald Niederreiter and Igor E Shparlinski. Dynamical systems generated by rational functions. In *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, pages 6–17. Springer, 2003.
10. Harald Niederreiter and Arne Winterhof. Incomplete exponential sums over finite fields and their applications to new inversive pseudorandom number generators. *Acta Arithmetica*, 93(4):387–399, 2001.

11. Harald Niederreiter and Arne Winterhof. On a new class of inversive pseudorandom numbers for parallelized simulation methods. *Periodica Mathematica Hungarica*, 42(1):77–87, 2001.
12. Harald Niederreiter and Arne Winterhof. On the lattice structure of pseudorandom numbers generated over arbitrary finite fields. *Applicable Algebra in Engineering, Communication and Computing*, 12(3):265–272, 2001.
13. Harald Niederreiter and Arne Winterhof. On the structure of inversive pseudorandom number generators. In *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, pages 208–216. Springer, 2007.
14. Gottlieb Pirsic and Arne Winterhof. On the structure of digital explicit nonlinear and inversive pseudorandom number generators. *J. Complexity*, 26(1):43–50, 2010.
15. Nora H. Sleumer. Hyperplane arrangements: Construction, visualization and applications. Master's thesis, Swiss Federal Institute of Technology, 2000.
16. Alev Topuzoğlu and Arne Winterhof. Pseudorandom sequences. In *Topics in geometry, coding theory and cryptography*, volume 6 of *Algebr. Appl.*, pages 135–166. Springer, Dordrecht, 2007.
17. Arne Winterhof. Recent results on recursive nonlinear pseudorandom number generators. In *Sequences and Their Applications–SETA 2010*, pages 113–124. Springer, 2010.