Dynamic properties of an exact algorithm for square root calculation

Marcelo Sobottka[a], Luiz P.L. de Oliveira[b,*]

[a] *Centro de Modelamiento Matemático, Universidad de Chile, Blanco Encalada, 2120, 7º piso Casilla, 170/3, Correo 3 Santiago, Chile*
[b] *Programa Interdisciplinar de Pós-Graduação em Computação Aplicada - PIPCA, Universidade do Vale do Rio dos Sinos – UNISINOS, Av. Unisinos 950, 93022-000 São Leopoldo, RS, Brazil*

Abstract

The digits of the square root of any real number can be consecutively calculated by hand with the use of a very popular exact algorithm. We show that the application of that algorithm defines a dynamic system in the sense that it can be reduced to the consecutive iteration of a map $\mathbb{H}$ defined in the semi-closed interval [0, 100). We prove that $\mathbb{H}$ is chaotic and topologically conjugated to the shift map in the Bernoulli space on 10 symbols. We also exhibit a natural measure for $\mathbb{H}$ which is mixing and of maximum entropy. Finally, we adapt the cryptography method proposed by Baptista [M.S. Baptista, Cryptography with chaos, Phys. Lett. A 240 (1998) 50–54] to the dynamics associated with $\mathbb{H}$, advantageously due to its dynamic properties.

Keywords: Exact algorithms; Chaos; Mixing; Cryptography

1. Introduction

In order to calculate the square root $\sqrt{x_0}$ of a nonnegative real number $x_0 \in \mathbb{R}_+$ one must use some numerical or arithmetical algorithm. There exists a very popular algorithm, described in the next section, which permits the hand calculation of $\sqrt{x_0}$. In the course of its use, the consecutive digits (always between 0 and 9 in decimal representation) are calculated in a fashion similar to the one of the long-division algorithm. As far as the algorithm is applied, the obtained digits are always exact. Hereafter, we refer to that square root algorithm as the *exact algorithm*.

In the case of rational results, the obtained sequence of digits is periodic or eventually periodic while, for irrational results, it is not. The fact that a perturbation (or error) in one of the digit results in a completely different sequence of digits suggests that, in some sense, the system defined by the algorithm exhibits sensitive dependence on initial conditions and, therefore, is chaotic. Besides, when applied to many rational numbers, the algorithm results in non periodic sequences, which suggests that the exact algorithm efficiently produces information. The goal of this paper is to study the dynamics associated with the application of that algorithm and make those ideas more precise. We show that the application of the exact algorithm can be reduced to the consecutive iteration of an one-dimensional map $\mathbb{H}$, called the *reduced square root map*, defined in the semi-closed interval [0, 100) (see Definition 5 below). The dynamic system defined by $\mathbb{H}$ is studied under both, topological and ergodic points of view.

Chaotic dynamics can produce information by deterministic means. Because of that, some encryption/decryption methodologies based on chaotic dynamics have been proposed. Recently, Baptista [1] proposed a methodology based on chaotic dynamics given by logistic map. It begins with the definition of a key composed by an association of the alphabetic symbols to subintervals (sites) of [0, 1] and an initial condition x_0. The general idea is to follow the chaotic orbit γ defined by x_0 to see how many iterations are necessary for γ consecutively reach the sites associated to the symbols which compose the plain text. Further discussions on this kind of methodology can be found in [3–5]. The method proposed in this paper falls within

* Corresponding author.
E-mail addresses: sobottka@dim.uchile.cl (M. Sobottka), lpluna@unisinos.br, luna@exatas.unisinos.br (L.P.L. de Oliveira).

the same scope but with more analytical knowledge on the used dynamics. This raises the efficiency of its use.

The paper is organized as follows. In Section 2, the exact algorithm is described. In Section 3, we show that the associated map $\mathbb{H}$ is topologically conjugated to the shift map σ on the space Σ_{10} of sequences (see (1)), given by $\sigma(s_1 s_2 s_3 \ldots) = (s_2 s_3 s_4 \ldots)$. It is worthwhile to recall that σ is chaotic on Σ_{10} under Devaney's sense [2]. Besides, we exhibit a natural measure for $\mathbb{H}$ and prove that $\mathbb{H}$ is conjugate to σ in the ergodic sense. In Section 4, we propose an application to cryptography. The conclusions are presented in Section 5. We refer the reader to [2] and [6] for the basics on dynamical systems and ergodic theory used here.

2. The exact algorithm for square root calculation

Let us denote the decimal representation of a positive real number S as $\overline{s_1.s_2s_3s_4\ldots}$, where s_1 is any nonnegative integer and $s_i \in \{0, 1, 2, \ldots 9\}$ for $i = 2, 3, 4 \ldots$. We take no representations ending in infinite strings of nines, avoiding representation nonuniqueness. For example, the number $\overline{1.00\ldots}$ is to be represented in this form and not as $\overline{0.99\ldots}$. Similarly, $\overline{53.23000\ldots}$ is adopted instead of $\overline{53.229999\ldots}$, etc.

Let $X = \{0, 1, 2, \ldots 9\}$ and $X^{\mathbb{N}} := \{s = (s_1, s_2, s_3, \ldots) \mid s_i \in X\}$ be the *Bernoulli Space* of sequences on ten symbols. Let Σ_{10} be the subspace of sequences on ten symbols not ending in infinite strings of nines, i.e.

$$\Sigma_{10} := \left\{(s_1, s_2, s_3, \ldots) \in X^{\mathbb{N}} \mid \forall n \in \mathbb{N}, \exists j > n \text{ with } s_j \neq 9\right\}, \quad (1)$$

with the usual metric. In order to simplify the notation, we identify each $\overline{s_1.s_2s_3s_4\ldots} \in [0, 10)$ with its corresponding sequence of digits $(s_1, s_2, s_3, s_4, \ldots) \in \Sigma_{10}$. This way, we can make the identification $\Sigma_{10} = [0, 10)$.

For a positive real number x_0, let $\sqrt{x_0} = \overline{s_1.s_2s_3\ldots s_j\ldots}$ be the decimal representation of its positive square root. The exact algorithm considered here gives the digits s_n as the greatest integers between 0 and 9, satisfying the following inequalities:

$$\begin{aligned}
&s_1^2 \leq x_0\\
&(10\overline{s_1} + s_2)^2 \leq 100x_0\\
&(10\overline{s_1s_2} + s_3)^2 \leq 100^2x_0\\
&\vdots\\
&(10\overline{s_1s_2s_3\ldots s_n} + s_{n+1})^2 \leq 100^n x_0,\\
&\vdots
\end{aligned}$$

These inequalities can be rewritten as

$$s_{n+1}^2 + y_n s_{n+1} \leq x_n, \quad n = 0, 1, 2, \ldots, \quad (2)$$

where $x_n = 100^n x_0 - 100\overline{s_1s_2s_3\ldots s_n}^2$ and $y_n = 20\overline{s_1s_2s_3\ldots s_n}$. This makes the calculation of the digits s_n of $\sqrt{x_0}$ recursive. Denoting $\Delta(x, y) := (-y + \sqrt{y^2 + 4x})/2$ and $\lfloor x \rfloor$ the integer part of x, the greatest natural solutions of those inequalities are given by:

$$s_{n+1} = \lfloor \Delta_n \rfloor, \quad (3)$$

where $\Delta_n := \Delta(x_n, y_n)$.

The quantities y_n and x_n are directly related to the successive approximations for $\sqrt{x_0}$ and the corresponding remainders, respectively. They can be expressed as:

$$\begin{aligned}
x_{n+1} &= 100[100^n x_0 - (10\overline{s_1s_2s_3\ldots s_n} + \overline{s_{n+1}})^2]\\
&= 100(x_n - y_n s_{n+1} - s_{n+1}^2) \quad (4)
\end{aligned}$$

and:

$$y_{n+1} = 20(10\overline{s_1s_2s_3\ldots s_n} + \overline{s_{n+1}}) = 10(y_n + 2s_{n+1}). \quad (5)$$

The substitutions of Eq. (3) into Eqs. (4) and (5) give the square root map, defined below.

Definition 1. Let $\mathbb{R}_+^2 := \left\{(x, y) \in \mathbb{R}^2 \mid x, y \geq 0\right\}$. The square root map $\mathcal{H} : \mathbb{R}_+^2 \to \mathbb{R}_+^2$ is given by

$$\begin{aligned}
\mathcal{H}(x, y) := (&100x - 100\lfloor \Delta(x, y) \rfloor^2\\
&- 100y\lfloor \Delta(x, y) \rfloor, 10y + 20\lfloor \Delta(x, y) \rfloor). \quad (6)
\end{aligned}$$

The successive iterations of that bi-dimensional map from a given initial condition $(x_0, 0)$, together with Eq. (3), give the digits of $\sqrt{x_0}$.

Proposition 2. *Given $(x_0, y_0) \in \mathbb{R}_+^2$, let S_0 be the positive root of $S^2 + y_0 S = x_0$ and $(x_1, y_1) = \mathcal{H}(x_0, y_0)$. Then the shift $S_1 = 10(S_0 - \lfloor S_0 \rfloor)$ is the positive root of $S^2 + y_1 S = x_1$. In other words, if $S_0 = \Delta(x_0, y_0)$ then $S_1 = \Delta(x_1, y_1)$.*

Proof. Given $(x_0, y_0) \in \mathbb{R}_+^2$, the equation $S^2 + y_0 S = x_0$ has only one positive solution which is given by $S_0 = \Delta_0$. Now, we use the expressions for x_1, y_1 and S_1 to verify that $S_1^2 + y_1 S_1 = x_1$. Indeed, we have:

$$\begin{aligned}
x_1 &= 100\left(x_0 - \lfloor \Delta_0 \rfloor^2 - y_0 \lfloor \Delta_0 \rfloor\right)\\
y_1 &= 10(y_0 + 2\lfloor \Delta_0 \rfloor),
\end{aligned}$$

which implies:

$$\begin{aligned}
S_1^2 + y_1 S_1 &= 100\,(S_0 - \lfloor S_0 \rfloor)^2\\
&\quad + 100\,(y_0 + 2\lfloor S_0 \rfloor)\,(S_0 - \lfloor S_0 \rfloor)\\
&= 100\left(S_0^2 + y_0 S_0 - y_0 \lfloor S_0 \rfloor - \lfloor S_0 \rfloor^2\right).
\end{aligned}$$

Since $S_0^2 = \Delta_0^2 = -y_0\Delta_0 + x_0 = -y_0 S_0 + x_0$, it follows that:

$$\begin{aligned}
&100\left(S_0^2 + y_0 S_0 - y_0 \lfloor S_0 \rfloor - \lfloor S_0 \rfloor^2\right)\\
&= 100\left(-y_0 S_0 + x_0 + y_0 S_0 - y_0 \lfloor S_0 \rfloor - \lfloor S_0 \rfloor^2\right)\\
&= 100\left(x_0 - \lfloor \Delta_0 \rfloor^2 - y_0 \lfloor \Delta_0 \rfloor\right) = x_1. \quad \square
\end{aligned}$$

Note that, even though $S_0 = \overline{s_1.s_2s_3\ldots}$ is an arbitrary nonnegative real number, $S_1 = 10\,(S_0 - \lfloor S_0 \rfloor) = \overline{s_2.s_3s_4\ldots}$ is less than 10. Then, for any initial condition (x_0, y_0), we have that $0 \leq s_n \leq 9$ for $n = 2, 3, \ldots$. Therefore, the orbits of $\mathcal{H}$ are rapidly attracted to:

$$\mathcal{R} = \left\{(x, y) \in \mathbb{R}_+^2 \mid x - 10y < 100\right\},$$

which is invariant under $\mathcal{H}$. The following corollary of Proposition 2 generalizes the square root digit-by-digit algorithm to any second degree algebraic equation of the form $S^2 + y_0 S = x_0$.

Corollary 3. *The positive root* $S_0 = \overline{s_1.s_2 s_3 \ldots}$ *of equation* $S^2 + y_0 S = x_0$*, with* $x_0 \geq 0$ *and* $y_0 \geq 0$*, can be obtained by iterating* $\mathcal{H}$ *from the initial condition* (x_0, y_0)*, i.e.,* $s_{n+1} = \lfloor \Delta_n \rfloor$, $n = 0, 1, 2, \ldots$ *where* $(x_n, y_n) = \mathcal{H}^n(x_0, y_0)$.

Proof. Given $(x_0, y_0) \in \mathbb{R}^2_+$, let $S_0 = \overline{s_1.s_2 s_3 s_4 \ldots} = \Delta_0$ the positive root of $S^2 + y_0 S = x_0$. Then, from Proposition 2, $S_1 = \overline{s_2.s_3 s_4 s_5 \ldots} = \Delta_1$ is the positive root of $S^2 + y_1 S = x_1$. By induction, we obtain $S_n = \overline{s_{n+1}.s_{n+2} s_{n+3} \ldots} = \Delta_n$, for any $n \in \mathbb{N}$. Then, $s_{n+1} = \lfloor S_n \rfloor = \lfloor \Delta_n \rfloor$. □

3. Dynamical properties of the exact algorithm

Proposition 4. $\Delta : \mathcal{R} \to \Sigma_{10} = [0, 10)$ *is a topological semi-conjugacy between* $\mathcal{H}$ *and the shift map* σ.

Proof. The continuity of Δ is obvious since it is a composition of continuous operations. Let $(x_0, y_0) \in \mathcal{R}$ and $(x_1, y_1) = \mathcal{H}(x_0, y_0)$. If $\Delta(x_0, y_0) = \overline{s_1.s_2 s_3 \ldots}$ then, from Proposition 2:

$$(\Delta \circ \mathcal{H})(x_0, y_0) = \Delta(x_1, y_1) = (s_2, s_3, s_4, \ldots)$$
$$= \sigma(s_1, s_2, s_3, \ldots) = (\sigma \circ \Delta)(x_0, y_0).$$

In addition to this, for each $S \in [0, 100)$, the solutions of $\Delta(x, y) = S$ in $\mathbb{R}^2_+$ are the points of the straight semi-line given by $x - Sy = S^2$, contained into $\mathcal{R}$. Those solutions have itinerary S, i.e. $\Delta(x, y) = S$. Therefore, we conclude that Δ is onto but not one-to-one. □

If (x_0, y_0) and (x'_0, y'_0) are such that: $\Delta(x_0, y_0) = \Delta(x'_0, y'_0) = (s_1, s_2, s_3, \ldots)$, then the equations $S^2 + y_0 S = x_0$ and $S^2 + y'_0 S = x'_0$ have the same positive root $S = \overline{s_1.s_2 s_3 \ldots}$. Accordingly, we define the equivalence relation $\sim$ on $\mathcal{R}$, given by:

$$(x, y) \sim (x', y') \Leftrightarrow \Delta(x, y) = \Delta(x', y').$$

Therefore, for each $(u, v) \in \mathcal{R}$, we define: $[(u, v)] = \{(x, y) \in \mathcal{R} |\ (x, y) \sim (u, v)\}$ and quotient $\mathcal{R}/_\sim = \{[(u, v)] |\ (u, v) \in \mathcal{R}\}$. Note that, for each $(u, v) \in \mathcal{R}$, $[(u, v)]$ is composed of the points $(x, y) \in \mathcal{R}$ of the straight semi-line given by:

$$x - Sy = S^2, \tag{7}$$

where $S = \Delta(u, v)$.

Considering S as a parameter, Eq. (7) defines a family of disjoint straight semi-lines covering $\mathcal{R}$. Then, for $(x, y) \sim (x', y')$ we have that (x, y) and (x', y') are over the same straight semi-line determined by the mentioned parameter S (see Fig. 1). Since there exists only one point $(u', 0) \in [(u, v)]$ with $0 \leq u' < 100$ we can identify $[(u, v)]$ to $u' \in [0, 100)$. Then we can identify $\mathcal{R}/_\sim$ to $[0, 100)$. The equivalence relation $\sim$ defines a projection $\Pi : \mathcal{R} \to [0, 100)$ along that family of straight semi-lines (7),

$$\Pi(x, y) = x' \quad \text{such that} \quad (x', 0) \sim (x, y). \tag{8}$$

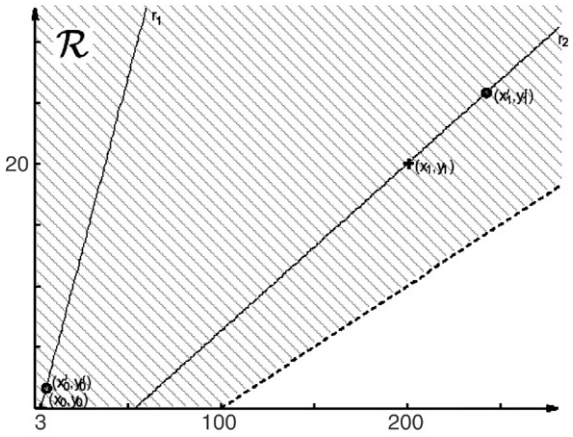

Fig. 1. The depicted region $\mathcal{R} \subset \mathbb{R}^2_+$. Two points of $\mathcal{R}$ are equivalent if they both belong to the same straight semi-line of the family defined by the Eq. (7). The map $\mathcal{H}$ takes one of those straight semi-line to another, as it is illustrated in the figure: $\mathcal{H}(x_0, y_0) = (x_1, y_1)$ and $\mathcal{H}(x'_0, y'_0) = (x'_1, y'_1)$.

Definition 5. The reduced square root map $\mathbb{H} : [0, 100) \to [0, 100)$ is given by

$$\mathbb{H}(x) = \Pi \circ \mathcal{H}(x, 0) = x' \Leftrightarrow (x', 0) \sim \mathcal{H}(x, 0),$$

whose analytical expression is

$$\mathbb{H}(x) = 100 \left(\sqrt{x} - \lfloor \sqrt{x} \rfloor\right)^2.$$

It is easy to verify that $\mathbb{H}$ is continuous at all points of [0,100) except at those of $\left\{n^2 |\ n \in \mathbb{N}, 1 \leq n \leq 9\right\}$.

The map $\mathbb{H}$ is nothing more than the square of ten- times the fractional part of $\sqrt{x}$. Therefore, it can be written as $\mathbb{H}(x) = r^{-1} \circ T \circ r(x)$, with $T(x) = 10x (\mathrm{mod}\ 10)$ and $r(x) = \sqrt{x}$ which is a topological conjugacy between T and $\mathbb{H}$. Notice that, the measure λ defined as:

$$\lambda([a, b)) = \frac{|\sqrt{b} - \sqrt{a}|}{10}, \tag{9}$$

is the r-projection onto $[0, 100)$ of the uniform Bernoulli measure on Σ_{10}.

Therefore, we have the following proposition:

Proposition 6. *The map* $\mathbb{H}$ *is chaotic. Furthermore, the measure* λ *is mixing for* $\mathbb{H}$ *and the unique maximal entropy measure.* □

It is important to notice that the orbit of $\mathbb{H}$ from an initial condition x_0 is closely related to the sequence of digits of $\sqrt{x_0}$. In fact, let $x_0 \in [0, 100)$ and $\sqrt{x_0} = \overline{s_1.s_2 s_3 \ldots}$. It is easy to see that if $x_n = \mathbb{H}^n(x_0)$ then $\sqrt{x_n} = \overline{s_{n+1}.s_{n+2} s_{n+3} \ldots}$. If $[0, 100)$ is divided into 10^d sub-intervals $I_k := \left[\frac{k^2}{10^{2(d-1)}}, \frac{(k+1)^2}{10^{2(d-1)}}\right)$ for $k = 0, 1, \ldots, 10^d - 1$, then, $x_0 \in I_k$ implies that $\frac{k}{10^{d-1}} \leq \sqrt{x_0} < \frac{k+1}{10^{d-1}}$, which means that $\sqrt{x_0} = \overline{s_1.s_2 s_3 \ldots}$ is such that $\overline{s_1 s_2 \ldots s_d} = k$. Therefore we have proved the following proposition.

Proposition 7. *Let* $[0, 100)$ *be divided into* 10^d *sub-intervals* $I_k := \left[\frac{k^2}{10^{2(d-1)}}, \frac{(k+1)^2}{10^{2(d-1)}}\right)$ *for* $k = 0, 1, \ldots, 10^d - 1$. *Then, the*

d-block of digits $\overline{s_{n+1}\dots s_{n+d}}$ *of* $\sqrt{x_0}$ *determines the sub-interval* I_k *to which* $x_n = \mathbb{H}^n(x_0)$ *belongs, i.e.,* $x_n \in I_{\overline{s_{n+1}\dots s_{n+d}}}$.

4. Encryption method

In this section, we propose a symmetrical encryption method based on the dynamics of the exact algorithm, given by $\mathbb{H}$, analogous to that proposed in [1]. Let A be a finite alphabet with $\sharp A$ units (symbols) and $K_d := \{0, 1, \dots, 10^d - 1\}$ for some $d \geq 1$. Consider the languages $\mathcal{L}_A := \bigcup_{n\geq 1} A^n$ and $\mathcal{L}_{\mathbb{N}} := \bigcup_{n\geq 1} \mathbb{N}^n$. In this section, we propose an encryption function $\varepsilon : [0, 100) \times \mathcal{L}_A \to \mathcal{L}_{\mathbb{N}}$. Usually, the elements of A are associated to numbers in order to make some algebraic operations possible or easy to be implemented in computers. In what follows $M = (M_j)_{1\leq j\leq L}$ is the original message with length L and $m = (m_j)_{1\leq j\leq L}$ its numerical version; $\tilde{m} = (\tilde{m}_j)_{1\leq j\leq L}$ is the encrypted version of M; the initial condition x_0 is the key.

Divide the interval $[0, 100)$ into 10^d semi-open intervals $I_k := \left[\frac{k^2}{10^{2(d-1)}}, \frac{(k+1)^2}{10^{2(d-1)}}\right)$, $k \in K_d$. These subintervals have the same length $1/10^d$, according to the natural measure λ given in (9). Define $\mathbb{I} = \{I_k \mid k \in K_d\}$ and a rather uniform association of the sites I_k to the symbols of A, given by an onto map $\varphi : \mathbb{I} \to A$. We can associate each I_k to the number k and, therefore, identify $\mathbb{I}$ with K_d. Let $x_0 \in [0, 100)$ be the encryption/decryption key, and $M = (M_j)_{1\leq j\leq L}$ a message to be transmitted. The encrypted version of M is defined as the sequence of numbers of iterations of $\mathbb{H}$, necessary for the orbit $x_n = \mathbb{H}^n(x_0)$ to visit a site associated to the consecutive letters of M. More precisely, $\tilde{m}$ is the sequence of natural numbers $\tilde{m} = (\tilde{m}_j)_{1\leq j\leq L}$ such that $\mathbb{H}^{\tilde{m}_j}(x_{\tilde{m}_{j-1}})$ falls, for the first time, in an interval I_k associated to M_j. This way, the encryption function ϵ is defined as $(x_0, M) \mapsto \tilde{m}$. The decryption of $\tilde{m}$ is done using the same key, in the obvious way: read each $\tilde{m}_j$ as the alphabet symbol M_j associated to the sub-interval I_k to which $\mathbb{H}^{\sum_{i=1}^{j}\tilde{m}_i}(x_0)$ belongs.

Because of the sensitivity of $\mathbb{H}$ on initial conditions, the use of (even slightly) wrong keys for decryption gives results with negligible correlation with the original message. Since λ is mixing for $\mathbb{H}$, this encryption method is well defined for λ-almost any key x_0. In opposition to the method proposed by [1], every site I_k is equiprobable for λ-almost all initial condition $x_0 \in [0, 100)$. This prevents the detection of any correlation between the frequency at which the symbols are used in a specific language and the statistical properties of the algorithm, given by the associated natural measure λ. Another advantage of our method is that it is machine-independent, since it only depends on the computation of the square root of a real number with the necessary precision.

An equivalent formulation for the algorithm, based on Proposition 7, is as follows. Let $M = (M_j)_{1\leq j\leq L}$ be the message to be transmitted. Let $\overline{s_1.s_2s_3\dots}$ be the decimal representation of $\sqrt{x_0} \in [0, 100)$. Then, putting $\tilde{m}_0 = 0$ we can find $\tilde{m} = (\tilde{m}_j)_{1\leq j\leq L}$ recursively by

$$\tilde{m}_j = \min\left\{n - \tilde{m}_{j-1} \mid n > \tilde{m}_{j-1}, \overline{s_{n+1}\dots s_{n+d}} \in \varphi^{-1}(M_j)\right\}.$$

In other words, to encrypt and decrypt it is only necessary to follow the d-blocks of the decimal expansion of $\sqrt{x_0}$.

As an example, let $d = 2$ and suppose that the units of the usual alphabet $A = \{a, b, c, \dots, z\}$ are associated, in their usual sequence, to the sub-intervals I_k, $k = 0, 2, \dots, 99$, until each one of the 100 sites is assigned,

$$(a, b, c, \dots, z, a, b, c, \dots, z, a, b, c, \dots, z, a, b, c, \dots, v).$$

Suppose that the message to be encrypted is $M = HI$. Therefore, $m \in \varphi^{-1}(H) \times \varphi^{-1}(I)$ where $\varphi^{-1}(H) = \{I_7, I_{33}, I_{59}, I_{85}\}$ and $\varphi^{-1}(I) = \{I_8, I_{34}, I_{60}, I_{86}\}$. The encrypted version of M is $\tilde{m} = (34, 55)$ if $x_0 = 2$, $\tilde{m} = (8, 17)$ if $x_0 = 3$, and $\tilde{m} = (7, 8)$ if $x_0 = \pi$. Another way to describe the method is by the use of Proposition 7. For example, for $x_0 = 2$, notice that the first time the digits corresponding to 'H' (07, 33, 59 or 85) appear in the decimal expansion of $\sqrt{2}$ is at the 34th place; a digit string corresponding to 'I' (34 in this case) next appears 55 places later.

Because of the sensitivity of $\mathbb{H}$ to the initial conditions, the use of wrong keys for decryption give results with negligible correlation with the original message. For example, for $x_0^{\text{wrong}} = 2.00001$ we have $\mathbb{H}^{34}(x_0^{\text{wrong}}) \approx 6.802 \in I_{26} \mapsto A$ and $\mathbb{H}^{89}(x_0^{\text{wrong}}) \approx 0.595 \in I_7 \mapsto H$ which gives $M^{\text{wrong}} = AH$.

Implementing the algorithm by the direct use of $\mathbb{H}$ is much more computationally expensive than extracting a square root and examining its digits. The proposed algorithm has a drawback concerning the number of digits (precision) required for square root extraction of the key x_0 in order to cipher the plain text. The number of digits grows with the number of characters of the plain text and the encryption becomes increasingly slow as the length of the message increases. In fact, if we associate with each letter of A the same quantities of subintervals of $\mathbb{I}$, then due to the mixing property of $\mathbb{H}$ we have for λ-almost any x_0 a time average $\sharp A$ to reach any letter. This implies that, to encrypt a given message M with length L, we need to compute the square root of λ-almost any x_0 with approximately $L \cdot \sharp A$ decimal precision. Therefore, the use of efficient methods to extract square roots with arbitrary precision is required. Obviously, this drawback can easily be worked around in practice. One solution is just to calculate more digits of the square root when the known digits are used up. Another obvious alternative would be to agree upon a fixed (but large) precision in advance, and then switch to another key when the limit is reached.

The same extensions considered in [1] can be implemented. For instance, the association φ can be considered as a component of the key (x_0, φ). A transient $\tilde{m}_0 = T$ can be defined in order to postpone the beginning of the cryptography/decryptography, which raises the contribution of the sensitive dependence on initial condition to the method security. In this case, the key is (x_0, φ, T). Also, a stochastic component can be added to the encrypting part of the method by the use of random numbers η_i to decide which turn among the many times a chosen trajectory crosses the aimed sites, is to be considered as the encryption of each unit. In such cases, for random numbers in the interval $[0, 1]$, if a condition such

as $\eta_i < 1/2$ is verified, then the corresponding $\tilde{m}_i$ is adopted. Otherwise, the transmitter continues to follow the orbit until another valid site is achieved and that condition is satisfied. The parameters η_i need not to be transmitted to the receiver (see [1] for details).

5. Conclusion

In this paper, we studied topological and ergodic properties of the exact algorithm for square root calculation of $x_0 \in \mathbb{R}$. The algorithm defines a two-dimensional dynamic system given by the map $\mathcal{H} : \mathbb{R}^2_+ \to \mathbb{R}^2_+$, which is a function of the remainders and the partial approximations for $\sqrt{x_0}$, with an attractor $\mathcal{R} \subset \mathbb{R}^2_+$. Inside $\mathcal{R}$, $\mathcal{H}$ can be reduced to a one-dimensional system given by the map $\mathbb{H} : [0, 100) \longrightarrow [0, 100)$. The orbit of $\mathbb{H}$ from an initial condition x_0 determines the order in which the digits of $\sqrt{x_0}$ appears in its decimal representation.

$\mathbb{H}$ is topologically conjugated to the shift map σ on Σ_{10}, implying that $\mathbb{H}$ is chaotic under Devaney's definition. In this sense, the exact algorithm for $\sqrt{x_0}$ calculation is chaotic. Moreover, the decimal representation of $\sqrt{x_0}$ is a chaotic sequence for almost all $x_0 \in \mathbb{R}$, in the sense that it is associated with a chaotic orbit of $\mathbb{H}$ for almost all initial condition $x_0 \in [0, 100)$.

Under the ergodic point of view, we exhibit a probability measure λ, which is mixing for $\mathbb{H}$. This allows us to consider the system under a statistical point of view. For example, the probability for a subset of $[0, 100)$ to be visited by the orbit associated to a generic condition can be estimated using Birkhoff's theorem. This gives an alternative way to conclude that the distribution of the decimal digits of the square root of a real number is almost always uniform. More precisely, for a fixed $d \in \mathbb{N}$, the groups of d digits appear with the same frequency in the decimal representation of $\sqrt{x}$, for almost all $x \in \mathbb{R}$.

Under the application scope, the dynamics defined by the exact algorithm can be used to define an encryption/decryption method, similar to the one proposed in [1], where the logistic map is used. However, because of its exactness, the proposed method has some advantages. The first is the fact that it is machine independent. Also, since we know the appropriate mixing measure, we can divide the domain of $\mathbb{H}$ in equiprobable sites to be associated with the alphabetic symbols. This overcomes the drawback of assigning alphabetic symbols to least probable sites, which would imply large numbers of iterations to the encryption/decryption. This may happen in the method proposed in [1], unless a previous numerical study of the natural measure of the logistic map is done.

The present study seems to be generalizable to $\sqrt[p]{x}$, $p \in \mathbb{N}$, $x \in \mathbb{R}_+$. The extension would begin from the corresponding inequalities, $(10s_1s_2s_3 \ldots s_n + s_{n+1})^p \leq 10^{pn}x_0$, but further details are out of the scope of this paper. In addition, similar studies can be developed for other exact algorithms, concerning the digit-by-digit calculation of other algebraic operations. They probably will define other kinds of dynamics or, at least, different conjugations to the shift map. However, the application to cryptography depends also on the information production of the algorithm as well as on the possibility of production of nonperiodic orbits from initial conditions with finite or periodic decimal representations. In our algorithm, this last issue is supported by experimental evidence for the conjecture that all irrational p-roots of rational numbers are normal, i.e. the distribution of d-blocks of digits in their decimal representation is uniform, for any $d = 1, 2, 3, \ldots$.

Acknowledgements

The authors would like to thank Professor Artur Lopes for inspiring discussions and advice on the subject. Also, the referees contributed to a significant improvement in the paper presentation. M. Sobottka was partially supported by the Brazilian financial agency CNPq.

References

[1] M.S. Baptista, Cryptography with chaos, Phys. Lett. A 240 (1998) 50–54.
[2] R.L. Devaney, An Introduction to Chaotic Dynamical Systems, Addison-Wesley Publishing Company, 1989.
[3] G. Jakimoski, L. Kocarev, Analysis of some recently proposed chaos-based encryption algorithms, Phys. Lett. A 291 (2001) 381–384.
[4] S. Li, X. Mou, Z. Ji, J. Zhang, Y. Cai, Performance analysis of Jakimoski–Kocarev attack on a class of chaotic cryptosystems, Phys. Lett. A 307 (2003) 22–28.
[5] S. Li, G. Chen, K.-W. Wong, X. Mou, Y. Cai, Baptista-type chaotic cryptosystems: Problems and countermeasures, Phys. Lett. A 332 (2004) 368–375.
[6] P. Walters, An Introduction to Ergodic Theory, Springer-Verlag, New York, 1982.