Random numbers generated by orbifold fixed points

E.Koorambas

8A Chatzikosta, 11521 Ampelokipi, Athens, Greece

Email: elias.koor@gmail.com

Abstract: Taking an orbifold with one compact extra dimension as a starting point, we show that random numbers are generated by recurrence modulo 2 over the Galois field of orbifold fixed points. Our suggestion may open a window for extra dimensions predicted by experiments.

PACS number(s):11.25.Mj, 03.65.Ta

Keywords: Compactification and four-dimensional models, Random number generators

Contents

This work is licensed under the Creative Commons Attribution 3.0 Unported License. To view a copy of this license, visit http://creativecommons.org/licenses/by/3.0/ or send a letter to Creative Commons, 444 Castro Street, Suite 900, Mountain View, California, 94041, USA.

1. Introduction

Orbifolds, originally introduced as ‘V –manifolds’ by Satake in the 1950s [1], and named by Thurston in the 1970s [2], [3], are useful generalizations of manifolds: locally they look like the quotient of Euclidean space by the action of a finite group. The concept of orbifolds has gained increasing popularity recently due to its application in many questions of theoretical physics such as [4], [5], [6], [7].

‘‘In various fields of interest, situations often arise in which the mathematical model utilizes a random sequence of numbers, events, or both. In many of these applications it is often advantageous to generate, by some deterministic means, a sequence which appears to be random, even if, upon closer and longer observation, certain regularities become evident. Monte Carlo experiments, for instance, have benefited greatly from computer programs for generating random numbers [20].’’

This paper describes random numbers generated by recurrence modulo2 over the Galois field of orbifold fixed points. Random numbers are generated by modulo 2 linear recurrence techniques, long used to generate binary codes for communications [8], [7], [9], [10], [11]. The idea of using finite fields in quantum theory has been discussed by several authors (see e.g., References [12-17]).

2. Random numbers generated by the orbifold fixed points

In the S^1/Z_2 orbifold, we compactify one extra dimension on a circle S^1, and we identify points under a Z_2 group action generated by

$$g : a \to -a \tag{1}$$

The emerging fundamental domain of the S^1/Z_2 orbifold is a 3 space bounded by the orbifold’s fixed points, i.e. the two points that are invariant under the orbifold action:

$$a_1 = 0, a_2 = \pi L \tag{2}$$

where L is the extra dimension radius. The orbifold S^1/Z_2, depicted in Figure1, is topologically the unit interval [0, 1] with the two fixed points corresponding to the endpoints of the interval.

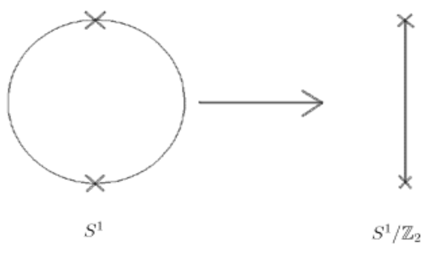

Figure 1: The orbifold S^1/Z_2

Furthermore, let S^1 be the manifold with the action of the finite group Z_2. The Euler-characteristic of the quotient space $O^1 \equiv S^1/Z_2$ can be computed by the Lefshetz formula [18]:

$$\mathrm{X}(O^1) = \frac{1}{|Z_2|} \sum_{g \in Z_2} \chi(a^g) \tag{3}$$

where $O^1 \equiv S^1/Z_2$ the quotient space and a^g the fixed point set of g. Here, we define an Euler-characteristic for the finite group Z_2 acting on the assembly of $S_1^1 \times S_2^1 \times .... \times S_n^1$ manifolds as follows:

$$\mathrm{X}(O_1^1, O_2^1, ..., O_n^1) = \frac{1}{|Z_2|} \sum_{g \in Z_2} \chi(a_1^g, a_2^g, ..., a_n^g), \tag{4}$$

where ($O_1^1 \equiv S_1^1/Z_2 \; \ldots O_n^1 \equiv S_n^1/Z_2$) the sequence of the quotient space and $(a_1^g, a_2^g, ..., a_n^g)$ the fixed point n-tuple[1].

Random numbers can be generated by recurrence modulo two over the Galois field of orbifold fixed points elements. This is achieved in the following steps.

First, starting with the Galois Field of two orbifold fixed points elements GF (2) is the smallest finite field. The two orbifold fixed points are 0, 1 being the addition and multiplication identities respectively. The field’s addition operation is given by the Table.1

Table.1 Addition

+	0	1
0	0	1
1	1	0

and the multiplication operation by the following Table.2

[1] Note: By following [19] the orbifold fixed point n-tuple is defined as follows: a) Any n-tupe $(x_0, ..., x_{n+1})$ orbifold fixed point is a function f with $domf = \{0, ..., n+1\}$ and $x_i = f(i)$ b) The Cartesian product of the orbifold $O_0 \times O_1 .... \times O_{n-1}$ is the set of all n-tuples f such that $f(i) \in O_i$,for $0 \le i \le n-1$.

Table.2 Multiplication

*	0	1
0	0	0
1	0	1

As a consequence of modular arithmetic which forms the basis of finite fields, these two orbifold fixed points elements and these operations constitute a system with many of important properties of familiar number system: additional and multiplication are commutative and associative, multiplication is distributive over addition, addition has an identity element (0) and an inverse element for every element. Multiplication has an identity element (1) and an inverse for every element but (0).

The addition and multiplication operation in GF (2) are also bitwise operators XOR and AND respectively.

Many familiar and powerful tools of mathematics work in GF (2) just as well as integers and real numbers. Since modern computers also represent data in binary code, GF (2) is an important tool for studying algorithms on these machines that can be defined by series of bitwise operators.

Next, by following [20], let $a = \{a_k\}$ be the sequence of 0 and Ls orbifold fixed points generated by the linear recurrence relation

$$a_k = c_1 a_{k-1} + c_2 a_{k-2} + ... + c_n a_{k-n} (\mathrm{mod}\, 2) \tag{5}$$

For any given set of integers $c_i\,(i = 1,2,...,n)$, each having the orbifold fixed points values 0 or 1, we require $c_n = 1$, and say that the sequence has degree n.

For fixed c_i, the recursion a_k is determined solely by the n-tuple $(a_{k-1}, a_{k-2}, ..., a_{k-n})$ of terms preceding it. Similarly a_{k+1} is a function solely of $(a_k, a_{k-1}, ..., a_{k-n+1})$. Each such n-tuple of fixed orbifold points, thus, has a unique successor governed by the recursion formula (5). The period p of a is clearly the same as the recurrence period of an n-tuple of fixed orbifold points. The period p of a linear recurring sequence cannot be greater than $2^n - 1$, for the n-tuple $(0,0,....,0)$ is always followed by $(0,0,....,0)$. For $p = 2^n - 1$, the necessary and sufficient condition is that the polynomial

$$f(x) = 1 + c_1 x + c_2 x^2 + .. + x^n \tag{6}$$

be primitive over GF (2) [8], [9].

As the function $f(x)$ is a primitive nth degree polynomial over GF (2), the sequence $a = \{a_k\}$ is a maximal – length linearly recurring sequence modulo 2. Such sequences have been studied, and used as a code in communications and theoretical information studies [10],

[11]. The following properties of sequence (5) are of immediate interest to the scope of this paper [8], [9].

[1] $\sum_{k=1}^{p} a_k = \frac{p+1}{2} = 2^{n-1}$ (7)

[2]For every distinct set of (0, 1) integers $s_1, s_2, ..., s_n$ not all zero, there exists a unique integer $u:(0 \le u \le p-1)$ such that for every k, $s_1 a_{k-1}, s_2 a_{k-2}, ..., s_n a_{k-n} = a_{k+u} (\bmod 2)$. This is often referred to as the "cycle-and add" property [20].
[3] For every non-zero (0, 1), a binary n-vector $(e_1, e_2, ..., e_n)$ occurs exactly once per n consecutive binary digits of a .

Note that properties [1] and [2] flow directly from the fact that each possible non-zero binary n-tuple $(a_{k-1}, a_{k-2}, ..., a_{k-n})$ must occur exactly once per cycle if the period of a is $p = 2^n - 1$. For the purposes of this paper, it is convenient to use a slightly different version of fixed orbifold points sequence a . We define a_k' as follows:

$$a_k' = (-1)^{a_k} = 1 - 2a_k \tag{8}$$

We see that if a_k takes on the fixed orbifold point values 0 and 1, then a_k' takes the values +1 and -1, respectively. The properties [1], [2] and [3], then, take the form:

[1'] $\sum_{k=1}^{p} a_k' = -1$ (9)

[2']For every distinct set of (0, 1) integers $s_1, s_2, ..., s_n$ not all zero, there exists a unique integer $u:(0 \le u \le p-1)$ such that $a_{k-1}^{s_1}, a_{k-2}^{s_2}, ..., a_{k-n}^{s_n} = a_{k+u}$.

[3']With the exception of the all ones vector, every ± 1 binary n-vector $(\varepsilon_1, \varepsilon_2, ..., \varepsilon_n)$ occurs exactly once per period as n consecutive element in a .

Let $g(x)$ be the ± 1-valued Boolean function of (0, 1) fixed orbifold point variables $x_1, x_2, ..., x_n$. For any $s = (s_1, s_2, ..., s_n)$, $s_i = 0$ or 1, fixed orbifold points define

$$\phi(s, x) = 2^{-n/2} (-1)^{s_1 x_1 + s_2 x_2 + ... + s_n x_n} \tag{10}$$

This 2^n function of x is the Redemacher-Walsh function [5] from an orthonormal basis for extra-dimensional 2^n -space. From this follows that $g(x)$ has components $G(s)$ given by

$$G(s) = 2^{-n/2} \sum_x g(x) \phi(x, s) \tag{11}$$

That is, $G(s)$ is the projection of $g(x)$ on $\phi(s, x)$, normalization so that

$$\sum_{s} G^2(s) = 1 \tag{12}$$

Similarly, we have

$$g(x) = 2^{n/2} \sum_{s} G(x)\phi(x,s) \tag{13}$$

We now consider the effect of setting $x_j = a_{k-j}$ in $g(x)$. As a function of k a binary ± 1 sequence $\gamma =|\gamma_k|$ is generated:

$$\gamma_k = \sum_{s} G(s)(-1)^{s_1 a_{k-1} + ... + s_n a_{k-n}} = \sum_{s} G(s) a_{k-1}^{s_1} a_{k-2}^{s_2} ... a_{k-n}^{s_n} \tag{14}$$

By property [2'], we now have the fourth property basic on [20];

[4] $\gamma_k = G(0) + \sum_{s \neq 0} G(s) a_{k+u(s)}$ (15)

where the mapping $u(s)$ of all binary n-vectors onto $\{0,1,.....p-1\}$ is one-to-one.

Let $a = \{a_k\}$ be the (0, 1) orbifold fixed points sequence generated by an nth degree maximal-length R linear recurrence modulo 2, as described previously. We define a set of numbers of the form

$$y_k = 0 * a_{qk+r-1} a_{qk+r-2}, ... a_{qk+r-R} (base 2) \tag{16}$$

where r is a randomly chosen integer, $0 \leq r \leq 2^n - 1$ and $R \leq n$.

That is, y_k is the binary expansion of a number whose representation is R consecutive digits. Successive y_k are spaced q digits apart [20]. For reasons essential to the analysis, we restrict $q \leq n$ and $\left(q, 2^n - 1\right) = 1$. We can then express y_k by

$$y_k = \sum_{t=1}^{R} 2^{-t} a_{qk+t-R} \tag{17}$$

Such numbers always lie in the interval $(0 < y_k < 1)$. Because of property [2], the randomness of the choice of r is equivalent to the statement that the initial value y_0 is a random choice [20]. It is convenient to work with a transformed set of numbers w_k rather than y_k. This transformed set of numbers is defined as follows: Let $a = \{a_k\}$ be the $1\pm$ sequence corresponding to $\alpha = \{\alpha_k\}$, and define

$$w_k = \sum_{t=1}^{R} 2^{-t} \alpha_{qk+t-R} \tag{18}$$

We see that y_k and w_k are related by

$$w_k = 1 - 2^{-R} - 2y_k \tag{19}$$

there is thus a translation between w_k and y_k [20].

3. Conclusion

We conclude that, random numbers can be generated by recurrence modulo 2 over the Galois field of orbifold fixed points GF (2). Since our 3-dimensional space bounded by orbifold's fixed points, these random numbers can be used to generate binary codes that may correspond to the extra dimensions signature [21], [22], [23]. This proposal may open a window for ruled out extra dimensions by experiments.

References

[1].chirτ Satake, On a generalization of the notion of manifold, Proc. Nat. Acad. Sciences 42 (1956), 359–363.

[2].William Thurston, The Geometry and Topology of Three-Manifolds (Chapter 13), Princeton University lecture notes (1978–1981).

[3].William Thurston, Three-dimensional manifolds, Chelonian groups and hyperbolic geometry, Bull. *Amer. Math. Soc*. **6** (1982), 357–381.

[4].T. Appelquist, H.C. Cheng, B.A. Dobrescu, *Phys. Rev*. D **64** (2001) 035 002 [arXiv: hep-ph/0012100] .

[5].A. Tasitsiomi, J. Gaskins, A.V. Olinto, [arXiv: astro-ph/0307375] .

[6].T. Appelquist, H.U.Yee, *Phys. Rev*. D **67** (2003) 055 002 [arXiv: hep-ph/0211023]

[7].K.M. Cheung, G. Landsberg, *Phys. Rev*. D **65** (2002) 076 003 [arXiv: hep-ph/0110346]

[8].S. W.Golomb, Sequences with Randomness Properties, Martin Co., Baltimore, Md., (1955). 2. NEAL ZIERLER,

[9].S. W.Golomb "Linear recurring sequences," *J. Soc. Indust. Apple. Math*., v. 7, (1959), pp.

[10].L.Baumert, .et al, Coding theory and its Applications to Communications Systems, Report 32-167, Jet Propulsion Laboratory, Pasadena, Calif., (1961)

[11].R. C. Titisworth & L. R. Welch, Modulation by Random and Pseudo-Random Sequences, Report 20-387, Jet Propulsion Laboratory, Pasadena, Calif., (1959)

[12]. Coish, H.R. Elementary particles in a finite world geometry. *Phys. Rev*. (1959), **114**, 383-393.

[13]. Shapiro, I.S. Weak interactions in the theory of elementary particles with finite space. *Nucl. Phys*. (1960), **21**, 474-491.

[14]. Nambu, Y. Field Theory of Galois Fields. In *Quantum Field Theory and Quantum Statistics*; Batalin, I.A., Isham, C.J., Eds.; Adam Hilger: Bristol, UK, (1987); pp. 625-636.

[15]. Vourdas, A. Quantum systems with finite Hilbert space. *Rep. Progr. Phys*. (2004), **67**, 267-320.

[16]. Vourdas, A.; Banderier, C. Symplectic transformations and quantum tomography in finite quantum systems. *J. Phys*. (2010), **43**, 042001: 1-18.

[17].Felix M. Lev Introduction to a Quantum Theory over A Galois Field *Symmetry* (2010), **2**, 1810-1845;

[18]. J.Bryan, J.Fulman Orbiflod Euler-characteristic and Number of Commuting m-tuple in symmetric group *Anneal of Combinatories* **2** (1998) 1-6 Spriger- Vevling

[19].J.Rotiman Introduction to modern set theory John Wiley & Son, Inc (1900) New York p.33

[20].C. Tausworthe Random Numbers Generated by Linear Recurrence Modulo Two *Mathematics of Computation*, Vol. 19, No. **90**, (1965) pp. 201-209

[21]. E.G. Adelberger, B.R. Heckel, A.E. Nelson Tests of the Gravitational Inverse-Square Law *Ann.Rev.Nucl.Part.Sci*.**53**: (2003) 77-121 [arXiv:hep-ph/0307284].

[22]. C.D. Hoyle, et al Sub-millimeter Tests of the Gravitational Inverse-square Law *Phys.Rev*.D **70**: (2004) 042004 [arXiv:hep-ph/0405262].

[23]. D.J. Kapner, et al Tests of the Gravitational Inverse-Square Law below the Dark-Energy Length Scale *Phys.Rev.Lett*. **98**: (2007) 021101 [arXiv:hep-ph/0611184]