Acta Appl. Math. manuscript No.
(will be inserted by the editor)

The vortex filament equation as a pseudorandom generator

Francisco de la Hoz · Luis Vega

Received: date / Accepted: date

Abstract In this paper, we consider the evolution of the so-called vortex filament equation (VFE),

$$\mathbf{X}_t = \mathbf{X}_s \wedge \mathbf{X}_{ss},$$

taking a planar regular polygon of M sides as initial datum. We study VFE from a completely novel point of view: that of an evolution equation which yields a very good generator of pseudorandom numbers in a completely natural way. This essential randomness of VFE is in agreement with the randomness of the physical phenomena upon which it is based.

Keywords Vortex filament equation · Schrödinger map on the sphere · Generalized quadratic Gauß sums · Explicit inversive congruential generators

Mathematics Subject Classification (2010) 11K45 · 11Lxx · 35Q35 · 35Q41

1 Introduction

The binormal flow,

$$\mathbf{X}_t = \kappa\mathbf{b}, \tag{1}$$

where t is the time, κ the curvature, and $\mathbf{b}$ the binormal component of the Frenet-Serret formulae, appeared for the first time in 1906 [24], and was rederived in [1], as

This work was supported by the Spanish Ministry of Economy and Competitiveness, with the project MTM2011-24054, and by the Basque Government, with the project IT641-13.

Francisco de la Hoz
Department of Applied Mathematics and Statistics and Operations Research, Faculty of Science and Technology, University of the Basque Country UPV/EHU, Barrio Sarriena S/N, 48940 Leioa, Spain
E-mail: francisco.delahoz@ehu.es

Luis Vega
Department of Mathematics, Faculty of Science and Technology, University of the Basque Country UPV/EHU, Barrio Sarriena S/N, 48940 Leioa, Spain
BCAM - Basque Center for Applied Mathematics, Alameda Mazarredo, 14, 48009 Bilbao, Spain
E-mail: luis.vega@ehu.es; lvega@bcamath.org

an approximation of the dynamics of a vortex filament under the Euler equations. It is also known as the vortex filament equation (VFE) or the localized induction equation (LIA). An equivalent expression of (1) is

$$\mathbf{X}_t = \mathbf{X}_s \wedge \mathbf{X}_{ss}, \tag{2}$$

where $\wedge$ is the usual cross-product, and s is the arc-length parameter. The tangent vector $\mathbf{T} = \mathbf{X}_s$ remains with constant length and, hence, we can assume that $\|\mathbf{T}\|_2 = 1$, for all time. Differentiating (2) with respect to s, we get

$$\mathbf{T}_t = \mathbf{T} \wedge \mathbf{T}_{ss}, \tag{3}$$

known as the Schrödinger map on the sphere.

The question of making sense of initial data with corners in (2)-(3) has recently received some attention. For instance, the existence of solutions starting with a single corner, which are precisely the self-similar solutions of (2)-(3), has been proven in [15] (see also [17] for the corresponding problem in the hyperbolic space); and numerical simulations of these solutions have been carried out in [6, 18]). Furthermore, the fact that this kind of solutions yields a well-posed problem has been shown in a long-term collaboration between Banica and Vega [2,3, 4,5]; in particular, the last paper of the series, [5], closes the question, because it proves that the problem with single-corner initial data is well-posed in an adequate function space.

Even if the solutions of (2)-(3) for single-corner initial data are well understood, very little has been done for more general initial data with several corners [21]. However, in a recently submitted paper [19], we have studied for the first time the evolution of (2)-(3), taking a regular planar polygon of M sides as the initial datum. The main ideas of [19] are as follows. In order to avoid working with the curvature κ and the torsion τ, we consider an alternative version of the Frenet-Serret formulae,

$$\begin{pmatrix}\mathbf{T}\\ \mathbf{e}_1\\ \mathbf{e}_2\end{pmatrix}_s = \begin{pmatrix}0 & \alpha & \beta\\ -\alpha & 0 & 0\\ -\beta & 0 & 0\end{pmatrix} \cdot \begin{pmatrix}\mathbf{T}\\ \mathbf{e}_1\\ \mathbf{e}_2\end{pmatrix}; \tag{4}$$

where

$$\alpha(s,t) = \kappa(s,t)\cos\left(\int^s \tau(s',t)ds'\right), \quad \beta(s,t) = \kappa(s,t)\sin\left(\int^s \tau(s',t)ds'\right). \tag{5}$$

Then, the Hasimoto transformation [16] adopts the form

$$\psi = \alpha + i\beta, \tag{6}$$

and transforms (2)-(3) into the nonlinear Schrödinger (NLS) equation:

$$\psi_t = i\psi_{ss} + i\left(\frac{1}{2}(|\psi|^2 + A(t))\right)\psi, \tag{7}$$

where $A(t)$ is a certain time-dependent real constant. The main idea is to work with (7), and, at a given t, to recover $\mathbf{X}(s,t)$ and $\mathbf{T}(s,t)$ from $\psi(s,t)$ by integrating (4), up to a rigid movement that can be determined by the symmetries of the problem.

Observe that, if we define $\mathbf{N} \equiv \mathbf{e}_1 + i\mathbf{e}_2$ (see [16]), then it is not difficult to check that (3) can be rewritten as

$$\mathbf{T}_t = \frac{i}{2}(\psi_s \bar{\mathbf{N}} - \bar{\psi}_s \mathbf{N}). \tag{8}$$

Therefore, if the system $\{\psi, \mathbf{T}, \mathbf{N}\}$ solves (8), then, defining

$$\tilde{\psi}(s,t) \equiv e^{i\omega(t)}\psi(s,t), \tag{9}$$

$\{\tilde{\psi}, \mathbf{T}, e^{i\omega(t)}\mathbf{N}\}$ is also a solution; i.e., the tangent vector $\mathbf{T}$ does not change, while the vectors $\mathbf{e}_1$ and $\mathbf{e}_2$ rotate in the normal plane $\omega(t)$ degrees around $\mathbf{T}$. Since in this paper (and in [19]) we are interested only in $\mathbf{T}$, we conclude that $\psi(s,t)$ can be chosen without loss of generality up to a complex value (that depends on time) with modulus one; in particular, we can choose $\psi(s,t)$ to be real, $\psi(s,t) \equiv |\psi(s,t)|$.

Given a regular planar polygon of M sides as $\mathbf{X}(s,0)$, there is no torsion; hence, from (5), $\psi(s,0)$ is precisely the curvature of the polygon, which is a $2\pi/M$-periodic sum of Dirac deltas:

$$\psi(s,0) \equiv \kappa(s) = \frac{2\pi}{M}\sum_{k=-\infty}^{\infty}\delta(s - \tfrac{2\pi k}{M}). \tag{10}$$

Then, bearing in mind the Galilean invariance of (7) and **assuming uniqueness**, we are able to obtain $\psi(s,t)$ at any rational multiple of $2\pi/M^2$. During all this paper, we assume that p and q are two **coprime** natural numbers. Defining $t_{pq} \equiv (2\pi/M^2)(p/q)$, it can be shown that

$$\psi(s,t_{pq}) = \frac{2\pi}{Mq}\hat{\psi}(0,t_{pq})\sum_{k=-\infty}^{\infty}\sum_{m=0}^{q-1} G(-p,m,q)\delta(s - \tfrac{2\pi k}{M} - \tfrac{2\pi m}{Mq}), \tag{11}$$

where $\hat{\psi}(0,t_{pq})$ is the mean of $\psi(s,t_{pq})$ over a period,

$$\hat{\psi}(0,t_{pq}) = \frac{M}{2\pi}\int_0^{2\pi/M}\psi(s,t_{pq})ds, \tag{12}$$

and

$$G(a,b,c) = \sum_{l=0}^{c-1} e^{2\pi i(al^2+bl)/c} \tag{13}$$

denotes a generalized quadratic Gauß sum. Remark that, as explained in the lines following (9), we can assume without loss of generality that $\hat{\psi}(0,t_{pq})$ is real.

An important property of the generalized quadratic Gauß sums is that

$$|G(-p,m,q)| = \begin{cases} \sqrt{q}, & \text{if } q \equiv 1 \bmod 2, \\ \sqrt{2q}, & \text{if } q \equiv 0 \bmod 2 \wedge q/2 \equiv m \bmod 2, \\ 0, & \text{if } q \equiv 0 \bmod 2 \wedge q/2 \not\equiv m \bmod 2; \end{cases} \tag{14}$$

therefore, we can write

$$G(-p,m,q) = \begin{cases} \sqrt{q}e^{i\theta_m}, & \text{if } q \equiv 1 \bmod 2, \\ \sqrt{2q}e^{i\theta_m}, & \text{if } q \equiv 0 \bmod 2 \wedge q/2 \equiv m \bmod 2, \\ 0, & \text{if } q \equiv 0 \bmod 2 \wedge q/2 \not\equiv m \bmod 2, \end{cases} \tag{15}$$

for certain θ_m that also depend on q. Hence, defining

$$\rho = \begin{cases} \frac{2\pi}{M\sqrt{q}}\hat{\psi}(0,t_{pq}), & \text{if } q \equiv 1 \bmod 2, \\ \frac{2\pi}{M\sqrt{\frac{q}{2}}}\hat{\psi}(0,t_{pq}), & \text{if } q \equiv 0 \bmod 2 \wedge q/2 \equiv m \bmod 2, \\ 0, & \text{if } q \equiv 0 \bmod 2 \wedge q/2 \not\equiv m \bmod 2, \end{cases} \tag{16}$$

we represent (11) as

$$\psi(s,t_{pq}) = \sum_{k=-\infty}^{\infty}\sum_{m=0}^{q-1} \rho e^{i\theta_m}\delta(s - \tfrac{2\pi k}{M} - \tfrac{2\pi m}{Mq}). \tag{17}$$

The coefficients multiplying the Dirac deltas are in general not real, except for $t = 0$ and $t_{1,2} = \pi/M^2$. Therefore, $\psi(s,t_{pq})$ does not correspond to a planar polygon, but to a skew polygon with Mq (for q odd) or $Mq/2$ (for q even) equal-lengthed sides.

In order to recover $\mathbf{X}$ and $\mathbf{T}$ from ψ, we observe that every addend $\rho e^{i\theta_m}\delta(s - \frac{2\pi m}{Mq})$ in (17), with $\rho \neq 0$, induces a rotation on $\mathbf{T}$, $\mathbf{e}_1$ and $\mathbf{e}_2$. More precisely, defining $c_\rho \equiv \cos(\rho)$, $s_\rho \equiv \sin(\rho)$, $c_{\theta_m} \equiv \cos(\theta_m)$, $s_{\theta_m} \equiv \sin(\theta_m)$,

$$\mathbf{M}_m = \begin{pmatrix} c_\rho & s_\rho c_{\theta_m} & s_\rho s_{\theta_m} \\ -s_\rho c_{\theta_m} & c_\rho c_{\theta_m}^2 + s_{\theta_m}^2 & (c_\rho - 1)c_{\theta_m}s_{\theta_m} \\ -s_\rho s_{\theta_m} & (c_\rho - 1)c_{\theta_m}s_{\theta_m} & c_\rho s_{\theta_m}^2 + c_{\theta_m}^2 \end{pmatrix} \tag{18}$$

is the matrix such that

$$\begin{pmatrix} \mathbf{T}(\frac{2\pi m}{Mq}^+) \\ \hline \mathbf{e}_1(\frac{2\pi m}{Mq}^+) \\ \hline \mathbf{e}_2(\frac{2\pi m}{Mq}^+) \end{pmatrix} = \mathbf{M}_m \cdot \begin{pmatrix} \mathbf{T}(\frac{2\pi m}{Mq}^-) \\ \hline \mathbf{e}_1(\frac{2\pi m}{Mq}^-) \\ \hline \mathbf{e}_2(\frac{2\pi m}{Mq}^-) \end{pmatrix}, \tag{19}$$

where all the vectors are row vectors. Notice that, when $\rho = 0$, $\mathbf{M}_m$ is just the identity matrix $\mathbf{I}$. From (18), it follows that the non-zero value of ρ is the angle between any two adjacent sides. Imposing that (11) corresponds to a closed polygon, i.e., that

$$\mathbf{M}_{Mq-1} \cdot \mathbf{M}_{Mq-2} \cdot \ldots \cdot \mathbf{M}_1 \cdot \mathbf{M}_0 \equiv \mathbf{I}, \tag{20}$$

there is very strong evidence that the non-zero value of ρ is given by

$$\cos(\rho) = \begin{cases} 2\cos^{2/q}(\frac{\pi}{M}) - 1, & \text{if } q \equiv 1 \bmod 2, \\ 2\cos^{4/q}(\frac{\pi}{M}) - 1, & \text{if } q \equiv 0 \bmod 2; \end{cases} \tag{21}$$

and the value of $\hat{\psi}(0,t_{pq})$ follows from (16).

The previous ideas suggest very strongly that $\psi(s,t)$ is also periodic in time, with period $2\pi/M^2$. Furthermore, bearing in mind the symmetries of the problem, it follows that also $\mathbf{T}$ is periodic in time, while $\mathbf{X}$ is periodic in time up to a movement of its center of mass with constant upward velocity.

Although the study of VFE is interesting per se, a recurring question is up to what extent it is valid as a simplified model for describing real vortex filament motion. In this paper, we would like to make a step forward in that direction, by proving that the evolution of $\mathbf{X}$ and $\mathbf{T}$ for a regular polygonal initial datum is essentially random, or, in other words, that it gives as a by-product a simple and powerful generator of pseudorandom numbers. More precisely, fixed q, we will focus on two quantities: the triple product of three consecutive tangent vectors, and the scalar product of a tangent vector and the second next one. Furthermore, taking these two quantities respectively as the real and imaginary parts of a complex number, we will have a generator of pseudorandom numbers located on a circumference of center ic_ρ^2 and radius s_ρ^2.

The structure of this paper is as follows. In Section 2, we study the aforementioned quantities. We prove that they depend exclusively on $\phi(p)$, which is defined as the inverse of a multiple of p in a finite ring:

$$\phi(p) \equiv \begin{cases} (4p)^{-1} \bmod q, & \text{if } q \equiv 1 \bmod 2, \\ p^{-1} \bmod (q/2), & \text{if } q \equiv 2 \bmod 4, \\ p^{-1} \bmod q, & \text{if } q \equiv 0 \bmod 4. \end{cases} \tag{22}$$

Therefore, it is convenient to consider three cases of growing difficulty, according to the oddness of q and $q/2$: Section 2.1 deals with q odd; Section 2.2 deals with q even, but $q/2$ odd; and Section 2.3 deals with both q and $q/2$ even.

In Section 3, we analyze the pseudorandom properties of $\phi(p)$. More precisely, we put it in the frame of the so-called explicit inversive congruential generators. Finally, in Section 4, we draw the main conclusions and point out future directions to extend this research.

2 Two interesting quantities

As we have mention in the introduction, we will divide the problem in three cases, according to the oddness of q and $q/2$.

2.1 Case with $q \equiv 1 \bmod 2$

The simplest case is when q is odd. Then, $\psi(s, t_{pq})$ in (17) adopts over the first period the form

$$\psi(s, t_{pq}) = \rho \sum_{m=0}^{q-1} e^{i\theta_m} \delta(s - \tfrac{2\pi m}{Mq}), \quad s \in [0, \tfrac{2\pi}{M}), \tag{23}$$

i.e., the vertices of $\mathbf{X}$, denoted by $\mathbf{X}_m$, are located at $s = \frac{2\pi m}{Mq}$, and the sides are the segments that join $\mathbf{X}_{m+1}$ and $\mathbf{X}_m$. As stated in the introduction, we are interested in calculating the triple product of $\mathbf{T}(\frac{2\pi m}{Mq}^-)$, $\mathbf{T}(\frac{2\pi m}{Mq}^+) \equiv \mathbf{T}(\frac{2\pi(m+1)}{Mq}^-)$, and $\mathbf{T}(\frac{2\pi(m+1)}{Mq}^+)$; and the scalar product of $\mathbf{T}(\frac{2\pi m}{Mq}^-)$ and $\mathbf{T}(\frac{2\pi(m+1)}{Mq}^+)$. Let us calculate the first quantity:

$$\left[\mathbf{T}(\tfrac{2\pi m}{Mq}^-), \mathbf{T}(\tfrac{2\pi m}{Mq}^+), \mathbf{T}(\tfrac{2\pi(m+1)}{Mq}^+)\right] = \left(\mathbf{T}(\tfrac{2\pi m}{Mq}^-) \wedge \mathbf{T}(\tfrac{2\pi m}{Mq}^+)\right) \cdot \mathbf{T}(\tfrac{2\pi(m+1)}{Mq}^+)$$

$$= \begin{vmatrix} \mathbf{T}(\frac{2\pi m}{Mq}^{-}) \\ \mathbf{T}(\frac{2\pi m}{Mq}^{+}) \\ \mathbf{T}(\frac{2\pi(m+1)}{Mq}^{+}) \end{vmatrix}. \tag{24}$$

It is important to bear in mind that both the triple product of three vectors and the scalar product of two vectors are rotation-invariant, and, thus, we do not have to determine the global rotation of the whole skew polygon, which is very involved. Instead, we can simply assume that $\mathbf{T}(\frac{2\pi m}{Mq}^{-}) = (1,0,0)$, $\mathbf{e}_1(\frac{2\pi m}{Mq}^{-}) = (0,1,0)$, and $\mathbf{e}_2(\frac{2\pi m}{Mq}^{-}) = (0,0,1)$, i.e., they form the identity matrix. Then, from (18)-(19),

$$\begin{pmatrix} \mathbf{T}(\frac{2\pi(m+1)}{Mq}^{-}) \\ \hline \mathbf{e}_1(\frac{2\pi(m+1)}{Mq}^{-}) \\ \hline \mathbf{e}_2(\frac{2\pi(m+1)}{Mq}^{-}) \end{pmatrix} = \begin{pmatrix} \mathbf{T}(\frac{2\pi m}{Mq}^{+}) \\ \hline \mathbf{e}_1(\frac{2\pi m}{Mq}^{+}) \\ \hline \mathbf{e}_2(\frac{2\pi m}{Mq}^{+}) \end{pmatrix} = \mathbf{M}_m, \tag{25}$$

and

$$\begin{pmatrix} \mathbf{T}(\frac{2\pi(m+1)}{Mq}^{+}) \\ \hline \mathbf{e}_1(\frac{2\pi(m+1)}{Mq}^{+}) \\ \hline \mathbf{e}_2(\frac{2\pi(m+1)}{Mq}^{+}) \end{pmatrix} = \mathbf{M}_{m+1} \cdot \begin{pmatrix} \mathbf{T}(\frac{2\pi(m+1)}{Mq}^{-}) \\ \hline \mathbf{e}_1(\frac{2\pi(m+1)}{Mq}^{-}) \\ \hline \mathbf{e}_2(\frac{2\pi(m+1)}{Mq}^{-}) \end{pmatrix}. \tag{26}$$

More precisely, $\mathbf{T}(\frac{2\pi m}{Mq}^{+})$ is the first row of $\mathbf{M}_m$, while $\mathbf{T}(\frac{2\pi(m+1)}{Mq}^{+})$ is the first row of $\mathbf{M}_{m+1} \cdot \mathbf{M}_m$. Defining $\varDelta_m = \theta_{m+1} - \theta_m$, $c_{\varDelta_m} = \cos(\varDelta_m)$, $s_{\varDelta_m} = \sin(\varDelta_m)$, a straight calculation shows that

$$\mathbf{T}(\frac{2\pi(m+1)}{Mq}^{+}) = \begin{pmatrix} c_\rho^2 - s_\rho^2 c_{\varDelta_m} & \begin{matrix} c_\rho s_\rho c_{\theta_m}(1 + c_{\varDelta_m}) \\ -s_\rho s_{\theta_m} s_{\varDelta_m} \end{matrix} & \begin{matrix} c_\rho s_\rho s_{\theta_m}(1 + c_{\varDelta_m}) \\ +s_\rho c_{\theta_m} s_{\varDelta_m} \end{matrix} \end{pmatrix}. \tag{27}$$

Therefore, (24) becomes

$$\begin{aligned} \begin{vmatrix} \mathbf{T}(\frac{2\pi m}{Mq}^{-}) \\ \mathbf{T}(\frac{2\pi m}{Mq}^{+}) \\ \mathbf{T}(\frac{2\pi(m+1)}{Mq}^{+}) \end{vmatrix} &= \begin{vmatrix} 1 & 0 & 0 \\ c_\rho & s_\rho c_{\theta_m} & s_\rho s_{\theta_m} \\ c_\rho^2 - s_\rho^2 c_{\varDelta_m} & \begin{matrix} c_\rho s_\rho c_{\theta_m}(1 + c_{\varDelta_m}) \\ -s_\rho s_{\theta_m} s_{\varDelta_m} \end{matrix} & \begin{matrix} c_\rho s_\rho s_{\theta_m}(1 + c_{\varDelta_m}) \\ +s_\rho c_{\theta_m} s_{\varDelta_m} \end{matrix} \end{vmatrix} \\ &= s_\rho^2 s_{\varDelta_m} = s_\rho^2 \sin(\theta_{m+1} - \theta_m) \\ &= s_\rho^2 \Im(e^{i\theta_{m+1}} e^{-i\theta_m}) \\ &= s_\rho^2 \Im\left[\frac{G(-p, m+1, q)}{\sqrt{q}} \frac{\bar{G}(-p, m, q)}{\sqrt{q}}\right], \end{aligned} \tag{28}$$

where we have used (15) in the last line. On the other hand, the generalized quadratic Gauß sums can be explicitly calculated (see for instance the Appendix of [19]):

$$\begin{aligned} G(-p, m, q) &= \sum_{l=0}^{q-1} e^{-2\pi i (p/q) l^2 + 2\pi i (m/q) l} \\ &= \begin{cases} \sqrt{q} \left(\frac{p}{q}\right) e^{2\pi i \phi(p) m^2/q}, & \text{if } q \equiv 1 \bmod 4, \\ -i\sqrt{q} \left(\frac{p}{q}\right) e^{2\pi i \phi(p) m^2/q}, & \text{if } q \equiv 3 \bmod 4, \end{cases} \end{aligned} \tag{29}$$

where $\phi(p)$ denotes the inverse of $4p$ in the finite ring $\mathbb{Z}_q = \{0, 1, \ldots, q-1\}$. Bearing in mind (15), and that the Jacobi symbol satisfies $\left(\frac{p}{q}\right)^2 = 1$, we get

$$\begin{aligned}\left|\begin{matrix}\mathbf{T}(\frac{2\pi m}{Mq}^-)\\ \mathbf{T}(\frac{2\pi m}{Mq}^+)\\ \mathbf{T}(\frac{2\pi(m+1)}{Mq}^+)\end{matrix}\right| &= s_\rho^2 \Im\left[e^{2\pi i\phi(p)(m+1)^2/q}e^{-2\pi i\phi(p)m^2/q}\right]\\ &= s_\rho^2\sin\left(\frac{2\pi\phi(p)(2m+1)}{q}\right), \qquad (30)\end{aligned}$$

where $s_\rho^2 = 1 - c_\rho^2$ is obtained from (21). The other quantity we are interested in is the scalar product of $\mathbf{T}(\frac{2\pi m}{Mq}^-) = (1,0,0)$ and $\mathbf{T}(\frac{2\pi(m+1)}{Mq}^+)$:

$$\begin{aligned}\mathbf{T}(\tfrac{2\pi m}{Mq}^-)\cdot\mathbf{T}(\tfrac{2\pi(m+1)}{Mq}^+) &= c_\rho^2 - s_\rho^2 c_{\Delta_m}\\ &= c_\rho^2 - s_\rho^2\cos(\theta_{m+1}-\theta_m)\\ &= c_\rho^2 - s_\rho^2\Re(e^{i\theta_{m+1}}e^{-i\theta_m})\\ &= c_\rho^2 - s_\rho^2\Re\left[\frac{G(-p,m+1,q)}{\sqrt{q}}\frac{\bar{G}(-p,m,q)}{\sqrt{q}}\right]\\ &= c_\rho^2 - s_\rho^2\Re\left[e^{2\pi i\phi(p)(m+1)^2/q}e^{-2\pi i\phi(p)m^2/q}\right]\\ &= c_\rho^2 - s_\rho^2\cos\left(\frac{2\pi\phi(p)(2m+1)}{q}\right). \qquad (31)\end{aligned}$$

Finally, taking (30) and (31) respectively as the real and imaginary parts of a complex number, we define

$$\begin{aligned}z_{q,m}(p) &\equiv \left|\begin{matrix}\mathbf{T}(\frac{2\pi m}{Mq}^-)\\ \mathbf{T}(\frac{2\pi m}{Mq}^+)\\ \mathbf{T}(\frac{2\pi(m+1)}{Mq}^+)\end{matrix}\right| + i\mathbf{T}(\tfrac{2\pi m}{Mq}^-)\cdot\mathbf{T}(\tfrac{2\pi(m+1)}{Mq}^+)\\ &= i\,c_\rho^2 - i\,s_\rho^2\exp\left(\frac{2\pi i\phi(p)(2m+1)}{q}\right). \qquad (32)\end{aligned}$$

Summarizing, fixed q and m, $[\mathbf{T}(\frac{2\pi m}{Mq}^-), \mathbf{T}(\frac{2\pi m}{Mq}^+), \mathbf{T}(\frac{2\pi(m+1)}{Mq}^+)]$, $\mathbf{T}(\frac{2\pi m}{Mq}^-)\cdot\mathbf{T}(\frac{2\pi(m+1)}{Mq}^+)$, and, hence, $z_{q,m}(p)$, depend exclusively on $\phi(p)$, i.e., on the inverse of $4p$ modulo q, which, as we will see in Section 3, is essentially random.

2.2 Case with $q \equiv 2 \bmod 4$

The cases with q even are similar, so we will omit most details. When q is even and $q/2$ is odd, $\psi(s, t_{pq})$ in (17) adopts over the first period the form

$$\psi(s,t_{pq}) = \rho\sum_{m=0}^{q/2-1} e^{i\theta_{2m+1}}\delta(s - \tfrac{4\pi m+2\pi}{Mq}), \quad s\in[0,\tfrac{2\pi}{M}), \qquad (33)$$

i.e., only the odd addends are to be considered. In this case, the vertices of $\mathbf{X}$, denoted by $\mathbf{X}_{2m+1}$, are located at $s = \frac{4\pi m+2\pi}{Mq}$; so we have to calculate $[\mathbf{T}(\frac{2\pi(2m-1)}{Mq}^-), \mathbf{T}(\frac{2\pi(2m-1)}{Mq}^+), \mathbf{T}(\frac{2\pi(2m+1)}{Mq}^+)]$ and $\mathbf{T}(\frac{2\pi(2m-1)}{Mq}^-)\cdot\mathbf{T}(\frac{2\pi(2m+1)}{Mq}^+)$. The case $t = t_{pq} = t_{12}$ is trivial, with the first quantity being zero, and the second one being $\cos(\frac{4\pi}{M})$; hence, we consider $q > 2$.

The calculations for the triple product are exactly the same as in (30), bearing in mind that we have to consider the right subscripts, i.e., substitute c_m and s_m by c_{2m-1} and s_{2m-1}, respectively, and redefine $\Delta_m = \theta_{2m+1} - \theta_{2m-1}$. Therefore,

$$\begin{aligned}
\begin{vmatrix} \mathbf{T}(\frac{2\pi(2m-1)}{Mq}^-) \\ \mathbf{T}(\frac{2\pi(2m-1)}{Mq}^+) \\ \mathbf{T}(\frac{2\pi(2m+1)}{Mq}^+) \end{vmatrix} &= s_\rho^2 s_{\Delta_m} \\
&= s_\rho^2 \sin(\theta_{2m+1} - \theta_{2m-1}) \\
&= s_\rho^2 \Im(e^{i\theta_{2m+1}} e^{-i\theta_{2m-1}}) \\
&= s_\rho^2 \Im\left[\frac{G(-p, 2m+1, q)}{\sqrt{2q}} \frac{\bar{G}(-p, 2m-1, q)}{\sqrt{2q}}\right]. \qquad (34)
\end{aligned}$$

The generalized quadratic Gauß sums are now given by

$$\begin{aligned}
G(-p, 2m+1, q) &= 2G(-2p, 2m+1, q/2) \\
&= \begin{cases} \sqrt{2q}\left(\frac{2p}{q/2}\right) e^{4\pi i\phi_1(p)(2m+1)^2/q}, & \text{if } q \equiv 2 \bmod 8, \\ -i\sqrt{2q}\left(\frac{2p}{q/2}\right) e^{4\pi i\phi_1(p)(2m+1)^2/q}, & \text{if } q \equiv 6 \bmod 8, \end{cases} \qquad (35)
\end{aligned}$$

where $\phi_1(p)$ is the inverse of $4(2p) = 8p$ in $\mathbb{Z}_{q/2}$. Bearing in mind that $4(2m+1)^2 - 4(2m-1)^2 = 32m$, (34) becomes

$$\begin{vmatrix} \mathbf{T}(\frac{2\pi(2m-1)}{Mq}^-) \\ \mathbf{T}(\frac{2\pi(2m-1)}{Mq}^+) \\ \mathbf{T}(\frac{2\pi(2m+1)}{Mq}^+) \end{vmatrix} = s_\rho^2 \sin\left(\frac{32\pi\phi_1(p)m}{q}\right), \qquad (36)$$

where $s_\rho^2 = 1 - c_\rho^2$ is obtained from (21). On the other hand, $(8p)\phi_1(p) \equiv 1 \bmod (q/2)$ implies that $8\phi_1(p)$ is the inverse of p in $\mathbb{Z}_{q/2}$, which we denote by $\phi(p)$. Therefore,

$$\begin{vmatrix} \mathbf{T}(\frac{2\pi(2m-1)}{Mq}^-) \\ \mathbf{T}(\frac{2\pi(2m-1)}{Mq}^+) \\ \mathbf{T}(\frac{2\pi(2m+1)}{Mq}^+) \end{vmatrix} = s_\rho^2 \sin\left(\frac{2\pi\phi(p)m}{q/2}\right), \qquad (37)$$

where we prefer to write $q/2$ in the denominator, because we are working in $\mathbb{Z}_{q/2}$. Reasoning in the same way, the equivalent of (31) is

$$\mathbf{T}(\tfrac{2\pi(2m-1)}{Mq}^-)\cdot\mathbf{T}(\tfrac{2\pi(2m+1)}{Mq}^+) = c_\rho^2 + (c_\rho^2 - 1)\cos\left(\frac{2\pi\phi(p)m}{q/2}\right), \qquad (38)$$

and of (32) is

$$\begin{aligned}
z_{q,m}(p) &\equiv \begin{vmatrix} \mathbf{T}(\frac{2\pi(2m-1)^{-}}{Mq}) \\ \mathbf{T}(\frac{2\pi(2m-1)^{+}}{Mq}) \\ \mathbf{T}(\frac{2\pi(2m+1)^{+}}{Mq}) \end{vmatrix} + i\mathbf{T}(\tfrac{2\pi(2m-1)^{-}}{Mq}) \cdot \mathbf{T}(\tfrac{2\pi(2m+1)^{+}}{Mq}) \\
&= i\, c_\rho^2 - i\, s_\rho^2 \exp\left(\frac{2\pi i\phi(p)m}{q/2}\right). \qquad (39)
\end{aligned}$$

Summarizing, all the quantities depend exclusively on $\phi(p)$, i.e., on the inverse of p modulo $q/2$.

2.3 Case with $q \equiv 0 \bmod 4$

When $q/2$ is even, $\psi(s, t_{pq})$ in (17) adopts over the first period the form

$$\psi(s, t_{pq}) = \rho \sum_{m=0}^{q/2-1} e^{i\theta_{2m}} \delta(s - \tfrac{4\pi m}{Mq}), \quad s \in [0, \tfrac{2\pi}{M}), \qquad (40)$$

i.e., only the even addends are to be considered. In this case, the vertices of $\mathbf{X}$, denoted by $\mathbf{X}_{2m}$, are located at $s = \frac{2\pi(2m)}{Mq}$; so we have to calculate $[\mathbf{T}(\frac{2\pi(2m)^{-}}{Mq}), \mathbf{T}(\frac{2\pi(2m)^{+}}{Mq}), \mathbf{T}(\frac{2\pi(2m+2)^{+}}{Mq})]$ and $\mathbf{T}(\frac{2\pi(2m)^{-}}{Mq}) \cdot \mathbf{T}(\frac{2\pi(2m+2)^{+}}{Mq})$. For that, we have to substitute in (30) c_m and s_m by c_{2m} and s_{2m}, respectively, and redefine $\Delta_m = \theta_{2m+2} - \theta_{2m}$. Therefore,

$$\begin{aligned}
\begin{vmatrix} \mathbf{T}(\frac{2\pi(2m)^{-}}{Mq}) \\ \mathbf{T}(\frac{2\pi(2m)^{+}}{Mq}) \\ \mathbf{T}(\frac{2\pi(2m+2)^{+}}{Mq}) \end{vmatrix} &= s_\rho^2 s_{\Delta_m} = s_\rho^2 \sin(\theta_{2m+2} - \theta_{2m}) \\
&= s_\rho^2 \Im(e^{i\theta_{2m+2}} e^{-i\theta_{2m}}) \\
&= s_\rho^2 \Im\left[\frac{G(-p, 2m+2, q)}{\sqrt{2q}} \frac{\bar{G}(-p, 2m, q)}{\sqrt{2q}}\right]. \qquad (41)
\end{aligned}$$

In this occasion, the generalized quadratic Gauß sums are slightly more involved. Let us decompose $q = 2^r q'$, where q' is odd; then,

$$G(-p, 2m, q) = G(-p, 2m, 2^r q') = G(-2^r p, 2m, q') G(-q'p, 2m, 2^r). \qquad (42)$$

On the one hand,

$$G(-2^r p, 2m, q') = \begin{cases} \sqrt{q'} \left(\frac{2^r p}{q'}\right) e^{2\pi i\phi_1(p)(2m)^2/q'}, & \text{if } q' \equiv 1 \bmod 4, \\ -i\sqrt{q'} \left(\frac{2^r p}{q'}\right) e^{2\pi i\phi_1(p)(2m)^2/q'}, & \text{if } q' \equiv 3 \bmod 4, \end{cases} \qquad (43)$$

where $\phi_1(p)$ is the inverse of $4(2^r p) = 2^{r+2} p$ in $\mathbb{Z}_{q'}$. On the other hand,

$$G(-q'p, 2m, 2^r) = e^{\pi i\phi_2(p)(2m)^2/2^{r+1}} \left(\frac{2^r}{q'p}\right) (1 - i^{q'p})\sqrt{2^r}, \qquad (44)$$

where $\phi_2(p)$ is the inverse of $q'p$ in $\mathbb{Z}_{2^r}$. Putting all together,

$$\begin{aligned}\frac{G(-p,2m+2,q)}{\sqrt{2q}}\,\frac{\bar{G}(-p,2m,q)}{\sqrt{2q}} &= e^{2\pi i\phi_1(p)(2m+2)^2/q'}e^{\pi i\phi_2(p)(2m+2)^2/2^{r+1}} \\ &\quad\cdot e^{-2\pi i\phi_1(p)(2m)^2/q'}e^{-\pi i\phi_2(p)(2m)^2/2^{r+1}} \\ &= e^{2\pi i[2^{r+2}\phi_1(p)+q'\phi_2(p)](2m+1)/q}. \end{aligned} \tag{45}$$

This last expression can be further simplified. Indeed,

$$\begin{aligned} 2^{r+2}p\,\phi_1(p)\equiv 1 \bmod q' &\Rightarrow 2^{r+2}p\,\phi_1(p)+q'p\,\phi_2(p)\equiv 1 \bmod q' \\ q'p\,\phi_2(p)\equiv 1 \bmod 2^r &\Rightarrow 2^{r+2}p\,\phi_1(p)+q'p\,\phi_2(p)\equiv 1 \bmod 2^r; \end{aligned} \tag{46}$$

then, applying the well-known Chinese remainder theorem,

$$2^{r+2}p\,\phi_1(p)+q'p\,\phi_2(p)\equiv p(2^{r+2}\phi_1(p)+q'\phi_2(p))\equiv 1 \bmod q, \tag{47}$$

if and only if $2^{r+2}\phi_1(p)+q'\phi_2(p)$ is the inverse of p modulo q, which we denote by $\phi(p)$:

$$2^{r+2}\phi_1(p)+q'\phi_2(p)\equiv\phi(p) \bmod q. \tag{48}$$

Inserting this last expression into (45), it follows from (41) that

$$\left|\begin{matrix}\mathbf{T}(\frac{2\pi(2m)}{Mq}^-) \\ \mathbf{T}(\frac{2\pi(2m)}{Mq}^+) \\ \mathbf{T}(\frac{2\pi(2m+2)}{Mq}^+)\end{matrix}\right| = s_\rho^2\sin\left(\frac{2\pi\phi(p)(2m+1)}{q}\right), \tag{49}$$

where $s_\rho^2=1-c_\rho^2$ is obtained from (21). In the same way, the equivalent of (31) is

$$\mathbf{T}(\tfrac{2\pi(2m)}{Mq}^-)\cdot\mathbf{T}(\tfrac{2\pi(2m+2)}{Mq}^+) = c_\rho^2+(c_\rho^2-1)\cos\left(\frac{2\pi\phi(p)(2m+1)}{q}\right), \tag{50}$$

and of (32) is

$$\begin{aligned} z_{q,m}(p) &\equiv \left|\begin{matrix}\mathbf{T}(\frac{2\pi(2m)}{Mq}^-) \\ \mathbf{T}(\frac{2\pi(2m)}{Mq}^+) \\ \mathbf{T}(\frac{2\pi(2m+2)}{Mq}^+)\end{matrix}\right| + i\mathbf{T}(\tfrac{2\pi(2m)}{Mq}^-)\cdot\mathbf{T}(\tfrac{2\pi(2m+2)}{Mq}^+) \\ &= i\,c_\rho^2 - i\,s_\rho^2\exp\left(\frac{2\pi i\phi(p)(2m+1)}{q}\right). \end{aligned} \tag{51}$$

Summarizing, all the quantities depend exclusively on $\phi(p)$, i.e., on the inverse of p modulo q.

We can combine the results of Sections 2.1, 2.2 and 2.3 into the following theorem:

Theorem 1 *Let us consider the triple product of three consecutive tangent vectors (given by* (30)*,* (37) *and* (49)*), and the scalar product of a tangent vector and the second next one (given by* (31) *and* (38) *and* (50)*). Then, those quantities depend exclusively on* $\phi(p)$*:*

$$\phi(p) \equiv \begin{cases} (4p)^{-1} \bmod q, & \textit{if } q \equiv 1 \bmod 2, \\ p^{-1} \bmod (q/2), & \textit{if } q \equiv 2 \bmod 4, \\ p^{-1} \bmod q, & \textit{if } q \equiv 0 \bmod 4. \end{cases} \tag{52}$$

Furthermore, taking the first quantity as the real part and the second quantity as the imaginary part of a complex number $z_{q,m}(p)$ *(defined respectively in* (32)*,* (39) *and* (51)*),* $z_{q,m}(p)$ *lies, for all* p*, on a circumference of center* ic_ρ^2 *and radius* s_ρ^2*, where* c_ρ *is given by* (21)*:*

$$z_{q,m}(p) = \begin{cases} i\,c_\rho^2 - i\,s_\rho^2 \exp\left(\frac{2\pi i \phi(p)(2m+1)}{q}\right), & \textit{if } q \not\equiv 2 \bmod 4, \\ i\,c_\rho^2 - i\,s_\rho^2 \exp\left(\frac{2\pi i \phi(p) m}{q/2}\right), & \textit{if } q \equiv 2 \bmod 4. \end{cases} \tag{53}$$

3 Randomness

In the previous section, we have shown in Theorem 1 how the triple product of three consecutive tangent vectors, and the scalar product of a tangent vector and the second next one, depend exclusively on $\phi(p)$ as defined in (52), i.e., we have transformed the problem into one of finding inverses in finite rings. The existence and uniqueness of $\phi(p)$ is guaranteed since $\gcd(p, q) = 1$. Hence, for any given q, both p and $\phi(p)$ can take $\varphi(q)$ different values in the corresponding finite ring, where $\varphi(q)$ is Euler's totient function, which gives the amount of positive integers less than or equal to q that are coprime to q (in fact, when $q \equiv 2 \bmod 4$, we have $\varphi(q) = \varphi(2(q/2) = \varphi(2)\varphi(q/2) = \varphi(q/2))$. On the other hand, $z_{q,m}(p)$ can take $\varphi(q/\gcd(q, 2m+1))$ different values, if $q \not\equiv 2 \bmod 4$; and $\varphi((q/2)/\gcd(q/2, m))$ different values, if $q \equiv 2 \bmod 4$. Therefore, we are interested in choosing m such that $z_{q,m}(p)$ gives the largest possible amount of different numbers, i.e., such that $\gcd(q, 2m+1) = 1$, if $q \not\equiv 2 \bmod 4$; and $\gcd(q/2, m) = 1$, if $q \equiv 2 \bmod 4$. Without loss of generality, we can take $m = 0$, if $q \not\equiv 2 \bmod 4$; and $m = 1$, if $q \equiv 2 \bmod 4$. Then, (53) becomes

$$z_q(p) = \begin{cases} i\,c_\rho^2 - i\,s_\rho^2 \exp\left(\frac{2\pi i \phi(p)}{q}\right), & \text{if } q \not\equiv 2 \bmod 4, \\ i\,c_\rho^2 - i\,s_\rho^2 \exp\left(\frac{2\pi i \phi(p)}{q/2}\right), & \text{if } q \equiv 2 \bmod 4, \end{cases} \tag{54}$$

which yields exactly $\varphi(q)$ different complex numbers lying on the same circumference. In other words, there is a one-to-one correspondence between $z_q(p)$ and $\phi(p)$. $\phi(p)$ can be efficiently computed, for instance, by the extended Euclidean algorithm; another more explicit (but less efficient) way is via Euler's theorem. For example, in $\mathbb{Z}_q$,

$$p^{\varphi(q)} \equiv 1 \bmod q \Leftrightarrow p^{\varphi(q)-1} \equiv p^{-1} \bmod q, \quad \forall p \in \mathbb{Z}_q / \gcd(p, q) = 1. \tag{55}$$

When q prime, this last expression is known as Fermat's little theorem (of which Euler's theorem is in fact a generalization); in that case, $\varphi(q) = q - 1$, so

$$p^{q-1} \equiv 1 \bmod q \Leftrightarrow p^{q-2} \equiv p^{-1} \bmod q, \quad \forall p \in \mathbb{Z}_q \backslash \{0\}. \tag{56}$$

In this paper, however, we are not interested so much in finding $\phi(p)$, but rather in its randomness properties or, equivalently, in the randomness properties of (54). There are diverse methods of generating pseudorandom numbers, the most popular ones being the linear congruential generators (LCGs) (see for instance [22, Section 3.2.1]). Given a large $q \in \mathbb{N}$ and $a, b, x_0 \in \mathbb{Z}$, a linear congruential sequence $(x_n)_{n\geq 0}$ of nonnegative integers smaller than m is defined by

$$x_{n+1} \equiv a x_n + b \bmod q, \quad n \geq 0. \tag{57}$$

Then, after a careful choice of q, a, b, x_0, a sequence $(u_n)_{n\geq 0}$ of linear congruential pseudorandom numbers uniformly distributed in the interval $[0, 1)$ is obtained by the normalization $u_n = x_n/q$, for $n \geq 0$.

The quality of LCGs heavily depends on the coarseness of the lattice structure of s-dimensional vectors $\mathbf{u}_n^{(s)} = (u_n, \ldots, u_{n+s-1})$ generated from the periodic sequence $(u_n)_{n\geq 0}$. It often happens [12] that the lattice can be covered by a small amount of parallel hyperplanes: a sadly well-known example is the formerly popular RANDU generator

$$x_{n+1} \equiv 65539 x_n \bmod 2^{31}. \tag{58}$$

Since RANDU satisfies $x_{n+2} \equiv 6x_{n+1} - 9x_n \bmod 2^{31}$, it fails most three-dimensional criteria for randomness. Indeed, taking (x_n, x_{n+1}, x_{n+2}) as "random" points in the three-dimensional space, these points lie in exactly 15 planes! Therefore, the results obtained through RANDU are to be seen as suspicious.

In order to solve de deficiencies of LCGs, nonlinear random generators have been introduced [7]. Their idea is that, given a large q prime number, the elements are generated recursively by means of an integer-valued nonlinear function f:

$$x_{n+1} \equiv f(x_n) \bmod q, \quad n \geq 0; \tag{59}$$

then, we apply again the normalization $u_n = x_n/q$ as in the LCGs, to obtain pseudorandom numbers uniformly distributed over $[0, 1)$. An important particular case are the inversive congruential generators (ICGs), introduced by [9]:

$$x_{n+1} \equiv \begin{cases} a\, x_n^{-1} + b \bmod q, & x_n \geq 1, \\ b, & x_n = 0, \end{cases} \quad n \geq 0, \tag{60}$$

with q prime, $a \not\equiv 0 \bmod q$, which are characterized by the absence of any lattice structure, although their computational generation is not so efficient as with the LCGs. Remark that, in the literature, it is customary to write

$$x_{n+1} \equiv a\overline{x}_n + b \bmod q, \quad n \geq 0, \tag{61}$$

where $\overline{z} \equiv z^{p-2} \bmod q$. From (56), $\overline{z}$ is simply the multiplicative inverse of z, if $z \not\equiv 0 \bmod q$; while $\overline{z}$ is zero, if $z \equiv 0 \bmod q$.

Due to Eichenauer-Herrmann [11] are as well the related explicit inversive congruential generators (EICGs), which are the relevant ones in this paper:

$$x_n \equiv \overline{an+b} \bmod q, \quad n \geq 0, \tag{62}$$

with q prime, $a \not\equiv 0 \bmod q$. It is immediate to see that x_n has a period equal to q, i.e., $\{x_0, \ldots, x_{q-1}\} = \mathbb{Z}_q$; hence, any EICG with the normalization $u_n = x_n/q$ passes the uniformity test for equidistribution in $[0,1)$. However, statistical independence properties of pseudorandom numbers are as important for stochastic simulations as uniformity properties. To study their statistical independence, Eichenauer-Herrmann used in [11] the so-called serial test, which analyzes the discrepancy of tuples of pseudorandom numbers, and which we explain briefly here. The idea is, for a given dimension $k \geq 2$ and for N arbitrary points $(\xi_0, \ldots, \xi_{N-1}) \in [0,1)^k$, to consider their discrepancy, which is defined as

$$D_N(\xi_0, \ldots, \xi_{N-1}) = \sup_J |F_N(J) - V(J)|, \tag{63}$$

where the supremum is extended over all the subintervals J of $[0,1)^k$; $F_N(J)$ is N^{-1} times the number of terms among $\xi_0, \ldots, \xi_{N-1}$ falling into J; and $V(J)$ denotes the volume of J.

In [11], given a sequence of numbers $(u_n)_{n\geq 0}$ obtained with an EICG, the k-dimensional points

$$\mathbf{u}_n = (u_{n+n_1}, \ldots, u_{n+n_k}) \in [0,1)^k, \quad 0 \leq n < p, \tag{64}$$

were considered, with $n_1, \ldots, n_k$ arbitrary integers satisfying $0 = n_1 < \ldots < n_k < p$, and the abbreviation

$$D_p^{(k)} = D_p(\mathbf{u}_0, \ldots, \mathbf{u}_{p-1}) \tag{65}$$

being used for the discrepancy of the points. Then, an EICG passes the k-dimensional serial test if $D_p^{(k)}$ is reasonably small. In this regard, the following two theorems were formulated in [11]:

Theorem 2 *Let $2 \leq k < p$. Then, the discrepancy $D_p^{(k)}$ for any EICG satisfies*

$$D_p^{(k)} < 2p^{-1/2}\left((k-1)\left(\frac{2}{\pi}\log p + \frac{7}{5}\right)^k + 1\right) + kp^{-1}.$$

Theorem 3 *Let $0 < t \leq 1$. Then there exist more than $A_p(t)(p-1)$ values of $a \in \mathbb{Z}_p^*$ such that the discrepancy $D_p^{(k)}$ for any corresponding EICG satisfies*

$$D_p^{(k)} \geq \frac{t}{2(\pi+2)}p^{-1/2}$$

for all dimensions $k \geq 2$, where

$$A_p(t) = \frac{(1-t^2)p}{(4-t^2)p + 12p^{1/2} + 9}.$$

Theorems 2 and 3 show that, in the EICG method, the discrepancy $D_p^{(k)}$ has on the average an order of magnitude between $p^{-1/2}$ and $p^{-1/2}(\log p)^k$. However, it is precisely in this range of magnitudes where the discrepancy of p independent and uniformly distributed points taken from $[0,1)^k$ is found, which is roughly $p^{-1/2}(\log\log p)^{1/2}$. In this sense, we can say that EICGs model true random numbers very closely, or, in Eichenauer-Herrmann's words, EICGs have *even better structural and statistical independence properties than the standard type*, i.e., than (60). Furthermore, they also behave very well in parallel and vector computations, as shown by Niederreiter in [23]. Indeed, if we define a family of N EICGs:

$$x_n^i \equiv \overline{a^i n + b^i} \bmod q, \quad n \geq 0, \quad i = 1, \ldots, N, \tag{66}$$

then, the N-tuples of the form $(x_n^1, \ldots x_n^N)$ have good statistical properties if all the N numbers $b^i\overline{a^i}$ are distinct. Summarizing, this approach is, in Niederreiter's words, *eminently suitable for the generation of parallel streams of pseudorandom numbers with desirable properties.*

In principle, it could be possible to work in $\mathbb{Z}_q$, with q an arbitrary natural number, although the most common choices are q prime, as in the definitions (60) and (62), or q a power of two. For instance, in [8], Eichenauer and Ickstadt study the equally good pseudorandom properties of EICGs defined by the inverses of the odd integers in $\mathbb{Z}_q$, with $q = 2^\omega$, $\omega \geq 5$:

$$x_n \equiv (an + b)^{-1} \bmod 2^\omega, \quad n \geq 0, \tag{67}$$

with $a \equiv 2 \bmod 4$, $b \equiv 1 \bmod 2$; it is immediate to see that x_n has a period equal to $q/2 = 2^{\omega-1}$, i.e., x_n takes all the possible odd values in $\mathbb{Z}_q$, or, in other words, $\{x_0, \ldots, x_{q/2-1}\} = \mathbb{Z}_q^*$.

Coming back to (54), all the previous arguments should be more than enough to justify the extremely good pseudorandom character of (54) and, hence, of $\mathbf{X}$ and $\mathbf{T}$. In particular, when q is an odd prime,

$$z_q(p) = i\, c_\rho^2 - i\, s_\rho^2 \exp(2\pi i u_p), \tag{68}$$

where $u_p = x_p/q$, and x_p is given by (62), with $a \equiv 4 \bmod q$, $b \equiv 0 \bmod q$; i.e., $x_p \equiv \overline{4p} \bmod q$. Therefore, by direct application of Theorems 2 and 3, u_p is a sequence of pseudorandom numbers uniformly distributed in the interval $(0,1)$, which, from our Theorem 1, implies that $z_q(p)$ is a sequence of pseudorandom numbers uniformly distributed in the circumference of center $i\, c_\rho^2$ and radius s_ρ^2. Observe that we have to exclude the case $p = 0$ and, hence, the numbers lie on $(0,1)$ instead of $[0,1)$. Nevertheless, since $u_0 = 0$, we are just omitting the first term of the sequence (and the point $z_0 = i\cos(2\rho)$ in the circumference), which makes this minor issue irrelevant for all purposes.

The same reasoning is valid when q is twice a prime number. Then, (68) also holds, with $u_p = x_p/(q/2)$ and $x_p \equiv \overline{p} \bmod (q/2)$, i.e., we are taking $a \equiv 1 \bmod (q/2)$ and $b \equiv 0 \bmod (q/2)$ in (62). Again, we exclude $u_0 = 0$, and the whole previous paragraph is valid in its integrity.

Let us mention also the case with $q = 2^\omega$. Then, (68) also holds, with $u_p = x_p/q$, and $x_p \equiv \overline{2p-1} \bmod q$, i.e, we are taking $a \equiv 1 \bmod q$ and $b \equiv -1 \bmod q$ in (67). Again, we have obtained a sequence of pseudorandom numbers uniformly distributed in the circumference of center $i\, c_\rho^2$ and radius s_ρ^2, but, unlike the two previous cases, it is not necessary to exclude any number.

Analyzing all the possible values of q lies certainly beyond the scope of this paper. Moreover, (68) is not the only possible probability generator which can be obtained from the evolution of $\mathbf{X}$ in $\mathbf{T}$. For instance, given N different primes $q_1, \ldots, q_N \geq 5$, it is possible to combine (68) in a way that closely resembles the so-called *compound approach* explained in [10]. Let us particularize (54) as

$$\frac{c_{\rho_j}^2 + iz_{q_j}(p)}{s_{\rho_j}^2} = \exp\left(\frac{2\pi i \phi_j(p)}{q_j}\right), \tag{69}$$

where ρ_j is the angle corresponding to q_j; $\phi_j(p) \equiv (4p)^{-1} \bmod q_j$; and $p \not\equiv 0 \bmod q_j$. Then,

$$\prod_{j=1}^{N} \frac{c_{\rho_j}^2 + iz_{q_j}(p_j)}{s_{\rho_j}^2} = \exp\left(2\pi i \sum_{j=1}^{N} \frac{\phi_j(p)}{q_j}\right). \tag{70}$$

Denoting now

$$u_p \equiv \sum_{j=1}^{N} \frac{\phi_j(p)}{q_j} \bmod 1, \tag{71}$$

(70) becomes

$$\prod_{j=1}^{N} \frac{c_{\rho_j}^2 + iz_{q_j}(p_j)}{s_{\rho_j}^2} = \exp(2\pi i u_p), \qquad p \not\equiv 0 \bmod q_j, \forall j. \tag{72}$$

The left-hand side is directly obtained from $\mathbf{T}$, and its good random properties follows directly from [10]. The only minor difference is that, in our case, p can take $(q_1 - 1) \cdot \ldots \cdot (q_N - 1)$ different values modulo $q_1 \cdot \ldots \cdot q_N$, while its equivalent in [10] can take all the $q_1 \cdot \ldots \cdot q_N$ values. However, in practice, taking $q_1, \ldots, q_N$ large enough, the amount of values that we are excluding is, for all purposes, irrelevant.

4 Conclusions

In this paper, we have considered the evolution of (2)-(3), taking a regular planar polygon of M sides as the initial datum. Bearing in mind the recent results in [19], where we gave very strong evidence that $\mathbf{X}(s,t)$ is a skew polygonal at times which are rational multiples of $2\pi/M^2$; we have studied (2)-(3) from a completely novel point of view: that of an evolution equation which yields a very good pseudorandom generator in a completely natural way.

Due to the algebraic complexity of the calculations involved, we have limited ourselves mainly to the study at rational times of two quantities, which are illustrative enough of the essential random character of (2)-(3): the triple product of three consecutive tangent vectors; and the scalar product of a tangent vector and the second next one. These quantities, when taken respectively as the real and imaginary parts of a complex number, yield an excellent generator of pseudorandom numbers uniformly located on a circumference. Furthermore, it is straightforward to combine different rational times to develop additional pseudorandom generators.

Although the main aim of this paper is to show the randomness in the evolution of (2)-(3), for which it is largely enough to work with $\mathbf{T}$, it is not irrelevant to mention here that, as observed in [19], $\mathbf{X}(0,t)$ is very intimately related to Riemann's nondifferentiable function,

$$f(t) = \sum_{k=1}^{\infty} \frac{\sin(\pi k^2 t)}{\pi k^2}, \tag{73}$$

which, as proved by Jaffard [20], is a multifractal and, in fact, fits under the so called Frisch-Parisi conjecture proposed in [14] (see also [13] for more details). Therefore, although giving a complete algebraic characterization of $\mathbf{X}(0,t)$ reveals as a complex task which clearly lies beyond the scope of this paper and which we postpone for the future, we can nonetheless expect an even richer randomness structure in $\mathbf{X}$.

The ideas presented here can be most probably extended to other types of evolution equations, in order to obtain new probability generators. Obviously, this approach is not intended for competing with commercially developed algorithms; even though, during the simulation of (2)-(3), large sequences of pseudorandom numbers with good statistical properties can be generated with virtually no additional cost, i.e., for free.

As we have said in the introduction, a recurring question is up to what extent VFE is valid as a simplified model. In this line, the random character of (2)-(3) proved in this paper is at the very least not in contradiction with the physical motion of a real vortex filament. Furthermore, we venture to suggest that finding the existence of well-behaved pseudorandom sequences of numbers *inside* the evolution of a proposed physical model might be a first test in validating that model with respect to the phenomenon that it is trying to describe. Indeed, real natural phenomena are in general characterized by their chaotic, truly random behaviour. Therefore, a model with an easily predictable structure might be suspected not to match reality accurately.

References

1. Arms, R.J., Hama, F.R.: Localized-Induction Concept on a Curved Vortex and Motion of an Elliptic Vortex Ring. Phys. Fluids **8**(4), 553–559 (1965)
2. Banica, V., Vega, L.: Scattering for 1D cubic NLS and singular vortex dynamics. Comm. Math. Phys. **286**(2), 593–627 (2009)
3. Banica, V., Vega, L.: Scattering for 1D cubic NLS and singular vortex dynamics. J. Eur. Math. Soc. (JEMS) **14**(1), 209–253 (2012)
4. Banica, V., Vega, L.: Stability of the selfsimilar dynamics of a vortex filament. Arch. Ration. Mech. Anal. **210**(3), 673–712 (2013)
5. Banica, V., Vega, L.: The initial value problem for the Binormal Flow with rough data. arXiv:1304.0996 (2013)
6. Buttke, T.F.: A Numerical Study of Superfluid Turbulence in the Self-Induction Approximation. J. Comput. Phys. **76**(2), 301–326 (1998)
7. Eichenauer, J., Grothe, H., Lehn, J.: Marsaglia's lattice test and non-linear congruential pseudo random number generators. Metrika **35**(1), 241–250 (1988)
8. Eichenauer, J., Ickstadt, K.: Explicit inversive congruential pseudorandom numbers with power of two modulus. Math. Comp. **62**(206), 787–797 (1994)
9. Eichenauer, J., Lehn, J.: A non-linear congruential pseudo random number generator. Statistische Hefte **27**(1), 315–326 (1986)
10. Eichenauer-Herrmann, J.: Explicit Inversive Congruential Pseudorandom Numbers: the Compound Approach. Computing **51**(2), 175–182 (1993)
11. Eichenauer-Herrmann, J.: Statistical independence of a new class of inversive congruential pseudorandom numbers. Math. Comp. **60**(201), 375–384 (1993)

12. Entacher, K.: Bad Subsequences of Well-Known Linear Congruential Pseudorandom Number Generators. ACM Trans. Model. Comput. Simul. **8**(1), 61–70 (1998)
13. Frisch, U.: Turbulence. The Legacy of A. N. Kolmogorov. Cambridge University Press (1995)
14. Frisch, U., Parisi, G.: Fully developped turbulence and intermittency. Proc. Internat. School Phys. Enrico Fermi, North-Holland, Amsterdam (1985)
15. Gutiérrez, S., Rivas, J., Vega, L.: Formation of singularities and self-similar vortex motion under the localized induction approximation. Comm. Partial Differential Equations **28**(5–6), 927–968 (2003)
16. Hasimoto, H.: A soliton on a vortex filament. J. Fluid Mech. **51**(3), 477–485 (1972)
17. de la Hoz, F.: Self-similar solutions for the 1-D Schrödinger map on the hyperbolic plane. Math. Z. **257**(1), 61–80 (2007)
18. de la Hoz, F., García-Cervera, C.J., Vega, L.: A Numerical Study of the Self-Similar Solutions of the Schrödinger Map. SIAM J. Appl. Math. **70**(4), 1047–1077 (2009)
19. de la Hoz, F., Vega, L.: Vortex Filament Equation for a Regular Polygon. arXiv:1304.5521 (2013)
20. Jaffard, S.: The spectrum of singularities of Riemann's function. Rev. Mat. Iberoam. **12**(2), 441–460 (1996)
21. Jerrard, R.L., Smets, D.: On the motion of a curve by its binormal curvature. J. Eur. Math. Soc. (JEMS) (2014). To appear
22. Knuth, D.E.: The Art of Computer Programming, vol. 2: Seminumerical Algorithms, third edn. Addison Wesley (1998)
23. Niederreiter, H.: On a new class of pseudorandom numbers for simulation methods. J. Comput. Appl. Math. **56**(1–2), 159–167 (1994)
24. Rios, L.S.D.: Sul moto d'un liquido indefinito con un filetto vorticoso di forma qualunque. Rend. Circ. Mat. Palermo **22**(1), 117–135 (1906). In Italian